UNIVERSITÉ DE LIMOGES

ÉCOLE DOCTORALE SCIENCES ET INGÉNIERIE N°653

FACULTÉ DES SCIENCES ET TECHNIQUES

Année : 2024

Thèse

pour obtenir le grade de

DOCTEUR DE L'UNIVERSITÉ DE LIMOGES

Discipline : Informatique

présentée et soutenue par

Fabien THOMAS-BRANS

le 25 mai 2024

Diagnostic et réparation de supports électroniques chiffrés et endommagés

Thèse dirigée par Pr Damien SAUVERON et Dr Thibaut HECKMANN

JURY :

Samia BOUZEFRANE	Professeur, Conservatoire National des Arts et Métiers	Présidente
Mohamed MOSBAH	Professeur, Bordeaux INP	Rapporteur
Assia TRIA	HDR, Directrice de l'IMT Mines Alès	Rapporteur
Thomas SOUVIGNET	Professeur associé, Université de Lausanne	Examinateur
Claudine THOMAS	Conseillère régionale Ile-de-France	Invité

« Si tu veux faire des films, t'as juste besoin d'un truc qui filme »

Aurélien Cotentin

À ma famille, À mes amis,

Remerciements

Je tiens à remercier la Professeure Samia BOUZEFRANE d'avoir tenue la fonction de présidente du jury.

Je souhaite également remercier les Professeur Mohamed MOSBAH et Docteur Assia TRIA d'avoir accepté d'être rapporteurs pour ma soutenance de thèse.

Je remercie également le Professeur Thomas SOUVIGNET d'avoir accepté d'être examinateur.

Enfin je tenais à remercier Madame Claudine THOMAS, le Professeur Damien SAUVERON, le Docteur Thibaut HECKMANN pour leur présence et leur soutien lors de ma soutenance de thèse.

Dans un premier temps, je tiens à remercier Thibaut HECKMANN et Damien SAUVERON sans qui cette thèse n'aurait pu être possible. La qualité de l'encadrement et la participation active dans le déroulement de la thèse ont pleinement contribué à son aboutissement.

Je tiens également à remercier Georges-Axel JALOYAN et Hadrien BARRAL pour leur travaux très précieux sur la correction des erreurs des lecture des mémoires NAND flash. Sans leurs compétences pointues dans le domaine, ces recherches n'auraient pas pu aboutir.

Je remercie également Aya FUKAMI, Quentin CLEMENT, Kostas MARKANTONAKIS, Matthieu REGNERY, Rémi GERAUD-STEWART, Thomas SOUVIGNET et David NACCACHE pour leur participation respectives aux publications qui ont été produites durant ma thèse.

Enfin je tiens à remercier mes amis et ma famille pour leur soutien durant cette étape importante.

Table des matières

Table des figures 5

Liste des tableaux 13

De l'analyse de défaillance à la rétro-conception hardware à des fins de forensique 15

Contexte de la forensique numérique 16
Champs d'application de la forensique numérique 17
Acteurs français de la forensique numérique 21
Réglementation française de la forensique numérique 24
Introduction à l'analyse de défaillance 30
L'assurance qualité 30
L'analyse de défaillance 38
Introduction sur la rétro-conception matérielle 44
Contributions 56

Analyse de l'environnement de travail 57

1.1 Classification des supports 58
1.2 Équipements des laboratoires 64
1.2.1 Observation optique 64
1.2.1.1 Binoculaire 64
1.2.1.2 Microscope 67
1.2.1.3 Machine à Rayons-X 70
1.2.1.4 Microscope électronique à balayage (MEB) 74
1.2.1.5 Interféromètre optique ou laser 79
1.2.1.6 Microscope confocal 81
1.2.1.7 Scanner à balayage acoustique (SAM) 85
1.2.1.8 Caméra thermique 88
1.2.2 Préparation d'échantillons 91
1.2.2.1 Chimie humide 91
1.2.2.2 Laser d'ablation 94
1.2.2.3 Graveur plasma 96
1.2.2.4 Microscope ionique focalisé (FIB) 99
1.2.2.5 Polissage 102
1.2.3 Interaction avec la cible 106
1.2.3.1 Station de probing 106
1.2.3.2 Box de lecture 109
1.2.4 Utilisation des équipements 110
1.3 Notions de la rétro-conception hardware 111
1.3.1 Bases d'électronique 111
1.3.1.1 La diode 112
1.3.1.2 Le transistor 114
1.3.1.3 Les résistances de tirage 121
1.3.2 Application de la rétro-conception 123
1.3.2.1 Au système électronique 123
1.3.2.2 À un composant électronique 124
1.4 Présentation des supports MultiMedia Card 132

1.4.1 Introduction des supports 132
1.4.2 Une MMC particulière, la carte Secure Digital (SD) 134
1.4.3 Architecture d'une MMC 136
1.4.4 Protocole de communication entre la MMC et l'hôte 139
1.4.4.1 La norme SD 139
1.4.4.2 La norme eMMC 144
1.4.4.3 La norme UFS 146
1.4.5 Gestion de la mémoire flash interne 148
1.4.5.1 Signaux de contrôle de la mémoire flash 148
1.4.5.2 Protocole de communication interne 150
1.4.5.3 Management des erreurs 153
1.5 Présentation et état de l'art de la Google Home 157
1.5.1 Démontage de la Google Home 158
1.5.2 Étude fonctionnelle 159

Création d'un processus de diagnostic 166
2.1 Protocole de diagnostic de supports MMC illustré sur carte SD 167
2.1.1 Diagnostic non-invasif 169
2.1.1.1 Inspection optique 169
2.1.1.2 Observations aux Rayons-X 2D et 3D 170
2.1.1.3 Analyse par microscopie acoustique à balayage 174
2.1.2 Diagnostic invasif 176
2.1.2.1 Tests électriques de base 176
2.1.2.2 Analyse par caméra infrarouge 176
2.1.2.3 Ouverture chimique de l'échantillon 180
2.2 Cas d'étude 182
2.2.1 Contexte 182
2.2.2 Présentation de l'échantillon 182
2.2.3 Analyse non-invasive de l'échantillon 183
2.2.3.1 Inspection optique 183
2.2.3.2 Observations aux Rayons-X 184
2.2.4 Analyse invasive de l'échantillon 186
2.2.4.1 Tests électriques 186
2.2.4.2 Analyse infrarouge 186
2.3 Discussion 190

Extraction et fiabilisation de la donnée 192
3.1 Extraction de la donnée 193
3.1.1 Rétro-ingénierie d'une MMC 194
3.1.2 Travail préparatoire 195
3.1.3 Interconnexion 201
3.1.3.1 Solutions commerciales 201
3.1.3.2 Solution non-commerciale 205
3.1.3.3 Lecteurs 213
3.1.4 Diagnostic des puces 214
3.1.4.1 Hypothèse de travail 214
3.1.4.2 Confirmation du comportement et des signaux 216

3.1.5 Lecture de la mémoire 222
3.2 Fiabilisation de la donnée 226
3.2.1 Préparation du composant 227
3.2.2 Lecture de la mémoire flash 230
3.2.3 Récupération de données pour la lecture de la SquashFS corrompu . 233
3.2.4 Génération de candidats cibles 236
3.2.5 Oracle basé sur une table d'inodes supplémentaires 237
3.2.6 Résultats et discussion 239
3.2.6.1 Fusionner plusieurs candidats cibles 239
3.2.6.2 Ratios de récupération 240
3.3 Conclusion 241

Conclusion 242

Conclusion et perspectives 242
4.1 Suite des travaux 245
4.2 Cas des mémoires défectueuses 247
4.3 Élargissement à d'autres supports 249
4.4 Coûts de réalisation 251
4.5 Perspective personnelle 254

Table des figures

1 Roue de Deming [1] 32
2 Observation optique des couches dans les composants lors d'une analyse de construction [2] 33
3 Exemple de courbe en baignoire théorique 35
4 Exemples d'équipements servant à la qualification des composants électroniques dans un laboratoire de fiabilité 36
5 Exemple du système d'observation optique Lynx EVO [3] 39
6 Exemples de défauts pouvant être observés sur les composants électroniques par des moyens optiques 40
7 Machine de visualisation en deux dimensions et de reconstruction en trois dimensions par Rayons-X [4] 40
8 Vue optique d'un composant PIC après décapsulation chimique [5] 41
9 Différentes étapes de corrosion sur un pad de composant en Aluminium provoquant un décollement du fil associé et une coupure de la continuité électrique [6] 42
10 Observation d'une fissure dans le substrat en silicium d'une puce au microscope électronique à balayage [7] 42
11 Schéma de la transmission du contenu de la chaîne émettrice jusqu'à la télévision du client 44
12 Setup d'un glitch avec la carte ChipWhisperer permettant d'induire une faute dans le fonctionnement d'un composant en jouant sur la tension d'alimentation [8] 48
13 Setup d'un banc d'attaque laser et électromagnétique permettant d'injecter une faute lors de l'exécution d'instructions d'un composant 48
14 Schéma illustrant la différence entre le chiffrement FBE et FDE [9] 50
1.1 Exemple d'un disque dur à plateau [10] 59
1.2 Exemple d'une clé USB composée de plusieurs éléments [11] 61
1.3 Exemple d'une clé USB monolithe [11] 62
1.4 Spectre de la lumière [12] 64
1.5 Schéma de cheminement de la lumière dans une binoculaire [12] 65
1.6 Schéma de principe de la distance de travail [12] 65
1.7 Exemple de deux équipements de conception différente pour l'observation macroscopique d'échantillons 66
1.8 Exemple d'utilisation d'une binoculaire pour observer une carte électronique [13] 67
1.9 Schéma de cheminement de la lumière dans un microscope [12] 68
1.10 Exemple de microscope de la marque Leica [14] 68
1.11 Exemple d'échantillons observés avec un microscope 69
1.12 Schéma de principe de la production d'un photon-X suite à la mobilité d'un électron [15] 70
1.13 Exemple de positionnement d'un échantillon dans une cabine de rayons-X de marque Zeiss [16] 71
1.14 Exemple de machine à Rayons-X pour la visualisation 2D et 3D de marque RX Solutions [17] 72
1.15 Vue d'un iPhone 12 aux Rayons-X en 2D [18] 73
1.16 Slices (interne et externe) du PCB d'une carte SD 73
1.17 Schéma de la colonne d'un microscope électronique à balayage [19] 74

1.18 Schéma des différentes interactions entre l'électron primaire et la matière [20] 75
1.19 Schéma de la poire d'interaction des électrons avec la matière [20] 76
1.20 Exemple de microscope électronique à balayage de la marque Zeiss [21] . . 77
1.21 Observation au microscope électronique à balayage d'un composant électronique après gravure de l'isolant [22] 78
1.22 Schéma de principe de combinaison des ondes lumineuses [23] 79
1.23 Schéma de principe de fonctionnement d'un microscope interférométrique [24] 80
1.24 Microscope interférométrique de la marque Bruker modèle contourx 100 [25] 81
1.25 Exemple d'image sur un composant électronique avec un microscope interférométrique [26] 82
1.26 Schéma de fonctionnement d'un microscope confocal [27] 83
1.27 Microscope confocal de la marque ZEISS modèle LSM900 [28] 84
1.28 Exemple d'acquisitions réalisées avec le microscope confocal marque Keyence modèle VK-X3000 [29] 85
1.29 Schéma de fonctionnement d'un SAM [30] 86
1.30 Intérieur de la chambre d'un SAM : présence du transducteur normalement plongé dans l'eau [31] 87
1.31 Exemple d'acquisition avec un SAM sur une carte électronique [30] 88
1.32 Positionnement de l'infrarouge dans le spectre [32] 88
1.33 Exemple de caméras thermiques de différentes gammes 89
1.34 Visualisation de la carte mère d'un iPhone pour de la recherche de défaut . 90
1.35 Utilisation de la caméra thermique pour visualiser les effets transitoires internes d'une carte microSD 91
1.36 Exemple d'espace de manipulation chimique pour le traitement des composants électroniques 92
1.37 Exemple d'ouverture chimique pratiquée sur un PIC16 93
1.38 Lasers d'ablation conçus pour usiner les composants électroniques 94
1.39 Exemple de gravure laser pour amincir la résine à la surface d'une carte microSD 95
1.40 Schéma de principe de fonctionnement d'un plasma 96
1.41 Exemple de machine de gravure plasma de la marque Corial [33] 97
1.42 Exemple de pistes d'un composant électronique vues au microscope électronique à balayage [22] 98
1.43 Exemple d'un équipement FIB [34] 99
1.44 Cross-section d'une spirale conductrice avec un FIB pour observer la tranche [35] 100
1.45 Exemple de modification de design avec un FIB : 2 pistes coupées, jointes par une nouvelle piste [36] 101
1.46 Schéma de principe d'une polisseuse [37] 102
1.47 Vue de la polisseuse Ultrapol de la marque Ultratec [38] 103
1.48 Vue d'une microsection d'une puce permettant l'observation et les mesures des couches internes [39] 104
1.49 Station de probing entrée de gamme de la marque VR Table [40] 106
1.50 Station de probing haut de gamme de la marque Cascade MPS150 [41] . . 107
1.51 Exemple de positionnement de probes sur wafer pour des mesures lors de la fabrication [41] 108

1.52 Exemple de positionnement de probes sur une cellule mémoire vue au microscope électronique [42] . . . 108
1.53 Exemple de box commerciales permettant la lecture de composants mémoires : Riffbox [43], Easyjtag [44] et Octoplus [45] . . . 109
1.54 Exemple d'un wafer de silicium, tranche de silicium servant de substrat lors de la fabrication des composants électroniques [46] . . . 112
1.55 Illustration de la jonction PN dans un substrat de silicium . . . 113
1.56 Schéma de fonctionnement des diodes et courbe de transfert associée . . . 114
1.57 Schéma structurel d'un transistor NMOS . . . 115
1.58 Schéma électronique et structurel d'un transistor NMOS lorsque la grille est soumise à un '0' . . . 115
1.59 Schéma électronique et structurel d'un transistor NMOS lorsque la grille est soumise à un '1' . . . 116
1.60 Schéma d'implantation des transistors CMOS . . . 116
1.61 Schéma de raccordement des transistors CMOS dans le silicium . . . 117
1.62 Fonctionnement d'un inverseur CMOS . . . 117
1.63 Schéma de câblage d'une fonction AND avec des transistors . . . 118
1.64 Schéma de cablage d'une fonction NAND avec des transistors . . . 119
1.65 Schéma de câblage d'une fonction OR avec des transistors . . . 119
1.66 Schéma de câblage d'une fonction NOR avec des transistors . . . 120
1.67 Schéma de câblage d'une fonction XOR avec des transistors . . . 121
1.68 Fonction utilisée comme exemple pour l'explication de la méthodologie de rétro-conception d'un composant . . . 126
1.69 Parallèle entre la vue optique de la fonction étudiée et un schéma du design 128
1.70 Étude de la vue zoomée de la fonction et parallèle avec le schéma des transistors . . . 129
1.71 Établissement de la table de vérité de la fonction selon les états des entrées 130
1.72 Évolution des ventes de smartphones dans le monde entre 2007 et 2021 . . 133
1.73 Forme et taille standard des cartes SD (de haut en bas : cartes SD, miniSD et microSD) . . . 134
1.74 Schéma de la composition interne d'une carte SD, comprenant les composants, les signaux et les bus de communication . . . 137
1.75 Vue optique d'une carte microSD après décapsulation laser et chimique exposant le contrôleur et la puce mémoire . . . 138
1.76 Vue aux Rayons-X d'une carte microSD sur laquelle sont mis en évidence le contrôleur et la puce mémoire . . . 139
1.77 Vue optique des plots de debug d'une carte SD après polissage du vernis . 140
1.78 Dimensions standard d'un support (carte microSD) référencé dans une datasheet [47] d'après les normes émises par le SD Association . . . 141
1.79 Machine à états assurant l'initialisation d'une carte SD d'après la norme JEDEC JESD84-A43 [48] . . . 142
1.80 Machine à états assurant le transfert des données d'une carte SD d'après la norme JEDEC JESD84-A43 [48] . . . 143
1.81 Protocole entre l'hôte et le contrôleur pour l'opération de lecture en mode SD [49] . . . 144
1.82 Protocole entre l'hôte et le contrôleur pour l'opération d'écriture en mode SD [49] . . . 144

1.83 Comparaison des pinouts des formats BGA153, BGA162 et BGA221 pour des eMMC . . . 145
1.84 Brochage des supports MMC sur différents formats . . . 145
1.85 Différence de pinout entre une eMMC et une UFS en package BGA153 . . 146
1.86 Illustration d'un transistor possédant une double grille (contrôle et flottante) 151
1.87 Cellule mémoire NAND flash MLC, illustration de l'évolution des charges permettant de charger la grille flottante et ainsi de stocker des données dans la cellule . . . 151
1.88 Modèle de distribution de tensions de seuil pour une cellule mémoire NAND flash de technologie MLC, les zones colorées représentant de potentielles erreurs de bits . . . 152
1.89 Vue de l'organisation d'une mémoire flash Micron [50] . . . 152
1.90 Exemple d'écriture de nouvelles données avec et sans wear-leveling dans une mémoire NAND flash [51] . . . 155
1.91 Image de la Google Home dans sa version 2016 . . . 158
1.92 Principaux composants du Google Home . . . 159
1.93 Vue de l'arrière de la carte IO . . . 160
1.94 Vue Rayons-X de la carte IO supérieure. Le circuit imprimé est composé de quatre couches, chacune donnant une image 2D. Les sept points de test visibles sur la Figure 1.93 sont tracés jusqu'aux composants respectifs . . . 161
1.95 Vue aux Rayons-X de la carte inférieure . . . 162
1.96 Vue optique de la carte principale avec les composants actifs mis en évidence après retrait des blindages RF . . . 163
1.97 Zoom sur le SoC Marvell Armada 1500 Mini Plus (référence : 88DE3006-BTK2) et sa mémoire flash NAND Toshiba 256MB (référence : TC58NVG1S3H-BAI6). Six points de test sont visibles en bas de l'image de gauche . . . 164
1.98 Vue aux Rayons-X de la carte mère inférieure. Le PCB est composé de quatre couches, chacune donnant une image 2D. Les six points de test sont tracés jusqu'aux composants respectifs. Deux autres points de test ont été tracés jusqu'à des broches non identifiées du SoC. Le trait rouge dans la couche 4 est connecté à VCC et il est utilisé pour tirer le point de test orange (`CE`) . . . 165
2.1 Diagramme de décision orienté forensique numérique appliqué sur les MMC endommagées . . . 167
2.2 Les étapes de la partie non-invasive du diagramme de décision . . . 168
2.3 Les étapes de la partie invasive du diagramme de décision . . . 168
2.4 Vues optiques de cartes microSD avec différents types de dommages visibles 169
2.5 Vue aux Rayons-X de cartes microSD présentant des défauts structurels : fissure dans la puce mémoire . . . 170
2.6 Radiographie 3D provenant d'une carte SD avec identification des pistes après une étude de rétroconception . . . 171
2.7 Radiographie 3D provenant d'une autre carte SD après une étude de rétro-ingénierie et l'identification des signaux . . . 172
2.8 Identification du rôle des signaux de la carte SD . . . 173

2.9 Identification des signaux (image du bas) d'après les bondings du contrôleur (image du haut) après une étude de rétroconception avec des slices d'une radiographie en 3D . . . 174
2.10 Exemple de corrosion suite à une infiltration d'humidité, entraînant une coupure de la continuité électrique [52] . . . 175
2.11 Acquisition infrarouge sur une carte microSD pendant les phases normales de mise sous tension et de lecture . . . 179
2.12 Vue optique des faces avant et arrière d'une carte SD provenant d'un cas réel, dans l'état dans lequel elle a été réceptionnée . . . 183
2.13 Diagnostic initial, à l'aide d'un microscope binoculaire, d'une partie de la carte SD étudiée : aucun défaut visible constaté . . . 184
2.14 Vue radiographique 3D des différentes couches d'intérêt de la carte SD étudiée : aucun défaut détecté . . . 185
2.15 Vue infrarouge de la carte SD témoin étudiée pendant les phases de mise sous tension et de lecture . . . 187
2.16 Vue infrarouge de la carte SD étudiée pendant les phases de mise sous tension et de lecture : un défaut est détecté en bas à droite . . . 188
3.1 Identification des plots de debug de cartes microSD . . . 195
3.2 Vue aux Rayons-X de la carte microSD étudiée . . . 197
3.3 Vue aux Rayons-X de la carte microSD étudiée . . . 198
3.4 Comparaison entre la datasheet d'une mémoire flash et son implantation réelle dans un package . . . 199
3.5 Les différentes étapes d'identification des bondings de la puce mémoire . . . 200
3.6 Report des noms attribués à chacun des bondings sur les vias correspondants afin de s'interconnecter dessus . . . 201
3.7 Exemple de tables à base d'aiguilles mobiles permettant la lecture des supports MMC . . . 202
3.8 Solution PCBite de la société Sensepeek [53] pour s'interconnecter sur des cartes électroniques . . . 203
3.9 Catalogue des solutions PCBite en fonction des applications . . . 203
3.10 Exemple d'adaptateurs permettant de s'interconnecter sur les plots de debug de supports MMC . . . 204
3.11 Logiciel VNR de la société Rusolut permettant d'appliquer les opérations logiques pour les relectures brutes des mémoires flash . . . 205
3.12 Comparaison entre une eMMC BGA221 et une carte microSD avec plots de debug apparents et recouverts de vernis . . . 207
3.13 Parallèle entre la vue Rayons-X prévoyant les ouvertures et la vue réelle après ablation laser du vernis . . . 209
3.14 Carte électronique dessinée sur mesure en fonction de la carte microSD . . . 211
3.15 Carte microSD et PCB correspondant, avant assemblage . . . 211
3.16 Vue de la carte microSD après fixation sur le PCB et établissement des connexions électriques avec les vias . . . 212
3.17 Photo du montage utilisé pour effectuer la capture des trames entre l'hôte et la carte microSD ainsi qu'avec la mémoire . . . 217
3.18 Vue du chronogramme de début des échanges entre le contrôleur et la mémoire avec l'analyseur logique Saleae . . . 218

3.19 Zoom sur le chronogramme permettant d'identifier les signaux Vcc et le Chip Enable (CE) . . . 219
3.20 Chronogramme des fonctions RESET et READ_ID d'après la norme ONFI 4.1 [54] . . . 219
3.21 Zoom sur la commande RESET permettant d'identifier les signaux Command Latch Enable (CLE) et Write Enable (WE) . . . 220
3.22 Zoom sur la commande READ_ID permettant d'identifier l'ensemble des signaux . . . 221
3.23 Deux équipements fonctionnant à base d'air chaud pour dessouder des composants . . . 228
3.24 Station de dessoudage PDR modèle IR E6 [55] . . . 229
3.25 Vue optique de l'assemblage de lecture de la mémoire, avec la connexion fil à fil entre la puce mémoire et une carte de lecture . . . 229
3.26 Analyse de l'entropie de Shannon (normalisée) de l'image principale en utilisant `binwalk`. L'axe des x désigne le décalage par rapport au début de la lecture, tandis que l'axe des y montre l'entropie d'une petite région centrée sur un décalage donné . . . 231
3.27 Différences apparaissant dans le fichier `/bin/bluetoothtbd` des deux candidats cibles pour le fragment `heNYlKQRQ8pfXf3Z3PPPrTiGCnkbaLLai2lenD8qRzA`. Le candidat de gauche présente une instruction (en vert) utilisant un registre indéfini `r6`, alors que le candidat de droite semble valide. Par conséquent, le candidat de gauche n'est pas valide, il est écarté . . . 240
4.1 Développement et validation d'une preuve de concept de manipulation sur des supports en zone NRBC . . . 253

Liste des tableaux

1 Dispositions relatives à l'attaque contre le chiffrement de pays de l'Europe [9] 22
1.1 Tableau de classification des supports avec leurs utilisations et les capacités de traitement . . . 63
1.2 Tableau des produits et mélanges en fonction des matériaux à attaquer . . 92
1.3 Tableau de comparaison de l'utilisation des équipements dans les laboratoires 110
1.4 Table de vérité de l'inverseur . . . 118
1.5 Table de vérité de la fonction AND . . . 118
1.6 Table de vérité de la fonction NAND . . . 119
1.7 Table de vérité de la fonction OR . . . 120
1.8 Table de vérité de la fonction NOR . . . 120
1.9 Table de vérité de la fonction XOR . . . 121
1.10 Tableau comparatif des différentes normes de carte SD avec leurs capacités et vitesses respectives . . . 135
1.11 Comparaison des signaux entre la carte SD et la carte microSD . . . 140
1.12 Comparaison des signaux entre la carte SD, la carte microSD et la mémoire eMMC BGA153 . . . 146
1.13 Position des signaux de la mémoire UFS en package BGA153 . . . 147
1.14 Trame de communication pour le protocole UFS entre l'hôte et le contrôleur 148
1.15 Valeur pouvant prendre le champ Type dans la trame de communication . 148
1.16 Signaux des mémoires NAND flash référencés dans la norme ONFI avec les fonctions respectives . . . 148
1.17 Commandes référencées dans la norme pour les échanges entre le contrôleur et la mémoire, pour les actions liées au statut ou aux pages . . . 149
3.1 Tableau comparatif des solutions pour dégager les points d'intérêt sur un support MMC . . . 208
3.2 Interprétation du round unique de la trame de RESET . . . 220
3.3 Interprétation des rounds de la trame de READ_ID . . . 221
3.4 Tableau comparatif des combinaisons possibles pour les ID relevés lors des échanges . . . 223
3.5 Tableau comparatif du second round de l'ID relevés lors des échanges . . . 223
3.6 Interprétation des différents rounds en hexa de l'ID de la mémoire . . . 223
3.7 Interprétation des différents rounds en hexa de l'ID de la mémoire . . . 224
3.8 Signification des différents rounds en hexa de l'ID de la mémoire . . . 224
3.9 Plan mémoire de l'image . . . 232
3.10 Plan des superblock de la SquashFS . . . 234
3.11 Structure d'un fragment compressé avec zlib . . . 235
3.12 Liste des fragments (identifiés par leur hash) avec de multiples candidats cibles et leur nombre de candidats respectifs . . . 238
3.13 Taux de récupération au niveau du bit, de l'octet et du fichier avant et après la réparation du bitflip. . . . 240

De l'analyse de défaillance à la rétro-conception hardware à des fins de forensique

Le présent mémoire a pour objet de retracer les travaux de recherche effectués durant ma thèse. Afin de mieux appréhender le déroulé de ces travaux, il faut tout d'abord les recontextualiser et évoquer ma démarche professionnelle. Cette thèse est réalisée dans le cadre d'une formation continue, après une expérience professionnelle de plus de quinze ans. Ma carrière m'a d'abord amené à exercer le poste de technicien en analyse de défaillance dans un laboratoire privé, puis d'ingénieur en rétro-conception matériel avant de basculer sur de la forensique numérique. Il s'agit de trois métiers qui, malgré leurs différences d'objectifs, possèdent des similitudes. Ils sont tous les trois voués à interagir sur les composants électroniques au plus bas niveau et les équipements de base, pour réaliser des opérations sont également similaires. Malgré ces similitudes, les interactions entre ces métiers restent assez faibles et des profils multidisciplinaires, sachant évoluer dans ces différentes activités, sont très rares. L'objet de ma réflexion qui m'a conduit à effectuer des travaux de recherche visait à répondre à une question : Comment amener des équipements et techniques évolués provenant de l'analyse de défaillance et de la rétro-conception matériel en faveur des activités de forensique numérique ? Afin de répondre à cette question, nous allons commencer par définir ce que sont les métiers et les cadres de travails de :

— la forensique numérique par son origine, le cadre légale d'intervention et les interactions entre les laboratoires ;
— l'analyse de défaillance et plus largement de l'assurance qualité au travers de son origine, des objectifs et de la démarche ;
— la rétro-conception matériel par son objectif.

Contexte de la forensique numérique

La forensique numérique (en anglais "Digital Investigation") est définie selon les différents codes législatifs, dont le Code de la Sécurité Intérieur [56], comme "l'ensemble des opérations techniques et d'analyse qui permettent de collecter, de conserver, d'exploiter et de présenter des éléments de preuves numériques en vue de l'identification des auteurs d'infractions commises sur des systèmes d'information". Dans ce chapitre, plusieurs textes de références provenant du Code de Procédure Pénale (CPP) seront utilisés afin de cadrer la forensique numérique du point de vue du droit : le délit de flagrance (article 56-1 [57]), les examens scientifiques ou techniques pouvant être pratiqués (article 77-1 [58]), l'interception des communications électroniques (article 100-1 [59]), les transcriptions d'échanges de communications électroniques (article 706-95 [60]) et de la captation des données numériques (article 706-102-1 [61]). Le principal objectif d'une investigation dans le numérique, tout comme une investigation dans l'univers du vivant, est de faire la lumière sur les faits tout en préservant les éléments de preuves. L'investigation

peut également se retrouver en entreprise dans le cadre des enquêtes internes. La démarche s'articule donc sur des procédures devant être rigoureuses, établies et validées à l'avance dans le but de maximiser les chances de succès lors de l'analyse.

La preuve judiciaire possède une histoire liée à celle de la justice. À l'origine, la justice est une notion rattachée aux premières civilisations pour régler des différents sur les possessions des fruits de la chasse et des récoltes. La justice s'est ensuite développée lors de l'antiquité et les premiers textes de lois peuvent être référencés dans le code d'Ur-Nammu [62] rédigé vers 2100 avant JC. D'après le livre de Jean Gaudemet, "Les institutions de l'Antiquité" [63], ce texte aurait été retrouvé sous la forme d'une tablette contenant un fragment d'un code Sumérien datant de la troisième dynastie d'Ur. Les lois sont exprimées sous la forme causalité, c'est-à-dire qu'un crime précis implique un châtiment en conséquence. Dans la partie du texte retrouvé, il n'apparaît pas de notion de jugement mais uniquement de crimes distincts. La première notion de preuve, qui pour le coup était factuelle, apparaissait dans une des lois qui dit : *Si un homme est accusé de sorcellerie, il doit se plier à l'épreuve de l'eau froide ; si son innocence est prouvée, son accusateur doit payer 3 shekels.* Dans cette loi, la notion de prouver l'innocence ou la culpabilité, entraînant la condamnation ou non, est mise en avant. Il ne s'agissait cependant pas d'une preuve matérielle ou d'un témoignage mais d'une épreuve sans fondement. Par la suite, la première civilisation à théoriser la justice était la civilisation romaine, qui utilisait déjà le rôle du juge chargé d'accumuler et d'examiner les preuves puis de rendre le jugement en fonction. Cette chronologie a été mise en avant par Aldo Schiavone, dans son livre "L'invention du droit en occident" [64]. Cependant, nous constatons dans tous les écrits qu'entre le code d'Ur-Nammu et la civilisation romaine, les traces avérées de la conversion de la croyance unique à la preuve n'est pas définie. Aujourd'hui la preuve est la base des procès modernes dans une majorité non négligeable des pays du monde. En France, l'administration de la preuve est décrite par les articles 427 à 457 du CPP [65]. Ces articles définissent un cadre juridique de ce qu'est une preuve matérielle, un témoignage, un rapport d'expertise judiciaire ainsi que les rédactions à produire, c'est-à-dire les rapports et procès-verbaux.

Champs d'application de la forensique numérique

Il existe plusieurs catégories dans le domaine de la forensique numérique, dépendant de la technologie du système d'information concerné. En effet, la forensique numérique ne se limite pas à un type de support et elle peut aussi bien concerner un support matériel au travers d'un ordinateur qu'un système d'information d'une entreprise qui aurait subi une intrusion. Parmi les différentes catégories, nous pouvons identifier :

— Le traitement des infractions sur des systèmes matériels, dans un environnement

virtuel : il s'agit d'apporter une réponse aux infractions liées aux systèmes, qui ne sont pas matérialisés physiquement. Même dans un environnement virtuel, les conséquences d'une infraction peuvent avoir des répercutions tangibles dans la vie des victimes (par exemple : pertes financières, pertes d'emplois, dépression). Il est donc possible d'identifier :

* La lutte contre la cybercriminalité. Dans ce contexte, la cybercriminalité qui peut se matérialiser par exemple sous la forme de piratage informatique, à savoir un accès non autorisé à un réseau pour en extraire de l'information ou déposer un logiciel malveillant ou, une attaque plus basique comme le DDOS (attaque par déni de service). D'un point de vue légal, on peut retrouver dans le code pénal, les articles 323-1 [66] sur l'atteinte, 323-2 [67] sur l'entrave et 323-3 [68] sur la modification des données issues de systèmes de traitement automatisés des données. Ainsi, les citations suivantes peuvent être extraites pour l'atteinte à un système de traitement automatisé des données : *"Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de cinq ans d'emprisonnement et de 150 000 € d'amende"*. L'entrave d'un système de traitement automatisés des données est décliné comme suit : *"Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende"*. Enfin, la modification des données issues de systèmes de traitement automatisés des données est décrit comme suit : *"Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende"*. De plus, la diffusion de moyens permettant de commettre les infractions préalablement énoncées sont décrites dans l'article 323-3-1 [69] par : *"Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions"*. Ce point est également couvert par l'article 323-4 [70] lorsque les faits sont commis par association. Les peines encourues sont quant à elles définies dans l'article 323-5 [71].
* La réponse aux incidents de sécurité qui concerne généralement les entreprises ou entités victimes d'une attaque ou d'un incident de sécurité. Le traitement de cette infraction consiste à comprendre la voie d'accès de l'attaquant pour déterminer les dommages, puis à récupérer ce qui peut l'être mais surtout à

corriger les failles pour éviter de nouvelles attaques.

— Le traitement des infractions sur des supports matériels : Le parallèle avec l'investigation sur des systèmes immatériels est le traitement des supports physiques. Les opérations réalisées peuvent intervenir à plusieurs moments dans le processus judiciaire et sont plus amplement détaillées dans la section *Réglementation française de la forensique numérique*. Elles se matérialisent principalement par :
  * La collecte et l'analyse de preuves numériques. Si l'ADN a été considéré très longtemps comme la reine des preuves, peut-on dire que dans la succession la preuve numérique est une dauphine ? Dans un environnement de plus en plus connecté ou chaque objet du quotidien est amené à communiquer avec son environnement et ses utilisateurs, la preuve numérique prend toute son envergure quand il s'agit de mettre en lumière des faits dans des affaires judiciaires. L'objectif est donc de prendre en charge un support physique pour en collecter, donc extraire, les données puis les analyser pour en déduire des faits et apporter un éclairage aux enquêteurs, avocats, et magistrats. La phase d'extraction pouvant être complexe à cause de la nature du support ou de son état, **les travaux réalisés dans cette thèse visent à proposer des solutions pour effectuer l'extraction des données.**

— L'enquête dans un univers virtuel : En complément des différentes investigations techniques pouvant être réalisées sur les systèmes matériel, il est également possible de réaliser des enquêtes dans l'univers virtuel, sans lien avec du matériel, pour relever des infractions réelles. Ces enquêtes peuvent prendre la forme de :
  * La lutte contre la cybercriminalité telle que la fraude en ligne ou le vol d'identité qui sont des activités grandement repandues et qui visent à soutirer directement de l'argent ou des données personnelles à leurs victimes. Le cadre légal contre ses activités est défini dans le code pénal par l'article 226-4-1 [72] pour l'usurpation d'identité est défini par : *"Le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature [...] est puni d'un an d'emprisonnement et de 15 000 € d'amende"*. En 2022, plus de 300000 personnes auraient été victimes d'un vol d'identité en France, dont l'origine provenait d'hameçonnage vocal ou par messagerie [73].

    Une autre infraction réalisée sur internet est la diffusion de contenus illicites. Principalement basée sur le partage d'images à caractère pédopornographique, elle regroupe également le partage d'images de stupéfiants ou d'armes visant par la suite à une commercialisation. Le cadre légal contre ses activités est défini dans le code pénal par l'article 226-1 [74] pour la violation de la vie privée sous les termes : *"Est puni d'un an d'emprisonnement et de 45*

000€ d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui". L'article 441-1 [75] décrit les peines encourues pour faux et usage de faux. L'article 227-23 [76] décrit sous les termes : *"Le fait, en vue de sa diffusion, de fixer, d'enregistrer ou de transmettre l'image ou la représentation d'un mineur lorsque cette image ou cette représentation présente un caractère pornographique est puni de cinq ans d'emprisonnement et de 75000€ d'amende"* l'acquisition et/ou la diffusion d'images à caractère pédopornographique. L'article décrit également des dispositions complémentaires en fonction de l'âge de la victime et des moyens de diffusions ou de consultation. Enfin, l'article 421-2-5 [77] décrit les peines encourues pour l'apologie du terrorisme comme suit : *"Le fait de provoquer directement des actes de terrorisme ou de faire publiquement l'apologie de ces actes est puni de cinq ans d'emprisonnement et de 75 000€ d'amende"*. Il est à noter que l'article prévoit des dispositions particulières et plus lourdes, si la diffusion est réalisée sur un canal de communication public sur internet *"Les peines sont portées à sept ans d'emprisonnement et à 100000€ d'amende lorsque les faits ont été commis en utilisant un service de communication au public en ligne"*.

  * Le suivi des activités criminelles en ligne. Dans le point précédent, nous avons évoqué le fait de relever les infractions qui prennent place directement sur internet, cependant une autre pratique consiste à ne pas relever les infractions mais à les renseigner pour en suivre les ramifications et étoffer une enquête. Ainsi, plutôt que de rechercher les images de stupéfiants pour localiser un revendeur précis, il peut être plus intéressant de suivre les activités sur le Clear et le Dark Web pour en remonter des réseaux de distribution plus complexes et mener une enquête beaucoup plus complète. L'un des acteurs principaux pour ces enquêtes en France est le centre de lutte contre les criminalités numériques (C3N) [78].

— La sécurisation des systèmes d'information : Outre les activités d'enquête et d'analyse des éléments numériques, la forensique peut prendre un autre aspect qui consiste à prodiguer des conseils pour la sécurisation des systèmes d'information, ce qui permet d'éviter de basculer dans des investigations via :

  * La protection des données. La perte d'informations est un risque important de compromission pour une entreprise ou un individu. Cette perte de donnée peut être par négligence ou par malveillance. Il s'agit donc d'enjeu clé pour la sécurisation des données. Ainsi prodiguer de bonnes pratiques à ses collaborateurs (lors de déplacements professionnels, de réunions ou de télétravail) permet de limiter les risques de voir des secrets industriels

disparaître ou d'ouvrir des portes d'accès au système d'information de l'entreprise.

* La protection de la vie privée : En parallèle de la sécurisation de la vie professionnelle d'une personne, il est également important de sensibiliser sur les risques concernant la vie privée. L'utilisation récurrente des réseaux sociaux ou des applications de partage d'informations favorisent certaines dérives (comme par exemple : diffamation en ligne, cyberharcèlement, de violation de la vie privée) dans la protection de l'identité numérique. Un acteur clé veillant sur la sécurisation des données personnelles est la Commission nationale de l'informatique et des libertés (CNIL) [79].

Acteurs français de la forensique numérique

La forensique numérique est un domaine d'activité au niveau international et malgré des organismes à vocation pluri-frontalière (par exemple : Interpol, Europol), les réglementations sont dépendantes de chaque pays. Une tentative d'harmonisation a cependant été faite en 2001 avec l'établissement de la convention de Budapest [80] qui a justement pour but de proposer des normes légales communes en matière de cybercriminalité pour les différents pays signataires. En 2022, c'est 66 pays qui étaient signataires de la convention pour la décliner dans son cadre légal propre. Les réglementations peuvent porter sur les différents aspects de la forensique numérique, que cela soit sur la collecte, l'analyse ou même les exigences pour rapporter les travaux (par exemple : rédaction de rapports, traçabilité des résultats).

Un exemple d'analyse sur les cadres légaux des différents pays européens peut être fait sur le traitement des données issues du chiffrement et de son attaque. Le Tableau 1 présente la comparaison des cadres législatifs dans différents pays Européens. Il est possible de constater que certains pays tels que la France, la Suède ou les Pays-Bas se sont appliqués à établir des lois spécifiques pour traiter des questions techniques pointues et offrent une solution législative complète pour leurs citoyens. D'autres pays comme la Grèce, l'Espagne ou la Belgique ont choisi un traitement de la question généraliste par rapport à des questions techniques. Ils s'appuient sur des textes plus globaux qui ne prennent pas spécifiquement en compte la question du chiffrement et de l'attaque de ce chiffrement mais au contraire, qui traitent plus particulièrement de l'infraction retenue pour la poursuite. Enfin certains pays comme l'Autriche, le Luxembourg ou la Norvège utilisent un cadre législatif général sans s'appliquer à introduire un aspect technique dans le traitement des infractions.

Le Tableau 1, illustre une différence sur les cadres législatifs des différents pays. Cependant cela n'empêchent pas les collaborations. Pour prendre un exemple concret,

Tableau 1 – Dispositions relatives à l'attaque contre le chiffrement de pays de l'Europe [9]

Pays	Cadre légal de l'attaque de chiffrement
Allemagne	Spécifique (Sections 94,98,100,102 du code de procédure)
Autriche	Général
Belgique	Adapté (Articles 39bis, 89ter, 90ter du code de procédure)
Croatie	Adapté (Articles 257 - 263 & 332 - 339)
République tchèque	Adapté (Sections 113 du code de procédure)
Danemark	Spécifique (Sections 780-81, 791b, 793-94 Loi de l'admin. judiciaire)
Espagne	Adapté (Articles 588bis à ter, 588sexies à septies du code de procédure)
Estonie	Adapté (§83, 91, 1265, 1267 du code de procédure)
France	Spécifique (Articles 230-1 à 5, 706-102-1 à 5 du code de procédure)
Grèce	Adapté (Article 258, Article 264 du code de procédure)
Hongrie	Adapté (Section 264, Article 3 du code de procédure)
Ireland	Général
Lettonie	Adapté (Sections 190, 192 du code de procédure)
Lithuanie	Adapté (Articles 145, 154, 158, 208 du code de procédure)
Luxembourg	Général
Norvége	Général
Pays-bas	Spécifique (Articles 126 du code de procédure)
Pologne	Spécifique (Article 19 §7 Loi Police & 218, 236a du code de procédure)
Portugal	Général
Roumanie	Adapté (Article 138 §1 et §3 du code de procédure)
Slovaquie	Adapté (Sections 90, 116 §6, 118 & 115 §11 du code de procédure)
Slovenie	Général
Suède	Spécifique (Article 2020 :62)

toujours basé sur la problématique de l'attaque du chiffrement des données dans le cadre de la forensique numérique, des échanges techniques affichés ou dissimulés ont pu voir le jour ces dernières années. La partie publique des échanges ont pris la forme soit de projets communs financés par l'Europe soit de conférences uniquement destinées aux agences de forensique numérique.

Les projets de collaboration européenne les plus importants à retenir sont :

— Cerberus (2019 à 2021) [81] : Le projet avait pour objectif de développer une plateforme de cassage de mots de passe à destination des forces de l'ordre européennes. La plus-value de cette plateforme est de fournir des algorithmes de cassage de mots de passe optimisés pour les smartphones les plus couramment rencontrés dans des dossiers critiques.

— Overclock (2021 à 2024) [82] : Basé sur la plateforme Cerberus, l'objectif du projet est d'étoffer la liste des algorithmes connus sur les smartphones. Pour arriver à l'objectif, les acteurs du projet doivent procéder à la rétro-conception logicielle de plusieurs cibles pour comprendre les sécurités et retrouver les algorithmes.

— Exfiles (2020 à 2023) [83] : Contrairement aux projets Overclock et Cerberus, Exfiles n'est pas destiné directement à l'exploitation de résultats pour proposer une solution finale aux forces de l'ordre. Il s'agissait de faire une veille technologique des moyens d'attaque software et hardware et de trouver des opportunités communes. Les livrables attendus n'étaient pas une plateforme ou des vulnérabilités logicielles, mais plutôt des résultats d'expérimentations alliant à la fois rétro-conception logicielle, rétro-conception matérielle, préparation physique de cibles et attaques électromagnétiques.

Les conférences notables[1] destinées aux laboratoires de forensique numérique à l'échelle internationale sont :

— Forensique Internationale : Il s'agit d'un groupe constitué de pays d'Europe, d'Asie et d'Amérique aux compétences avancées dans le domaine de la rétro-conception matérielle et logicielle. Les entités sont libres d'échanger en bilatérale sur des problématiques communes. Une réunion a lieu annuellement pour échanger sur les derniers investissements, conseiller les autres laboratoires sur des manipulations et techniques, ou présenter des travaux d'intérêt public ou en diffusion restreinte.

— Vulnérabilité Composant : Le groupe comporte sensiblement les mêmes acteurs et le même fonctionnement que le précédent. Les objectifs sont similaires et ce sont les cibles qui diffèrent. En effet, ce groupe n'est plus basé sur l'étude d'un système en entier mais uniquement sur l'accès à la donnée dans un composant. Les plus gros systèmes traités sont équivalents à des clés USB mais généralement l'intérêt va se porter uniquement sur le contrôleur ou la mémoire. Ce groupe va avoir accès à des équipements de pointe et va utiliser des techniques extrêmement avancées, réservées à des spécialistes dont les compétences ne sont connues que dans un milieu très fermé.

En France, la forensique numérique regroupe différents acteurs publics et privés :

— Les services d'enquêtes (Gendarmerie, Police, Douanes, Bureau d'Enquêtes et d'Analyses pour la sécurité de l'aviation civile (BEA)). Ils interviennent dans l'ensemble des catégories de la forensique numérique car ils ont la charge de prévenir les risques, puis de mener les différentes investigations au niveau des populations. S'il existe plusieurs services pour réaliser cette mission c'est à cause de la pluralité des métiers et des secteurs de compétences. Le BEA est chargé d'enquêter lorsqu'un incident a lieu en France ou dans les eaux internationales et qu'il implique un aéronef français. La gendarmerie interviendra seule dans l'enquête si le crash a lieu à l'international avec au moins une victime française ou si l'avion est immatriculé en France.

1. Le nom réel des conférences, ainsi que la liste des participants ne seront pas rapportés dans ce mémoire par soucis de discrétion. Les noms utilisés seront des noms similaires francisés

— Les ministères (de l'intérieur ou des armées). Ils interviennent principalement dans la forensique numérique pour leurs propres missions de sécurisation du territoire et sur des théâtres internationaux. Leurs champs d'application sont sur l'investigation matérielle et immatérielle ainsi que sur de l'enquête pour certaines affaires se déroulant sur des bases militaires. L'investigation passe par la constitution d'une cellule de crise spécialisée, en fonction de la nature des travaux à mener.
— L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) [84]. Le rôle de l'agence est d'apporter toute la prévention possible aux entreprises et particuliers permettant de protéger les données numériques. L'agence réalise également les investigations dématérialisées sur les incidents d'entreprises pour protéger les intérêts économiques et stratégiques de la nation.
— Les laboratoires d'expertises privées. Ils ont pour rôle de fournir des expertises au système judiciaire français et d'apporter des éclaircissements sur des points techniques précis, préalablement définis par le magistrat en charge du dossier. L'ensemble des modalités de commission d'un expert et du déroulement de son travail sera plus amplement décrit dans la section *Réglementation française de la forensique numérique.*

Le nombre des acteurs peut paraître important et il semble y avoir une certaine redondance, mais le nombre de dossiers annuels à traiter et la diversité des missions sont très importants. Par exemple, la Police scientifique déclare traiter près de 500000 scellés par an grâce à leurs cinq laboratoires [85]. Ce nombre couvrant tous les domaines d'activités de la forensique et pas uniquement le domaine numérique, il est donc à relativiser. Au même titre qu'il s'agit uniquement des chiffres de la Police scientifique il conviendrait d'additionner ceux traités par les autres acteurs.

Réglementation française de la forensique numérique

En France, le texte qui va donner les règles à suivre pour une expertise est le Code de Procédure Pénale [86]. Le code décrit sous forme d'articles les actions et documents à produire dans le cadre d'une expertise, quel que soit le domaine (c'est-à-dire biologique, balistique, médicine légale, psychologique, ou encore numérique). Il décrit également le contexte et les modalités de désignation d'un expert ainsi que son champ d'action dans l'article 156 [87]. L'objet de la commission d'un expert est de répondre à une question d'ordre technique : *"Toute juridiction d'instruction ou de jugement, dans le cas où se pose une question d'ordre technique, peut [...] ordonner une expertise"*. Les questions qui sont posées à l'expert doivent être précises et explicites comme indiqué dans l'article : *"Le ministère public ou la partie qui demande une expertise peut préciser dans sa demande les questions qu'il voudrait voir poser à l'expert"*.

Dans un premier temps, il est nécessaire de comprendre que le droit français ne permet pas les mêmes actes techniques d'investigation selon l'autorité ordonnant les travaux : Officier de Police Judiciaire (OPJ), procureur ou juge d'instruction. Le terme utilisé pour réaliser les travaux ordonnés par un officier de police judiciaire ou un procureur entre dans le cadre d'une réquisition à personne qualifiée et ces travaux peuvent être réalisés par toute personne qualifiée désignée par l'entité l'employant. Ainsi les compétences de la personne qualifiée sont à la libre évaluation de son employeur sans que l'officier de police judiciaire ou le procureur n'ait à apposer un avis. D'ailleurs, la réquisition ne porte pas sur une personne nominativement mais sur un service. C'est alors le chef de service qui déléguera les opérations à toute personne qu'il jugera compétente pour mener l'opération technique. En opposition, les travaux ordonnés par un juge d'instruction sont décrits par une Ordonnance de Commission d'Expert (OCE) nominative et la personne réalisant les travaux est appelé expert. Les modalités de désignation de l'expert sont décrites dans les articles 157 à 157-2 du CPP. L'article 157 [88] définit qu'un expert est inscrit sur une liste déposée à la Cour de cassation ou en Cour d'appel : *"Les experts sont choisis parmi les personnes physiques ou morales qui figurent sur la liste nationale dressée par la Cour de cassation ou sur une des listes dressées par les cours d'appel dans les conditions prévues par la loi n° 71-498 du 29 juin 1971 relative aux experts judiciaires"*. Dans l'article 157, il est mentionné que l'expert peut être une personne morale. Si tel est le cas, un personnel rattachée à cette entité doit réaliser les actes techniques. La possibilité de proposer une personne physique, en cas de désignation d'une personne morale, est décrite dans l'article 157-1 [89] : *"Si l'expert désigné est une personne morale, son représentant légal soumet à l'agrément de la juridiction le nom de la ou des personnes physiques qui, au sein de celle-ci et en son nom, effectueront l'expertise"*. L'article 157-2 [90] précise que l'expertise peut également être confiée à un organisme de l'état. Dans ce cas les dispositions de l'article 157-1 s'appliquent.

Comme indiqué dans les trois articles, et contrairement à la personne qualifiée, l'expert est une personne inscrite sur une liste officielle déposée dans un tribunal, après avoir préalablement déposée un dossier démontrant les compétences techniques et les aptitudes à déposer au tribunal. Dans certaines exceptions, couvertes par l'article 157 [88], si le magistrat ne dispose pas dans une liste, d'un expert capable de réaliser les travaux nécessaires, il peut faire appel à une personne tierce portant des compétences significatives : *"À titre exceptionnel, les juridictions peuvent, par décision motivée, choisir des experts ne figurant sur aucune de ces listes"*. Le choix de cet expert particulier peut donc se faire sur recommandation d'un autre expert, sur la base de publications scientifiques ou encore après la participation à des évènements de communication en lien avec le domaine judiciaire. Dans ce cas, l'expert appelé expert non inscrit, devra signer une prestation de serment qui sera inclut dans le rapport d'expertise.

Un officier de police judiciaire peut soumettre une réquisition à une personne qualifiée en s'appuyant sur plusieurs articles du CPP, dépendant des circonstances des faits :

— Enquête en flagrance selon l'article 60, pour des faits qui viennent de se produire ou qui sont en cours. Il s'agit d'une réponse rapide de la justice permettant dans un temps court d'orienter l'enquête.

— Enquête préliminaire selon l'article 77, qui permet de travailler à partir d'indices sur des faits présumés ou avérés pour en découvrir les auteurs et les circonstances. L'élément déclencheur de l'enquête peut être hétéroclite allant de la disparition inquiétante, au trafic de stupéfiants, à l'escroquerie, ou encore à la découverte de cadavre.

À partir de l'analyse des différents articles du Code de Procédure Pénale abordant le travail effectif de l'expert, il est possible de décrire les étapes classiques d'une expertise. Lors de travaux de recherche dans le domaine de la forensique numérique, notre démarche devra prendre en compte des étapes strictes. Cette analyse est d'autant plus importante, que nous développons un protocole standard pour l'analyse des supports et que nos travaux pourraient altérer les preuves. Les différentes étapes d'une expertise sont :

1. Prendre en compte le scellé et procéder à son ouverture. Si d'après le cadre légal définit dans l'article 97 du CPP [91], seuls des officiers de police judiciaire sont habilités à confectionner un scellé en présence du suspect ou à défaut de témoin cosignataire du scellé, l'ouverture de celui-ci est administrée par l'article 163 du CPP [92], dans le cadre d'examens techniques : *"Pour l'application de leur mission, les experts sont habilités à procéder à l'ouverture ou à la réouverture des scellés"*. L'ouverture du scellé doit se faire précautionneusement car le contenant ainsi que le carton de scellé doivent être conservés et réutilisés lors de la reconstitution de celui-ci.

2. Effectuer les opérations d'extraction de la donnée numérique. L'expert ou la personne qualifiée doit ainsi répondre à la mission qui lui a été confiée conformément à l'article 158 du CPP [93]. Cette mission doit être clairement définie et le technicien doit se limiter au cadre de sa mission : *"La mission des experts qui ne peut avoir pour objet que l'examen de questions d'ordre technique est précisée dans la décision qui ordonne l'expertise"*. Il pourra cependant faire mention de tout élément pouvant servir à la manifestation de la vérité. La phase d'extraction de la donnée est indispensable dans le contexte de la forensique numérique et une règle prédomine, ne pas altérer les données. Pour garder la preuve et permettre une contre-expertise, le technicien doit autant que possible effectuer les opérations nécessaires pour garantir l'intégrité de la donnée qu'il doit extraire. Si cela est indispensable, les experts peuvent être amenés à modifier la donnée (écriture de fichiers dans un journal de log d'un système, remplacement

de zone inintelligible dans une copie de mémoire), mais uniquement si l'accord est précisé sur la réquisition ou l'ordonnance de commission d'expert. L'expert devra faire mention de ces modifications de données dans son rapport. Il devra également au préalable avoir réaliser une copie bit à bit des données originales et la fournir en annexe de son rapport. Cette modification de la donnée prend également en considération les opérations effectuées sur l'extraction (c'est-à-dire le déchiffrement de la donnée).

3. Effectuer des actes de diagnostic et réparation. Dans certains cas l'extraction de la donnée n'est pas directement possible par le technicien et il faut procéder au diagnostic puis à la réparation du système ou d'une partie de ce dernier. Il arrive que l'expert qui est compétent dans l'extraction de la donnée ne le soit pas pour d'autres étapes. Dans ce cas, le CPP prévoit au travers de l'article 159 [94] de pouvoir faire cohabiter plusieurs experts sur la même mission : *"Le juge d'instruction désigne l'expert chargé de procéder à l'expertise. Si les circonstances le justifient, il désigne plusieurs experts"*. L'article 162 [95] prévoit qu'un expert désigné puisse utiliser les travaux réalisés par un second expert, sur un champ de compétences qui n'est pas le sien : *"Si les experts demandent à être éclairés sur une question échappant à leur spécialité, le juge peut les autoriser à s'adjoindre des personnes nommément désignées, spécialement qualifiées par leur compétence"*.

4. Procéder à l'étude du système. Même si un expert est reconnu pour ses compétences en électronique, par exemple, il ne maîtrise pas nécessairement l'ensemble des systèmes électroniques. Il peut donc avoir besoin d'effectuer des travaux d'étude sur le système concerné en amont à la récupération de la donnée. Ces travaux peuvent uniquement consister à relever les références des composants et étudier leurs documentations. Dans d'autres cas, il est possible d'avoir recours à la rétro-conception hardware, qui est autorisée selon certaines conditions présentées dans la section *Introduction sur la rétro-conception matérielle*.

5. Effectuer l'analyse des données extraites. Cette étape consiste à traiter les données extraites pour fournir des preuves, à charge ou à décharge. Le travail ne s'effectue pas sur le scellé lui-même mais sur une copie pour ne pas altérer les données lors d'éventuels traitements. L'analyse, même si elle est dépendante de l'expert qui la réalise, se doit d'être objective. Il doit apporter un éclaircissement sur des questions précises qui lui ont été posées pour éclairer les différentes parties et aider le juge à prendre une décision.

6. Refermer le scellé ou en confectionner un nouveau. L'article 163 du CPP [92] prévoit qu'à l'issue des travaux, l'expert doit refermer le scellé dans son conditionnement d'origine. Il est cependant autorisé, si le conditionnement d'origine n'est pas

conforme et ne garantit plus l'intégrité des données, de reconditionner un scellé : *"Pour l'application de leur mission, les experts sont habilités à procéder [...] au reconditionnement des objets qu'ils étaient chargés d'examiner"*. Enfin l'expert est habilité à confectionner un nouveau scellé à partir d'éléments contenus dans un scellé précédent. Par exemple dans le domaine automobile, le scellé d'origine peut être une voiture dans son intégralité mais l'expert peut être requis pour travailler sur le calculateur d'airbag suite à un accident. Dans ce cas, l'expert est habilité à ouvrir le scellé « voiture », prélever le calculateur pour effectuer ses travaux, puis refermer le scellé « voiture » sans réintroduire le calculateur, celui-ci étant scellé indépendamment. L'expert aura donc confectionné un nouveau scellé. Plus généralement dans le domaine informatique, les experts distinguent la phase d'extraction de la donnée et la phase d'analyse. À l'issue de l'extraction, les experts déposent la donnée brute sur un support qui devient un scellé, ce qui permettra en cas d'une expertise complémentaire ou d'une contre-expertise de se concentrer sur l'analyse sans refaire l'extraction.

À noter que les règles sont différentes pour une réquisition car la personne qualifiée n'est pas autorisée à changer le conditionnement d'un scellé, ni à réouvrir un scellé qu'elle aurait préalablement refermé pour un complément dans son travail.

7. Fournir un rapport qui d'après l'article 166 du CPP [96], doit reprendre la mission qui lui a été confiée puis conclure en répondant aux questions qui lui ont été posées en faisant description des opérations réalisées : *"Lorsque les opérations d'expertise sont terminées, les experts rédigent un rapport qui doit contenir la description desdites opérations ainsi que leurs conclusions"*. L'expert doit également mentionner le nom et la qualité des personnes qui l'ont assisté lors de ses travaux : *"Les experts signent leur rapport et mentionnent les noms et qualités des personnes qui les ont assistés, sous leur contrôle et leur responsabilité, pour la réalisation des opérations jugées par eux nécessaires à l'exécution de la mission qui leur a été confiée"*. Le rapport aura pour but d'être dans une forme succincte mais précis sur les opérations et les termes car il s'agira du document de travail pour les différentes parties. Les étapes 2 à 5 seront à effectuer si la mission demandée à l'expert en fait mention, tandis que les étapes 1, 6 et 7 seront effectuées systématiquement comme l'exige CPP.

Dans cette partie, nous avons présenté la forensique numérique, son fonctionnement et ses implications en droit français. Cependant, même si toutes ces actions doivent répondre au CPP, les actes techniques doivent également suivre un processus de qualité afin de garantir la conformité des méthodes et des résultats. Ainsi, les laboratoires d'expertises devront appliquer les concepts de l'Assurance Qualité, que nous allons présenter dans

la section suivante. Dans l'introduction du mémoire, il est mentionné qu'une de mes démarches est de transposer des techniques présentes dans les laboratoires d'analyse de défaillance à la forensique numérique. Or ces laboratoires sont généralement positionnés dans les services d'assurance qualité en entreprise, ce qui représente un autre argument pour décrire cette activité.

Introduction à l'analyse de défaillance

L'assurance qualité

L'assurance qualité (AQ ou ASQ) ou en anglais "Quality Assurance" (QA) représente la mise en œuvre des processus permettant à un produit ou à un service de maintenir ses capacités pour un temps donné. L'assurance qualité est basée sur un système de gestion de la qualité (SGQ) visant à garantir que le produit concerné soit conforme et fiable pour son utilisateur final. Le système de gestion de la qualité est basé sur la norme ISO 9001 [97].

La notion d'assurance qualité est apparue durant le XXe siècle avec la démocratisation de l'industrie manufacturière. Dans les années 1920, la société Western Electric a donné l'impulsion initiale sur la qualité des productions de son usine de Hawthorne près de Chicago. Pour cela, l'entreprise décide de fonder en 1925 une filiale nommée Bell Telephone Laboratories [98], regroupant l'ensemble des laboratoires technologiques de l'entreprise mère. L'objectif est de centraliser les productions en une seule filiale capable d'alimenter les autres entreprises du groupe. La centralisation de la production couplée avec l'étude de celle-ci devait permettre de fiabiliser les processus de fabrication et de gagner en productivité. Pour mener à bien ce projet, les dirigeants de Western Electric décident de muter à la tête d'un laboratoire axé sur la qualité des produits, un employé de la maison mère qui est à la fois physicien et statisticien. Il s'agit de Walter A. Shewhart [99]. Pour mener à bien sa mission Walter A. Shewhart dispose d'un budget important. Le regroupement de la production en une filiale permet à son équipe d'avoir accès à un grand nombre d'échantillons de tests. L'équipe peut ainsi mener une étude complète sur la qualité des produits lors du cycle de production et déterminer une méthode de contrôle graphique basée sur des mesures de paramètres physiques. Dans les années 1950, cette méthode sera déclinée sous forme d'un livret de formation à destination des ouvriers et ingénieurs de l'entreprise Western Electric pour une application dans les usines du groupe. Le nom de ce livret maintenant mondialement connu est "Statistical Quality Control Handbook" [100].

Un autre personnage important de la création des concepts de l'assurance qualité est un physicien, mathématicien et statisticien du nom de William Edwards Deming. Son intérêt pour la qualité débuta durant ses études lorsque pendant deux étés il travailla dans l'entreprise Hawthorne. Par cette expérience, il eut l'occasion de découvrir les travaux de Shewhart sur la maîtrise de la qualité, connaissances qu'il complétera en 1930 grâce à des études sur la statistique à l'université de Londres. À l'issue de sa formation et en clôture de ses travaux de recherche avec Shewhart, William Edwards Deming [101] aura l'opportunité de donner des conférences pour faire connaître le management de la qualité aux industries dans le monde entier.

L'assurance qualité a pris de l'ampleur au fil des décennies en se démocratisant largement dans les entreprises pour couvrir les productions et les services mais aussi les principes à appliquer lors de la production. L'une des normes les plus connues a été créée en 1987 par l'organisation internationale de normalisation (ISO) [102]. Il s'agit de la norme ISO 9001 qui établit les principes et les exigences orientés clients, mais aussi la motivation et l'engagement de la direction pour définir les processus dans un but d'amélioration continue. Une entreprise peut donc décider de se faire certifier selon la norme ISO 9001, si elle respecte les principes qui la compose [103].

L'assurance qualité, telle qu'imaginée par Deming, repose sur plusieurs principes clés illustrée sur le roue de Deming en Figure 1 :

1. La planification : Il faut identifier des objectifs de qualité puis définir des critères d'acceptation pour permettre d'établir des plans et des processus garantissant la réussite des objectifs.
2. Le contrôle : L'entreprise doit mettre en œuvre des actions permettant de surveiller et d'évaluer la production ou la fourniture de services. Le but est de s'assurer que les normes de qualité préalablement établies soient respectées. Le contrôle peut prendre différentes formes comme des inspections de la chaîne de production, des tests de produits finis. Les personnels ne sont pas en reste car des audits peuvent être réalisés pour valider leurs bonnes connaissances de la démarche qualité de l'entreprise. En plus des différents contrôles internes, des audits externes peuvent être réalisés périodiquement par des organismes de certification indépendants afin de permettre à l'entreprise d'obtenir et de conserver la certification ISO 9001.
3. Amélioration continue : La démarche d'assurance qualité promeut l'amélioration continue des processus. Les problèmes identifiés lors d'audits internes ou externes, ainsi que les incidents rencontrés sont analysés pour en déterminer leurs causes. Cela permet d'établir un plan d'actions correctives et/ou préventives qui devra être mis en place afin d'éviter leurs récurrences.
4. Implication des acteurs : L'assurance qualité doit être suivie par l'ensemble des acteurs de la chaîne de production. Ainsi chaque employé de l'entreprise a son rôle à jouer pour établir, modifier, tester, valider et appliquer les processus. La responsabilité de l'application de l'assurance qualité ne se limite donc pas simplement aux dirigeants d'une entreprise, qui prennent des mesures, mais à tous les individus (ouvriers, cadres, prestataires ou sous-traitants) présents qui doivent les faire vivre.

Il est facile de déduire que rendre des produits fiables est une activité coûteuse pour l'entreprise, car cela nécessite la création d'emplois dédiés et la prise en compte de processus qui ralentissent la mise sur le marché de nouveaux produits, cependant le

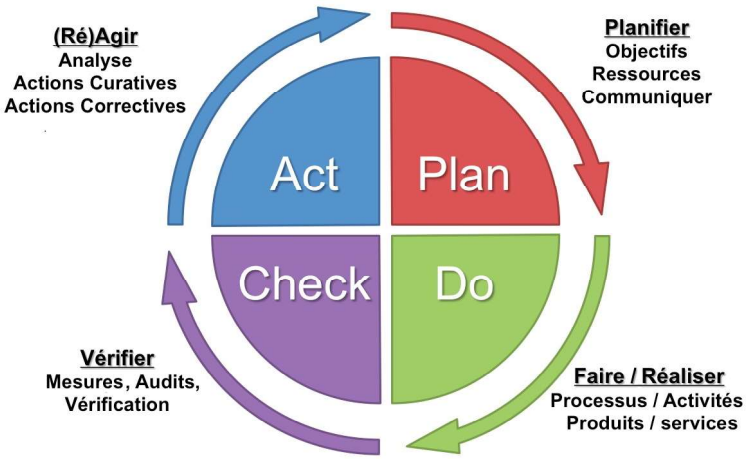


FIGURE 1 – Roue de Deming [1]

bénéfice en contre-partie est significatif. L'entreprise n'a pas à faire face à une obsolescence incontrôlée de ses produits engendrant des coûts importants de garantie. L'assurance qualité tient donc une place vitale dans la satisfaction des clients ce qui a un impact positif dans la réputation d'une entreprise.

Pour décliner le suivi de l'assurance qualité au quotidien, les grandes entreprises ont tendance à créer un service dédié permettant de gérer tous les aspects importants. Les entreprises évoluant dans le domaine de l'électronique et qui commercialisent des cartes ou des composants électroniques possèdent un service d'assurance qualité, ce qui leur permet de prétendre à des normes telle que ISO 9001. Dans ce service, il est possible de retrouver une équipe gérant la relation client, une équipe gérant les tests de fiabilités, une équipe de qualification et encore une équipe réalisant des analyses de défaillance.

Pour mieux appréhender le rôle de chaque équipe du service global de l'assurance qualité, nous allons prendre comme illustration une entreprise qui fabrique des systèmes électroniques à destination de clients professionnels. Une telle entreprise va acheter des composants à des fabricants ou à des fournisseurs indépendants, que l'on appelle des brokers. Elle va ensuite développer ses produits suivant des phases de prototypage, de tests, de validations en respectant les recommandations émises par le service de l'assurance qualité. Le but de celles-ci est d'assurer une traçabilité dans les différentes phases du développement pour identifier les défauts de procédés ou dans le produit pour les corriger à la racine. Pour valider que le prototype respecte les exigences du cahier des charges, il faut mettre en place des opérations permettant de tester les différents paramètres du système, puis les valider par rapport à des références.

L'entreprise disposera donc dans son service d'assurance qualité d'un laboratoire d'analyse de défaillance. Ce laboratoire dispose de nombreux équipements, qui seront développés plus loin dans la section *Équipements des laboratoires*, qui permettent d'effectuer des tests électriques ou mécaniques, des observations optiques, des observations

aux Rayons-X et infra-rouges et des mesures acoustiques. Les membres du laboratoire d'analyse de défaillance doivent procéder à une analyse poussée de la structure (Figure 2) de chacun des éléments du système indépendamment et collectivement. Ainsi, ils disposent aussi bien des composants à l'unité avant qu'ils soient implantés sur le prototype, que de systèmes totalement implantés. Pour chacun des éléments, ils doivent remplir un rapport qui respecte un template généraliste, préalablement défini dans l'assurance qualité, ce qui garantit une homogénéité des analyses et des rendus pour tous les rédacteurs. L'analyse de construction est inutile si elle n'est pas exploitée. Par conséquent, les concepteurs du système doivent en analyser les rapports pour corriger les éventuels défauts, ou sélectionner un autre composant dans le cas où une analyse de construction met en évidence une incompatibilité entre les paramètres du-dit composant avec le système.

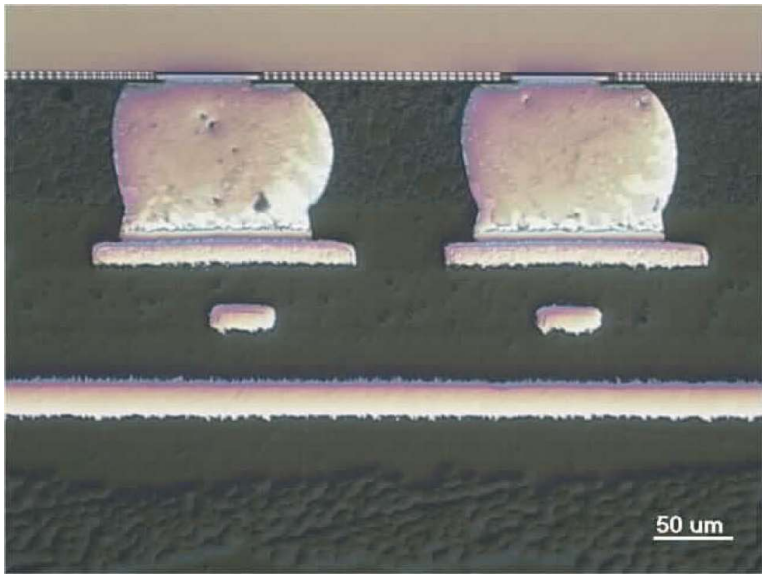


FIGURE 2 – Observation optique des couches dans les composants lors d'une analyse de construction [2]

Une fois la conception du système terminée, notre entreprise dispose d'un prototype prêt pour l'industrialisation et la mise sur le marché. Toutefois, avant de fabriquer le produit à grande échelle, un autre laboratoire du service d'ASQ tient un rôle important, il s'agit de la qualification. Comme son nom le laisse penser, la mission de ce laboratoire est de qualifier un nouveau produit. Cela signifie que ses personnels vont analyser le cahier des charges pour le synthétiser dans un document de travail (ou un logiciel). Ils vont faire de même avec les rapports d'analyse de construction de chacun des composants constituant le système. Il arrive également qu'ils mènent une analyse plus administrative sur les fabricants des composants en fonction du secteur d'activité cible, dans le but de confirmer les lignes d'approvisionnement des composants afin de trouver le fournisseur le plus fiable respectant par exemple des normes ISO. Une fois l'ensemble des résultats renseignés, les techniciens du laboratoire de la qualification vont devoir croiser les données

pour ressortir des informations telles que les sources potentielles de défaut (les composants les plus susceptibles d'être défaillants en premier) ou des estimations sur le vieillissement du système en suggérant des tests à effectuer. Un indicateur généralement utilisé pour schématiser la courbe de vie d'un composant ou système est appelé courbe en baignoire. Cette courbe a été introduite entre les années 1950 et 1960 et même s'il n'est pas possible de définir une paternité précise, elle peut être attribuée à trois personnalités de l'ingénierie :

— Elmer E Lewis : est un chercheur reconnu dans le domaine de la fiabilité et de la théorie des systèmes. Il a travaillé à la NASA (National Aeronautics and Space Administration) en tant qu'ingénieur de recherche et a apporté d'importantes contributions dans la fiabilisation des systèmes spatiaux. Il a participé au développement de méthodes pour évaluer et améliorer la fiabilité des systèmes par de la statistique et il a publié de nombreux articles et livres dont "Introduction to reliability engineering" édité pour la première fois en 1987 [104].

— Herman O. Hartley : est un statisticien et mathématicien particulièrement connu pour avoir créé le département de statistiques de l'université du Texas. Il a reçu de nombreuses récompenses pour ses travaux. Il a enseigné dans plusieurs universités américaines et anglaises.

— Richard E. Barlow : a coécrit avec Frank Proschan le livre "Mathematical Theory of Reliability" [105] en 1970, qui est un ouvrage de référence dans le domaine de la fiabilité pour ses fondements théoriques de la fiabilité des systèmes. Après sa formation en mathématiques finalisée par un doctorat à l'université de Stanford, il a été professeur à l'université de Berkeley et conseiller scientifique pour les laboratoires Boeing.

La courbe en baignoire (représentée en Figure 3) est développée dans plusieurs ouvrages [106, 107]. Elle a pour but de schématiser simplement la probabilité qu'un élément soit en défaut en fonction de la vie de l'ensemble des éléments. Elle est composée de trois phases qui s'appellent période de jeunesse, période utile et période de fin de vie. Une étude préalable permet de déterminer pour un produit donné la vie globale voulue. On s'attend, par exemple, qu'un produit électroménager ait une durée de vie de 10 ans donc une entrée dans la période de fin de vie à 10 ans. À ce moment-là les statistiques montrent que le produit peut très rapidement perdre ses caractéristiques. Une autre date importante est la fin de période de jeunesse. Il s'agit de la période pour laquelle un système connaît des défauts de fabrication entraînant un vieillissement trop précoce. Normalement la fin de la période de jeunesse correspond à la fin de la garantie des produits, ce qui implique qu'il n'est donc pas utile de souscrire aux extensions de garantie des équipements électroménager car à la fin de la garantie classique, le produit est entré dans la période utile.

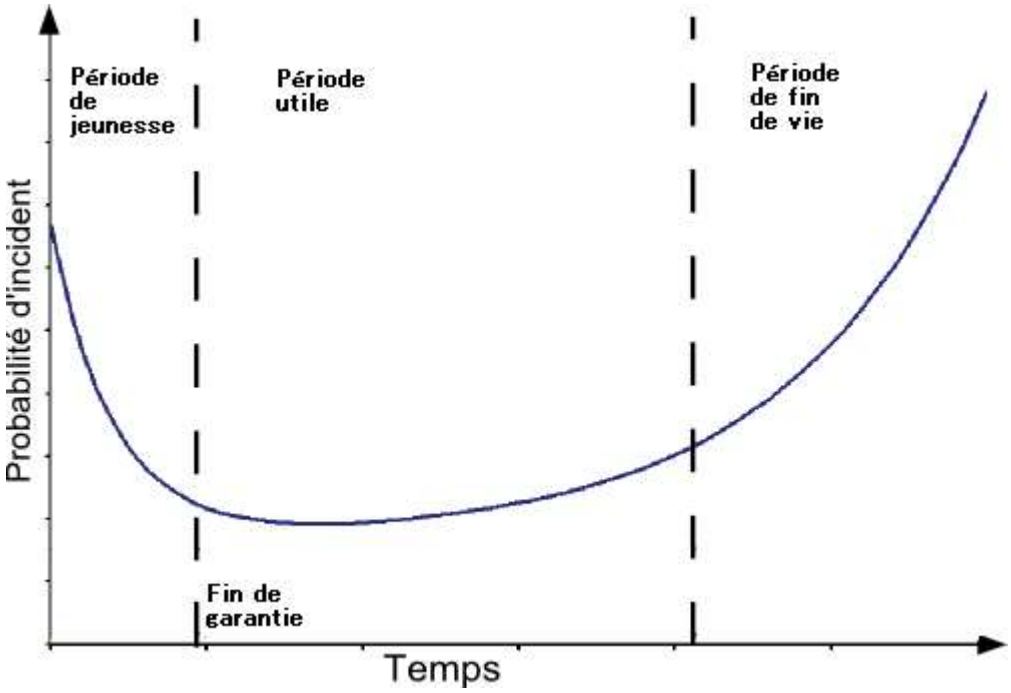


FIGURE 3 – Exemple de courbe en baignoire théorique

Revenons à l'entreprise de notre exemple. Elle a conçu un nouveau système avec succès et est prête à le commercialiser. Toutefois, elle possède un nouveau laboratoire du service d'assurance qualité qui entre en jeu, pour la fiabilité. Durant l'étape de conception et avant la mise sur le marché, l'équipe de la qualification a fait une analyse des risques sur le nouveau produit et elle a émis des réserves quant au vieillissement de celui-ci. L'équipe de la fiabilité a pour mission de lever ces réserves, au travers des tests qui vont être réalisés par prélèvement d'échantillons en sortie de la chaîne de production. Ce prélèvement s'effectue sous forme d'un lot avec un nombre significatif de systèmes, pouvant atteindre la centaine dans le cas de composants simples. Plusieurs lots vont être formés car chaque lot est destiné à une unique campagne de tests de vieillissement faisant varier les paramètres de température, d'humidité et de temps d'exposition. Pour réaliser ces opérations, des équipements spécifiques sont utilisés, comme des étuves (Figure 4a) ou des analyseurs paramétriques (Figure 4b). Une campagne de tests typiques pour un lot peut être :

1. Test électrique initial pour valider que les paramètres électriques typiques de l'ensemble du lot sont conformes aux spécifications.
2. Étuvage du lot permettant d'accélérer le vieillissement naturel du composant en respectant des abaques de température pour simuler la fin de la période de jeunesse.
3. Test électrique de fin de jeunesse permettant de compter le nombre de composants non fonctionnels et d'identifier également ceux qui entament une dérive de leurs caractéristiques électriques, même s'ils sont encore dans la plage de tolérance.

4. Étuvage du lot permettant d'accélérer le vieillissement de la fin de la période de jeunesse dans la phase de période utile.
5. Test électrique de période utile permettant de mettre à jour le décompte de composants non fonctionnels ou en cours de dérive de caractéristiques.
6. Répétition de la phase d'étuvage puis de tests électriques pour déterminer en fonction des chiffres la fin de la période utile et la chute dans la période de fin de vie.

Cet exemple de campagne ne prend en paramètre de vieillissement que la température, mais d'autres campagnes sont généralement menées en parallèle sur d'autres lots faisant changer la température et l'humidité. Pour l'ensemble des tests, des échantillons peuvent être prélevés pour les différents lots et envoyés dans le laboratoire qui réalise des analyses de défaillance. La nature des analyses sera décrite plus précisément dans la suite de cette section, mais il faut retenir que le laboratoire a pour but d'effectuer des tests physiques et des préparations pour identifier la nature d'un défaut et tenter de remonter à ses causes.

(a) Étuve de vieillissement de composants [108]

(b) Analyseur paramétrique de composants électroniques de la marque Keithley [109]

FIGURE 4 – Exemples d'équipements servant à la qualification des composants électroniques dans un laboratoire de fiabilité

La dernière équipe qui composera le service d'assurance qualité aura la charge de la relation client. Une fois les phases de développement et les tests associés validés avec succès, le produit est mis sur le marché avec une estimation d'une durée de vie et d'une durée de garantie. Il est vendu avec succès à des entreprises ou des particuliers qui commencent à l'utiliser dans leurs applications, cependant ils peuvent rencontrer des difficultés sur l'utilisation des produits. Pour pallier ces difficultés, l'entreprise dispose d'une équipe chargée de prendre en compte les différentes demandes pour les étudier et essayer d'apporter un appui aux clients. L'équipe réalise la prise de contacte initiale, le

dispatching de la demande en fonction de la nature de la question (question technique, question de capacité du produit, question commerciale, analyse de défaillance), le suivi de traitement de la demande, puis centralise les résultats pour produire la réponse finale au client.

L'ensemble de ces activités qui compose le service de l'assurance qualité permet à l'entreprise de rassurer les clients, ce qui a pour effet de les fidéliser. Les missions du service d'assurance qualité ne s'arrêtent pas uniquement aux laboratoires de fiabilité, de qualification, d'analyses de défaillance et à l'équipe relation client, il doit aussi concevoir, distribuer et contrôler les fiches et méthodes permettant à l'ensemble des employés de connaître les processus de la qualité de l'entreprise.

Dans la description du service d'ASQ d'une entreprise, nous avons introduit le laboratoire d'analyse de défaillance. Il a été introduit en présentation de l'introduction, qu'un des objectifs de mes travaux est d'apporter certaines techniques de l'analyse de défaillance dans le domaine de la forensique numériques. Nous allons maintenant entrer plus en détail sur les rôles de celui-ci, car le laboratoire dispose de plusieurs compétences intervenant dans les différents stades de la vie du produit. Ainsi il réalise :

— Les analyses de construction (ou technologiques) qui consistent à déstratifier un composant ou un système, à prendre les mesures et caractériser les paramètres physiques de celui-ci. Cela permet de comparer le produit par rapport à des données théoriques. Lors de la conception d'un composant ou d'un système cela permet de valider que la fabrication est conforme au cahier des charges, ou de rectifier la chaîne de production.

— Les analyses de défaillance dites "process" qui consistent à étudier les composants ou systèmes rencontrant des défauts lors de la phase de fiabilisation. Comme évoqué précédemment un nombre d'échantillons par lot est prélevé puis apporté au laboratoire pour que celui-ci le rétro-concoive suivant une méthodologie précise, que nous développerons dans le paragraphe page 39. Le but de l'analyse est de décomposer progressivement le composant pour rechercher un défaut visuel ou électrique. Une fois ce défaut identifié, le technicien doit comprendre la nature du défaut et ses implications, ce qui permet dans certains cas de comprendre la "root cause" (cause initiale) du défaut.

— Les analyses de défaillance dites "client" qui reprennent les mêmes concepts que pour celles dites "process". La différence tient principalement dans la qualité du rendu car il ne sera plus destiné à une diffusion interne mais sera diffusé en externe, entraînant une implication pour l'entreprise qui s'engagera sur la conclusion apportée.

L'analyse de défaillance

L'analyse de défaillance, dont nous donnerons un exemple de processus utilisé pour effectuer une analyse, est une approche qui a pour objectif d'améliorer la fiabilité des systèmes en tentant d'identifier les sources de défaillance. Elle joue donc un rôle essentiel dans la gestion des risques et de l'assurance qualité pour les entreprises.

L'analyse de défaillance est également un concept qui a émergé au milieu du XXe siècle, en parallèle avec le développement de l'assurance qualité. L'activité est très liée à l'industrie et à l'ingénierie avec comme leader les industries aérospatiales et la production de matériel militaire. L'objectif principal est la compréhension des mécanismes de défaillance pour en identifier les causes et par conséquent pour améliorer la fiabilité des systèmes et des produits. De nos jours, l'analyse de défaillance est une discipline largement répandue dans divers domaines industriels, tels que l'aérospatiale, l'automobile, l'énergie, les télécommunications, la fabrication ou la santé. L'activité est en constante évolution avec de nouvelles méthodes et approches qui continuent à émerger avec la démocratisation de nouveaux équipements permettant d'aller plus loin quant aux tests réalisables. Pour aborder les différents aspects des nouvelles techniques, plusieurs conférences sont organisées. Parmi les conférences notables de ce domaine, nous pouvons identifier :

— L'ANADEF [110] est une association scientifique qui a pour but de réunir les techniciens des laboratoires français afin de leur permettre de travailler ensemble sur des thématiques de recherche commune. Créée en 2001 par plusieurs laboratoires, l'association anime annuellement des groupes de travail sur différents sujets qui se concrétisent par des échanges dans une conférence annuelle. À l'heure actuelle, plus de 40 sociétés sont adhérentes à l'association.

— L'European Symposium on Reliability of Electron Devices, Failure Physics and Analysis (ESREF) [111] est une conférence dont l'organisation change chaque année parmi les universités et entreprises partenaires. L'objectif de la conférence est de présenter les avancées avec les acteurs européens du domaine pour des présentations, des posters, des workshops et un salon de revendeurs d'équipements. En 2023, la 34eme édition s'est tenue en France en partenariat entre l'université de Bordeaux et le CNES.

— L'International Symposium for Testing and Failure Analysis (ISTFA) [112] est une conférence créée par l'ASM international, qui est une société spécialisée dans le semi-conducteur et qui a pour but de regrouper la majeure partie des experts internationaux de l'analyse de défaillance. Cette conférence, qui en 2024 connaîtra sa 50ème édition, se présente comme l'ESREF, par un partage sous différentes formes (présentations, posters, workshops et salon de revendeurs d'équipements).

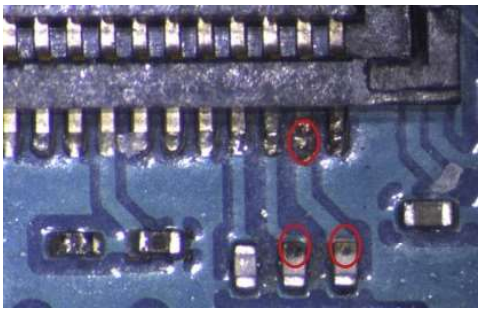
Les différentes conférences permettent aux experts des laboratoires de mettre en commun des techniques et des recherches malgré la compétition entre les entreprises. Grâce à ces échanges, un certain nombre d'ouvrages ont été publiés dont celui qui est considéré comme la référence dans la majeure partie des laboratoires d'électronique. Il s'agit d'un recueil d'articles de conférences publié en 2004 par l'ASM international, sous le nom "Microelectronics failure analysis Desk Reference fifth edition" [113].

En concaténant différentes sources dont le livre référence mentionné précédemment, et sans s'attacher à une liste précise de matériels, il est possible de décliner un protocole d'analyse de base :

1. Observation optique à la binoculaire (Figure 5) pour rechercher les défauts dans le package des composants ou sur la carte électronique. Les défauts les plus courants peuvent être une broche arrachée sur un composant, les effets de la délamination provoquant des décollements du package (Figure 6a), une piste coupée sur la carte électronique (Figure 6b), une fissure dans un package de composant qui aurait une propagation sur la puce en silicium.

FIGURE 5 – Exemple du système d'observation optique Lynx EVO [3]

(a) Défaut suite à une délamination : formation d'une bulle dans la résine [114]



(b) Corrosion d'un connecteur de téléphone provoquant une coupure de la connexion électrique [115]

FIGURE 6 – Exemples de défauts pouvant être observés sur les composants électroniques par des moyens optiques

2. Observation aux Rayons-X (Figure 7) pour figer l'état observable de l'intérieur du composant. Sans confirmation du défaut ou de sa nature, il est peu probable d'identifier un défaut avec une simple vue 2D voir 3D aux rayons-X, d'autant plus que sur une carte électronique les sources de défauts peuvent être multiples. L'idée de faire une acquisition à cette étape tient plus à figer la situation pour une recherche postérieure. En effet, il s'agit du début de l'analyse et aucune action pouvant aggraver ou créer un nouveau défaut n'a encore été effectuée. Cela ne sera potentiellement plus le cas lorsque le composant ou système aura été mis une première fois sous tension, et à ce moment-là, il sera possible de revenir à cette première vue aux Rayons-X, pour observer une zone précise.

FIGURE 7 – Machine de visualisation en deux dimensions et de reconstruction en trois dimensions par Rayons-X [4]

3. Analyse de la documentation pour trouver les informations des paramètres électriques pouvant être testés. Pour les cartes électroniques, le but sera de rechercher les ports de debug ou les points de tests permettant de tester les

tensions ou les communications. Pour un composant, il faudra regarder les valeurs nominales, minimales et maximales de certains paramètres pour les confirmer. Cette étape se fait en prenant en compte les remarques du client qui aura indiqué les caractéristiques qu'il dénonce.

4. Validation du défaut par des tests électriques conformément aux recherches documentaires faites précédemment. À ce stade, l'analyse peut s'arrêter si le défaut mentionné par le client n'est pas confirmé ou que l'ensemble des spécifications sont conformes.
5. Retour sur les vues optiques et Rayons-X. La confirmation du défaut électrique a permis d'identifier une localisation (un composant ou une ligne d'alimentation précise sur un système, une broche de composant précise), et permet donc de se focaliser plus précisément sur les vues optiques et Rayons-X.
6. Analyse structurelle du composant ou du système. Dans le cas d'un système, le but va être de suivre le signal en défaut puis de dessouder et tester individuellement chacun des composants présents sur la ligne concernée. Lorsque le composant défectueux est identifié, l'analyse se transforme en une analyse classique d'un composant, à savoir depackager la puce de silicium pour observer les empilements technologiques (puce en silicium, frame, bondings, ...) (Figure 8).

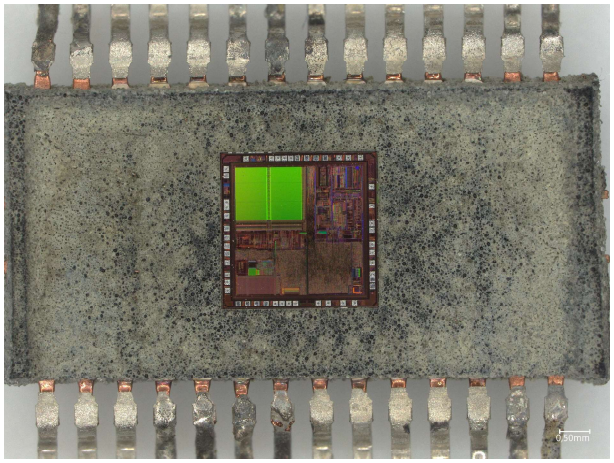


FIGURE 8 – Vue optique d'un composant PIC après décapsulation chimique [5]

Les défauts qui peuvent être identifiés facilement sont :

— des corrosions au niveau des pistes ou des pads des composants (Figure 9) provoquant une migration du cuivre des pistes et donc une discontinuité des signaux électriques. Cette délamination peut être identifiée avec un scanner acoustique à balayage (SAM) et provient généralement d'un vieillissement accéléré du composant à cause d'un stress thermique associé à de l'humidité.

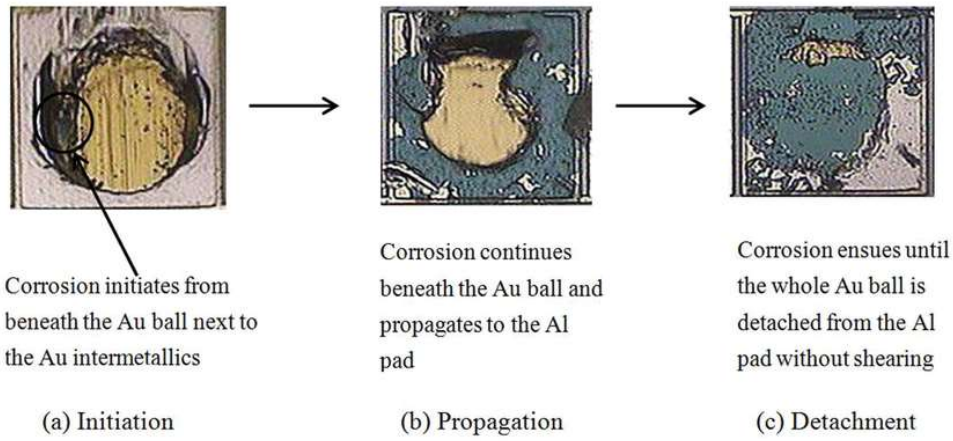


FIGURE 9 – Différentes étapes de corrosion sur un pad de composant en Aluminium provoquant un décollement du fil associé et une coupure de la continuité électrique [6]

— des micro-fusions dans la puce en silicium provenant de surcharges de courant lors d'un fonctionnement. Ces micro-fusions forment des ponts entre les différentes couches du composant provoquant des courts-circuits, rendant le composant partiellement ou totalement non fonctionnel. Elles peuvent être repérées en utilisant des équipements d'imagerie thermique ou de luminescence à l'échelle micrométrique.

— des fissures au niveau de la puce (Figure 10) provoquant des coupures dans les pistes voir des décollement des niveaux métalliques du composant. Ces fissures peuvent provenir d'un stress mécanique lié à des contraintes extérieures ou une mauvaise dissipation de la chaleur du composant en fonctionnement créant des déformations excessives. La recherche peut être faite par des techniques d'observation à base de laser ou d'électrons pour analyser les dissipations dans la structure du composant et ainsi exposer une anomalie dans cette dissipation.

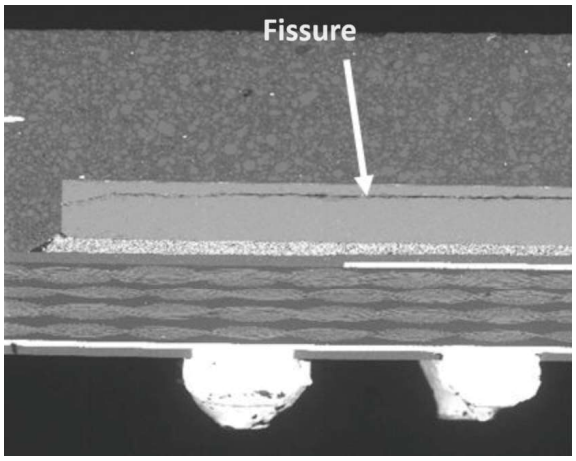


FIGURE 10 – Observation d'une fissure dans le substrat en silicium d'une puce au microscope électronique à balayage [7]

7. Si le défaut est localisé, le but de l'analyse sera de rechercher les causes probables et d'émettre des hypothèses permettant d'aider le demandeur. Ainsi, l'exemple d'un excès de courant sur un composant sera remonté au client en avançant l'hypothèse que son application consomme plus que prévue et donc que le composant est mal dimensionné. Cependant, une seconde hypothèse peut être que le système du client subit des pics imprévus de courant qui demanderaient simplement à être étudiés puis lissés. Cette phase se fait donc en trinôme entre le technicien qui a réalisé l'analyse, le conseiller en relation client de l'entreprise et le technicien du client.

Comme nous l'indiquions en préambule de cette méthodologie, nous ne nous attachons pas pour le moment à des équipements particuliers et nous n'avons exposé que les possibilités. Les équipements disponibles dans les laboratoires ainsi que leurs fonctionnements seront détaillés dans la section *Équipements des laboratoires*.

Dans la première section, nous avons présenté la forensique numérique en concluant que l'activité avait besoin d'un cadre pour garantir la bonne tenue des expertises. Ce besoin est grandement comblé par l'assurance qualité qui fournit, avec entre autres la norme ISO9001, un guide des bonnes pratiques et de la bonne tenue du laboratoire. La norme aide également pour le formalisme dans la rédaction de process et des documents liés à l'expertise. Un manager de laboratoire d'expertise provenant d'un laboratoire d'analyse de défaillance pourra apporter une plus-value en déclinant des pratiques comme le test régulier des équipements, le rangement mensuel du laboratoire suivi d'un audit interne ou encore la tenue des indicateurs de réussite ou d'échec permettant une constante amélioration. En plus de management du laboratoire, un analyste de défaillance apportera avec lui des connaissances et des équipements rarement utilisés au quotidien dans les expertises et qui seront réellement utile au traitement de supports fortement endommagés. En complément de connaissances sur l'analyse de défaillance, il peut être intéressant que la forensique numérique soit complétée par l'étude fonctionnelle de systèmes peu ou pas documentées. Cette activité qui sera déclinée dans la section suivante s'appelle la rétro-conception matérielle.

Introduction sur la rétro-conception matérielle

La rétro-ingénierie, ou ingénierie inverse ou inversée, est l'activité qui consiste à étudier un objet pour en déterminer le fonctionnement interne, la méthode de fabrication et elle peut-être réalisée dans l'intérêt de le modifier [116]. Dans la culture scientifique ou industrielle, le terme de rétro-ingénierie ou de rétro-conception est souvent connoté négativement. Pour une société, il est associé à une action malveillante qui consiste à étudier les secrets des produits concurrents. Le parallèle pour les particuliers consiste en l'étude des sécurités d'un produit pour les contourner et ainsi s'affranchir de licences. L'exemple le plus marquant en France est le piratage des chaînes de télévision payante dont Canal+ à la fin des années 1990. Lors des conférences HARDWARE.IO en 2015 [117] et HARRIS en 2023, le CEO de la société Texplained a présenté l'activité de la rétro-conception matérielle en introduisant son propos par le fonctionnement du système des années 1990-2000 de Canal+ suivi de l'historique des piratages.

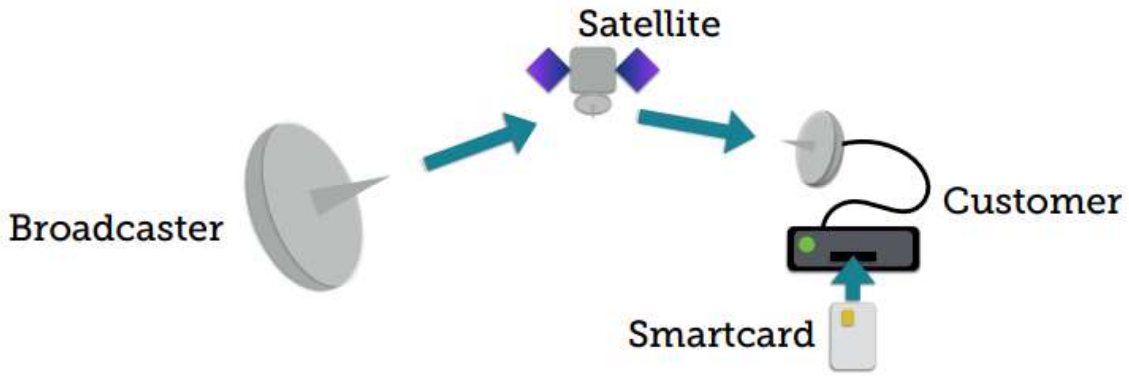


FIGURE 11 – Schéma de la transmission du contenu de la chaîne émettrice jusqu'à la télévision du client

La Figure 11 décrit le fonctionnement des chaînes de télévision payante par satellite. Le diffuseur découpe les images et le son en plusieurs trames qui sont émises par une antenne jusqu'au satellite qui a la charge d'acheminer ses trames jusqu'à l'antenne du client. Le client, chez lui, possède un récepteur qui concatène les trames reçues pour les ré-acheminer vers la télévision. À la différence des chaînes gratuites, les chaînes payantes ajoutent une sécurisation dans les trames émises. Les utilisateurs ne disposant pas de la clé de sécurité, ne peuvent pas réaligner correctement les trames et par conséquent la télévision reçoit une image brouillée. La première solution retenue par Canal+ pour la sécurisation consistait à mettre une clé dans une carte à puce. Le client ne disposant que du décodeur sans la carte à puce ne pouvait pas déchiffrer les trames. Cependant, certaines personnes ayant des connaissances en rétro-conception matérielle ont travaillé sur le système et ont réussi à localiser l'emplacement du stockage de la clé. Ils l'ont ensuite revendue, permettant à des particuliers de regarder Canal+ sans l'abonnement. Lorsque la société s'est rendue

compte de cette attaque, elle a décidé de complexifier le système en changeant la clé mais cela n'a eu que peu d'effet. La première génération de décodeurs étant devenue trop vulnérable, la société Canal+ a décidé de les changer pour adapter le niveau de sécurité. Ainsi dans la génération suivante de décodeurs, un algorithme de permutation des trames a été ajouté matériellement. Toutefois, le système n'a pas résisté à l'efficacité des attaquants. C'est ainsi que Canal+ a basculé sur des sécurisations logicielles pouvant être plus facilement mises à jour à distance et ne nécessitant pas le changement du parc des décodeurs. L'enseignement à tirer de cet exemple est la doctrine des reversers hardware, qu'Olivier Thomas a d'ailleurs rappelé lors de son intervention à HARRIS 2023, **En reverse hardware, la question n'est pas, "est-ce qu'on arrivera à attaquer le système" mais "en combien de temps et à quel prix ?"**.

Toutefois, la rétro-conception ne présente pas que des approches négatives. Dans l'industrie, les fabricants ont recours à cette technique sur leurs propres produits pour valider leur fiabilité et leur sécurité. Nous avons eu l'occasion de l'aborder dans la partie *Introduction à l'analyse de défaillance*, les laboratoires d'analyse de défaillance réalisent fréquemment des préparations de leurs propres échantillons pour valider la bonne application de la chaîne de production, afin d'adapter leurs process. Les techniciens ont donc recours à des équipements et manipulations similaires aux attaquants externes, mais avec un avantage certain, car ils connaissent avec exactitude la composition et les dimensions de différents éléments qu'ils vont rencontrer. Il existe pourtant un contexte à mi-chemin entre l'évaluation industrielle de ses propres produits et l'attaque des produits inconnus. Il s'agit des attaques de sécurité réalisées dans le cadre d'audit. Pour les composants électroniques, l'évaluation de sécurité est une activité confiée à un organisme indépendant spécialisé portant le nom de Centre d'Évaluation de la Sécurité des Technologies de l'Information (CESTI). L'activité des CESTI est rigoureusement réglementée et encadrée par un organisme d'État appelé l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) [84]. Nous avons présenté l'ANSSI comme l'agence en charge de la prévention, de forensique numérique en cas d'incident dans les entreprises, ainsi que de la défense des intérêts de l'état dans le cyber. Un des axes majeurs pour la sécurisation des intérêts de la France passe par la garantie que les composants mis sur le marché pour des applications sécurisées soient réellement difficiles à attaquer. En effet, il est important que les composants réalisant des opérations sensibles tels que les puces de cartes bancaires ou les puces de chiffrement des téléphones ou ordinateurs, soient testées et validées contre les attaques, allant des plus classiques aux plus évoluées. Pour échelonner la classification des produits, l'ANSSI applique la certification, conformément au décret 2002-535 [118], utilisant la méthode de critères communs. Les critères communs sont des normes dont une version a été normalisée par l'ISO sous la norme ISO15408 permettant d'évaluer objectivement la sécurité des systèmes et logiciels informatiques. La

méthode est décrite sur le site [119] et appliquée par plusieurs pays, donnant une envergure internationale et une homogénéisation des évaluations. En France, l'ANSSI décline donc les Critères Communs sous la forme de règles à suivre pour l'évaluation, accessibles sur son site internet [120]. Cependant, même si l'ANSSI a la charge de donner la certification, ce n'est pas l'agence qui réalise les évaluations des systèmes ou logiciels. Pour cette tâche, l'ANSSI se repose sur des laboratoires privés (CESTI) au nombre de cinq en France, deux à compétences logicielles et trois à compétences matérielles. Les entreprises souhaitant faire certifier un produit, doivent donc prendre l'attache d'un des CESTI pour effectuer l'évaluation technique et de l'ANSSI pour l'étude du dossier d'habilitation et son éventuelle acceptation. L'évaluation d'un produit par un CESTI n'est pas gratuite, ainsi pour chaque nouvelle demande l'entreprise requérante doit fournir en plus d'une rémunération à la hauteur du travail à effectuer, un nombre d'échantillons significatif et les documentations techniques utiles à l'évaluation. Une fois le contrat signé entre les deux parties, le CESTI devra effectuer l'étude la plus poussée possible dans le temps imparti et avec les ressources fournies. La note finale du produit représentera donc, en quelque sorte, le niveau attendu pour qu'un attaquant face au produit puisse réaliser des attaques, en fonction des éléments dont il dispose en amont.

Lors d'une évaluation, différents paramètres auront une influence sur le résultat final :

— La facilité d'accès à la documentation technique ou au code source. Cela permet à un attaquant d'avoir plus ou moins de facilité pour identifier les attaques possibles et comment les réaliser. Pour catégoriser l'accès à la donnée, on la représente sous forme de couleur. Pour un accès total à la donnée on dit que l'on travaille en boîte blanche, pour un accès partiel (juste un firmware d'update disponible ou auto-interdiction d'accès à certaines ressources) c'est une boîte grise et pour une attaque totalement à l'aveugle c'est une boîte noire.

— Le niveau de l'attaquant qui est attendu entre novice, senior ou expert du domaine. Le niveau de compétences de la personne aura un impact sur la capacité de trouver ou d'imaginer des scenarii d'attaques, puis de les mener à bien. Le niveau de l'attaquant est également représentatif de l'adversaire contre qui on veut se défendre entre le simple amateur dans sa maison jusqu'aux niveaux étatiques pouvant détenir des moyens démesurés.

— La nature du matériel utilisé aura un impact sur les performances de l'attaquant. Cet aspect a été abordé en corrélation avec le niveau de l'attaquant, où un amateur aura moins de capacités matérielles et surtout beaucoup moins d'équipements coûteux. Les attaques de base, manipulant les courants des systèmes ne nécessitant pas un équipement onéreux, seront plus fréquentes que l'étude et la modification de design recourant des matériels de laboratoire valant plusieurs millions d'euros.

— Le temps nécessaire à l'attaque qui est toujours chiffré au niveau d'une évaluation

doit être estimé et représentatif de la durée de vie du produit. Un produit de sécurité dispose d'une durée de vie sur le marché avant d'être dépassé technologiquement. Par exemple, le taux de renouvellement d'un composant sécurisé d'une carte bancaire, dont la durée est limitée à 3 ans sera moins critique qu'un composant utilisé pour sécuriser des communications pour une entreprise. En effet, des équipements en flotte d'entreprise seront un investissement très onéreux pour l'entreprise qui comptera sur cette solution pendant une longue période, peut-être 10 ans. Comme le produit est fabriqué et utilisé sur une longue période, la rentabilité d'effectuer une recherche longue dessus offrira plus de temps d'exploitation des résultats. À l'inverse, une puce de carte bancaire qui est naturellement amenée à être remplacée au bout de 3 ans, laissera une fenêtre de recherche plus courte. D'ailleurs, si l'attaque est trop longue, lorsque l'attaquant aura trouvé une faille, le produit sera proche de l'obsolescence.

— La reproductibilité de l'attaque représente la capacité pour un attaquant de jouer le même scénario à plusieurs reprises avec le même résultat. Lorsqu'un attaquant imagine et teste un scénario sur un système, celui-ci peut connaître un succès inattendu. La création du scénario consiste à imaginer une réaction du système qui va découler d'une suite de mise en difficulté de celui-ci. Pour l'attaquant, cela revient à imaginer une série d'actions pour estimer une réaction. Souvent la réaction du système n'est pas celle attendue et donc l'attaque échoue. Parfois le système réagit et l'attaquant doit en comprendre le comportement. S'il y parvient, l'attaquant doit en déduire si son attaque est exploitable mais également si son attaque est reproductible. Sachant que les tests sont généralement réalisés sur des échantillons témoins, la reproductibilité de l'attaque sera un facteur important lors du basculement sur la cible réelle.

Lors des évaluations de sécurité faites par les CESTI les techniques à base de glitch de courant ou tension (Figure 12), les attaques électromagnétiques (Figure 13a) ou les attaques laser (Figure 13b) sont fréquemment utilisées car leur temps de mise en œuvre est plus compatible avec les exigences de la certification du produit. Cependant, pour certains équipements très sensibles, les CESTI peuvent avoir recours à la rétro-conception. Ils doivent donc rester au fait des évolutions des techniques pour tendre vers l'état de l'art dans l'ensemble des domaines. L'ANSSI jouera d'ailleurs un rôle de contrôle au travers des audits annuels de l'ensemble des CESTI pour valider la continuité dans le niveau des prestations fournies.

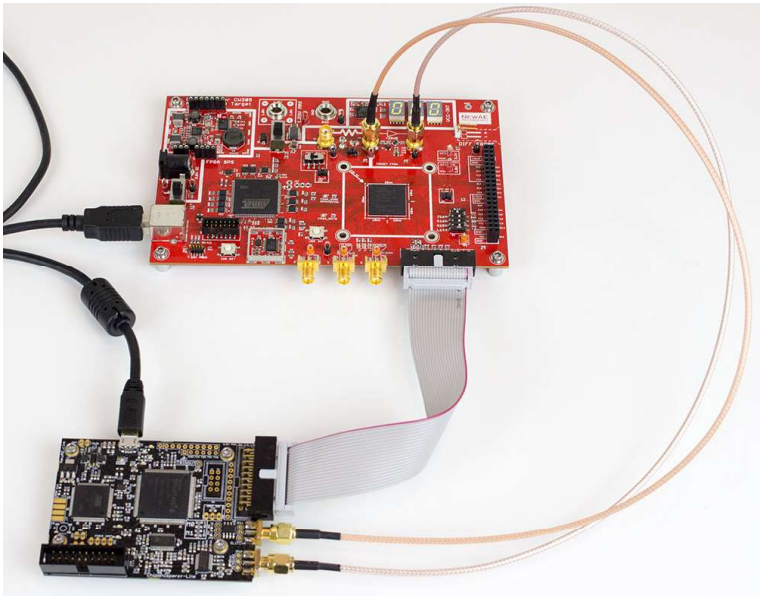
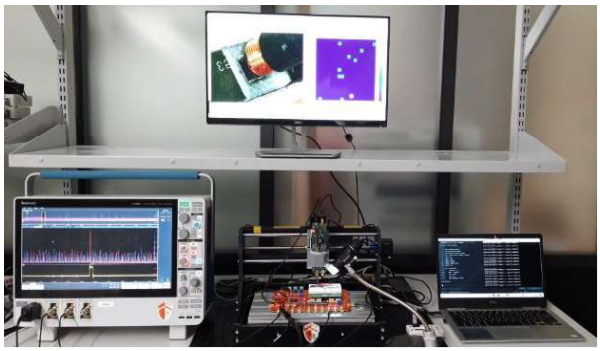
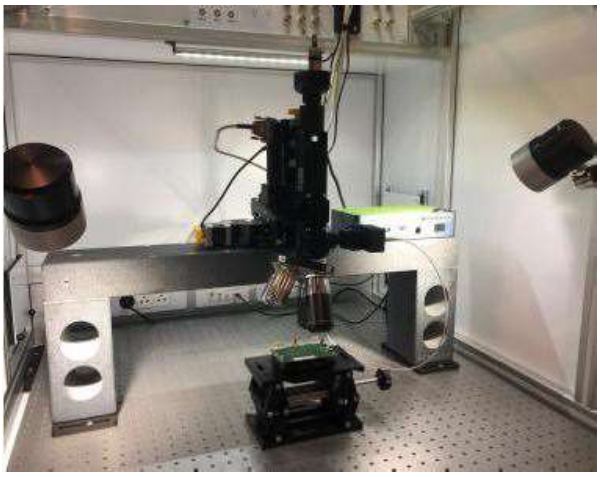


FIGURE 12 – Setup d'un glitch avec la carte ChipWhisperer permettant d'induire une faute dans le fonctionnement d'un composant en jouant sur la tension d'alimentation [8]



(a) Banc d'émission électromagnétique [121]



(b) Banc d'attaque laser [122]

FIGURE 13 – Setup d'un banc d'attaque laser et électromagnétique permettant d'injecter une faute lors de l'exécution d'instructions d'un composant

Un dernier acteur identifiable dans le domaine de la rétro-conception se situe au niveau des laboratoires forensiques. Qu'ils appartiennent à l'État comme la gendarmerie, la police ou qu'ils soient privés, ces laboratoires ne disposent que très rarement d'informations provenant des fabricants. Or, il est fréquent que les supports numériques provenant d'un scellé soient endommagés. Ainsi, l'expert forensique en charge du scellé doit mettre en œuvre tous les outils à disposition pour localiser le défaut et le corriger ou le contourner. Pour cela, il doit comprendre les fonctionnalités du support numérique en utilisant des techniques de rétro-ingénierie.

Une autre part importante de l'activité d'un expert consiste au déchiffrement de la donnée extraite d'un support. Au début des années 2010, pour effectuer une extraction des données utilisateurs d'un téléphone portable, il suffisait de relire la mémoire de celui-ci. Pour cela, il y avait deux solutions qui consistaient, soit à s'interconnecter sur des endroits distincts de la carte électronique, soit à retirer la mémoire. Dans les deux cas, le composant était lu avec un lecteur du commerce. Il existait d'ailleurs une multitude de lecteurs compatibles vendus pour cette activité. En 2013, la marque Apple a complexifié l'activité en introduisant le chiffrement de la mémoire, donc de la donnée utilisateur. Ainsi pour accéder aux photos ou messages de l'utilisateur, il ne suffisait plus de lire le contenu de la mémoire, qui apparaissait chiffré, il fallait également trouver l'algorithme permettant de le chiffrer, ainsi que la clé de chiffrement. Même si l'algorithme ne changeait pas d'un téléphone Apple à l'autre, la clé était unique à chaque appareil. L'extraction de données sur smartphone a donc évolué nécessitant un terminal fonctionnel et déverrouillé pour être exploité. Il s'agissait d'un chiffrement dit FDE (Full Disk Encrypted) car l'ensemble du "disque", c'est-à-dire la mémoire, était chiffré et déchiffré en une fois. Cela signifiait que pour un attaquant, connaître l'algorithme et trouver la clé permettait d'accéder à l'ensemble des données. Le chiffrement FDE a également été retrouvé sur les téléphones Android dès la version 6, avant une évolution avec Android 7 vers le mode FBE (File Base Encryption). Le FBE ne signifie plus un chiffrement complet de la mémoire en une fois, mais que chaque fichier est chiffré indépendamment (Figure 14). La clé d'origine n'est pas directement utilisée et pour chaque fichier c'est une clé dérivé différente qui est utilisée. Ainsi, pour un expert, connaître la clé d'origine ne permet pas de récupérer l'ensemble des données de la mémoire. Il va devoir également rétro-concevoir l'ensemble des algorithmes de dérivation utilisés pour chaque fichier pour en faire le déchiffrement. Cela apportera une complexification importante du niveau attendu de l'attaque.

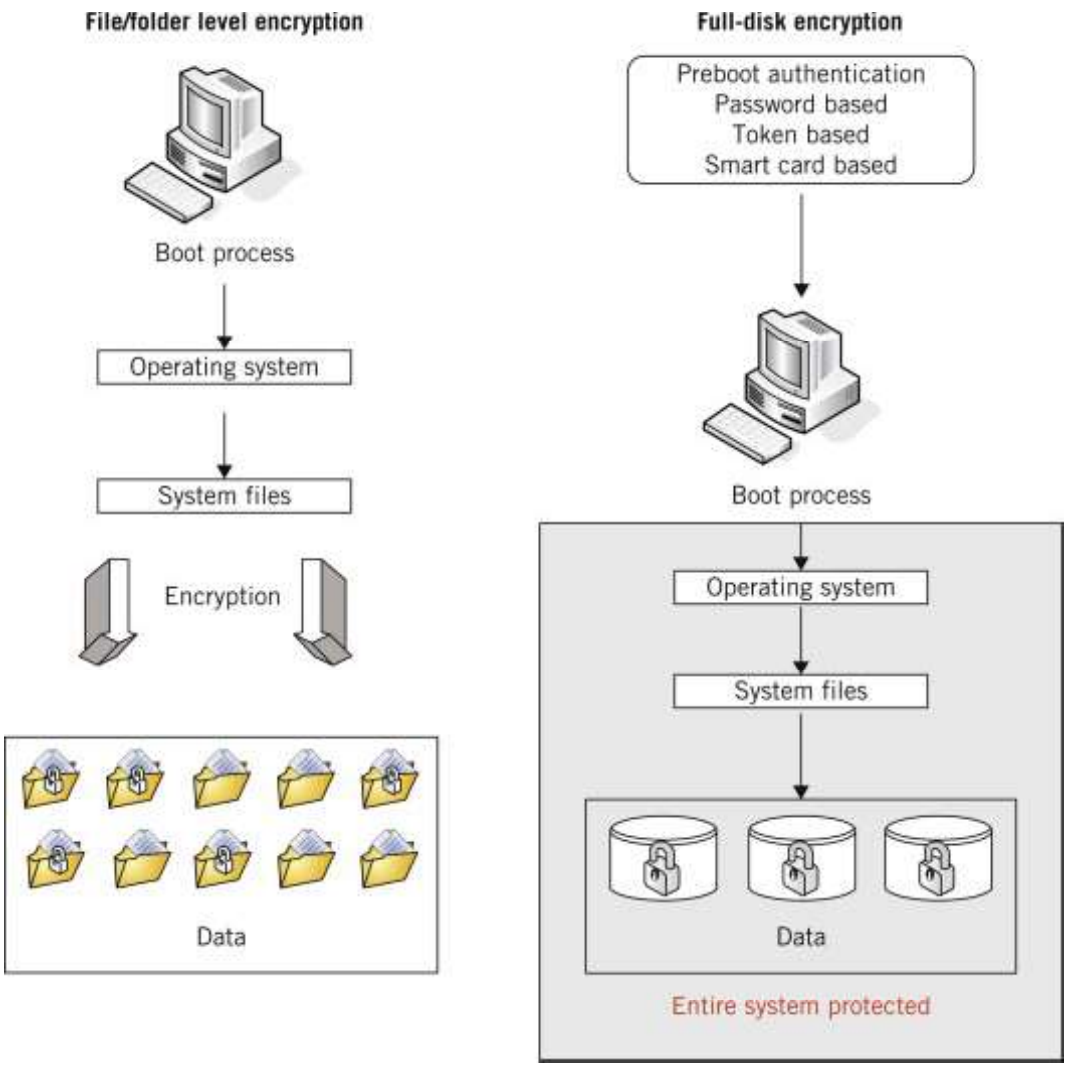


FIGURE 14 – Schéma illustrant la différence entre le chiffrement FBE et FDE [9]

Aujourd'hui la notion de protection de la vie privée des utilisateurs est toujours un argument commercial fort, comme le montre le site Apple : « confidentialité intégrée. C'est ça Apple » [123], ou les campagnes de publicité à la télévision « Privacy. That's iPhone. » de 2019-2020. Lorsque ce n'est pas la marque elle-même qui prend les devants pour la sécurisation de ses produits, ce sont des regroupements d'états à l'échelle européenne ou mondiale qui légifèrent en ce sens. En 2015, lors de la conférence Blackhat, Charlie Miller et Chris Valasek ont démontré la possibilité d'une attaque du système UCONNECT équipant les véhicules JEEP. Pour réaliser cette attaque [124], ils ont étudié le protocole CAN, leur permettant de rejouer certaines trames critiques prenant le contrôle de certaines fonctionnalités de la voiture. Un autre exemple récent d'attaque sur véhicule a été réalisé dans le cadre d'un challenge par la société Synacktiv sur une voiture de la marque Tesla [125]. Dans le cadre de ce challenge technique, ils ont réussi à trouver des failles concernant le système multimédia embarqué, l'élément qui accède et stocke les données utilisateurs, liées, entre autres, à la navigation du véhicule. Ces deux exemples

illustrent la pertinence de la direction prise par la Commission économique pour l'Europe des Nations unies (en anglais United Nations Economic Commission for Europe soit UNECE). En 2021, l'UNECE a publié le règlement R155 [126] destiné aux constructeurs automobiles pour la sécurisation des équipements embarqués dans les véhicules. Cette réglementation prévoit la sécurisation des bus de communication entre les boîtiers du véhicule, donc du bus CAN à l'origine de l'attaque sur les JEEP, mais aussi un chiffrement de la donnée utilisateur, empêchant les opérations de type extraction et relecture de la mémoire. Cette réglementation a eu un effet remarqué sur le marché du travail, car de nombreuses offres d'emplois sont apparues durant l'été 2021, provenant des constructeurs automobiles et de leurs prestataires.

Nous avons abordé la présence de chiffrement dans des systèmes différents et nous avons également identifié des acteurs ayant recours à la rétro-ingénierie, mais en plus de l'aspect technique, il faut tenir compte de l'aspect légal de l'activité. Pour cela, nous allons étudier des cas d'utilisation de la rétro-ingénierie pour définir si l'activité est légale ou si un cadre existe :

— Les analyses de construction : Lorsqu'une entreprise étudie ses propres produits, on ne peut pas réellement parler de rétro-conception mais plus de déprocessing, car les actes techniques réalisés ne visent pas à étudier la fabrication ou le fonctionnement d'un produit inconnu, mais à travailler sur un produit dont les fonctions et le process sont déjà connus de l'entreprise.

— Les évaluations de sécurité : Là encore le cadre légal n'est pas applicable aux travaux car le laboratoire d'évaluation agit comme un prestataire de service commandité directement par le possesseur de la propriété intellectuelle du produit. La société demandant l'évaluation doit cependant faire attention au cadre de l'utilisation de ses données auprès de ses prestataires. Pour éviter toute déconvenue, il est important de faire signer des accords de non-divulgation (NDA) aux entreprises prestataires même si l'article 1112-2 du Code Civil [127] protège déjà les différentes parties.

— L'espionnage industriel : Contrairement aux activités précédentes, l'espionnage industriel possède un cadre législatif visant à protéger les entreprises victimes. La loi française sur l'espionnage industriel est la loi n° 2018-670 du 30 juillet 2018 [128] relative à la protection du secret des affaires, qui a été adoptée en juillet 2018 et entrée en vigueur le 1er septembre 2018. Cette loi définit l'espionnage industriel comme l'acquisition, l'utilisation ou la divulgation d'un secret d'affaires par des moyens autres que ceux légalement autorisés. Un secret commercial est défini comme toute information qui a une valeur commerciale parce qu'elle n'est pas généralement connue ou facilement vérifiable par d'autres, et que le détenteur a pris des mesures raisonnables pour la garder secrète. Les personnes

reconnues coupables d'espionnage industriel peuvent être condamnées à une peine d'emprisonnement pouvant aller jusqu'à trois ans et à une amende pouvant aller jusqu'à 300 000 euros. Les entreprises reconnues coupables d'espionnage industriel sont passibles d'une amende pouvant aller jusqu'à 1 million d'euros. Outre les sanctions pénales, la loi prévoit des recours civils et les personnes ou les entreprises victimes d'espionnage industriel peuvent poursuivre les auteurs de l'infraction pour obtenir des dommages-intérêts.

— La forensique numérique : Il s'agit de l'activité la plus couverte par les cadres légaux car l'implication est très importante. Il faut comprendre que la forensique numérique est une activité qui est coûteuse pour l'administration française, même si elle est réalisée par une entité de l'État qui travaille gratuitement. En effet, même si les opérations ne sont pas facturées à la justice, les moyens humains et matériels mis en œuvre pour réaliser une analyse forensique sont très importants. L'utilisation de tels moyens n'est donc jamais prise à la légère et les magistrats doivent s'assurer que la procédure est conforme aux différentes lois afin d'éviter le vice de procédure. Dans ce contexte, la France dispose d'un cadre juridique assez étendu qui permet aux enquêteurs d'accéder légalement aux données. Le législateur envisage plusieurs outils, comme la loi n° 2019-222 du 23 mars 2019 relative à la lutte contre le terrorisme et la criminalité organisée qui a donné aux enquêteurs, avec les articles 706-102-1 à 5 [61, 129, 130], la possibilité d'accéder à distance à un appareil ou à un dispositif. Les techniques plus invasives ne sont pas en reste, car la rétro-ingénierie est couverte par les articles 230-1 à 5 [131, 132, 133], qui permettent au procureur de nommer un expert ou un centre d'expertise accrédité, d'effectuer ces opérations spécifiques. D'autres articles existent dont l'article 706-102-7, qui exige des experts de produire un rapport détaillé de leurs activités afin qu'elles soient consignés dans un procès-verbal. Cet article a été abrogé pour permettre aux experts de protéger le secret et l'efficacité des méthodes utilisées et ainsi éviter la divulgation aux fabricants, qui pourraient produire des contre-mesures, mais aussi pour éviter de donner des idées aux malfaiteurs.

En complément de l'aspect légal de la rétro-ingénierie, il existe aussi un cadre légal pour les données chiffrées, définissant à la fois les possibilités pour les forces de l'ordre, mais aussi les risques pour les mises en cause. L'article 434-15-2 du Code Pénal [134] décrit les peines encourues pour l'utilisation de moyens de cryptologie lors de la commission d'un crime ou délit. L'article définit également la peine encourue en cas de refus de communiquer sur le moyen de cryptologie utilisé : *"Est puni de trois ans d'emprisonnement et de 270000€ d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite*

convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre Ier du Code de Procédure Pénale. Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450000 € d'amende".

Il existe deux jurisprudences notables illustrant l'application de l'article précédemment mentionné. La première jurisprudence provient d'une cour de cassation en date de novembre 2022. Dans ce dossier le suspect a été arrêté en possession de produits stupéfiants, ainsi que de deux smartphones verrouillés. Il a refusé de communiquer les mots de passe des smartphones : *"Il a été poursuivi pour détention et offre ou cession de cannabis ainsi que pour refus de remettre la convention secrète de déchiffrement d'un moyen de cryptologie, en s'opposant à la communication du code de déverrouillage d'un téléphone susceptible d'avoir été utilisé pour les besoins d'un trafic de stupéfiants".* Lors d'un premier jugement en 2018, le suspect a été reconnu coupable concernant les produits stupéfiants, mais relaxé concernant le refus de communiquer ses mots de passe ; *"Par jugement du 15 mai 2018, le tribunal correctionnel l'a condamné pour infractions à la législation sur les stupéfiants, mais relaxé du délit de refus de remettre ou de mettre en œuvre la convention secrète d'un moyen de cryptologie".* Après plusieurs passages en appel et en cassation entre juillet 2019 et 2022, le dossier se retrouve de nouveau devant la cour de cassation en novembre 2022. Suite à l'étude du dossier, la cour de cassation a conclu qu'un smartphone est nativement conçu pour embarquer des dispositifs de chiffrement. Dans ce cas, aucune transformation par un moyen de cryptologie est appliqué aux communications donc cela ne peut rentrer dans le cadre de l'article 434-15-2 du Code Pénal. *"La mise en œuvre d'un moyen de cryptologie suppose la transformation à l'occasion de la communication entre plusieurs personnes de données claires pour les rendre incompréhensibles ou de données codées pour les rendre claires. Dès lors la clé de déverrouillage de l'écran d'accueil d'un smartphone n'est pas une convention secrète de chiffrement car elle n'intervient pas à l'occasion d'un message et ne vise pas à rendre incompréhensibles ou compréhensibles des données au sens de l'article 29 de la loi du 21 juin 2004 mais tend seulement à permettre d'accéder aux données et aux applications d'un téléphone, lesquelles peuvent être ou non cryptées".*

La seconde jurisprudence provient d'une cour de cassation en date de décembre 2019. Il s'agit d'un recours suite au jugement d'un suspect arrêté en possession de produits stupéfiants accompagné par une somme importante d'argent et de téléphones portables. Le point marquant dans ce dossier est le recours à l'article 434-15-2 du Code Pénal lors du passage en cour d'appel : *"en ce que la cour d'appel a reconnu le demandeur coupable de refus de remettre aux autorités judiciaires ou de mettre en œuvre la convention secrète de déchiffrement d'un moyen de cryptologie".* Par ailleurs, ce dossier met en

évidence un point important sur l'utilisation d'un smartphone utilisant des conversations chiffrées pour communiquer et ne pouvant pas être déchiffrées par les experts. La cour s'est basée sur l'article 434-15-2 du Code Pénal concernant les communications depuis le smartphone, qui ne devaient probablement pas être natives. De plus, dans ce dossier, l'incapacité de contourner le chiffrement des données, et son refus de communiquer ses mots de passe a visiblement desservi le suspect : *"Attendu que pour déclarer le prévenu coupable de refus de remettre aux autorités judiciaires ou de mettre en œuvre la convention secrète de déchiffrement d'un moyen de cryptologie, l'arrêt relève que M. R... a refusé de communiquer aux enquêteurs les codes de ses téléphones, rendant ainsi impossible leur exploitation ; que les juges ajoutent que les éléments découverts en sa possession au moment de son interpellation, soit la plaquette de résine de cannabis et les sommes d'argent très importantes, dont l'analyse des billets a démontré la présence d'un taux de cannabis et de cocaïne supérieurs à ceux habituellement rencontrés sur les billets en circulation normale, laissent présumer un usage du téléphone portable en lien avec des infractions à la législation sur les stupéfiants"*. La conclusion de la cour de cassation donnant raison à la cour d'appel déclarant coupable le suspect de possession et de commercialisation de produits stupéfiants : *"Attendu qu'en l'état de ces motifs dénués d'insuffisance et relevant de son appréciation souveraine, la cour d'appel a justifié sa décision sans inverser la charge de la preuve"*.

Dans cette longue mais nécessaire introduction, nous avons brossé un large panorama du contexte de la thèse au travers les différentes présentations de forensique numérique, de l'assurance qualité et de la rétro-conception matérielle. Nous avons eu l'occasion d'aborder des similitudes dans certaines des approches. La forensique numérique au niveau d'un laboratoire d'expertise est une activité qui demande une rigueur et une discipline similaire au concept de l'assurance qualité. De plus, une expertise scientifique sur un équipement endommagé nécessite des connaissances en électronique et en conception des systèmes qui s'apparente aux connaissances requises dans un laboratoire d'analyse de défaillance. Enfin l'évolution des politiques des entreprises et des règlements a introduit des notions de sécurisation des systèmes et de chiffrement de la donnée. Il faut passer par une phase d'analyse et de rétro-conception à la fois logicielle et matérielle. Outre les fondements techniques, l'ensemble de ces activités trouve également des parties communes dans les documents qui les définissent. Ainsi, les normes encadrant l'assurance qualité dans une entreprise peuvent être déclinées pour assurer la parfaite exécution d'une expertise judiciaire. De plus, les cadres législatifs entre la forensique numérique et la rétro-ingénierie sont imbriqués et le recours à cette dernière ne se fait pas sans passer par le cadre d'une expertise judiciaire. Ces différents exemples démontrent la porosité des frontières entre ces disciplines rendant intéressant les échanges entre les acteurs, démontrant également l'intérêt de carrières basculant d'un métier à l'autre. Prenant l'exemple de ma carrière

qui a débuté dans l'analyse de défaillance, me permettant de me familiariser avec les processus et la technologie des composants, j'ai pu basculer dans la rétro-conception matérielle où j'ai pu utiliser mes connaissances acquises par la relation étroite entre la chaîne de production des composants et le laboratoire d'analyse. J'ai également pu me familiariser dans ces deux métiers à une multitude d'équipements. Enfin mon basculement dans l'activité de forensique numérique axée sur le diagnostic et la réparation de supports (smartphones, clés USB, cartes mémoires) m'a permis d'apporter une vision différente et plus professionnelle. Cette dernière activité me permettant d'utiliser à la fois mes compétences en process qualité, en déroulé d'une analyse, mais aussi mes connaissances sur la fiabilité des composants. Après plusieurs années d'adaptation à ce nouvel environnement de travail, j'ai choisi de faire une thèse pour renforcer le transfert de techniques entre le monde de l'analyse de défaillance et de forensique numérique. En effet, mes recherches préparatoires ont montré que les process au sein des différents laboratoires forensiques sont très disparates et les équipements utilisés restent similaires. L'objectif de ma thèse est donc de proposer un axe de réflexion sur une base d'harmonisation des process pour le diagnostic et la réparation de supports numériques endommagés, tout en généralisant l'utilisation d'équipements que très rarement exploités dans les expertises judiciaires.

Contributions

Pour aborder les éléments mentionnés précédemment, le mémoire va s'articuler en trois grands chapitres :

— Analyse de l'environnement de travail, qui consistera à présenter la réflexion que j'ai pu mené sur la classification des différents supports de stockage pour prioriser nos travaux. Nous répertorierons également les équipements rencontrés dans les laboratoires d'analyse de défaillance pour confirmer leurs utilisations dans les laboratoires de forensique numérique. Cela permettra d'identifier de nouvelles possibilités pour le traitement des scellés. Enfin, en cohérence avec le résultat de la classification des supports, nous présenterons le fonctionnement théorique des supports de type MultiMedia Card (MMC) et de la Google Home, ainsi que les notions d'électronique nécessaires à la compréhension des travaux.

— Création d'un processus de diagnostic dans le cadre de de forensique numérique, qui consistera à présenter le protocole développé pour permettre un diagnostic plus rigoureux des supports MMC. Ce protocole ainsi développé sera ensuite illustré par son utilisation sur un cas d'étude.

— Extraction et fiabilisation de la donnée, qui consistera, dans la continuité du protocole de diagnostic, à présenter comment procéder à la récupération des données des scellés endommagés. Ce chapitre couvrira également les problématiques de fiabilité de la lecture lors de l'interaction directe avec une mémoire en s'attachant principalement aux corrections des erreurs.

Les travaux ont permis la rédaction de trois articles suivants :

— **New Diagnostic Forensic Protocol for Damaged Secure Digital Memory Cards** [135] paru en 2022 sur le site **IEEE Access**.

— **A forensic analysis of the Google Home : Repairing compressed data without error correction** [136] paru en 2022 dans un numéro du magazine **Forensic Science International : Digital Investigation**.

— **Case of study for *in situ* memory reading on damaged MultiMedia Card** [137] paru en 2024 dans le volume 48 du magazine **Forensic Science International : Digital Investigation**.

Chapitre 1

Analyse de l'environnement de travail

Dans ce chapitre, nous allons discuter de la sélection des cibles sur lesquelles il sera le plus pertinent de développer un processus de diagnostic. Le but sera d'identifier le type de stockage sur lequel nous rencontrons actuellement des difficultés. Nous accompagnerons la sélection d'une cible par un panorama des équipements communément utilisés dans les laboratoires d'analyses de défaillance et de forensique numérique. Cette liste sera complétée par des équipements rarement utilisés en forensique numérique, mais qui ont démontré leur intérêt lors d'analyses de défaillance. Cette liste ne sera pas exhaustive car depuis la création du processus, d'autres équipements avec un potentiel intéressant ont été identifiés. Ils ne seront pas développés dans le cadre de ce mémoire car à l'heure actuelle, leurs capacités et leurs champs d'application n'ont pas encore été totalement cernés dans le contexte de la forensique numérique. Dans ce chapitre, nous listerons des équipements et leurs champs d'utilisation sur les supports ; la description des travaux menés sur la mise au point du processus de diagnostic et ses débouchés seront abordés dans les chapitres suivants.

1.1 Classification des supports

Pour déterminer sur quel type de support il était le plus intéressant d'effectuer nos recherches, plusieurs méthodes ont été imaginées. La première méthode de calcul et de classification qui a été envisagée consistait à référencer dans un tableau, pour chaque support rencontré, s'il s'agissait d'un smartphone, d'une tablette, d'un ordinateur ou d'un autre équipement (et dans ce cas son type). Après avoir analysé un grand nombre de supports, nous souhaitions, en première approche, analyser les résultats de classification afin de focaliser nos recherches sur le support le plus fréquemment rencontré. Après une première analyse sur cette méthode, il fut déduit qu'elle n'était pas la plus pertinente car l'objectif premier était de pouvoir identifier un type de stockage de données sur lequel un diagnostic avancé était nécessaire. Or, compte tenu des flux des supports numériques entrant dans les laboratoires, il s'avère que les plus fortes demandes concernent les smartphones. En s'intéressant aux premières étapes de la réception d'un smartphone dans un laboratoire, l'opérateur commence par identifier sa marque et son modèle. Ensuite, il s'intéresse à son état : soit fonctionnel, soit endommagé. En fonction de ces informations, il oriente le smartphone dans l'équipe la mieux adaptée au traitement. Ce tri des smartphones, même s'ils sont fonctionnels, implique une différence des opération à réaliser compte tenu des différences technologiques. Par conséquent, une méthode de classification des supports basée exclusivement sur la nature de celui-ci n'était pas optimale.

La réflexion fut portée sur le triage effectué lors de la réception d'un support. Nous avons constaté que pour des supports fonctionnels, les smartphones et les tablettes de

marques identiques étaient traités avec les mêmes outils, par la même équipe et avec le même protocole. De même, une clé USB et un disque dur externe en boîtier, pouvaient subir le même protocole. À l'inverse, un protocole particulier était appliqué pour les smartphones d'une marque précise. Notre attention s'est alors portée sur la composition des différents supports, d'un point de vue stockage de la donnée. Nous avons constaté que les tablettes et smartphones d'un même fabriquant et d'une même génération avaient recours à la même technologie de stockage de la donnée. Cette technologie pouvait cependant évoluer en fonction des générations des produits. Le fait de s'interroger sur le modèle du support pour choisir le protocole à appliquer revenait à identifier la technologie de stockage. Prenant en compte cette observation, nous en avons déduit que la classification des supports devait être faite par leur technologie interne plutôt que par leur type ou marque. Par conséquent, nous avons choisi de référencer les supports reçus au sein d'un laboratoire sur une période donnée, puis pour chaque support de se documenter sur la technologie de stockage interne. Cette étude a été effectuée à posteriori sur des tableaux d'indicateurs bruts sur une période de trois ans. Pour des raisons de sécurité et de confidentialité, l'étude a été menée sur des indicateurs anonymisés de toutes références à un dossier judiciaire. Les tableaux contenaient uniquement le type, la marque et le modèle du support sans aucune autre information et ses travaux sont restés centralisés au niveau du laboratoire, pour ne pas divulguer d'informations sur les capacités de traitement des supports.

Trois technologies sont ressorties de l'études des différents supports. Pour chacune d'elles, nous allons expliquer leur fonctionnement ainsi que les actions menées dessus en laboratoire.

— Le disque dur à plateau (Hard disk drive ou HDD), présenté en Figure 1.1, est composé de plusieurs plateaux magnétiques écrits et lus par une tête de lecture. Il est également constitué d'une carte électronique permettant la communication avec un hôte ainsi que la gestion des actions effectuées. Pour cela, cette carte est constituée d'un contrôleur et d'une mémoire dans lequel se trouve le firmware.

FIGURE 1.1 – Exemple d'un disque dur à plateau [10]

Les cas de dysfonctionnement classiques des disques durs à plateau peuvent provenir d'un défaut d'un plateau magnétique entraînant généralement une perte importante de données. Le bras pilotant la tête de lecture peut également être défaillant, ce qui implique qu'il faille extraire les disques et les repositionner sur un nouveau bras. Deux paramètres sont à prendre en compte pour cette opération, car elle est critique. L'opération doit se faire dans un environnement sans poussière car les disques y sont sensibles. Généralement on effectue cette opération sous une hotte à flux laminaire. De plus, les plateaux fonctionnent de manière synchronisée, ce qui signifie que la transplantation des plateaux doit se faire sans créer de décalage d'angle d'un plateau à l'autre. Le dernier défaut, qui est le plus courant mais le plus facilement réparable, provient de la carte électronique qui peut subir une surpuissance (surtension ou excès de courant). Dans ce cas, l'un des composants de la carte est défectueux, avec pour conséquence que le disque supporté par l'hôte. La solution la plus simple et la plus répandue, sachant qu'elle évite de passer par la phase de diagnostic de la carte électronique, consiste à se procurer la carte d'un disque identique [1]. D'un disque à l'autre le firmware peut être différent. Ainsi, avant de remplacer la carte *donneuse* dans le disque à réparer, il faudra extraire la puce mémoire de l'ancienne carte pour la transplanter sur la nouvelle. Le disque dur à plateau n'est maintenant plus utilisé que pour de grosses capacités de stockage, le coût des supports nouvelles générations étant très chers en comparaison [2]. Nous constatons qu'ils sont présents essentiellement dans les ordinateurs haute performance, les serveurs d'entreprise ou dans les solutions de stockage (NAS). Ils sont toujours utilisés dans les supports de conception plus ancienne tels que les consoles de jeu (PlayStation 4), souvent incompatibles avec d'autres technologies de stockage.

— Le support de stockage fragmenté, comme celui présenté en Figure 1.2, est composé de plusieurs éléments distincts, assemblés sur une carte électronique pour former le système de stockage. Il est constitué d'un contrôleur qui assure les communications respectives avec l'hôte et les puces mémoires qui stockent les données. Les puces mémoires sont basées sur la technologie flash. Il existe plusieurs types de stockages fragmentés recourant à des protocoles différents pour les échanges avec l'hôte. Les échanges en interne au support peuvent également prendre plusieurs formes avec des accès plus ou moins directs à la mémoire flash.

1. Lorsqu'on utilise un produit similaire pour en récupérer un ou plusieurs éléments, on utilise le terme de *donneur* pour le produit similaire et ses éléments associés.

2. Cette remarque était adaptée lors de l'étude initial entre 2018 et 2020. Cependant, malgré la crise du semi-conducteur qui a négativement impacté les prix des systèmes électroniques, le prix du Tera-octet d'un disque SSD a considérablement baissé. Pour comparaison, à l'été 2023 avec un budget de 250€, on se procure un HDD de 4To ou un SSD de 2To ou 4To selon la marque et la vitesse, alors qu'en 2019 on pouvait se procurer qu'un SSD de 1To.

FIGURE 1.2 – Exemple d'une clé USB composée de plusieurs éléments [11]

Les défauts subits par ces supports peuvent provenir soit d'un composant vital (le contrôleur ou la mémoire), soit d'un composant auxiliaire (une résistance ou une capacité), soit de la carte électronique. Ils peuvent être générés par un excès de tension ou de courant provenant de l'hôte, entraînant une défaillance sur l'un des éléments préalablement énoncés. Pour les supports mobiles comme les clés USB, d'autres défaillances peuvent survenir suite à un stress mécanique trop important, entraînant des dégradations des composants ou de pistes de la carte électronique. Le traitement de ces supports se fait en extrayant les puces mémoires pour les lire indépendamment. Cette opération d'extraction nécessite de dessouder le composant, soit à l'air chaud, soit à l'aide d'une machine. Le composant est ensuite inséré dans un lecteur commercial pour tenter d'extraire les données. D'un point de vue matériel, la complexité de l'opération réside dans la phase de diagnostic et d'extraction du composant mémoire. Il s'agit d'une opération couramment réalisée dans les laboratoires de forensique numérique. L'opération d'analyse après la lecture demande une connaissance du système de fichiers de la part de l'opérateur. Les données sont ordonnées dans la mémoire afin d'optimiser les vitesses de transfert et la durée de vie des cellules de celle-ci. De ce fait elles ne sont pas directement intelligibles et rangées dans l'ordre des fichiers. Parmi les différents types de support à stockage fragmenté, on peut retrouver les disques Solid-State Drive (SSD) basés sur des puces mémoires utilisant la technologie flash ou Non-volatile Memory Express (NVME), des Internets des Objets (Internet of Things ou IoT), les téléphones anciennes générations (par exemple Samsung Galaxy S5) et bien-sûr beaucoup de clés USB.

— Le support de stockage monolithe, comme celui présenté en Figure 1.3, est conçu avec les mêmes éléments que le support fragmenté, mais avec une forme différente. Les supports monolithes regroupent dans le même package le contrôleur, les puces mémoires et les composants auxiliaires.

FIGURE 1.3 – Exemple d'une clé USB monolithe [11]

Les deux supports fragmenté et monolithe, ayant la même composition, les défauts sont similaires mais le traitement est différent, car il n'est pas possible de séparer facilement les composants pour les vérifier indépendamment dans les supports monolithes. Ces supports monolithiques sont donc plus complexes à traiter et demande une plus grande connaissance en électronique ainsi que des moyens plus importants. Il existe des solutions commerciales pour traiter certains supports (nous l'aborderons dans la partie *Interconnexion*), mais pour une grande partie des supports, le travail doit être fait par l'opérateur lui-même. Parmi les exemples de supports monolithiques, on peut retrouver les clés USB, les mémoires amovibles (compact flash, SD et microSD) et les composants mémoires destinés à des systèmes (NVME, embedded MultiMedia Card (eMMC) et Universal Flash Storage (UFS)). Les mémoires SD, microSD, eMMC et UFS sont technologiquement regroupées dans la famille des MultiMedia Card (MMC) qui sera détaillée dans la section *Protocole de communication entre la MMC et l'hôte*. Les MMC étant plus rapides et plus fiables que ne le sont les mémoires flash seules, elles sont utilisées dans les dernières générations d'appareils mobiles et embarqués qui intègrent également le chiffrement pour sécuriser le stockage des données. Ces composants plus récents sont devenus le type de stockage le plus communément utilisé dans les systèmes. Nous pouvons les retrouver dans les smartphones, les tablettes, les systèmes multimédias des voitures, certains IoT tels que les caméras et les drones.

Tableau 1.1 – Tableau de classification des supports avec leurs utilisations et les capacités de traitement

Stockage	Type support	Défaut	Réparabilité
HDD	Ordinateur gaming	Plateau magnétique	Échec
	NAS	Tête de lecture	Avancé
	Console de jeu	Carte électronique	Intermédiaire
Fragmenté	SSD	Contrôleur	Facile
	IoT	Carte électronique	Facile
	Ancien téléphone	Composant annexe	Facile
	Clé USB	Mémoire	Échec
Monolithe	Smartphones Tablettes Systèmes multimédias des voitures IoT NVME de SSD	D'un élément de la carte électronique	Avancé si référencé Sinon échec

Une fois les différentes technologies de stockage identifiées et référencées dans un Tableau 1.1, les supports concernés y ont été associés ainsi que leurs niveaux de réparabilités. Il en est ressorti que les types de supports nécessitant le plus d'attention sont les MMC. Il s'agit de mémoires de type monolithique contenus entre autre dans les smartphones, les tablettes, les systèmes multimédias des voitures, les IoT et incluant les mémoires de type NVME présentes dans certains disques SSD. Du fait de leur présence dans une grande quantité de supports, et de leur structure complexe, il est très difficile pour les laboratoires de forensique numérique de procéder à leur diagnostic ou à leur réparation. Nous avons donc fait le choix de focaliser nos travaux sur cette technologie, utilisant ainsi des eMMC et des cartes microSD pour effectuer nos expérimentations et développer notre processus de diagnostic, généralisable à l'ensemble des MMC.

1.2 Équipements des laboratoires

Dans cette partie, nous allons présenter les différents équipements communs dans les laboratoires d'analyse de défaillance et de forensique numérique. Nous avons comparé les équipements des laboratoires dans lesquels nous intervenons régulièrement et qui sont connus pour être à la pointe des technologies actuelles. Nous avons abordé chaque équipement pour des capacités globales, indépendamment de la marque et du modèle. La raison de ce choix réside dans la disparité des réseaux de distribution des équipements entre les pays. Lorsque nous aborderons les capacités et les utilisations d'un équipement, il s'agir d'une vision globale. De même, la sélection des équipements courants dans les laboratoires d'analyse de défaillance ou dans les laboratoires de forensique numérique sera faite par rapport aux expériences passées dans les laboratoires fréquentés (carrière, visite ou partenariat).

1.2.1 Observation optique

1.2.1.1 Binoculaire

1.2.1.1.1 Principe de fonctionnement

La binoculaire ou stéréo-microscope est un équipement utilisant la lumière pour effectuer des observations. L'équipement intervient dans le spectre du visible, dont la longueur d'onde est comprise entre 400nm et 700nm, comme le montre la Figure 1.4.

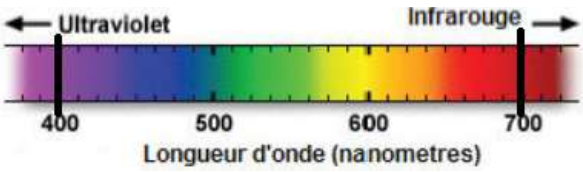


FIGURE 1.4 – Spectre de la lumière [12]

La binoculaire est équipée de plusieurs jeux de lentilles (Figure 1.5) acheminant et focalisant la lumière pour permettre l'observation de l'échantillon par l'utilisateur. Sur ce type d'équipement, l'échantillon est positionné sur une platine ou une base. La lumière est émise par une source extérieure provenant d'une lampe ou d'un spot LED autour de l'objectif. L'objectif est la source d'entrée de la lumière dans l'équipement. Il s'agit d'un élément avec un effet de grossissement fixe. Sur certains équipements, l'objectif est amovible et peut être remplacé pour changer le grossissement, ce qui affecte la distance de travail.

La distance de travail (Working Distance ou WD) est l'écartement exprimé en millimètres entre l'échantillon et l'objectif (Figure 1.6). La modification de ce paramètre

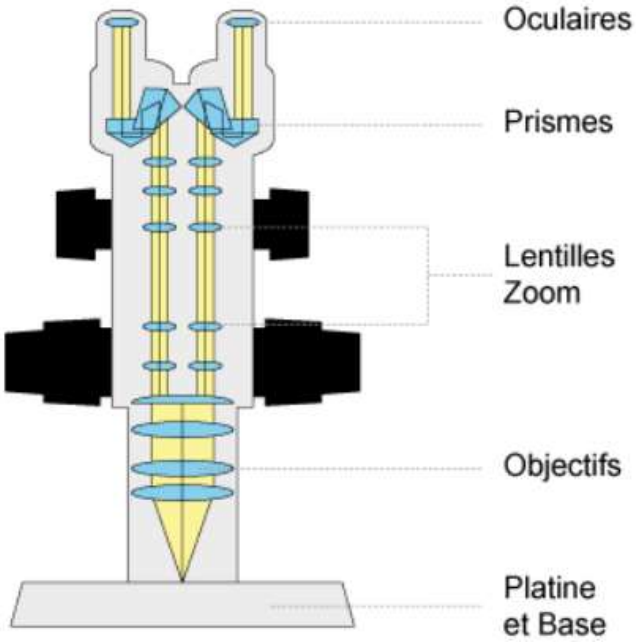


FIGURE 1.5 – Schéma de cheminement de la lumière dans une binoculaire [12]

permet d'influer sur l'Ouverture Numérique (ON) se répercutant directement sur la résolution de l'équipement. Même s'il peut être intéressant de changer l'objectif pour accroître le grossissement maximum de l'équipement, cela réduira la distance de travail, pouvant perturber l'aisance des manipulations effectuées.

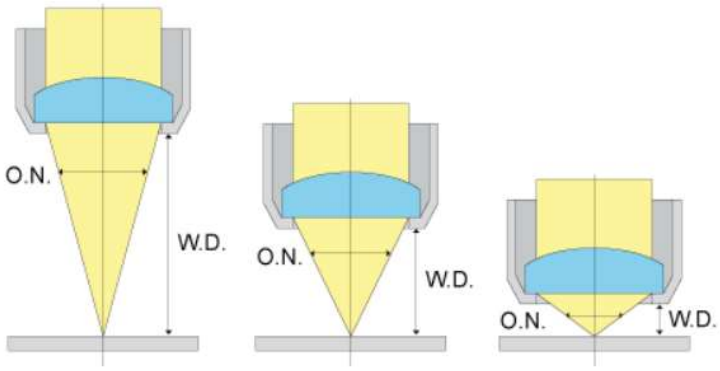


FIGURE 1.6 – Schéma de principe de la distance de travail [12]

Après avoir traversé l'objectif, le faisceau de lumière est séparé en deux faisceaux parallèles qui poursuivent leur chemin dans deux séries de lentilles. Ces séries de lentilles sont réglables en hauteur, ce qui permet de jouer sur deux paramètres. La série du bas sert à régler la netteté par rapport au grossissement courant, alors que la série du haut sert à régler le grossissement. L'étage suivant est composé de prismes qui redirigent les deux faisceaux vers les oculaires, éléments de sortie qui permettent l'observation à l'utilisateur. Sur certains équipements, les oculaires sont amovibles et peuvent être remplacés pour

modifier les plages de grossissement de l'équipement.

1.2.1.1.2 Application de l'équipement

Les binoculaires sont des équipements donnant une vision d'un échantillon à l'échelle macroscopique. Elles peuvent prendre plusieurs formes, avec des oculaires comme le modèle Leica (Figure 1.7a) ou avec un écran intégré remplaçant les oculaires comme le modèle Lynx (Figure 1.7b). Les binoculaires disposent classiquement d'une plage de grossissement allant de x0.5 à x10, rendant les manipulations plus aisées sur des échantillons. Ce grossissement peut subir un zoom numérique par 10 dans le cas d'un couplage avec une caméra.

(a) Binoculaire Leica équipé d'oculaires [13]

(b) Stéréo-microscope sans oculaire Lynx EVO [138]

FIGURE 1.7 – Exemple de deux équipements de conception différente pour l'observation macroscopique d'échantillons

Une binoculaire sert à réaliser des manipulations précises ou de l'observation d'assemblage. En effet, avec un faible grossissement, il est possible de visualiser les packages des composants pour observer leurs états ou les marquages. Avec un fort grossissement, il est possible d'observer en détail des soudures ou une fissure dans un package (Figure 1.8). Cependant, cet équipement ne permettra pas de visualiser des éléments fins, tels que la composition des puces en silicium. Pour cela, il faudra privilégier un microscope.

FIGURE 1.8 – Exemple d'utilisation d'une binoculaire pour observer une carte électronique [13]

1.2.1.2 Microscope

1.2.1.2.1 Principe de fonctionnement

Le principe de fonctionnement d'un microscope est similaire à celui d'une binoculaire, à savoir l'utilisation d'une lumière dans le spectre du visible, même si certaines configurations ont recours à d'autres sources (par exemple : UV, infrarouge).

La Figure 1.9 présente le chemin de la lumière dans un microscope. À noter que la figure présente un modèle à double sources lumineuses pour un éclairage par le dessus pour les éléments opaques ou par le dessous pour les éléments transparents. Pour l'utilisation sur des composants électroniques, seule la source supérieure sera utilisable. Par conséquent l'explication de l'équipement va se concentrer sur cette source. Contrairement à la binoculaire, le microscope embarque sa propre source lumineuse. Le faisceau de lumière sort de la source et traverse des lentilles ou des filtres, avant de se réorienter en direction de l'échantillon grâce à un miroir. Le faisceau traverse l'objectif pour se réfléchir sur l'échantillon, posé sur la platine porte objet. Le faisceau réfléchit repasse par l'objectif et retourne en direction du miroir, appelé "miroir de champ", qui a la particularité d'être transparent pour la lumière provenant de l'échantillon. Enfin le faisceau passe dans un prisme qui permet de le réorienter à la fois sur une caméra placée au-dessus de la colonne et dans les objectifs.

Contrairement à la binoculaire, le changement de grossissement sur un microscope ne se fait pas avec des lentilles en interne, mais par le changement de l'objectif. Pour cela, il faut faire basculer la tourelle qui les porte, mais cette reconfiguration a un effet sur la distance de travail. En effet, chaque objectif possédant sa propre distance de travail, un changement d'objectif implique un réglage de la focalisation. Comme pour la binoculaire, les oculaires et les objectifs sont remplaçables permettant une évolution de la configuration.

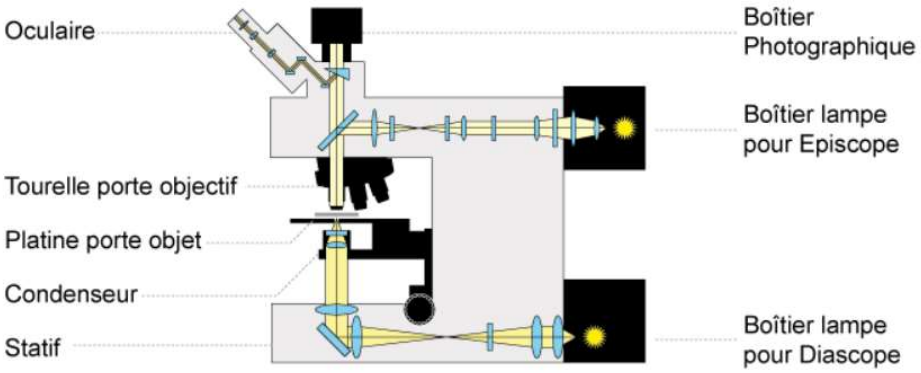


FIGURE 1.9 – Schéma de cheminement de la lumière dans un microscope [12]

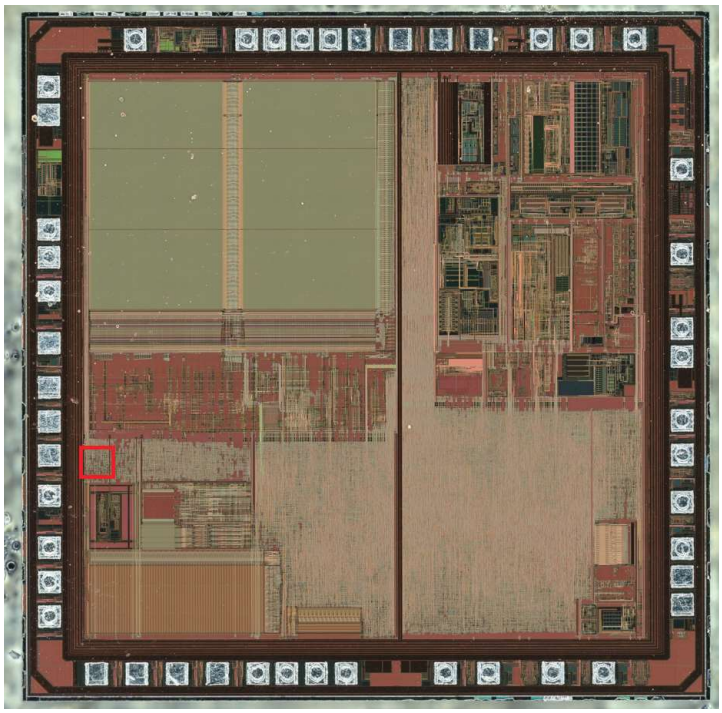
1.2.1.2.2 Application de l'équipement

Le microscope est utilisé pour effectuer des observations de la structure des puces électroniques, car il propose un grossissement important, allant de x5 à x150. Ce grossissement peut être multiplié par 10 avec la caméra située au-dessus de la colonne. La Figure 1.10 présente un microscope de la marque Leica avec un fonctionnement manuel. D'autres équipements peuvent être motorisés pour le changement de l'objectif ou le déplacement de la platine.

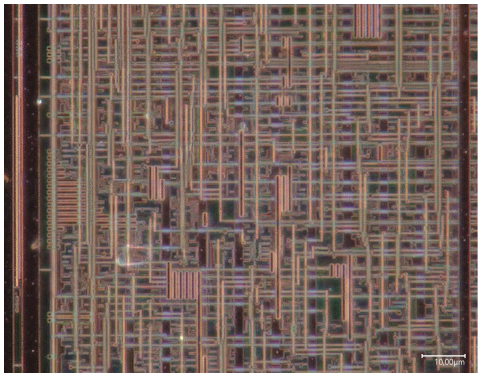
FIGURE 1.10 – Exemple de microscope de la marque Leica [14]

En électronique, le microscope est généralement utilisé pour effectuer des cartographies des puces internes des composants, comme l'illustre la Figure 1.11a. Il est également

possible de faire des observations des éléments internes des puces pour en observer leur conception, comme le montre la Figure 1.11b.



(a) Cartographie au microscope d'un PIC16 (Zoom encadré en rouge)



(b) Zoom sur une zone pour observer les pistes du composant

FIGURE 1.11 – Exemple d'échantillons observés avec un microscope

1.2.1.3 Machine à Rayons-X

1.2.1.3.1 Principe de fonctionnement

Le principe de l'équipement est basé sur les photons-X, qui est un quantum d'énergie associé à une onde électromagnétique. Les photons-X nécessaires au fonctionnement des équipements industriels peuvent avoir deux sources de production différentes : une source scellée qui contient un élément émettant naturellement des photons-X, ou un filament en tungstène utilisé sous haute tension. Pour cette dernière, les atomes de tungstène sont soumis à un fort champ électrique, déclenchant une mobilité des électrons d'une couche de valence à une autre. Le changement de couche d'un électron a pour effet de créer un photon-X, comme illustré sur le schéma de la Figure 1.12.

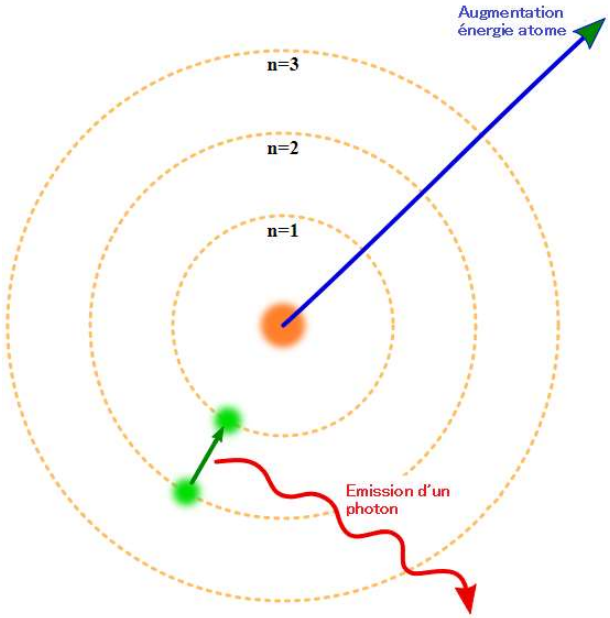


FIGURE 1.12 – Schéma de principe de la production d'un photon-X suite à la mobilité d'un électron [15]

Dans les deux cas, le faisceau de photons-X produit par la source est accéléré par une colonne pour être projeté sur l'échantillon à observer. Les photons-X produits sont de deux natures différentes : les photons de faible énergie et les photons de forte énergie. Ces derniers qui possèdent une fréquence élevée ont des effets néfastes sur les objets à observer. Ils doivent donc être filtrés, pour ne laisser que les photons de faible énergie atteindre l'échantillon et ainsi ne pas l'endommager. Les filtres sont situés directement en sortie de la colonne d'émission. La Figure 1.13 présente l'intérieur d'une chambre de machine à Rayons-X permettant de faire de l'acquisition en deux ou trois dimensions.

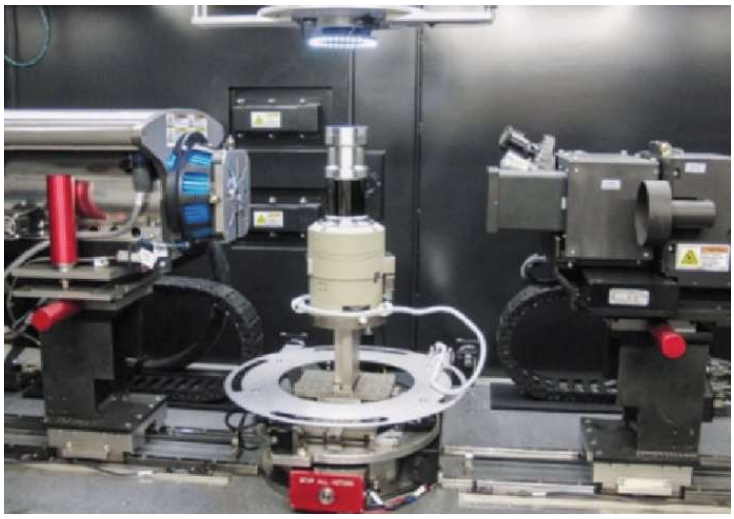


FIGURE 1.13 – Exemple de positionnement d'un échantillon dans une cabine de rayons-X de marque Zeiss [16]

La colonne à émission se situe sur la gauche de l'image. Les photons-X vont être produits et canalisés dans ce tube, avant d'être projetés sur l'échantillon, qui se trouve au centre de l'image. Le détecteur, sous forme d'une matrice, est positionné sur la partie droite de la figure, soit de l'autre côté de la source par rapport à l'échantillon. Le mode d'observation est donc par transmission, car le faisceau de photons sort de la source, traverse l'échantillon puis sont acquis par le détecteur. Étant en transmission, l'observation est influencée par la densité des matériaux traversés. Plus le matériau sera dense, plus il faudra projeter de photons-X, dans le but d'en réceptionner une quantité suffisante au niveau du détecteur, pour avoir une image exploitable. Le détecteur présent sur l'équipement étant une matrice, l'image produite est une composition en deux dimensions et en niveau de gris dépendant directement de la densité des matériaux traversés. C'est la différence d'énergie entre la sortie du tube et le détecteur qui permet de réaliser une image en deux dimensions.

Sur les équipements qui font de l'observation trois dimensions, comme la machine Zeiss de la Figure 1.13 ou la machine RX-Solutions de la Figure 1.14, les échantillons sont positionnés à la verticale et maintenus par une pince capable de tourner à 360° sur elle-même. Cette technique est appelée tomographie 3D à rayons-X. Elle se fait par une succession d'images 2D acquises à des angles différents, lorsque l'échantillon tourne. La série d'images est ensuite traitée par un logiciel, qui est en charge de calculer le centre de rotation en fonction des déformations de chacune des images. Une fois le centre de rotation calculé, le logiciel est capable de reconstruire la pièce en trois dimensions et de la redécouper en tranches (slices) sur plusieurs axes, permettant à l'utilisateur de naviguer dans l'échantillon progressivement.

FIGURE 1.14 – Exemple de machine à Rayons-X pour la visualisation 2D et 3D de marque RX Solutions [17]

1.2.1.3.2 Application de l'équipement

Sur une scène de crime (par exemple : un crash aérien, une scène NRBC [3]), disposant d'un nombre important d'objets électroniques, l'imagerie à Rayons-X 2D permet de réaliser un pré-triage afin de ne faire parvenir au laboratoire que les objets qui sont potentiellement analysables (exemple constater la destruction ou fissuration du silicum).

Dans les laboratoires d'analyse de défaillance ou de forensique numérique, les machines d'imagerie par Rayons-X sont utilisées pour faire du diagnostic de composants ou systèmes électroniques. En deux dimensions, elles servent à effectuer une observation du système dans son intégralité, par exemple un iPhone 12 (Figure 1.15). Le but est de rechercher un défaut d'assemblage ou un stress mécanique flagrant. À cause de la complexité des systèmes, il est rarement possible d'observer un défaut dans un composant ou sur une carte en deux dimensions. En effet, les éléments se superposant sur la vue, il est difficile d'identifier des informations de couches ou d'empilements. Pour cela, il faudra utiliser la fonctionnalité de tomographie pour obtenir une vue en trois dimensions, et ainsi naviguer dans les différentes couches du système.

La Figure 1.16 est une reconstruction 3D d'une carte SD, sur laquelle il est possible de visualiser la couche extérieure (Figure 1.16a), c'est-à-dire la couche du PCB. Il est également possible de visualiser sur une autre slice la couche interne du PCB (Figure 1.16b), qui permet le raccordement des différentes puces électroniques qui

3. Sur des scènes de crime de type NRBC, il n'est pas possible de transporter des équipements de laboratoire. Cependant, des travaux ont montrés l'utilisation possible d'équipements Rayons-X moins onéreux et mobiles [139].

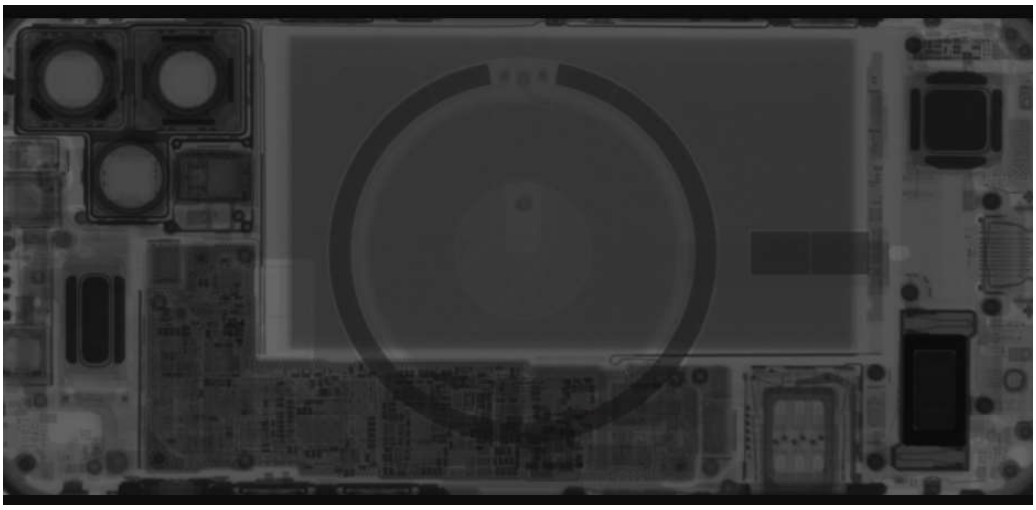
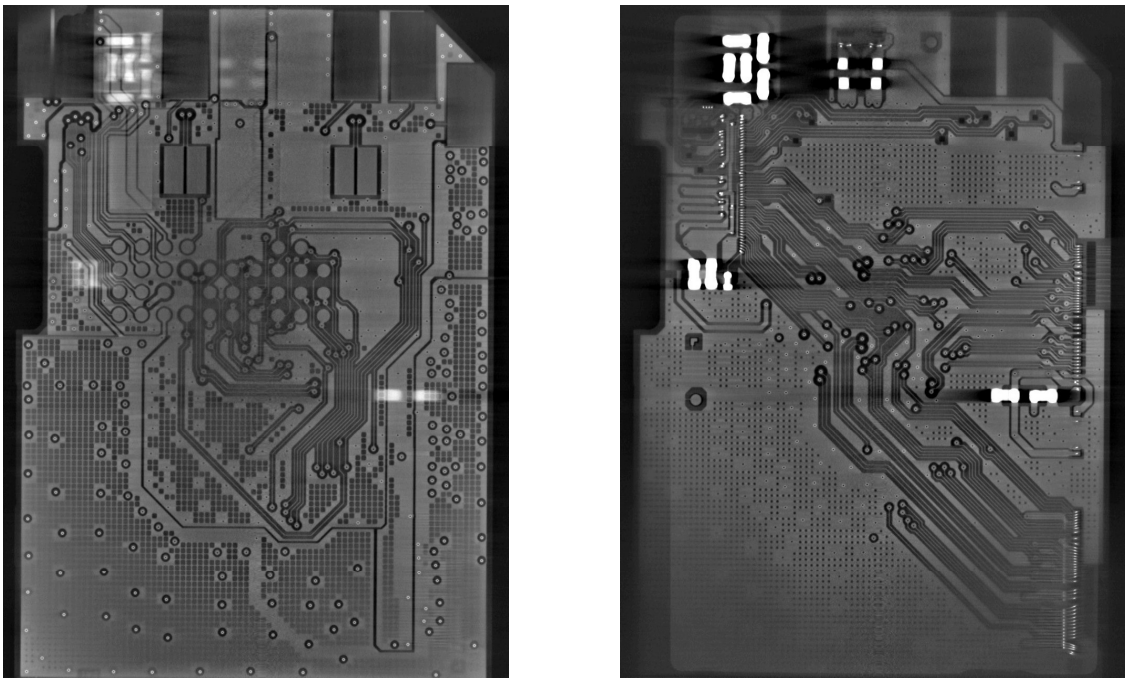


FIGURE 1.15 – Vue d'un iPhone 12 aux Rayons-X en 2D [18]

composent la carte SD. L'observation en 3D permet d'observer séparément les différentes couches, ce qui donne à l'utilisateur l'opportunité de suivre des pistes ou de rechercher plus aisément une anomalie, par rapport à une vue en deux dimensions.



(a) Niveau métallique externe

(b) Niveau métallique interne

FIGURE 1.16 – Slices (interne et externe) du PCB d'une carte SD

1.2.1.4 Microscope électronique à balayage (MEB)

1.2.1.4.1 Principe de fonctionnement

Le microscope électronique à balayage est une observation de la matière par ses électrons. Pour cela, le microscope doit produire un faisceau d'électrons libres, grâce à un filament en tungstène soumis à un fort champ électrique. Sous l'effet du champ électrique, les électrons quittent les couches de valence des atomes du filament puis traversent une colonne qui les canalise et les accélère au travers d'ouvertures limitantes (apertures) et lentilles de condenseurs (schéma de la colonne sur la Figure 1.17). Plusieurs détecteurs sont positionnés dans la chambre de l'équipement, permettant de capturer différentes informations, dépendant de la nature de l'électron.

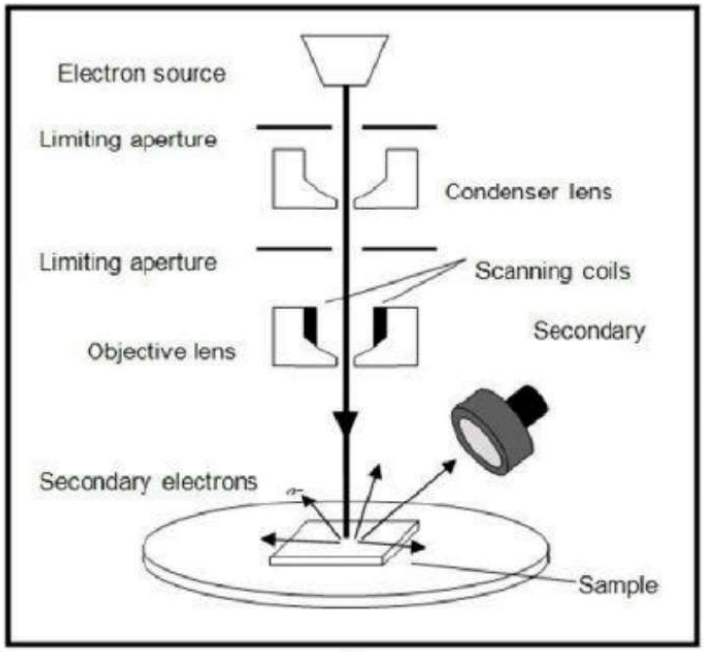


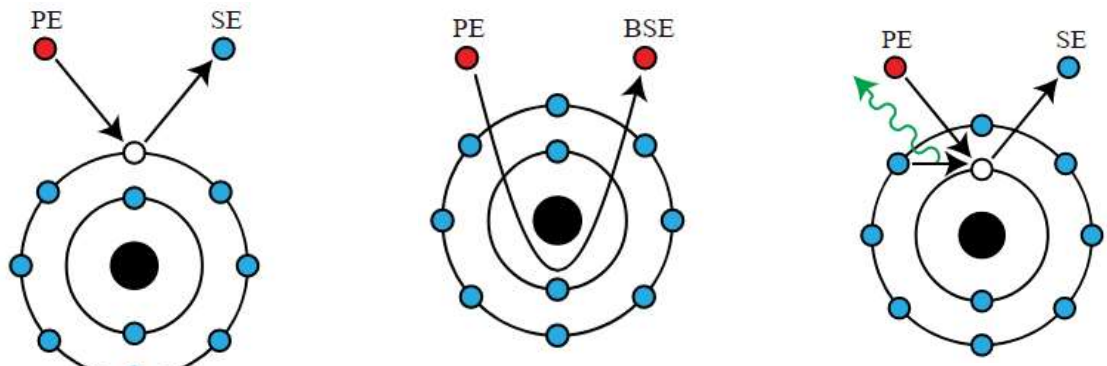
FIGURE 1.17 – Schéma de la colonne d'un microscope électronique à balayage [19]

L'électron émis par la colonne est appelé électron primaire, nommé PE. Il est représenté en rouge sur la Figure 1.18. Il existe plusieurs interactions possibles de l'électron primaire avec la surface de l'échantillon observé, qui auront une propriété différente à observer :

— Si l'électron primaire percute un électron de la matière cible pour prendre sa place, l'électron ainsi projeté est appelé électron secondaire, nommé SE sur la Figure 1.18a. Pour chaque atome de matière, il existe une énergie propre dépendante de la couche de valence. Le capteur SE2 des microscopes électroniques à balayage est capable de récupérer les électrons secondaires et d'en analyser leurs plages d'énergie. Ce procédé permet de faire une cartographie d'une zone en fonction des différentes plages d'énergie, en niveau de gris.

— Si l'électron primaire pénètre jusqu'au noyau de l'atome pour être dévié et ré-expédié en dehors de la matière, l'électron ne porte plus le nom de primaire mais d'électron rétro-diffusé, en anglais BackScattered Electron ou BSE sur la Figure 1.18b. Le champ gravitationnel du noyau de l'atome modifie l'énergie propre de l'électron primaire. L'électron rétro-diffusé possède donc une nouvelle énergie pouvant être analysée par un détecteur spécifique. Comme pour les électrons secondaires, l'image produite sera basée sur les énergies, il s'agira de celle de l'électron rétro-diffusé, représenté en niveau de gris. Les images réalisées avec les électrons rétro-diffusés sont possibles car ces derniers sont sensibles au numéro atomique des atomes cibles. Les atomes lourds réémettront plus d'électrons que les atomes légers.

— Si l'électron primaire produit un électron secondaire, un photon-X (Figure 1.18c), donc un quantum d'énergie et une onde électromagnétique, sont produits. Ce photons-X possède des propriétés inhérentes à la matière qui les produits. Un détecteur spécifique qui capte les photons-X et analyse précisément leurs énergies peut être ajouté au microscope, ce qui permet de construire une cartographie représentative des matériaux rencontrés à la surface de l'échantillon. Le détecteur est en mesure d'indiquer si dans une zone précise il reçoit des photons d'énergies différentes. Il n'est cependant pas capable d'indiquer correctement la proportion de chaque photon par rapport à la quantité totale. Cette analyse est donc qualitative et non quantitative.



(a) Électron secondaire

(b) Électron rétro-diffusé

(c) Photons-X et électrons secondaires

FIGURE 1.18 – Schéma des différentes interactions entre l'électron primaire et la matière [20]

Quel que soit le détecteur utilisé, la remise en forme de l'image reste la même. Le faisceau projeté sur la surface de l'échantillon ne représente qu'un point nanométrique, donc les informations collectées correspondent à l'instant donné qu'à un point précis de l'échantillon. Pour effectuer une image complète d'une zone, il faut que le faisceau

la balaye. Pour chaque point couvert par le faisceau, les informations sont collectées et insérées sur une matrice, qui sera convertie en image à la fin du balayage. La production d'une image à partir d'un MEB n'est donc pas instantanée et demande un temps d'acquisition et de traitement dont la durée est directement corrélée à la qualité de l'image produite.

Sachant que les électrons primaires peuvent produire plusieurs interactions avec la matière, il faut aussi comprendre comment elles se produises. Lorsque le faisceau d'électrons primaire frappe la surface de l'échantillon, ils pénètrent la matière sous la forme d'une poire appelée "poire d'interaction", visible en Figure 1.19. La profondeur et la largeur maximum de la poire vont dépendre de la puissance de faisceau d'électrons. Une forte puissance, obtenue avec des tensions d'accélération comprises entre 20keV et 30keV, produit une poire d'interaction profonde, ce qui augmente les chances d'obtenir des informations avec des électrons rétro-diffusés ou des photons-X. À l'inverse, une tension d'accélération comprise entre 3keV et 10keV ne produit qu'une faible poire d'interaction, limitant l'observation à des électrons secondaires. Malgré une forte tension, la profondeur maximum de la poire d'interaction reste de l'ordre du micromètre, ce qui ne permet pas de faire des observations des couches profondes d'un composant électronique, mais donne une vision avec une très grande résolution de la surface d'un échantillon.

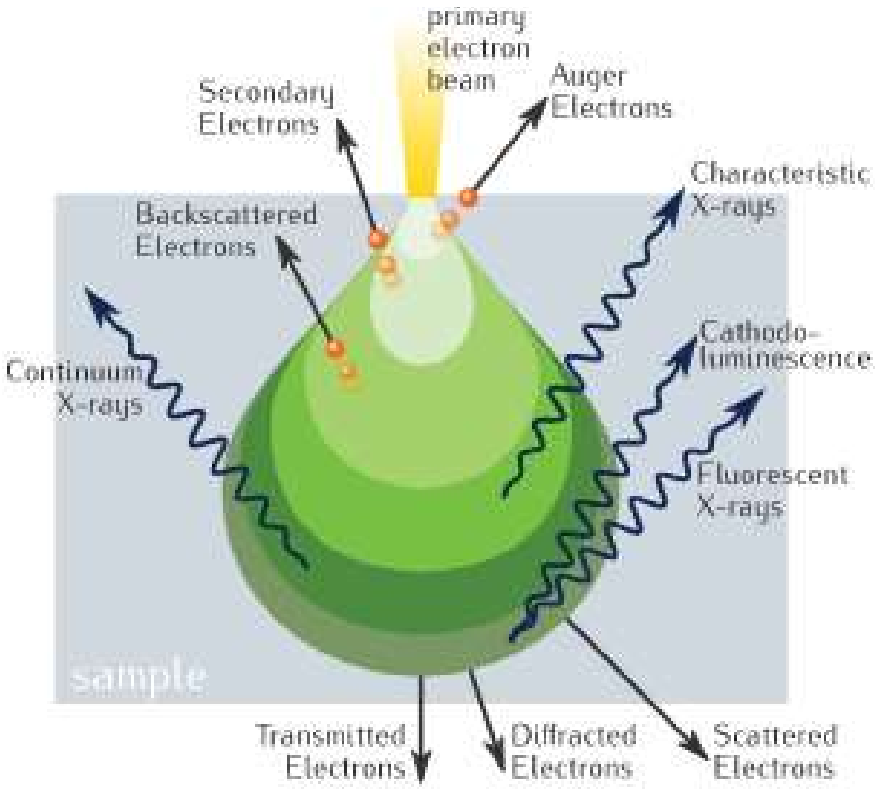


FIGURE 1.19 – Schéma de la poire d'interaction des électrons avec la matière [20]

Les microscopes électroniques à balayage, tels que ceux de la gamme Evo de ZEISS dont un exemplaire est présenté en Figure 1.20, possèdent de série les détecteurs d'électrons secondaires et rétro-diffusés. Les détecteurs de photons-X sont en option. La qualité du microscope dépend de la qualité de sa colonne, qui doit produire un faisceau d'électron avec une plage d'utilisation en tension et en courant large, ainsi que de la qualité et du positionnement de ses détecteurs.

FIGURE 1.20 – Exemple de microscope électronique à balayage de la marque Zeiss [21]

1.2.1.4.2 Application de l'équipement

Les microscopes électroniques à balayages sont principalement utilisés pour effectuer des observations d'éléments présents à la surface d'un échantillon. Dans les laboratoires d'analyse de défaillance, il est possible d'observer des pistes d'une puce électronique pour localiser un défaut. Dans les laboratoires de forensique numérique, l'équipement est utilisé pour rechercher des zones d'intérêt dans les designs des puces électroniques. Le but est d'avoir une meilleure connaissance de la structure du composant, pour identifier certaines fonctionnalités, par exemple localiser des plans mémoires. Pour ces observations, il faut préalablement préparer l'échantillon mécaniquement ou chimiquement afin d'exposer le

niveau de piste à observer, comme le montre la Figure 1.21. En effet, la poire d'interaction étant de faible profondeur, il ne sera pas possible d'observer un niveau de métal positionné sous un autre. De plus, la résolution de l'équipement permet d'observer en détail les pistes d'un échantillon, cependant l'observation intégrale de la surface d'une puce représente une quantité importante de données à pouvoir stocker et manipuler. Prenons l'exemple d'un échantillon observé avec une résolution de 1nm/pixel. Pour une puce mesurant 1cm par 1cm, il faudra enregistrer une matrice de 10millions par 10millions de pixels. Cette acquisition n'étant pas réalisée en une fois, la surface sera découpée en images de taille moindre, qu'il faudra ensuite rassembler dans l'analyse.

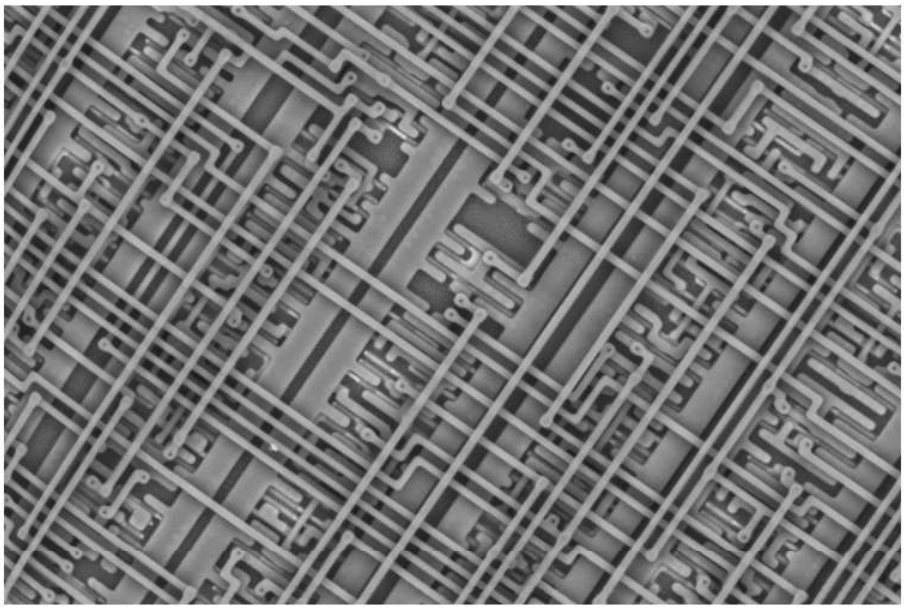


FIGURE 1.21 – Observation au microscope électronique à balayage d'un composant électronique après gravure de l'isolant [22]

1.2.1.5 Interféromètre optique ou laser

1.2.1.5.1 Principe de fonctionnement

Le principe de l'interférométrie est basé sur la combinaison des ondes, qu'elles soient lumineuses ou lasers. En effet, la lumière ou un laser est une onde d'une longueur et d'une amplitude propre. Deux ondes de même nature (c'est-à-dire deux ondes de même longueur et de même amplitude) peuvent interagir entre elles. Lorsqu'elles sont synchronisées, leurs amplitude s'additionnent, comme le montre la partie gauche de la Figure 1.22. À l'inverse, si les ondes sont en opposition de phase, elles s'annulent, comme le montre la partie droite de la Figure 1.22.

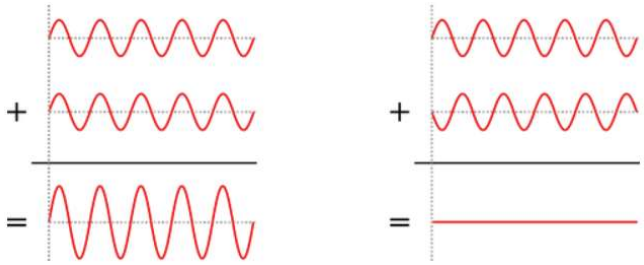


FIGURE 1.22 – Schéma de principe de combinaison des ondes lumineuses [23]

Pour l'utilisation du principe de l'interférométrie dans un équipement d'observation, un faisceau de lumière sera divisé en deux par un séparateur de faisceau (c'est-à-dire un miroir partiellement réfléchissant), comme le montre la Figure 1.23. Un des deux faisceaux va être dirigé vers l'objectif, tandis que l'autre va être projeté pour se réfléchir sur l'échantillon, avant de remonter au capteur (ou sur l'objectif).

Dans un microscope interférométrique, il s'agit de comparer les différences des phases entre l'onde qui a un chemin direct et celle qui se réfléchit sur l'échantillon. Lorsque l'équipement est réglé sur la surface de l'échantillon, le chemin entre le faisceau direct et celui réfléchi sont les mêmes, donc les ondes s'additionnent. Cela implique qu'une différence de hauteur sur l'échantillon crée proportionnellement un déphasage des ondes, et donc un changement d'aspect sur l'image observée. La Figure 1.24 présente un microscope utilisant le principe de l'interférométrie pour effectuer des mesures sur des composants électroniques.

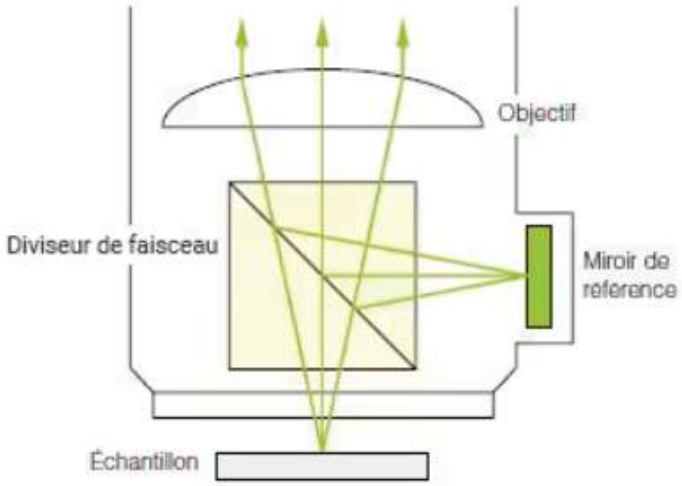


FIGURE 1.23 – Schéma de principe de fonctionnement d'un microscope interférométrique [24]

1.2.1.5.2 Application de l'équipement

Dans les laboratoires d'analyse de défaillance, les microscopes interférométriques sont utilisés pour effectuer des mesures de planarité ou de rugosité des échantillons. Ces mesures sont généralement effectuées durant les phases de conception ou de production sur des composants prélevés directement sur les chaînes. Il s'agit de procéder à des mesures pour valider qu'une surface est aussi plane que souhaitée ou que la rugosité résiduelle après un polissage soit conforme. La Figure 1.25 présente l'observation d'une différence de planarité sur un composant électronique, faite avec un microscope interférométrique. Dans cet exemple, il y a une différence de planarité entre le centre et les bords de l'image.

FIGURE 1.24 – Microscope interférométrique de la marque Bruker modèle contourx 100 [25]

1.2.1.6 Microscope confocal

1.2.1.6.1 Principe de fonctionnement

Le principe d'un microscope confocal est basé sur la mesure des points focaux d'un échantillon. En optique, lorsque la lumière traverse une lentille, celle-ci se retrouve focalisée en un point. Ce point de focalisation représente le point de netteté de l'élément observé. Lorsque l'échantillon sort de ce plan, il devient de plus en plus flou. Sur un microscope classique, l'objectif est de régler la hauteur de l'échantillon pour garder la surface à observer sur le plan focal de la colonne optique. Un microscope confocal utilise ce principe pour effectuer des mesures de hauteur.

La Figure 1.26 présente le chemin optique dans un microscope confocal. Une source émet une onde lumineuse, qui traverse un miroir, suivie d'une lentille qui la focalise sur l'échantillon. La lumière se réfléchit sur l'échantillon pour revenir au miroir, puis elle est

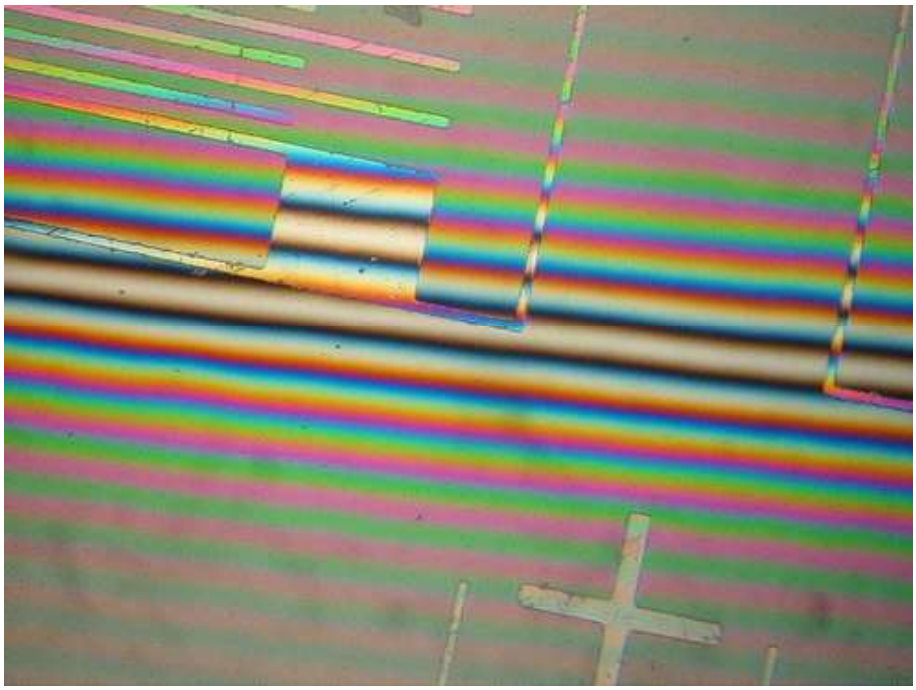


FIGURE 1.25 – Exemple d'image sur un composant électronique avec un microscope interférométrique [26]

redirigée vers un capteur. Si l'échantillon est correctement positionné sur le plan focal de la colonne, le faisceau de lumière qui arrive au capteur est correctement focalisé. À l'inverse, si l'échantillon n'est pas aligné avec le plan focal, le faisceau de lumière qui arrive au capteur est défocalisé. Le capteur n'enregistre pas l'image directement, mais une information de focalisation à son niveau.

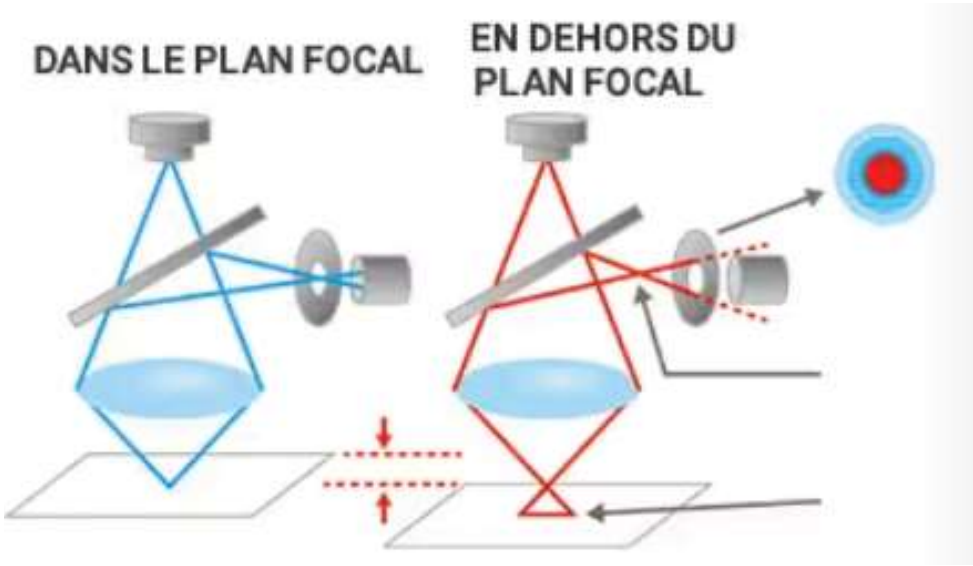


FIGURE 1.26 – Schéma de fonctionnement d'un microscope confocal [27]

La Figure 1.27 montre la composition d'un microscope confocal. Le microscope présente les mêmes éléments qu'un microscope optique, mais il possède également un capteur, sous forme d'une matrice, et une platine motorisée permettant de faire les observations de hauteur. Pour effectuer cette mesure, l'utilisateur positionne l'échantillon et règle la hauteur de base. Ensuite, il définit une plage de hauteur à balayer (axe Z), qui va être parcourue durant l'acquisition. Le microscope effectue donc le balayage en Z et sauvegarde la valeur pour la focalisation optimale pour chacun des pixels. Cela produit une cartographie en dégradé de couleur en fonction des hauteurs des éléments.

FIGURE 1.27 – Microscope confocal de la marque ZEISS modèle LSM900 [28]

1.2.1.6.2 Application de l'équipement

Dans le domaine de l'électronique, l'équipement est utilisé, par les laboratoires d'analyse de défaillance, pour mesurer la hauteur des composants électroniques. Lors des phases de conception ou de qualification, des échantillons sont prélevés des chaînes de production puis mesurés pour relever les hauteurs des couches internes. Le microscope confocal est donc utilisé pour réaliser ces mesures, comme le montre des exemples sur la Figure 1.28.

FIGURE 1.28 – Exemple d'acquisitions réalisées avec le microscope confocal marque Keyence modèle VK-X3000 [29]

1.2.1.7 Scanner à balayage acoustique (SAM)

1.2.1.7.1 Principe de fonctionnement

Le scanner à balayage acoustique est une technique d'observation qui permet de déterminer la présence d'air dans un package de composants, en utilisant la propagation d'une onde acoustique. L'échantillon est immergé dans l'eau tandis qu'un transducteur projette une onde acoustique de l'ordre de 10 à 100MHz. L'onde émise par le transducteur se propage dans l'eau, puis dans le package du composant, jusqu'à se réfléchir sur des éléments plus denses (par exemple un support en cuivre, une puce en silicium, des broches de composants). Ce changement de surface n'a qu'une faible incidence sur la forme de l'onde, comme le montre la Figure 1.29. À l'inverse, lorsque de l'air est présent dans le package, celle-ci à la propriété d'inverser l'onde, permettant à l'équipement de la détecter.

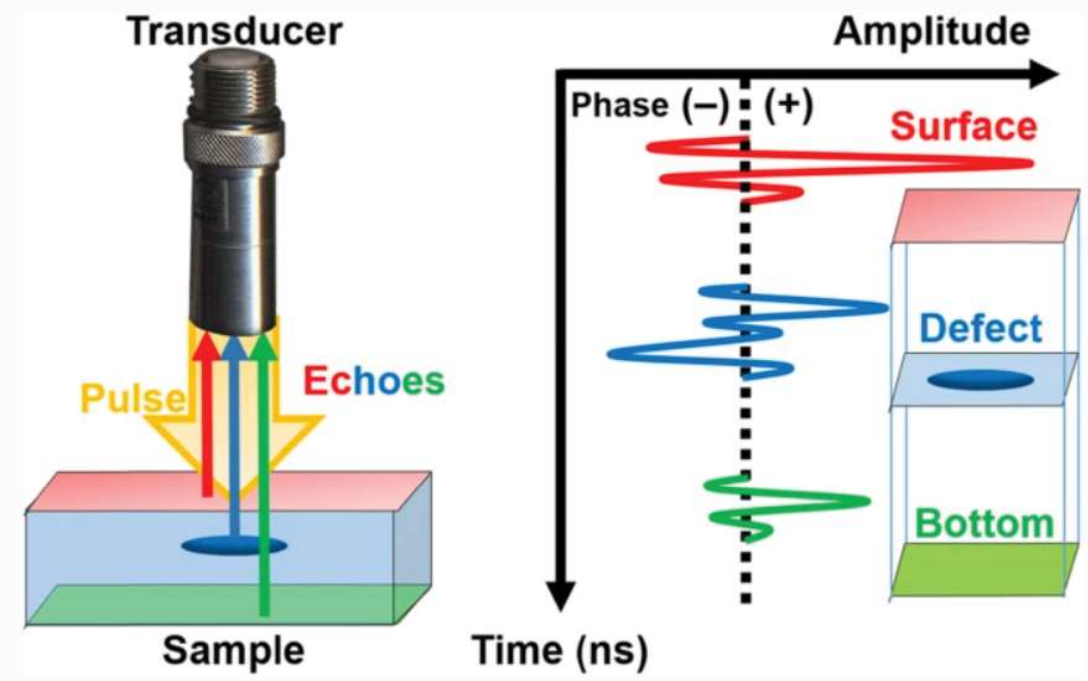


FIGURE 1.29 – Schéma de fonctionnement d'un SAM [30]

Un SAM est composé d'un bac d'eau permettant d'accueillir un ou plusieurs échantillons à observer (Figure 1.30). Un bras motorisé mobile sur les axes X et Y déplace la tête de mesure, elle-même mobile sur l'axe Z. La mobilité de la tête sert à descendre le transducteur dans l'eau, puis au réglage de la hauteur par rapport à l'échantillon. Le but est d'obtenir une forme d'onde optimale pour effectuer les mesures, c'est-à-dire avec des pics d'amplitude significatifs. La mobilité des axes X et Y sert au balayage de la sonde sur les échantillons, produisant une cartographie.

1.2.1.7.2 Application de l'équipement

Le SAM est utilisé dans les laboratoires d'analyse de défaillance pour la recherche et le diagnostic de plusieurs défauts structurels [140]. C'est un moyen de diagnostic non-invasif pour observer la propagation de l'humidité dans le composant. Lorsqu'un composant a subi un stress mécanique ou thermique important, celui-ci peut être déformé, et des poches d'air peuvent se créer. Ces poches d'air, appelées également délaminations, sont observables avec le SAM, selon le principe présenté précédemment. Dans un processus de qualification des composants électroniques, il est important de détecter les déformations mécaniques ou thermiques et leurs effets. En cours d'utilisation dans une application, si une fissure se crée dans le package, de l'eau peut pénétrer et remplacer l'air. De même, une délamination peut favoriser la présence de condensation d'humidité à la surface de la puce en silicium. Dans les deux cas, la présence d'eau dans le package peut créer des

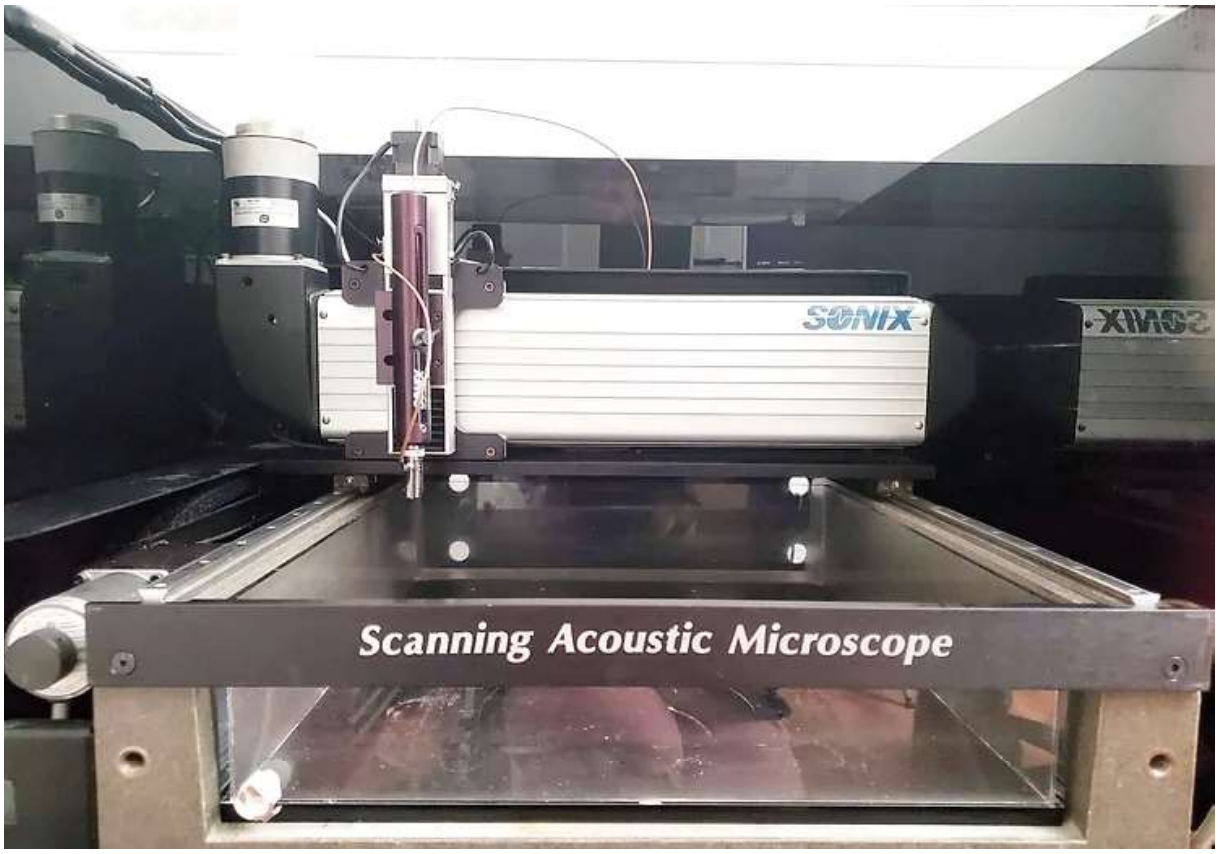


FIGURE 1.30 – Intérieur de la chambre d'un SAM : présence du transducteur normalement plongé dans l'eau [31]

corrosions d'éléments tels que les fils de bondings en cuivre ou des pistes situées à la surface de la puce. Pour limiter les risques, il est important de détecter la présence d'air dans le package à l'aide d'équipements tels que le SAM. La Figure 1.31 présente une image produite avec un SAM sur une carte électronique, à deux focalisations différentes. Sur l'image de gauche, il est possible d'observer la surface des composants, alors que sur l'image de droite, la focalisation est faite dans le package. La vue de l'intérieur du package permet d'identifier une délamination dans un des composants.

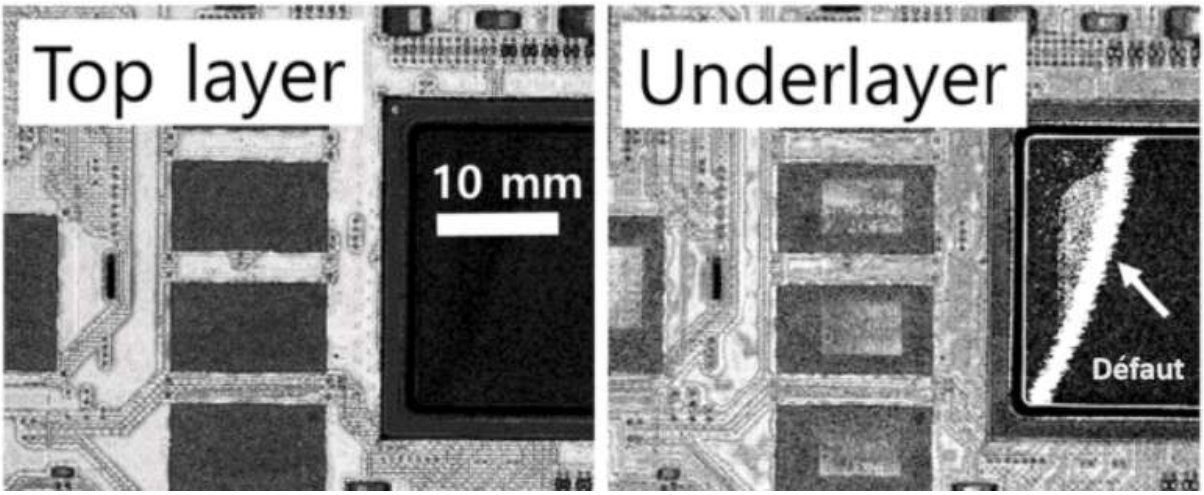


FIGURE 1.31 – Exemple d'acquisition avec un SAM sur une carte électronique [30]

1.2.1.8 Caméra thermique

1.2.1.8.1 Principe de fonctionnement

Les caméras thermiques sont basées sur la captation des ondes dans le spectre de l'infrarouge. Ces ondes possèdent une longueur comprise entre 0,7mm et 1mm, c'est-à-dire dans une bande de fréquences contiguë à celle du visible, comme le montre la Figure 1.32.

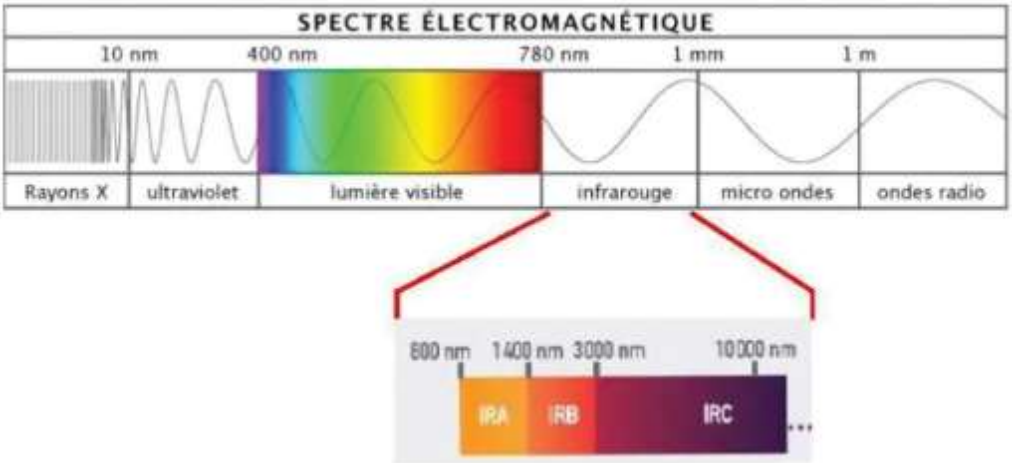


FIGURE 1.32 – Positionnement de l'infrarouge dans le spectre [32]

Les caméras thermiques sont équipées de capteurs sous la forme de matrices sensibles à la longueur d'onde de l'infrarouge. Après réception par la matrice, une cartographie est reconstituée avec un logiciel, ce qui permet d'afficher avec un dégradé de couleur le résultat de la captation. Cette couleur est arbitraire mais traditionnellement il s'agit d'un spectre du bleu au rouge, où le bleu représente les zones froides et le rouge les zones chaudes. La qualité de la cartographie dépend de plusieurs paramètres :

— Le nombre de cellules présentes sur la matrice : Pour une taille de cartographie fixe, plus il y a de cellules sur une même ligne ou une même colonne, plus l'information sera précise.
— La taille de la matrice : Plus l'envergure de la matrice sera grande, plus elle aura de chance de capter de l'information. Par conséquent, plus la cartographie finale sera précise.
— Le taux de rafraîchissement : Il s'agit du temps nécessaire au capteur pour extraire le contenu de la matrice et permettre une nouvelle acquisition. Un capteur rapide donnera un taux de rafraîchissement important et donc une observation quasi continue, limitant la perte des informations.

Par rapport aux paramètres énoncés, il existe différentes gammes de caméras thermiques, débutant par des modèles entrée de gamme comme la VOLTCRAFT WBP120 (Figure 1.33a) pour un budget d'environ 500€. Il est possible de retrouver un modèle milieu de gamme, comme la caméra FLIR ETS320 (Figure 1.33b), pour un budget de 5000€. Enfin, la caméra FLIR T865 (Figure 1.33c) est un modèle haut de gamme, avec son budget de 30000€. En complément des informations liées à la cartographie thermique, certaines caméras peuvent intégrer une caméra optique en option. Cette caméra permet de superposer la cartographie thermique à l'image optique, ce qui aide l'utilisateur à identifier les zones d'intérêt.

(a) Caméra entrée de gamme VOLTCRAFT WBP-120 [141]

(b) Caméra milieu de gamme FLIR ETS320 [142]

(c) Caméra haut de gamme FLIR T865 [143]

FIGURE 1.33 – Exemple de caméras thermiques de différentes gammes

1.2.1.8.2 Application de l'équipement

Dans le cadre des travaux sur des systèmes d'électroniques, les caractéristiques recherchés pour la caméra sont le nombre de cellules de la matrice, et le taux de rafraîchissement. En effet, les éléments constituant une carte électronique peuvent être de faible dimension, comme par exemple une capacité au format 0201 qui mesure 2mm

par 1mm. Ces petits éléments doivent pouvoir être observés avec la caméra thermique, d'autant plus que les capacités en question servent au découplage des alimentations. Elles servent donc de fusibles pour éviter la dégradation des composants vitaux. De plus, lorsqu'une capacité est en défaut, les composants peuvent détecter l'anomalie et couper immédiatement l'alimentation. D'un point de vue thermique, il s'agit de changement d'états observables pendant seulement quelques millisecondes. Ces effets transitoires rapides et d'une faible dimension doivent être observés pour un diagnostic efficace des experts en forensique numérique. La Figure 1.34 présente le résultat de l'utilisation d'une caméra thermique sur une carte mère d'iPhone. Il s'agit d'une vue hors fonctionnement qui illustre le besoin d'une bonne résolution de caméra par rapport à la taille des éléments observés.

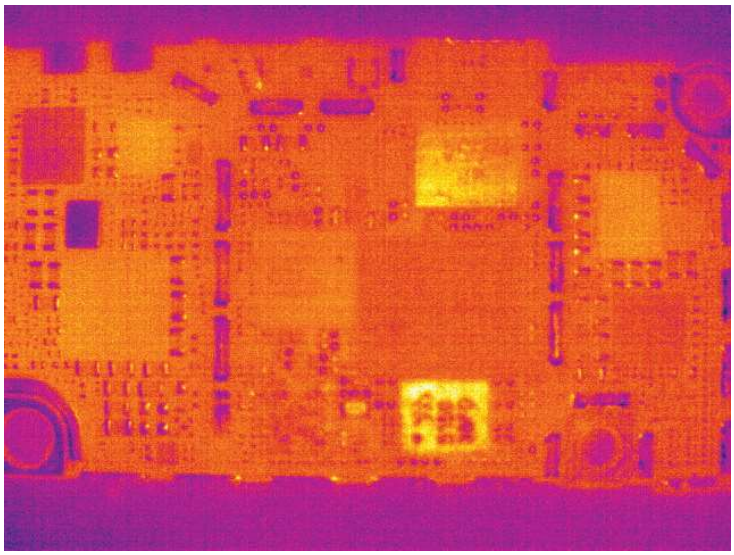
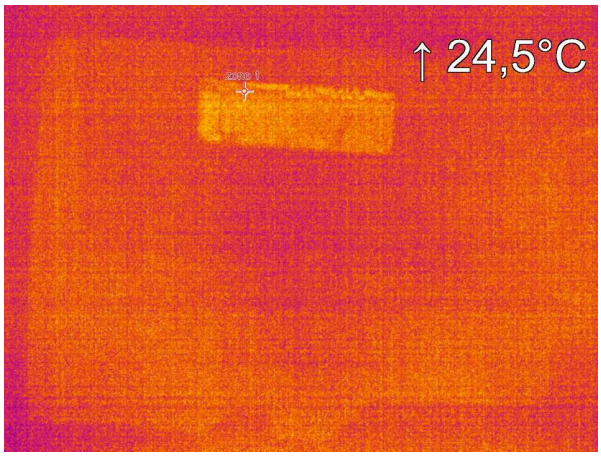
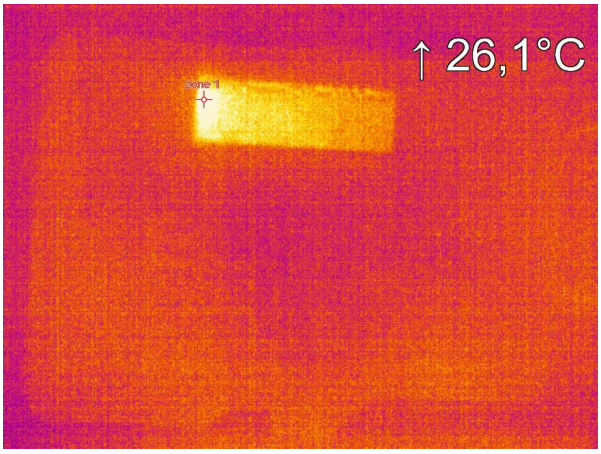


FIGURE 1.34 – Visualisation de la carte mère d'un iPhone pour de la recherche de défaut

Le Figure 1.35 illustre l'utilisation d'une caméra thermique pour l'observation des effets transitoires dans un système électronique. Pour cet exemple, une carte microSD est mise sous tension puis initialisée. Sur la Figure 1.35a, il est possible de distinguer la forme de la carte ainsi qu'une zone rectangulaire correspondant à une élévation de température du contrôleur intégré. À la suite de l'initialisation, la carte est utilisée avec la lecture d'un fichier. Cette action est observable thermiquement sur la Figure 1.35b par une intensification de la couleur du rectangle. Cela signifie donc que le contrôleur situé à cet emplacement effectue beaucoup plus d'opérations, entraînant une élévation de sa température.



(a) Carte microSD après mise sous tension : contrôleur présentant une faible activité, avec une chauffe homogène



(b) Carte lors de son utilisation : contrôleur présentant une forte activité, particulièrement sur sa partie gauche

FIGURE 1.35 – Utilisation de la caméra thermique pour visualiser les effets transitoires internes d'une carte microSD

1.2.2 Préparation d'échantillons

1.2.2.1 Chimie humide

1.2.2.1.1 Principe de fonctionnement

L'utilisation de chimie humide est la technique la plus invasive des laboratoires pour atteindre des éléments dans un composant électronique. Cette technique est à utiliser avec précaution car elle présente de forts risques de dégradation des fonctions du composant, pouvant le rendre inopérant. De plus, la chimie humide est dite anisotrope, ce qui signifie que, contrairement à d'autres techniques, l'attaque se produit dans toutes les directions sur l'échantillon, pouvant engendrer des infiltrations. Enfin, le dernier aspect de la chimie humide est l'in-homogénéité de la gravure qui doit être prise en considération. Pour une couche uniforme, l'attaque ne se fera pas nécessairement à la même vitesse sur l'ensemble de la surface. D'autres paramètres peuvent influencer la gravure, tels que l'état de la surface, la température locale, ou la densité des éléments environnants.

Les manipulations de produits chimiques dans un cadre professionnel doivent se faire dans le respect de plusieurs articles du Code du Travail (article L4412-1 [144] et article R4412-1 à 160 [145]). Les réglementations imposent aux entreprises de mettre en place des moyens de protection pour leurs employés. Les manipulations doivent être faites, si possible, dans une cabine avec une aspiration et des filtres adaptés. Les déchets doivent également être collectés et évacués en respectant des protocoles et une traçabilité. L'ensemble des règles conduisent à disposer, dans les laboratoires d'analyse de défaillance ou de forensique numérique, d'un espace dédié à la manipulation des produits comme

celui présenté sur la Figure 1.36.

FIGURE 1.36 – Exemple d'espace de manipulation chimique pour le traitement des composants électroniques

1.2.2.1.2 Application de l'équipement

Nous avons regroupé dans le Tableau 1.2 les produits de référence utilisés pour mener des attaques chimiques sur les composants électroniques [4].

Tableau 1.2 – Tableau des produits et mélanges en fonction des matériaux à attaquer

Produit/mélange	Température	Éléments attaqués
Acide nitrique fumant 99%	90°C	Résines, Vernis, Cuivre
Acide nitrique fumant 99% (60%) Acide sulfurique (40%)	40°C	Résines, Vernis
Acide nitrique 65%	Ambiant	Cuivre
Acide chlorhydrique 30%	Ambiant	Aluminium
Acide fluorhydrique 45%	Ambiant	Oxyde de Silicium
Acide nitrique 65% (50%) Acide chlorhydrique 30% (50%)	60°C	Tout métaux (sauf l'or)

Une des applications les plus courantes est le retrait de la résine des composants. D'après le Tableau 1.2, il est possible d'utiliser de l'acide nitrique fumant 99%. Ce produit est très agressif pour les éléments en cuivre, dont les packages peuvent être composés de cuivre. Pour garder le composant fonctionnel, il peut être intéressant de mélanger l'acide

4. Le choix des produits ou mélanges exposés dans le Tableau 1.2 provient de l'analyse de plusieurs articles. Les produits ont été testés en faisant évoluer les paramètres (par exemple : les concentrations, les températures, les temps d'exposition,). Le Tableau 1.2 regroupe donc les produits et mélanges que j'utilise dans mes opérations en fonction de ces résultats

nitrique fumant 99% à hauteur de 60% avec 40% d'acide sulfurique. En effet, l'acide sulfurique génère du sulfate de cuivre, difficilement attaqué par l'acide nitrique, créant ainsi une couche de passivation sur les surfaces sensibles.

L'application de l'acide peut se faire en bain, en plongeant l'échantillon entièrement. Cette attaque aura l'avantage d'être rapide, mais difficilement contrôlable. Ainsi, pour une approche plus précise, la dépose du produit en goutte à goutte est préférable. Un exemple d'ouverture chimique avec de l'acide nitrique fumant 99% déposé en goutte à goutte est visible sur la Figure 1.37.

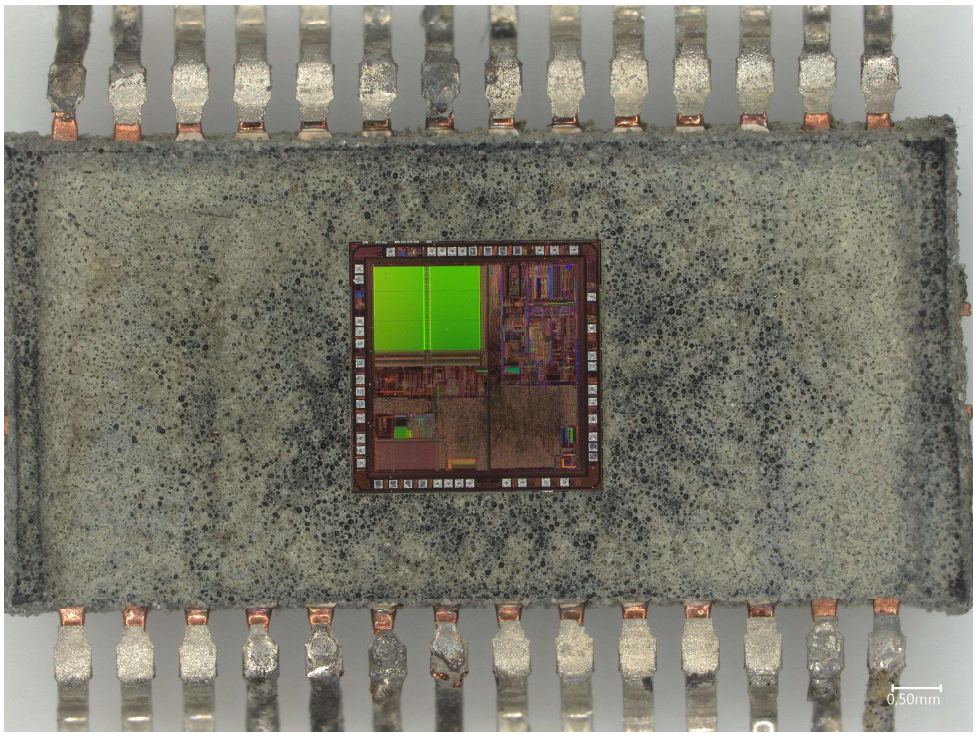


FIGURE 1.37 – Exemple d'ouverture chimique pratiquée sur un PIC16

Pour arriver à ce résultat, il faut déposer des gouttes d'une solution d'acide sur une zone précise du composant, ce qui va dissoudre la résine du boîtier. La goutte se chargeant rapidement en résine, elle ne doit pas stagner sur l'échantillon. Il faut donc prévoir un écoulement de l'acide dans un récipient de récupération. Cette opération est délicate mais permet une gravure avec un contrôle visuel permanent. Le résultat, même s'il est plus long et contraignant pour l'opérateur, est donc beaucoup plus fiable qu'une attaque par bain, si l'objectif est de garder le composant fonctionnel.

1.2.2.2 Laser d'ablation

1.2.2.2.1 Principe de fonctionnement

Le laser d'ablation est un équipement basé sur une source laser, utilisée pour usiner de la matière. Un laser est une onde unidirectionnelle sous forme d'une sinusoïde caractérisée par sa longueur d'onde et sa puissance. Il existe un nombre limité de lasers d'ablation disponibles sur le marché européen. Les fabricants sont Control Laser Corporation (CLC) (Figure 1.38a) et Digit Concept (Figure 1.38b).

(a) Laser de la marque CLC modèle FALIT [146]

(b) Laser de la marque Digit Concept modèle SESAME [147]

FIGURE 1.38 – Lasers d'ablation conçus pour usiner les composants électroniques

Les deux équipements sont basés sur la même conception. Ils utilisent une source laser d'une longueur d'onde fixe, avec un spot d'un diamètre d'environ 50μm. Le spot laser est dirigé par un jeu de miroirs pour être projeté sur l'échantillon sur la zone souhaitée. Lors d'une ablation laser, une faible quantité de matière est retirée. La profondeur de la gravure n'est pas facilement contrôlable, car elle dépend de la nature du matériau usiné. Pour effectuer une gravure plus profonde qu'une impulsion le permet, il faut en faire plusieurs. Par conséquent, une gravure se fait par une succession de tirs laser à une fréquence réglable. L'intervalle entre chaque tir est important, car pour éviter la surchauffe de la zone autour de l'ablation, il faut laisser à la matière le temps de refroidir. Les équipements effectuent donc plusieurs balayages d'une même zone avec un temps de repos entre chaque passage.

Le logiciel associé permet de paramétrer le type d'ablation à effectuer, c'est-à-dire la taille et la position de l'ablation, la puissance du laser et le nombre de passage du laser sur la zone. Pour positionner la zone théorique de l'ablation sur l'échantillon, les équipements disposent d'une caméra et d'un laser de visé.

1.2.2.2.2 Application de l'équipement

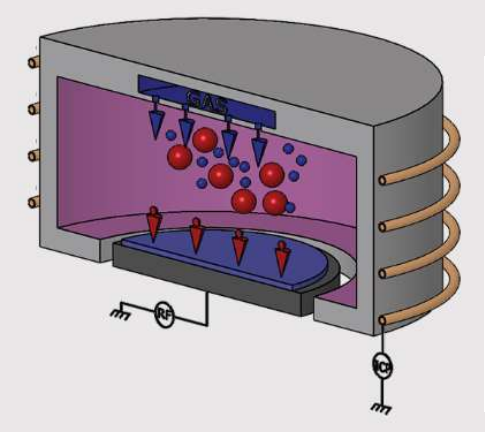
La longueur d'onde du laser provenant de la source est un paramètre important pour les applications sur des composants électroniques. Pour une ablation optimale sur de la résine époxy et les vernis, il est préférable d'utiliser un laser utilisant la longueur d'onde 1064nm, tandis que pour les pistes de cuivre, il est préférable d'utiliser la longueur d'onde 512nm. Le choix de la longueur d'onde optimale pour un matériau ne signifie pas que le laser n'aura aucun effet sur les autres matériaux. Ainsi, le laser 1064nm peut graver le cuivre, si la puissance est suffisante. Cependant, la gravure ne sera pas aussi rapide que sur les autres matériaux. Il y a tout de même un critère important à prendre en compte lors d'une tentative de gravure, il s'agit de l'opacité de la matière. Pour que le laser ait un effet, la matière doit absorber l'onde. Les matériaux transparents comme le verre ne subiront pas les effets du laser, car ils laisseront passer l'onde jusqu'à la couche inférieure. Le coefficient d'absorption de la matière cible sera donc capital pour une efficacité optimale dans la longueur d'onde d'utilisation du laser. Notons qu'il existe des modèles de laser qui offrent la possibilité d'utiliser plusieurs longueurs d'onde laser au sein d'un même appareil. Ce phénomène peut être dangereux lorsqu'il est question d'utiliser cet équipement à proximité d'une puce de composant. En effet, le laser est destructif pour les transistors, car il peut influencer leurs programmations ou les altérer. Le retrait de la résine à la surface du composant (Figure 1.39) se fait avec précaution, en se tenant à distance de la puce électronique. La puissance laser déposée au niveau du transistor est suffisante pour modifier le niveau de Fermi et faire passer les électrons de l'atome de silicium dans la bande de conduction. Une atteinte directe du laser sur le silicium ne permet donc plus de garantir l'intégrité des données ; ce qui n'est pas permis pour une utilisation judiciaire. La fin de la gravure doit être effectuée par une autre technique, par exemple en chimie humide.

FIGURE 1.39 – Exemple de gravure laser pour amincir la résine à la surface d'une carte microSD

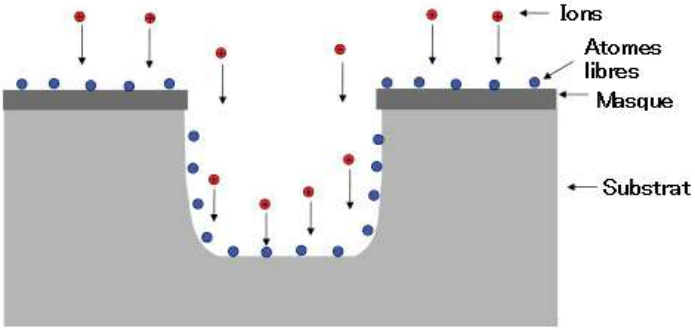
1.2.2.3 Graveur plasma

1.2.2.3.1 Principe de fonctionnement

Le graveur plasma est un équipement utilisant la ionisation d'un gaz pour effectuer une gravure. L'échantillon se situe entre une anode et une cathode dans une chambre sous vide (Figure 1.40a). Un champ électrique circule depuis la cathode en direction de l'anode, sur laquelle est positionné l'échantillon. Pour effectuer la gravure, un gaz est introduit par petite quantité dans la chambre. Il est ionisé par le champs électrique, et les ions sont projetés par le champs en direction de l'échantillon. Les matériaux de surface exposés aux ions sont donc gravés lentement.



(a) Intérieur d'une chambre de plasma [33]



(b) Effets de la gravure [148]

FIGURE 1.40 – Schéma de principe de fonctionnement d'un plasma

Le schéma de la Figure 1.40b illustre le principe de la gravure par plasma. Les ions sont projetés sur l'échantillon verticalement, créant une gravure isotrope. Cette propriété peut avoir un intérêt, car il est possible de masquer volontairement une zone qui ne sera pas gravée. Cependant, cet équipement peut créer des défauts de gravure, si des particules sont présentes à la surface de l'échantillon. Il faut donc bien nettoyer l'échantillon avant de débuter une gravure. L'isotropie de la gravure ainsi que sa vitesse et sa sélectivité peuvent être travaillées en jouant sur le paramétrage de la machine. Il est possible de faire évoluer la puissance du champ électrique, la quantité et la nature des gaz, et de réguler la température de l'échantillon pendant la gravure. Le réglage de ces paramètres favorisera par exemple l'élimination des résidus de gravure et le redépot de ceux-ci. Enfin, il peut être intéressant de jouer sur la nature du gaz utilisé pour influer sur la sélectivité des matériaux à retirer. Par exemple, les gaz fluorés servent à graver le silicium ou son oxyde, alors que les gaz chlorés sont plus efficaces sur le cuivre.

FIGURE 1.41 – Exemple de machine de gravure plasma de la marque Corial [33]

La Figure 1.41 présente un équipement de gravure plasma de la marque Corial. Il est composé d'une chambre de gravure pour positionner l'échantillon. Il dispose également d'une caméra sur le dessus pour observer l'avancement de la gravure et la contrôler.

1.2.2.3.2 Application de l'équipement

Dans les laboratoires d'analyse de défaillance et de forensique numérique, les équipements de gravure plasma sont utilisés pour préparer les échantillons à des fins d'observation. Ils servent dans les phases de qualification des composants pour valider la conformité de fabrication des structures internes. Ils servent également à retirer progressivement des couches d'un composant en défaut. Ce procédé sert à rechercher et localiser un défaut dans les différentes couches, pour en déduire son origine. La Figure 1.42 présente l'état de surface d'un composant après sa gravure. Il est possible d'observer, au microscope électronique à balayage (section *Microscope électronique à balayage (MEB)*), la disposition des différents niveaux de pistes métalliques d'un composant électronique, après le retrait de l'isolant qui les englobait.

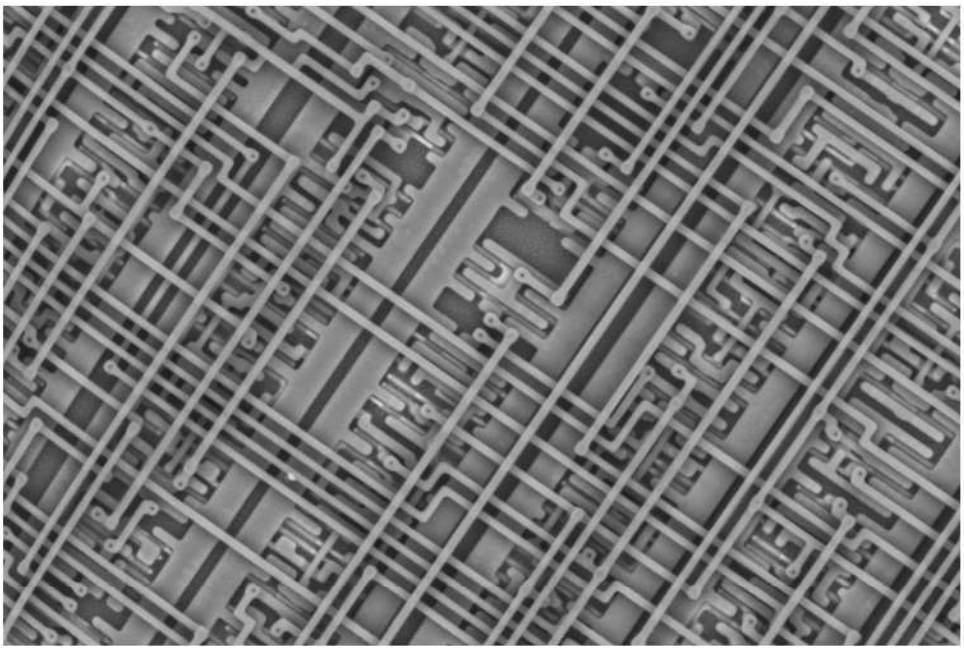


FIGURE 1.42 – Exemple de pistes d'un composant électronique vues au microscope électronique à balayage [22]

1.2.2.4 Microscope ionique focalisé (FIB)

1.2.2.4.1 Principe de fonctionnement

Le microscope ionique focalisé est un équipement qui combine plusieurs principes préalablement développés sur d'autres équipements. Il peut être résumé par l'utilisation d'un plasma de gravure combiné à un microscope électronique à balayage (MEB). Le principe du plasma a été développé dans la section *Graveur plasma*. L'échantillon est gravé par la projection d'ions provenant de la ionisation d'un gaz. À la différence d'un plasma classique, l'ensemble de l'échantillon n'est pas exposé aux ions, il s'agit uniquement d'un faisceau condensé couvrant une surface nanométrique. La focalisation et la visée sont réalisées sur le même principe que pour le microscope électronique à balayage, présenté dans la section *Microscope électronique à balayage (MEB)*, mais avec la petite distinction que les électrons secondaires ne sont pas engendrés par des électrons primaires. En effet, l'observation par ion se fait par implantation des ions gallium à la surface de l'échantillon, qui a pour effet d'arracher des atomes de la surface. Ce phénomène se traduit donc par une observation destructrice pour l'échantillon. Pour limiter les dégradations, certains FIB sont également couplés avec une colonne MEB, dans cette configuration, l'équipement est dit *DUAL BEAM*. La colonne électronique, non destructrice, est utilisée pour la localisation et le positionnement de l'échantillon, tandis que la colonne FIB est utilisée pour réaliser les opérations de modification de l'échantillon. En complément de la colonne ionique, un injecteur est positionné proche de la surface de l'échantillon. Il a pour rôle d'introduire des éléments conducteurs dans le faisceau d'ion dans le but de créer un dépôt de matière conductrice électrique. La Figure 1.43 présente un FIB avec la colonne ionique surplombant la chambre, ainsi que les différentes caméras et injecteurs.

FIGURE 1.43 – Exemple d'un équipement FIB [34]

1.2.2.4.2 Application de l'équipement

Il existe deux utilisations principales pour un FIB. La première a été mentionnée précédemment, il s'agit de la destructivité des ions qui remplacent les atomes de surface, ce qui provoque un phénomène de gravure. Cette utilisation permet dans le cadre des travaux sur des composants électroniques, de faire des micro-sections localisées à la surface d'un échantillon. Lorsque la micro-section est réalisée au FIB, le terme de "boîte FIB" est utilisé. Le but recherché est le même que pour le polissage (voir section *Polissage*), à savoir observer ou mesurer différentes épaisseurs d'une structure. Cependant, cette opération est effectuée sur une zone contrôlée, ce qui permet de garder le reste du composant intact, donc fonctionnel. Un exemple de boîte FIB est visible sur la Figure 1.44, il s'agit d'une observation d'une spirale conductrice, ce qui permet d'effectuer une mesure et une qualification des processus de fabrication de la structure. Cette technique est largement utilisée dans les laboratoires d'analyse de défaillance lors des phases de conception des nouveaux composants.

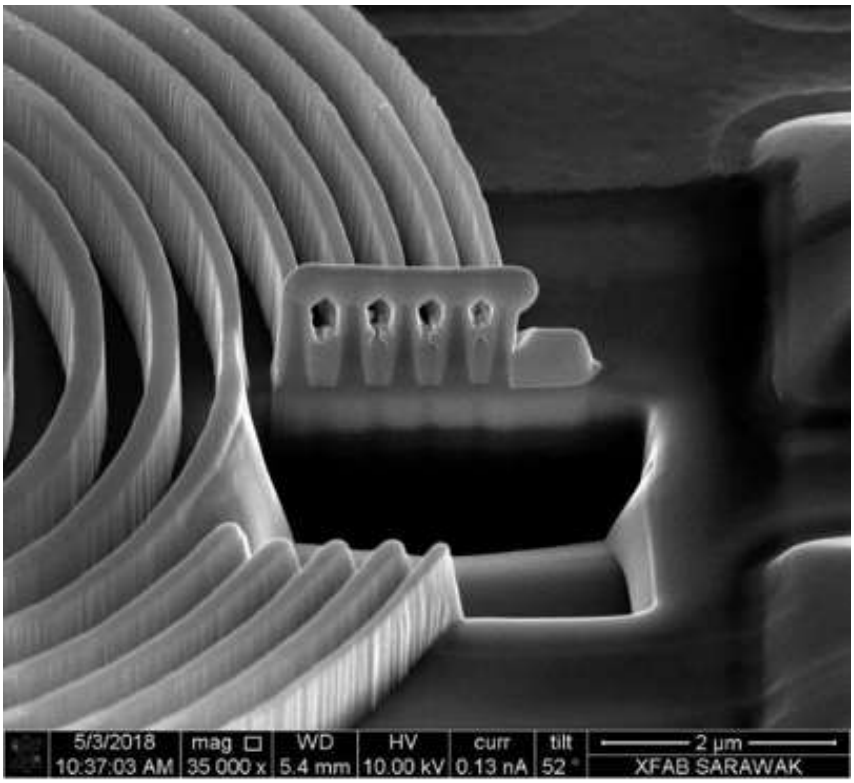


FIGURE 1.44 – Cross-section d'une spirale conductrice avec un FIB pour observer la tranche [35]

La seconde utilisation est la modification de design avec le FIB, comme le montre la Figure 1.45. Dans la présentation de l'équipement, il a été mentionné que le FIB pouvait effectuer une gravure précise avec les ions, ainsi qu'un dépôt de matière conductrice. En combinant ces deux fonctionnalités, il est possible d'effectuer des modifications directement sur les pistes d'une puce électronique. Dans un premier temps, la colonne électronique permet de repérer les pistes d'intérêt. Ensuite, une première série de gravures est réalisée pour couper les deux pistes métalliques. Pour finir, une nouvelle piste est créée par dépôt de métal entre les deux pistes. Le signal présent sur une des pistes se retrouve donc sur l'autre. Ce procédé est régulièrement utilisé dans les laboratoires d'analyse de défaillance lors de la conception d'un nouveau composant. Si une première version d'une puce est réalisée, mais qu'une erreur de design s'est produite, la fonction souhaitée peut ne pas être conforme. Plutôt que d'intégrer les corrections et de relancer une production d'un nouvel échantillon, les laboratoires effectuent directement les modifications sur l'échantillon en défaut. Pour cela, ils ont recours au FIB, dans le but d'apporter la modification, puis de la valider, avant de l'intégrer au design, réduisant ainsi les délais et les coûts de conception.

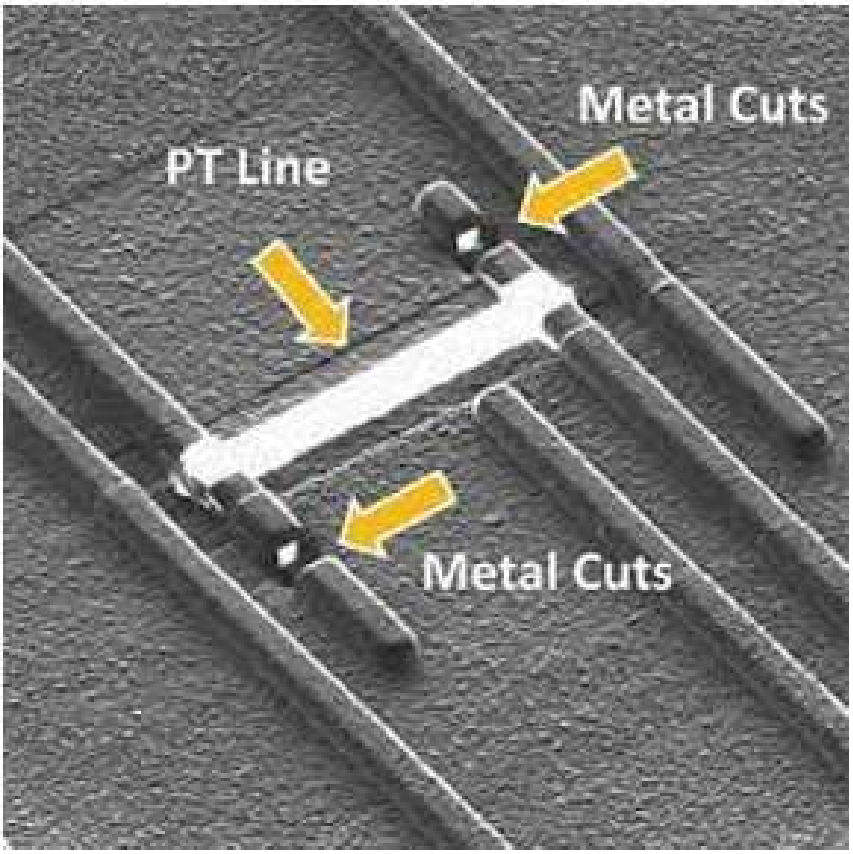


FIGURE 1.45 – Exemple de modification de design avec un FIB : 2 pistes coupées, jointes par une nouvelle piste [36]

1.2.2.5 Polissage

1.2.2.5.1 Principe de fonctionnement

Le polissage est une autre technique utilisée sur les composants électroniques durant les phases de fabrication ou d'analyse. Également appelée planarisation mécano-chimique, cette méthode permet de réduire des irrégularités de surface à l'aide d'un plateau abrasif et d'un slurry (c'est-à-dire une solution contenant des micro-particules solides principalement de la silice pour une utilisation sur de l'oxyde de silicium).

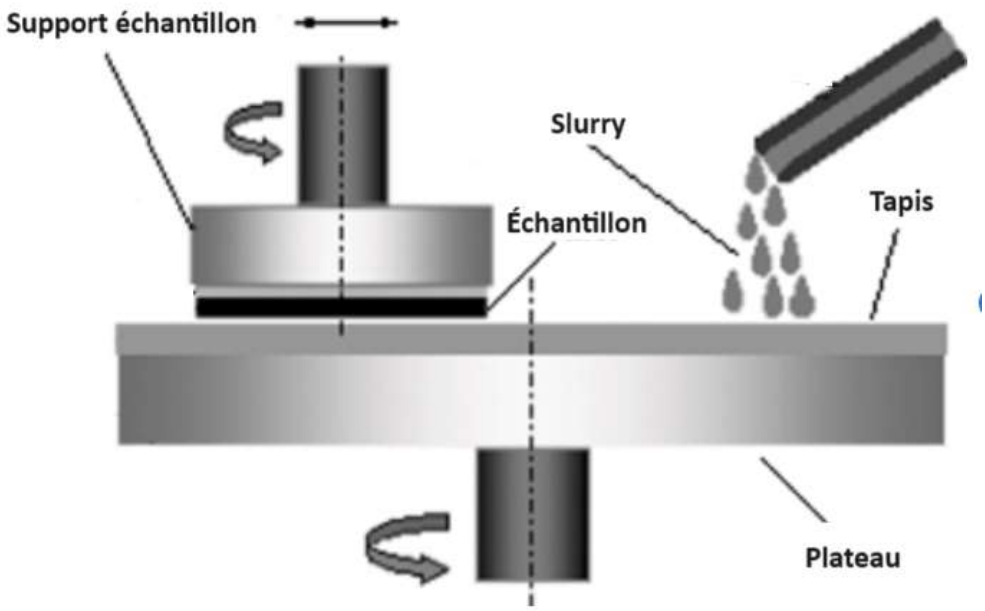


FIGURE 1.46 – Schéma de principe d'une polisseuse [37]

Comme nous le présentons sur la Figure 1.46, le support est fixé sur l'échantillon, avec la surface à polir orientée vers le bas. L'équipement dispose d'une arrivée pour les slurries qui vont dépendre de la nature du tapis de polissage utilisé. Les tapis sont posés sur un plateau qui tourne sur lui-même à 360°. Ils peuvent être en carbure de silicium (SiC) possédant des grains relativement gros et ils sont utilisés avec de l'eau comme slurry. L'eau a pour effet de refroidir la surface polie et d'évacuer les déchets. D'autres tapis neutres existent, mais ils ne servent pas directement au polissage, mais aux étapes de finition. La gravure se fait par l'effet mécanique des slurries, qui sont des particules fines en suspension. Pour un polissage optimal en réduisant les effets de sur-gravures sur les bords, plusieurs parties de l'équipement sont mobiles. Le plateau fait tourner le tapis sur lui-même, comme mentionné précédemment. Le porte échantillon comporte deux mouvements, il tourne sur lui-même et se déplace latéralement. L'ensemble des paramètres de déplacement et de rotation sont réglables, ce qui permet à l'utilisateur d'optimiser le résultat obtenu.

FIGURE 1.47 – Vue de la polisseuse Ultrapol de la marque Ultratec [38]

La Figure 1.47 présente le modèle Ultrapol du fabricant Ultratec, l'un des modèles les plus utilisés dans les laboratoires de forensique numérique. Sur cet équipement, il est possible de distinguer un panneau de commande pour le réglage des paramètres. Le plateau et le porte échantillon présentés sur la Figure 1.46 sont également présents. De plus, l'équipement possède une colonne équipée d'un écran de visé. Il s'agit d'un système de réglage de la planarité de l'échantillon. Pour que la gravure soit la plus plane possible, il faut faire en sorte que l'échantillon soit apposé parallèlement sur le plateau. Pour corriger l'inclinaison, la colonne projette un faisceau lumineux sur la face arrière de l'échantillon, qui se réfléchit et revient dans la colonne. Lors du mouvement de l'échantillon, en cas de réglage correct, le faisceau reste immobile sur l'écran. Cette fonctionnalité n'est utilisable que pour les échantillons présentant une face arrière réfléchissante, comme par exemple les substrats de silicium.

1.2.2.5.2 Application de l'équipement

Dans le domaine de l'électronique, en dehors de la chaîne de fabrication, il existe deux principales applications pour une polisseuse. La première consiste à faire un polissage parallèle. L'échantillon est positionné avec la surface vers le bas dans le but de le planariser ou d'usiner lentement la couche supérieure. Cette gravure intervient dans les laboratoires, pour la préparation des échantillons avant une phase de recherche de défauts internes. La seconde application consiste à effectuer une micro-section d'un composant. Il s'agit d'une coup perpendiculaire donnant l'accès aux éléments internes des packages ou des puces. Pour cette manipulation, l'échantillon est usiné perpendiculairement par rapport au tapis, ce qui permet de graver le composant sur la tranche. Le résultat d'une micro-section d'une puce est visible sur la Figure 1.48. Avec cette préparation, il est possible d'effectuer les mesures des épaisseurs des couches internes. Les techniciens peuvent prendre les mesures nécessaires à la validation du respect des spécifications lors de la fabrication des composants.

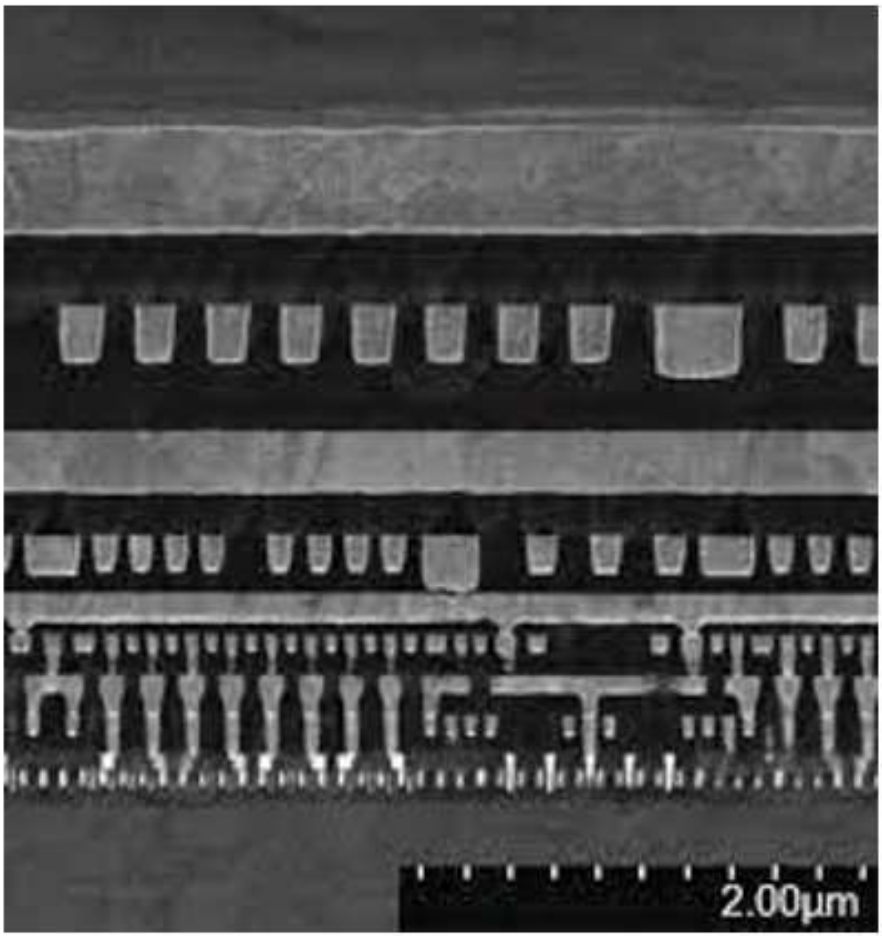


FIGURE 1.48 – Vue d'une microsection d'une puce permettant l'observation et les mesures des couches internes [39]

Pour arriver au résultat présenté sur la Figure 1.48, il faut appliquer plusieurs étapes de polissage. Dans un premier temps, il faut s'approcher de la zone d'intérêt. Cette phase n'a pas besoin d'être précise donc un tapis SiC gros grain peut être utilisé. Pour rappel, ces tapis s'utilisent avec de l'eau comme slurry. Lors de l'arrivée dans la zone d'intérêt, l'opérateur est amené à changer de disque pour réduire la taille des grains, toujours avec du papier SiC. Un défaut identifiable pour la gravure par polissage est la présence de rayures laissées par le tapis. Lors d'un changement de tapis pour un grain plus fin, les premières secondes ne consistent pas à graver mais à éliminer les rayures laissées par le tapis précédent. Pour corriger ce défaut correctement, il faut être progressif dans le choix des tapis et ne pas directement passer à un tapis à gros grains vers un tapis de finition. Comme il faut utiliser plusieurs tapis avant d'arriver aux finitions, il faudra donc anticiper cette gravure pour ne pas dépasser la zone d'intérêt.

Après l'utilisation du dernier tapis SiC, l'opérateur doit utiliser des disques de finition, qui sont des plateaux en feutre. Ils s'utilisent avec des slurries à base de particules en suspension dans un fluide. La gravure ne se fait plus avec le tapis mais avec les particules du slurry, d'où une très faible vitesse de gravure. Pour un état de surface parfait, la solution possédant les particules les plus fines s'appelle la Silice Colloïdale, dont les particules de silicium mesurent 0,04μm. Après application de cette dernière étape, il faut manipuler les échantillons avec précaution, car leurs surfaces sont très sensibles aux rayures.

1.2.3 Interaction avec la cible

1.2.3.1 Station de probing

1.2.3.1.1 Principe de fonctionnement

La station de probing est un équipement basé sur des pointes métalliques fines mobiles qui servent à s'interconnecter sur un composant ou un système électronique. Il existe plusieurs gammes de station en fonction des besoins des utilisateurs. Pour des manipulations sur des bus de communication matérialisés par des plots larges sur une carte électronique, il est préférable d'utiliser une station avec des pointes larges, qui sont assez rigides et donc peu sensibles aux vibrations. Ces pointes ont la forme d'aiguilles positionnées sur des bras articulés autour d'un cadre. L'une des stations la plus courante sous cette forme est la VR Table (Figure 1.49).

FIGURE 1.49 – Station de probing entrée de gamme de la marque VR Table [40]

Pour des opérations plus précises, des pointes fines sont nécessaires. Dans ce cas, il est préférable d'utiliser un équipement haut de gamme comme la station Cascade MPS150 présentée sur la Figure 1.50. Cette catégorie de station est équipée de micro-manipulateurs qui servent à positionner les pointes avec une précision du nanomètre. Pour faciliter les opérations, l'équipement intègre une binoculaire.

FIGURE 1.50 – Station de probing haut de gamme de la marque Cascade MPS150 [41]

Il existe deux catégories de probes utilisables sur les stations haut de gamme. Les probes passives sont des pointes, d'un diamètre pouvant descendre jusqu'à 1μm, qui s'accrochent à des bras directement reliés aux appareils de mesures. Ces probes sont conçues pour se connecter à des pistes ou à des broches de composants électroniques. Elles sont fortement déconseillées pour les puces électroniques car elles sont rigides et risques de les endommager. Pour ces manipulations, il existe des pointes souples encore plus fines (0.1μm) qui sont dites actives. Elles sont extrêmement flexibles ce qui limite les risques de dommages sur les pistes des composants. De plus, ces pointes sont équipées d'un amplificateur permettant de réduire les interférences avec les signaux circulant sur les pistes, réduisant ainsi les risques d'altération du comportement du composant.

1.2.3.1.2 Application de l'équipement

La station de probing sert à effectuer des mesures directement sur les composants électroniques. Elles peuvent intervenir à la fois durant la phase de fabrication ou d'étude des circuits électroniques. Les tests effectués en phase de fabrication consistent à poser des probes sur des plots de debug (Figure 1.51), préalablement insérés dans le design lors de la conception. Avec cet équipement, les opérateurs des laboratoires d'analyse de défaillance peuvent interagir directement avec une fonction précise d'un circuit électronique, pour effectuer des mesures, vérifier des signaux et ainsi corriger d'éventuels erreurs de conception.

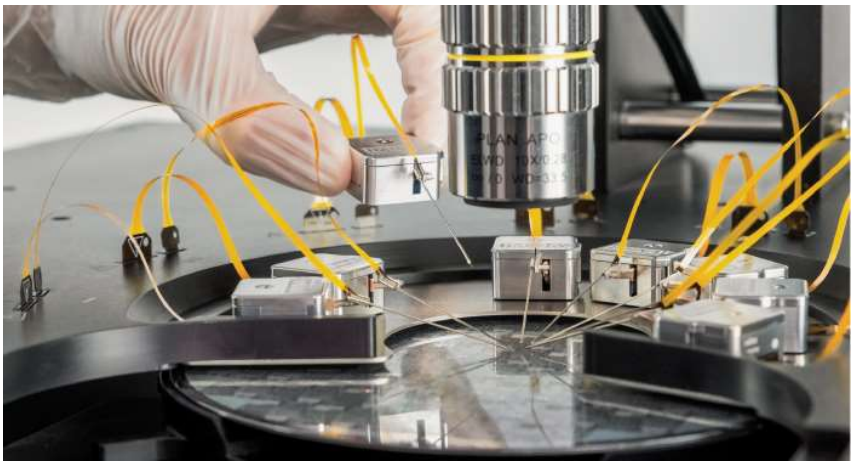


FIGURE 1.51 – Exemple de positionnement de probes sur wafer pour des mesures lors de la fabrication [41]

L'équipement peut aussi être utilisé lors de l'étude d'un système ou composant électronique. Un opérateur pose des probes sur des plots pour tenter d'acquérir des signaux provenant d'une fonction ou de communiquer directement avec cette fonction. Cette opération est faite soit sur les plots appartenant au design du circuit, soit sur les pistes de la puce, ou sur des plots créés au besoin avec l'aide d'un FIB (section *Microscope ionique focalisé (FIB)*). La Figure 1.52 présente un exemple de réalisation d'interconnexions sur une cellule mémoire.

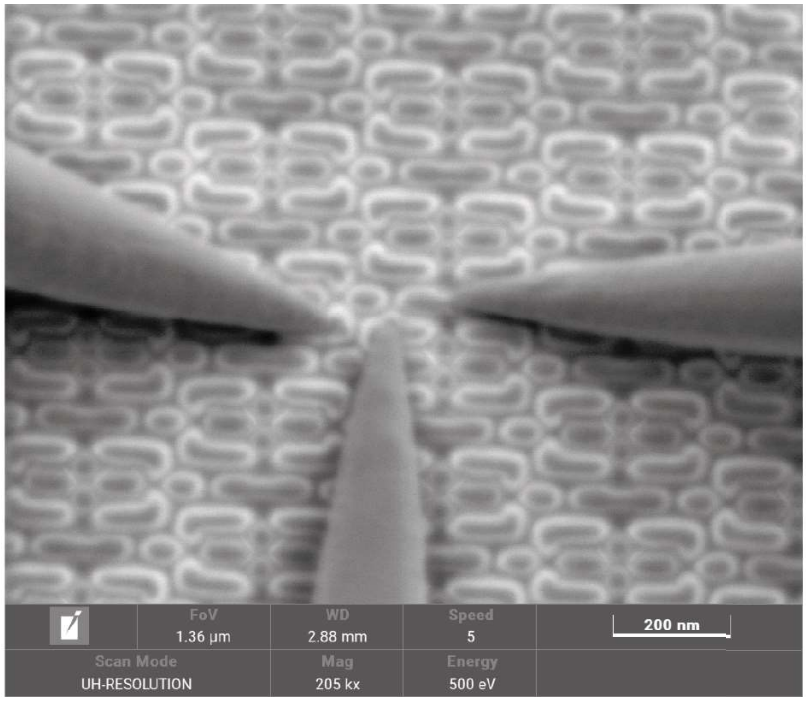


FIGURE 1.52 – Exemple de positionnement de probes sur une cellule mémoire vue au microscope électronique [42]

1.2.3.2 Box de lecture

Les box de lectures sont des outils commerciaux qui servent à lire le contenu des composants mémoires. Il existe plusieurs types de box en fonction des composants que l'opérateur souhaite relire, et rare sont les box qui permettent de lire l'ensemble des composants. Technologiquement, elles sont basées sur des cartes programmables telles que des Raspberrys [149] ou des Arduinos [150], et contiennent un script spécifiquement développé pour réaliser cette fonction. Les box les plus onéreuses peuvent être basées sur une technologie beaucoup plus polyvalente, à savoir une carte Field Programmable Gate Arrays (FPGA). Ces cartes sont des matrices de fonctions, programmables par langage Very High-Speed Integrated Circuit Hardware Description Language (VHDL) ou Verilog, alors que les autres cartes sont à base de micro-contrôleurs programmés en langage C.

Sachant que les mémoires possèdent des paramètres internes propres pour la lecture et l'écriture (c'est-à-dire : une taille de pages, une taille de blocs, une taille de secteurs), les box ont besoin de connaître ces paramètres pour effectuer la lecture. Pour celles à base de micro-contrôleurs, les configurations sont faites à partir d'une base de données contenant des identifiants propres aux puces. À l'initialisation, la box récupère la référence interne de la puce, puis la recherche dans sa base de données pour appliquer les bons paramètres de lecture. Cela signifie que si la mémoire n'est pas référencée, le composant ne pourra pas être lu. Pour des raisons commerciales, ces box sont verrouillées, empêchant un utilisateur de changer le code interne ou de programmer ses propres paramètres. Dans ce cas, les box FPGA sont beaucoup plus polyvalentes, d'où un prix plus conséquent. La Figure 1.53 présente plusieurs box de lecture à base de micro-contrôleurs disponibles sur le marché. Les développements FPGA quant à eux ne sont pas rattachés à une carte précise et peuvent être utilisés sur plusieurs plates-formes.

FIGURE 1.53 – Exemple de box commerciales permettant la lecture de composants mémoires : Riffbox [43], Easyjtag [44] et Octoplus [45]

1.2.4 Utilisation des équipements

À partir des descriptifs des différents équipements, il est possible de les regrouper dans un tableau comparatif (Tableau 1.3) résumant les fonctions et les utilisateurs classiques. Dans ce tableau, l'utilisation des équipements est comparée entre les laboratoires de forensique numérique et les laboratoires d'analyse de défaillance. Des couleurs sont attribuées pour chaque type d'utilisation :

— Vert : L'équipement est souvent utilisé et par beaucoup de laboratoires
— Rouge : L'équipement n'est pas utilisé ou à la marge
— Orange : L'équipement est rarement utilisé ou par très peu de laboratoire

Cette analyse comparative permet d'identifier les équipements les moins utilisés et de réfléchir à leur transfert pour de possibles applications. Deux équipements rarement utilisées dans les laboratoires de forensique numérique sont la caméra thermique en complément du diagnostic électrique normal et le scanner acoustique à balayage. Leurs utilisations seront étudiées dans le cadre de la création du process de diagnostic du chapitre *Protocole de diagnostic de supports MMC illustré sur carte SD*.

Tableau 1.3 – Tableau de comparaison de l'utilisation des équipements dans les laboratoires

Catégorie	Équipement	Laboratoire de forensique numérique	Laboratoire d'analyse de défaillance
Observation	Binoculaire	Inspection de la carte et des composants	
		Manipulations diverses	
	Microscope	Observation des puces	Observation des puces
	Confocal	NA	Mesure d'épaisseurs
	Interféromètre	NA	Mesure d'épaisseurs
	Rayons-X	Recherche de défauts composants ou cartes	
		Rétro-conception	
	MEB	Rétro-conception	Recherche de défauts
	SAM	NA	Recherche de délamination
	Caméra thermique	Recherche surchauffe globale	Étude d'effets transitoires
			Localisation de défauts
Préparation d'échantillon	Chimie humide	Retrait de couches permettant l'observation ou la manipulation	
	Laser d'ablation	Retrait de couches permettant l'observation ou la manipulation	
	Plasma	Rétro-conception	Recherche de défauts
	FIB	Modification de design	Correction d'erreurs design
	Polissage	Rétro-conception	Recherche de défauts
Interaction avec la cible	Box de lecture	Lecture des composants	NA
	Station de probing	Interception signaux d'intérêt	Interception signaux debug

1.3 Notions de la rétro-conception hardware

1.3.1 Bases d'électronique

Il existe deux familles de composants dits actifs et passifs. Les composants dits passifs sont par exemple les résistances ou condensateurs. Ils permettent de modifier les paramètres électriques d'un signal sans interagir avec les informations circulant dans le système. On qualifie de composant électronique actif tout composant permettant de traiter les informations circulant dans un système électronique. Souvent reliés à des blocs mémoires et périphériques annexes, ils vont ainsi réaliser des opérations logiques binaires (addition, concaténation) pour accomplir leur tâche prédéfinie. Ces opérations sont réalisées à l'aide d'une multitude d'interrupteurs appelés "*transistors*" (section *Le transistor*). Un processeur comme celui de l'iPhone 11 peut ainsi contenir jusqu'à 8.5 milliards de transistors répartis en plusieurs couches, sur une surface en silicium de 1cm^2, appelée "*puce*" ou "*die*" [151]. Cette puce électronique est ensuite encapsulée dans de la résine d'époxy, qui servira de boîtier, et reliée à des broches externes à l'aide de fils d'or de quelques micromètres de diamètre appelés fils de bonding.

Il existe plusieurs formules de bases qui régissent les composants électroniques, qu'ils soient actifs ou passifs. La première formule à connaître est la loi d'ohm. Il s'agit d'une formule qui donne la relation entre la tension appliquée aux bornes d'un élément résistif dont U est la tension en Volts, R est la valeur de résistance en Ohms et I est l'intensité du courant en Ampères.

$$U = R \cdot I$$

Cette première formule est importante car elle permet de calculer la valeur de l'intensité du courant traversant une résistance. Pour schématiser avec un élément plus concret, à savoir un entonnoir, la tension représente la quantité d'eau totale à faire passer par celui-ci. La résistance correspond au diamètre de l'entonnoir, donc la capacité de l'eau à passer. Enfin l'intensité du courant correspond au débit de l'eau pour traverser la section courante de l'entonnoir. Concrètement, un diamètre plus petit implique, pour une quantité d'eau transférée identique, un débit de passage de l'eau supérieure. Ce phénomène sera le même pour l'électricité dans une résistance. Plus la valeur de la résistance sera faible, pour une tension constante, plus la valeur du courant sera importante. Sachant que comme pour l'eau, l'intensité du courant est une force destructrice lorsqu'elle est trop importante, il s'agit d'un paramètre clé dans les systèmes. L'intensité du courant associé à la tension aux bornes du système permettent de calculer la puissance appliquée, d'après la formule :

$$P = U \cdot I$$

Une autre notion intéressante à prendre en compte dans le fonctionnement d'un circuit électronique est la loi de nœuds. Elle régit la répartition du courant dans un nœud, c'est-à-dire à une intersection entre plusieurs branches d'un circuit. Le fonctionnement de l'intensité du courant est similaire à l'intensité de l'eau d'un fleuve. Lorsque l'eau d'un fleuve rencontre un embranchement, le flux principal est divisé par le nombre de branches disponibles. Cette découpe est proportionnelle en la quantité d'eau acceptable pour chaque branche, et la quantité d'eau sortante est égale à la quantité d'eau entrante. Il n'y a ni perte, ni création d'eau à l'embranchement. Le courant connaît le même phénomène lors de l'arrivée sur un embranchement, avec 'I' le courant provenant de la source, 'I1' et 'I2' les courants des branches de sortie.

$$I = I1 + I2$$

1.3.1.1 La diode

Dans la section précédente, nous avons mentionné les composants actifs et un de leur plus célèbre composant de base, le transistor. Cependant, il existe un élément encore plus basique, qui lui-même constitue la base des transistors contenu dans les composants actifs, il s'agit de la diode. Avant de présenter le fonctionnement de la diode, il faut présenter sa composition. Classiquement, la base d'un composant actif est un substrat en silicium. Visuellement, cela ressemble à un grand disque gris qui présente un effet miroir grâce à un polissage de précision (Figure 1.54).

FIGURE 1.54 – Exemple d'un wafer de silicium, tranche de silicium servant de substrat lors de la fabrication des composants électroniques [46]

Le silicium est un matériau dit semi-conducteur, c'est-à-dire que naturellement il est isolant. Cependant, lors de l'apport d'éléments (dopage) dans la structure atomique d'un semi-conducteur, la propriété électrique de celui-ci change. Le dopage se fait donc en

apportant des électrons ou des trous à la matrice d'atomes du silicium. Il est possible de créer un silicium dit de type N par un apport d'atomes en excédant d'électrons, généralement grâce à du bore. Cela crée une forte densité d'électrons libres dans ce silicium dopé. À l'inverse, il existe des siliciums en manque d'électrons, donc avec une forte présence de trous, créant ainsi un dopage de type P. Pour ce type de dopage, il s'agit d'atomes de phosphore qui sont classiquement utilisés. Il existe plusieurs procédés permettant de faire ces dopages, dont l'implantation avec un plasma.

La capacité de créer deux zones distinctes sur une couche nanométrique à la surface d'un substrat en silicium permet de créer des associations telles que la jonction PN. Comme son nom l'indique, la jonction PN est la mise côte à côte d'une zone dopée P et d'une zone dopée N, comme le montre la Figure 1.55

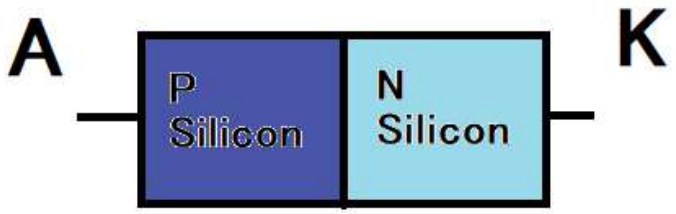
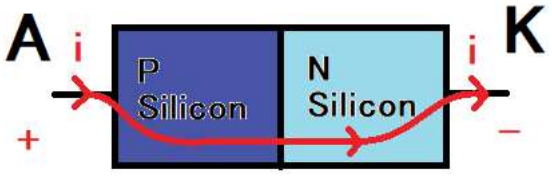
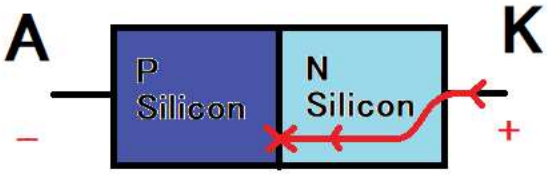


FIGURE 1.55 – Illustration de la jonction PN dans un substrat de silicium

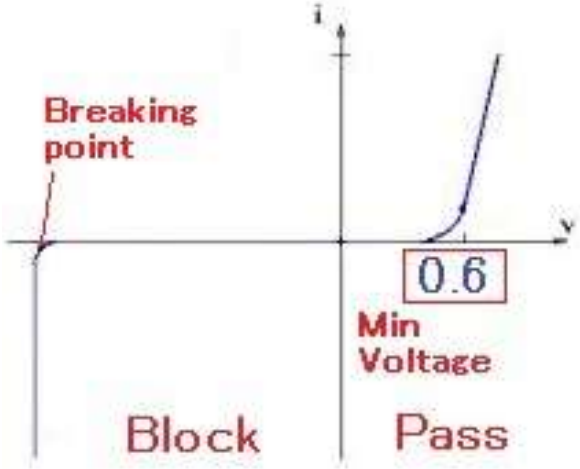
Lorsque l'on accole une zone P et une zone N, auxquelles on applique une tension, dans le sens PN le courant réussit à passer (Figure 1.56a), alors que dans le sens NP, la jonction effectue une barrière (Figure 1.56b). Électriquement parlant, cette définition n'est pas rigoureuse, car il existe des phénomènes additionnels. Dans le sens inverse (sens NP), il existe une tension pour laquelle le courant peut passer, appelée tension de claquage inverse. En dessous de cette tension, le courant est bloqué, alors qu'une fois cette tension dépassée, le courant connaît une avalanche (Figure 1.56c), n'ayant comme limite que la source qui l'émet. Cette situation est réversible, pour peu que le courant soit limité et que le silicium ne se soit pas dégradé. Dans le sens direct, il existe également une tension minimum permettant le passage du courant, due à une résistance du matériau (Figure 1.56d). Cependant, cette tension est beaucoup moins élevée que la tension de claquage. En effet, la tension de seuil en direct est située autour de 0,6V à 0,7V, inférieure à la tension de fonctionnement des systèmes et loin de la tension de claquage. Cette structure ainsi créée est appelée : une diode.



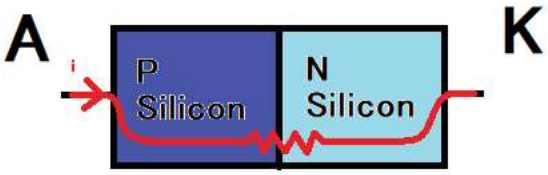
(a) Diode en directe



(b) Diode en inverse



(c) Fonction de transfert



(d) Schéma représentant une résistance de jonction

FIGURE 1.56 – Schéma de fonctionnement des diodes et courbe de transfert associée

1.3.1.2 Le transistor

Dans la section *La diode*, nous avons introduit les notions de substrat et de zones de dopage permettant de créer une jonction PN et une diode. À partir de cette structure, il est possible de créer un élément plus complexe qu'est le transistor de technologie Metal Oxide Semiconductor (MOS). La Figure 1.57 présente la structure d'un transistor MOS dit de type N. Le type du transistor est défini par la nature des deux zones de dopage (donc N), appelées drain et source, dans une zone de dopage opposée (donc P), appelé caisson. Dans un aspect fonctionnel, la source est la borne qui est reliée à la source d'alimentation (tension pour un PMOS ou masse pour un NMOS). Si nous considérons uniquement les jonctions du transistor, le drain sur lequel est appliqué le potentiel le plus élevé est une zone N. Le caisson étant de nature P, la jonction ainsi créée est une jonction NP, donc une jonction bloquante. En l'état, il n'est pas possible d'utiliser le transistor et pour ajouter une fonctionnalité, il faut ajouter une grille qui change localement les propriétés du caisson P.

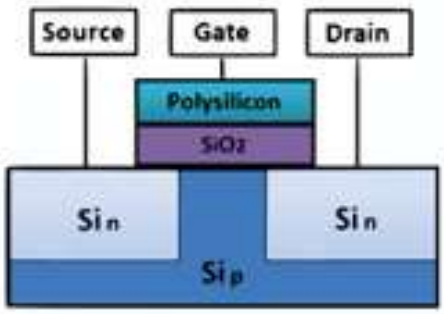


FIGURE 1.57 – Schéma structurel d'un transistor NMOS

La grille permet de piloter le transistor d'une manière très simple. Lorsqu'un niveau logique '0' est appliqué sur la grille, le transistor est bloqué. Cela signifie que physiquement aucun mécanisme ne se met en place permettant des échanges entre le drain et la source. Le courant qui arrive sur le drain est bloqué, comme le montre la Figure 1.58.

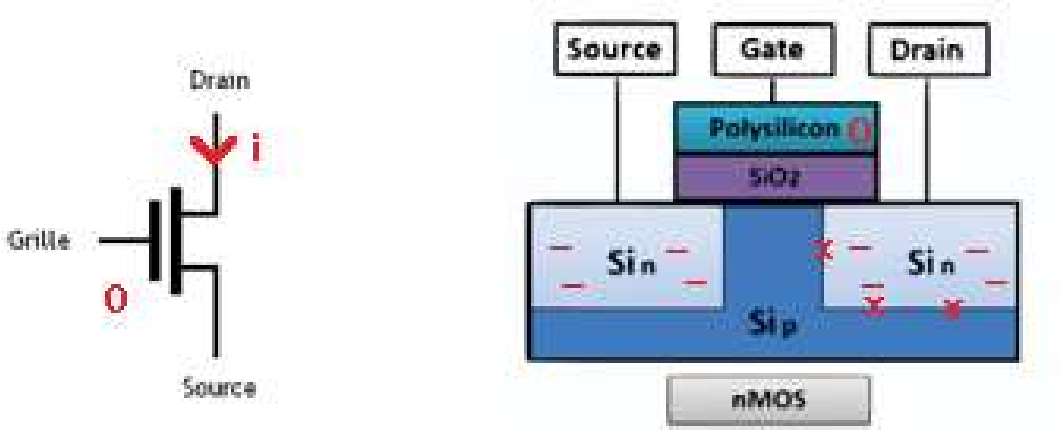


FIGURE 1.58 – Schéma électronique et structurel d'un transistor NMOS lorsque la grille est soumise à un '0'

Le second état que peut prendre le transistor est l'état passant. Si nous visualisons le transistor comme un interrupteur, l'état précédent signifie que l'interrupteur est ouvert, ne déclenchant aucune action. À l'inverse, l'état passant correspond à un interrupteur fermé qui laisse passer le courant. Pour en arriver à ce stade, il faut faire une action sur la grille pour engendrer une réaction physique dans le transistor. Lorsqu'une tension suffisante est appliquée sur la grille, la charge de celle-ci attire les électrons de la source. Les électrons migrent progressivement depuis la source dans le caisson. L'accumulation des électrons permettent de former un canal entre la source et le drain. Ce phénomène est appelé l'effet de champ. Cela permet au courant électrique de circuler entre le drain et la source, assurant la conductivité électrique, comme le montre la Figure 1.59.

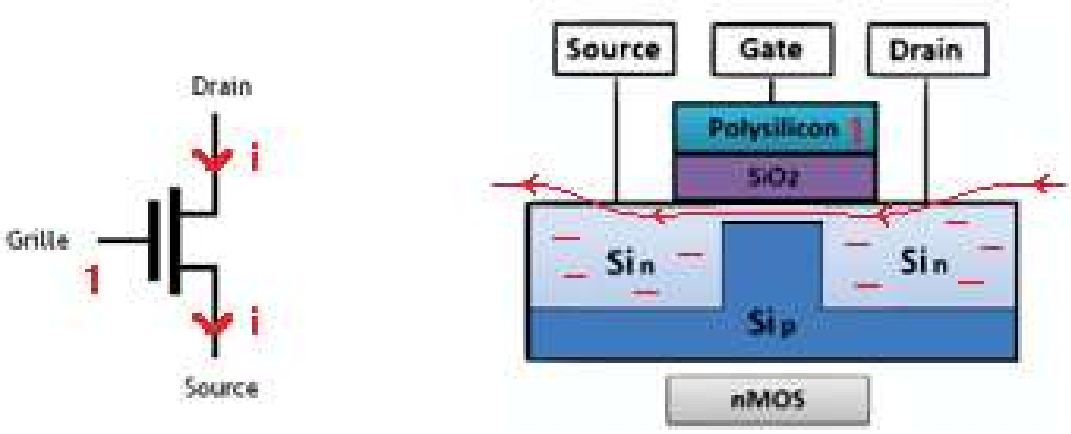


FIGURE 1.59 – Schéma électronique et structurel d'un transistor NMOS lorsque la grille est soumise à un '1'

Jusqu'à présent, j'ai détaillé le fonctionnement d'un transistor en me basant sur la technologie MOS avec un transistor de type N. Cependant, le transistor peut également être réalisé avec un drain et une source de type P et dans ce cas, le caisson passera en N. Si les zones sont inversées, le comportement physique l'est aussi, ce qui signifie que pour déclencher l'effet de champ entre le drain et la source, ce n'est plus des électrons qui sont attirés mais des trous. Pour attirer ces trous, il ne faut plus appliquer une tension sur la grille, mais appliquer un '0'. Le transistor sera donc passant pour un '0' sur la grille et bloqué si c'est un '1'. Ce comportement complémentaire entre le transistor NMOS et le transistor PMOS a donné le nom à cette technologie : Complementary Metal Oxide Semiconductor (CMOS) [152]. Pour fonctionner, elle a besoin d'être constituée systématiquement d'un nombre pair de transistors (Figure 1.60), avec autant de NMOS que de PMOS.

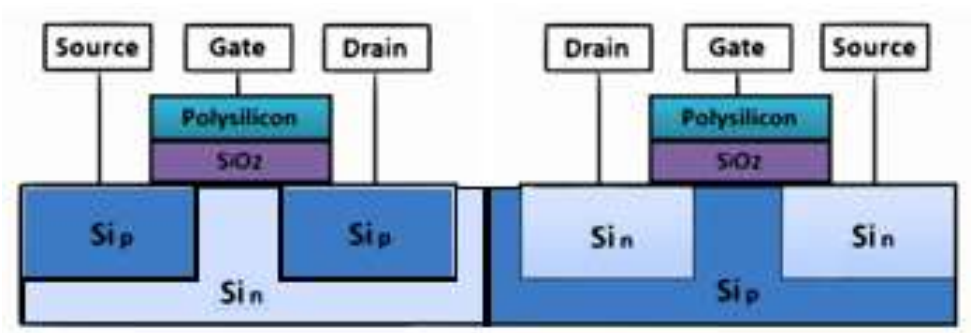


FIGURE 1.60 – Schéma d'implantation des transistors CMOS

Lors de la conception d'un circuit à base de transistors CMOS, les transistors NMOS sont disposés en liaison avec la masse, alors que les transistors PMOS sont en liaison avec l'alimentation. La fonction la plus simple à réaliser avec deux transistors est l'inverseur.

Le rôle de cette fonction logique est, comme son nom l'indique, d'inverser un signal numérique. Le schéma structurel de cette fonction est représentée en Figure 1.61. Ce sont les grilles reliées entre elles qui forment l'entrée de la fonction.

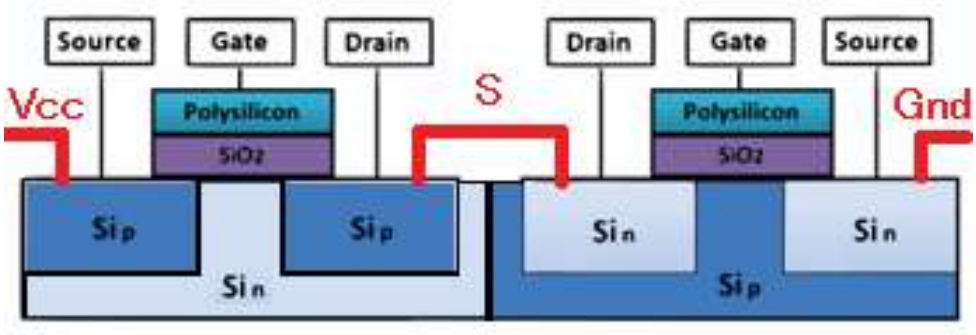
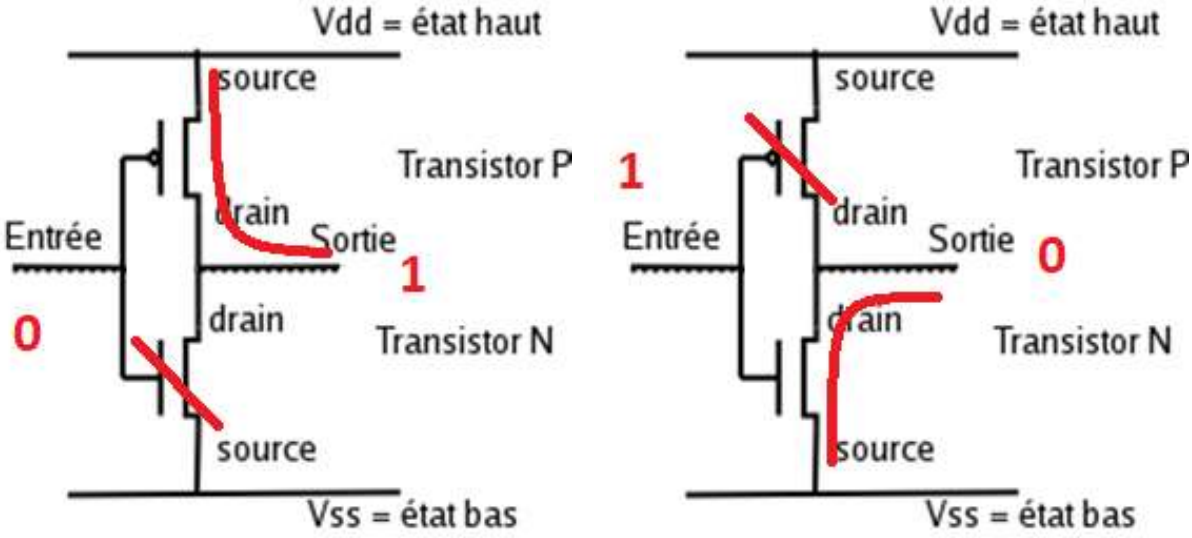


FIGURE 1.61 – Schéma de raccordement des transistors CMOS dans le silicium

Il est possible de valider le comportement de la fonction logique de l'inverseur en appliquant un signal sur l'entrée et en observant la sortie. Sur la Figure 1.62a, l'entrée reçoit un '0' logique, cela a pour effet de bloquer le transistor bas (NMOS), tout en fermant le transistor haut (PMOS). La liaison entre la sortie et le Vcc est fermée, tandis que celle avec la masse est ouverte. En d'autres termes, la sortie se retrouve directement reliée au Vcc lui appliquant ainsi un niveau '1'. Le bloc logique a donc inversé un signal à '0' en '1' et la table de vérité 1.4 se confirme. La Figure 1.62b illustre le comportement lorsque l'entrée reçoit un '1', produisant un '0' en sortie.



(a) Inversion d'un '0' en '1'

(b) Inversion d'un '1' en '0'

FIGURE 1.62 – Fonctionnement d'un inverseur CMOS

Le comportement de la fonction logique inverseur peut être résumée dans la table de vérité (Tableau 1.4).

Tableau 1.4 – Table de vérité de l'inverseur

Entrée	Sortie
0	1
1	0

L'inverseur reste une structure très simple n'utilisant que deux transistors. Pour un composant moderne, il est possible de compter plus de 500 fonctions logiques différentes possèdent un nombre d'entrées dépendant du besoin. Il est tout de même possible de référencer les fonctions logiques suivantes associées avec leurs tables de vérité :

1. Fonction AND (ET) : La fonction prend '1' en sortie S uniquement lorsque les entrées A et B sont elles-mêmes à '1'.

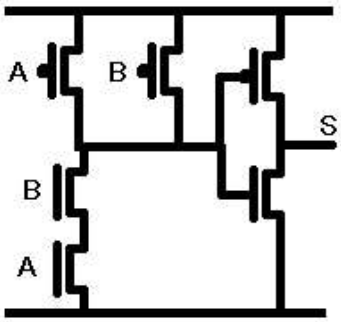


FIGURE 1.63 – Schéma de câblage d'une fonction AND avec des transistors

Tableau 1.5 – Table de vérité de la fonction AND

A	B	S
0	0	0
0	1	0
1	0	0
1	1	1

Équation :

$$S = A \cdot B$$

2. Fonction NAND (Non-ET) : La fonction est l'inverse de la porte AND. Elle prend '0' en sortie S uniquement lorsque les entrées A et B sont à '1', donc elle prend '1' dans les autres cas.

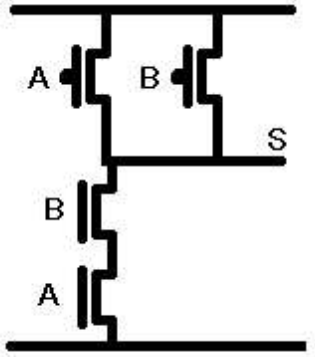


FIGURE 1.64 – Schéma de cablage d'une fonction NAND avec des transistors

Tableau 1.6 – Table de vérité de la fonction NAND

A	B	S
0	0	1
0	1	1
1	0	1
1	1	0

Équation :

$$S = \overline{(A \cdot B)}$$

3. Fonction OR (OU) : La fonction prend '1' en sortie S lorsqu'une des entrées A ou/et B est à '1'.

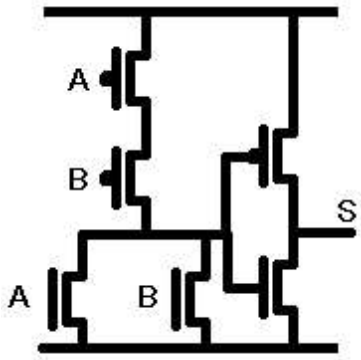


FIGURE 1.65 – Schéma de câblage d'une fonction OR avec des transistors

Tableau 1.7 – Table de vérité de la fonction OR

A	B	S
0	0	0
0	1	1
1	0	1
1	1	1

Équation :

$$S = A + B$$

4. Fonction NOR (Non-OU) : La fonction est l'inverse de la porte OR. Elle prend '0' en sortie S lorsqu'une des entrées A ou B est à '1' (donc également lorsque les deux entrées sont à '1'), donc elle prend '1' lorsque les entrées A et B sont à '0'.

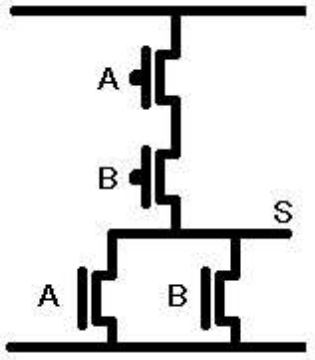


FIGURE 1.66 – Schéma de câblage d'une fonction NOR avec des transistors

Tableau 1.8 – Table de vérité de la fonction NOR

A	B	S
0	0	1
0	1	0
1	0	0
1	1	0

Équation :

$$S = \overline{(A + B)}$$

5. Fonction XOR (OU-EXCLUSIF) : La fonction prend '1' en sortie S lorsqu'une seule des entrées A ou B est à '1'.

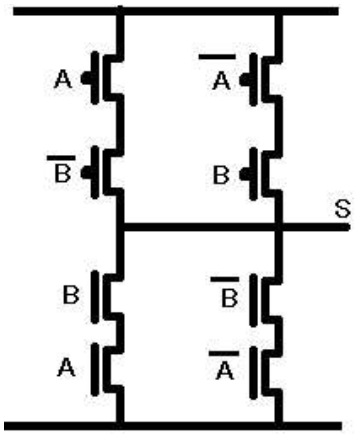


FIGURE 1.67 – Schéma de câblage d'une fonction XOR avec des transistors

Tableau 1.9 – Table de vérité de la fonction XOR

A	B	S
0	0	0
0	1	1
1	0	1
1	1	0

Équation :

$$S = A \oplus B$$

1.3.1.3 Les résistances de tirage

Dans les montages des circuits à base de transistors CMOS, nous avons schématisé la sortie des fonctions logiques. Ces sorties sont produites par le raccordement de transistors reliés soit à l'alimentation soit à la masse. Il n'y a donc pas de connexion directe entre la sortie de la fonction logique et la source de tension. Ce fait permet d'introduire deux notions simples d'électronique. La sortie ou l'entrée du système à base de transistors CMOS est vue comme de simples diodes depuis l'extérieur. De plus, la sortie CMOS n'est pas conçue pour tirer beaucoup de courant et lorsque les transistors ne sont pas pilotés, elle se retrouve dans un état flottant. Nous allons développer ces deux aspects :

— Les diodes de protection : Lors de l'étude de la conception d'un composant CMOS, nous avons présenté celui-ci comme une série de jonction-PN, donc de diodes. Lorsque le composant est piloté, ces jonctions sont modifiées pour permettre au

courant de circuler, ce qui n'est pas le cas lorsque le transistor est inerte. Dans ce cas, les électrons reprennent leurs places et les jonctions rejouent leur rôle. La particularité de la technologie CMOS, c'est la faible quantité de courant qui peut être acheminé par le transistor, donc une certaine fragilité structurelle. Lors de l'utilisation d'un composant dans un système, celui-ci peut être soumis à des surcharges ou décharges électriques. Pour protéger les transistors situés aux entrées et aux sorties du composant, des diodes de protections sont ajoutées. Elles sont dimensionnées pour résister à des décharges électrostatiques (ESD) de plusieurs milliers de volts. Lorsque le composant est inerte, il est possible de visualiser l'état de ces diodes avec un multimètre. Pour visualiser une diode de protection d'une sortie, il faut positionner la sonde positive sur la masse du composant et la sonde neutre sur la sortie à tester. La diode de protection de la sortie deviendra passante avec une valeur proche des 0.6V. Cette opération est également réalisable pour les diodes de protection des entrées ou les signaux bidirectionnels. La visualisation de la valeur de tension de seuil de la diode renseigne si celle-ci est fonctionnelle ou endommagée, donnant une information sur l'état de fonctionnement du composant.

— Les résistances de tirage : Une résistance de tirage est une résistance située entre une entrée/sortie de composant et la source d'alimentation (Vcc ou masse), pour qu'elle ne reste pas flottante. Une ligne est dite flottante lorsqu'elle n'est pas pilotée par le composant ou par son environnement. Le risque majeur est que la valeur de cette entrée change de manière incontrôlée (par exemple, à la suite d'un effet capacitif d'une piste à proximité), introduisant des valeurs erronées dans le composant, ce qui influencerait sa valeur de sortie. Pour empêcher cette situation, les concepteurs de systèmes électroniques ne laissent pas une broche de composant sans potentiel. Ils ont recours à des résistances de tirage pour forcer une ligne à un potentiel précis, lorsqu'elle n'est pas pilotée par le composant. La résistance est dite de pull-up (ou tirage) lorsqu'il s'agit de ramener l'alimentation sur la ligne, tandis que la résistance de pull-down (ou rappel) ramène la masse sur la ligne.

1.3.2 Application de la rétro-conception

1.3.2.1 Au système électronique

Avant de définir ce qu'est la rétro-ingénierie matérielle appliquée au système, il est nécessaire de définir ce qu'est un système électronique. Il s'agit de tout appareil pouvant réaliser des opérations de calculs logiques et pouvant interagir avec son environnement à l'aide de capteurs. Un système électronique est composé d'une unité de traitement logique, accompagnée par des composants auxiliaires remplissant des rôles complémentaires. Parmi les activités annexes qui peuvent être rencontrées, il y a entre autres le stockage mémoire, l'alimentation ou la gestion des périphériques (c'est-à-dire : une antenne Bluetooth ou une caméra pour un smartphone). L'unité de traitement peut prendre plusieurs formes telle qu'un contrôleur, nom donné à un composant contenant un processeur, une mémoire et des interfaces de communication.

Les composants sont reliés entre eux par des pistes en cuivre séparées par un support isolant, appelé circuit imprimé (aussi appelé PCB – *Printed Circuit Board*). L'information circule entre les composants par une variation de signaux basculant entre deux valeurs électriques. Cette variation est comprise par les composants comme une alternance de '0' et '1' logiques, leur donnant ainsi le nom de signaux numériques. L'ensemble des composants et du PCB représentent le système électronique.

La démarche de rétro-conception d'un système électronique consiste à identifier les fonctionnalités de chaque composant. Ces fonctionnalités pouvant être une mémoire de stockage, une mémoire de calcul, un module de communication, une unité de calcul ou un module de sécurisation de la donnée. Une fois les fonctionnalités d'intérêt identifiées, il faut comprendre comment elles sont reliées. Pour cela, il faut suivre les pistes métalliques dans le but de comprendre l'agencement des fonctions et en ressortir une fonctionnalité plus globale. L'étude s'arrête lorsque l'analyste comprend l'ensemble des mécanismes d'intérêt. Les points d'intérêt lors de la rétro-conception d'une carte électronique seront ainsi d'identifier :

— Les dépendances d'un composant pour le réparer : Ceci intervient lors des phases de diagnostic et de réparation d'un système électronique. Le but est de suivre un signal précis pour trouver ses interactions avec les composants et ainsi localiser le ou les potentiels éléments en défaillance. Les défauts à localiser peuvent être des courts-circuits, liés à un composant qui aurait fondu, ou des circuits-ouverts, liés à des pliures excessives ou à de la corrosion. En fonction du défaut localisé, il existe plusieurs solutions pour tenter de réparer le problème dans le but de rendre le système de nouveau fonctionnel.

— Un signal spécifique pour l'étudier : Contrairement à l'approche précédente, l'étude d'un signal n'est généralement pas une approche bienveillante mais a pour objectif

principal d'identifier son chemin et son rôle pour l'intercepter. De l'interception du signal découlera une tentative d'écoute ou de modification. Cette démarche est généralement réalisée dans les analyses de sécurité et elle est orientée sur des signaux assurant la sécurisation. L'attaquant cherchera donc à comprendre la nature du signal, son protocole, les valeurs pour pouvoir les perturber et induire pour les éléments environnants de fausses informations.

— Les signaux de communication pour s'interconnecter : Dans le but de dialoguer directement avec le composant ; cette démarche peut intervenir lorsqu'il est question de reprogrammer ou d'extraire de la donnée d'un composant. La nature et le rôle du composant, tout comme la mission de l'opérateur vont impacter la finalité de la manipulation. Un profil d'expert forensique aura pour intérêt la communication directe avec un composant mémoire pour récupérer et analyser les données contenues. Cette analyse aura pour but de consolider les connaissances dans le cadre d'une enquête, afin d'apporter des preuves d'actes répréhensibles infligés ou subis. À l'inverse un profil d'attaquant, tel que décrit à propos d'un CESTI dans la section *Introduction sur la rétro-conception matérielle*, aura pour objectif de communiquer avec un composant réalisant des opérations de calcul et contenant généralement des secrets de sécurisation (algorithme et clé de chiffrement, code d'exécution propriétaire, etc). L'objectif de cette manipulation sera d'altérer le comportement d'un composant de sécurité.

Les travaux de rétro-conception de système permettent de mieux comprendre la fonction de chacun des éléments. Cependant, la seule connaissance des composants d'une carte ne suffisent pas à mener une étude complète. Un même composant peut posséder plusieurs fonctionnalités, qui demandent de prolonger la rétro-conception à l'échelle du composant lui-même.

1.3.2.2 À un composant électronique

En complément de l'analyse sur une carte électronique, il peut arriver d'interagir directement avec un composant. Pour cela, les points d'intérêts lors de la rétro-conception seront :

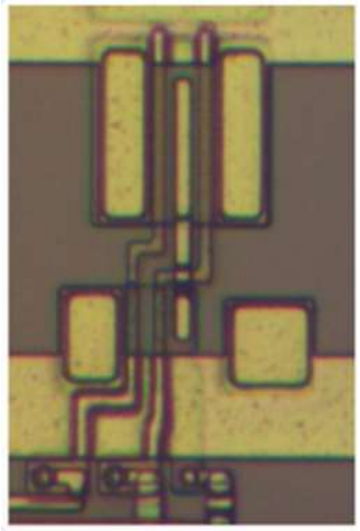
— D'identifier les signaux de communication pour s'interconnecter : la démarche sera la même que pour la carte électronique. Nous l'avons abordé dans la présentation des composants électroniques, mais certains composants sont des systèmes miniaturisés contenant eux-mêmes plusieurs puces. Prenons l'exemple d'un système MMC, constitué de puces mémoires et d'un contrôleur, qui ne serait pas fonctionnel ; si un maillon de la chaîne est défaillant, c'est l'ensemble de la donnée qui semble perdue. En effet, la donnée d'intérêt est contenue dans les

puces mémoires, cependant elle ne reste accessible que tant que le contrôleur est fonctionnel. La défaillance de celui-ci rend le système inopérant malgré la rétention toujours effective de la donnée dans la mémoire. Dans le cadre d'une analyse forensique, l'expert aura pour but de s'interconnecter directement avec les mémoires en contournant le contrôleur pour extraire directement les données brutes. Pour cela, il faut connaître le système pour agir sur lui et la rétro-conception en est la clé. Un autre objectif pouvant être poursuivi consiste à espionner les bus d'intérêt contenant des communications sensibles (comme sur les cartes électroniques). La technologie et la dimension d'un composant rendent l'opération plus complexe dans un composant que dans un système électronique, mais cela reste possible.

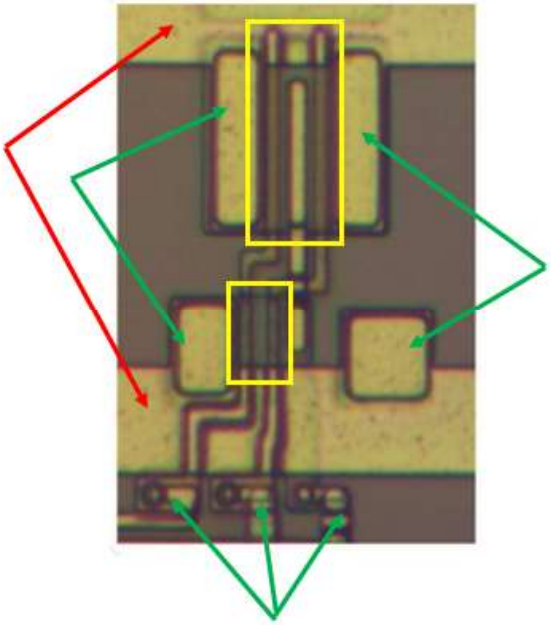
— De contourner une sécurité pour accéder à la donnée : La sécurisation des composants électroniques peut prendre plusieurs formes et intervient à plusieurs phases de la création du composant. La fabrication d'un composant est réalisée sur une chaîne standard. Après cette étape, il est programmé et son fonctionnement est validé. Seulement une fois la validation effectuée, les sécurités du composant sont activée, empêchant par exemple une modification d'un firmware ou l'accès à une clé de chiffrement. Pour sécuriser le composant, le fabricant dispose de plusieurs techniques. Il peut par exemple rendre inactif le bus de programmation ou détruire des fusibles. En parallèle de la sécurisation du composant, qui peut être commune à un modèle, l'utilisateur peut ajouter sa propre sécurisation (par exemple un code PIN pour une carte SIM ou un mot de passe pour un smartphone). Dans ce cas, l'attaquant devra trouver dans le composant le lieu qui gère le verrouillage des données. Ensuite, il devra perturber le fonctionnement du composant pour que celui-ci n'effectue pas la vérification de sécurité ou l'interprète mal : par exemple, faire en sorte qu'un code pin erroné soit interprété comme vrai.

C'est deux opérations peuvent avoir un intérêt pour les experts judiciaires, car le chiffrement ou le verrouillage peut empêcher l'accès à la donnée. Comme nous avons abordé dans l'introduction (section *Introduction sur la rétro-conception matérielle*), que le cadre légal permet aux experts de procéder à des opérations plus invasives. Certains de ces experts possèdent une bonne connaissance des fonctions logiques que peuvent contenir les composants, permettant d'aller plus loin dans l'expertise. Ils sont capables de comprendre les liaisons entre les transistors pour retrouver les équations de chaque fonctions logiques. Ils peuvent ensuite relier les fonctions entre elles pour avoir une vision globale du composant et ainsi retrouver l'implémentation d'algorithmes de chiffrement ou des méthodes de sécurisation des composants. Afin d'illustrer nos propos, nous allons donc développer la méthodologie appliquée par un rétro-concepteur face à une cellule inconnue.

Pour procéder à l'étude d'une nouvelle cellule, il faut d'abord comprendre son architecture. Nous allons baser notre exemple sur la Figure 1.68a qui a été trouvée sur internet [153].



(a) Vue optique de la cellule à rétro-concevoir [153]



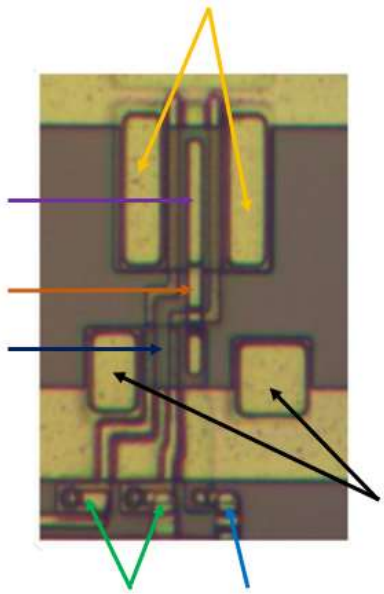
(b) Identification basique des éléments

FIGURE 1.68 – Fonction utilisée comme exemple pour l'explication de la méthodologie de rétro-conception d'un composant

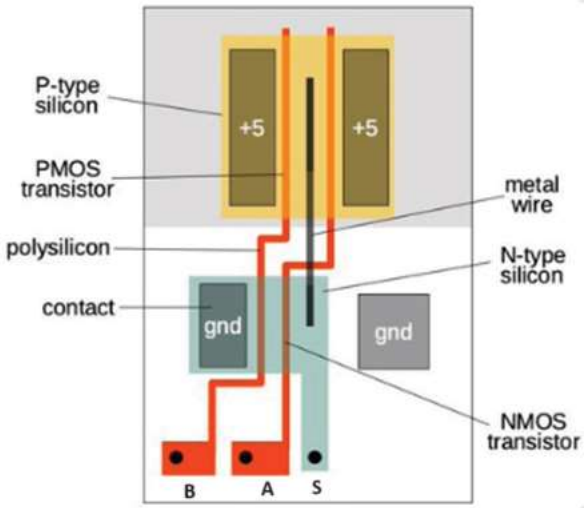
La démarche de rétro-conception est la suivante :

1. Repérer les différentes couches : Cette étape consiste à identifier la technologie des éléments en notre présence. Pour rappel, sur la vue en coupe d'un composant on peut distinguer des transistors au niveau du substrat et des pistes qui les relient. Ces pistes sont présentes sur plusieurs niveaux et sont interconnectées par des vias. Sur notre Figure 1.68a, nous devons retrouver ces éléments que sont les pistes et les transistors. Il faut également comprendre la forme que prendront les vias pour interpréter les interconnexions entre les éléments. A partir de la Figure 1.68a, il est possible de produire la Figure 1.68b, sur laquelle nous avons identifié les éléments. Dans un premier temps, les transistors sont encadrés en jaune, et ils sont au nombre de 4 (pour rappel, la technologie CMOS implique un nombre pair de transistors). Nous pouvons également repérer des rails qui sont les pistes, indiqués en rouge. Enfin nous pouvons repérer des vias, qui ont le même aspect métallique que les pistes. Ils sont indiqués en vert sur la Figure 1.68b et au nombre de 7. Une fois l'identification des éléments faite, il va falloir les interpréter, et entre autres déterminer si les vias sont des entrées, des sorties ou réalisent d'autres fonctions.

2. Comprendre la structure : Dans l'étape précédente, nous avons repéré des transistors au nombre de 4, divisée en 2 groupes de 2. Dans ces groupes, nous devons retrouver 2 NMOS et 2 PMOS. Technologiquement pour que des transistors aient les mêmes propriétés physiques, un paramètre est à prendre en compte, il s'agit de la dimension de la grille. En effet, les transistors PMOS doivent être plus grands que les transistors NMOS, pour garder des caractéristiques électriques similaires. De plus, comme nous l'avons évoqué dans la section *Le transistor*, les transistors PMOS sont situés au niveau de l'alimentation et les NMOS sont du côté de la masse. En combinant ces notions et en les appliquant à la Figure 1.68b, il est possible de dire que les transistors PMOS sont situés dans le carré jaune du haut et les NMOS dans le carré jaune du bas. Maintenant, il convient de s'attacher à différencier les vias. Les pistes identifiées en rouge sont des rails d'alimentation, ils sont donc sur un plan différent des transistors. Pour les relier physiquement à une grille ou une source, il faut créer un pont, donc utiliser des vias. Compte tenu de la position des rails d'alimentation et des transistors (Figure 1.69a), nous pouvons en déduire que les vias en noir permettent de relier une source de transistor à la masse et les vias identifiés en jaune permettent de faire la liaison avec l'alimentation au niveau des PMOS. Il reste donc 3 vias sur les 7 précédemment identifiés à traiter. Nous constatons que les deux vias en vert arrivent directement sur des pistes qui suivent les transistors. Nous en déduisons donc qu'il s'agit des contacts de grille et conformément aux notions précédemment vues, il s'agit des entrées. La sortie de la fonction se faisant sur des drains, il doit s'agir du contact bleu. Toujours sur la Figure 1.69a, nous distinguons une piste identifiée par les flèches violet, orange foncé et bleu foncé. Ce sont des vias et une piste qui permet de relier les drains des transistors PMOS avec un des NMOS, lui-même relié à la sortie. L'image peut ainsi être schématisée comme indiquée Figure 1.69b.



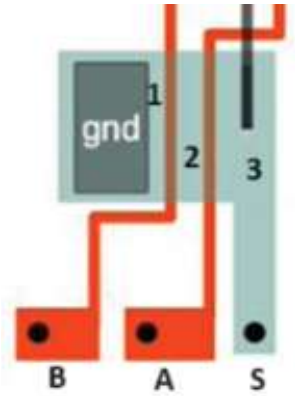
(a) Identification avancée de éléments de la fonction logique



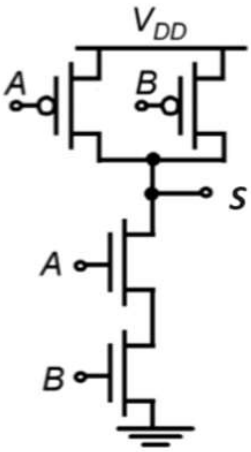
(b) Schéma équivalent correspondant à la vue optique [153]

FIGURE 1.69 – Parallèle entre la vue optique de la fonction étudiée et un schéma du design

3. Ressortir le schéma : À partir de la vue optique et du schéma du design correspondant, l'étape suivante consiste à trouver comment les transistors sont reliés les uns aux autres. Pour commencer, il faut partir d'une source et comprendre si les transistors sont en série ou en parallèle. Sur la Figure 1.69b, nous partons du via provenant de la masse, ce qui nous permet de passer par deux transistors NMOS en série. Pour une meilleure compréhension, nous allons décrire plus en détail cette interprétation. Si nous partons du via qui fait contact avec la masse, nous arrivons sur un premier transistor, plus précisément sur sa sources (Figure 1.70a qui est la vue zoomée de la Figure 1.69b). Ce premier transistor dispose donc d'une grille identifiée par le repère 1 reliée à l'entrée B et ressort par un drain identifié par le repère numéro 2. Si nous poursuivons le chemin nous tombons sur une nouvelle grille reliée à l'entrée A. Cela signifie que le drain du premier transistor (entrée B) est commun à la source du second (entrée A), par conséquent les transistors sont en série. Le drain de ce second transistor est identifié par le repère 3 sur la Figure 1.70a. À ce stade, nous pouvons donc dessiner le schéma des transistors entre la masse et la sortie sur la Figure 1.70b. L'étape suivante consiste à reproduire l'opération sur la partie haute de la fonction, donc sur les transistors PMOS. En partant des vias provenant du rail d'alimentation, nous arrivons aux sources des deux transistors de chaque côté. En suivant le chemin dans les transistors, nous ressortons sur des drains communs allant à la sortie. Les transistors PMOS sont donc en parallèle, et nous pouvons les ajouter à la Figure 1.70b.



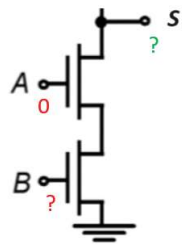
(a) Zoom sur la partie basse de la Figure 1.69b



(b) Schéma des transistors de la fonction logique

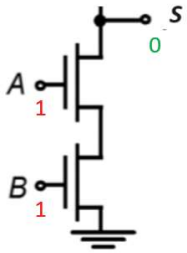
FIGURE 1.70 – Étude de la vue zoomée de la fonction et parallèle avec le schéma des transistors

4. Produire la table de vérité : À partir du schéma établi dans la Figure 1.70b, nous effectuons la même opération de mise à '0' ou '1' des entrées, que dans la section *Le transistor*. Cela permet de simuler les états ouverts ou fermés des transistors et ainsi d'en déduire la sortie. En fonction, nous éditons une table de vérité. Dans un premier temps, nous allons uniquement nous focaliser sur la partie basse avec les transistors NMOS. La Figure 1.71a montre le comportement lorsque l'entrée A est à '0'. Le transistor NMOS est ouvert donc la sortie n'est pas reliée à la masse. La table de vérité ne peut pas être complétée. Il en va naturellement de même si l'entrée B est à '0', quel que soit la valeur de A. Il faut donc que les deux entrées soient à '1' pour que la sortie soit à '0'. De cette déduction, nous pouvons compléter la table de vérité, conformément à la Figure 1.71b. Nous pouvons également faire une seconde déduction. La sortie doit toujours avoir une valeur, par conséquent, si seule une combinaison peut apporter un '0' en sortie dans ce cas, les autres combinaisons apportent un '1'. Dans un cas concret, il n'est donc pas nécessaire de faire la rétro-conception de la partie PMOS des fonctions logiques. Dans cet exemple nous allons tout de même confirmer les informations en rouge dans la table (Figure 1.71b). Pour cela, conformément à la Figure 1.71c, nous appliquons un '0' sur l'entrée A, ce qui ferme le transistor. Quel que soit la valeur de B, la sortie se retrouve à '1'. Il est possible de passer deux cases de la table en vert, pour signifier la confirmation. Nous effectuons la même déduction si nous appliquons un '0' sur l'entrée B, ce qui permet de confirmer la dernière valeur de la table (Figure 1.71d).



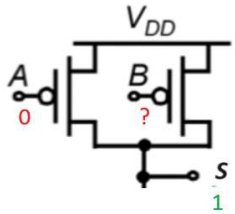
A	B	F
0	0	
0	1	
1	0	
1	1	

(a) Partie NMOS entrée A à '0'



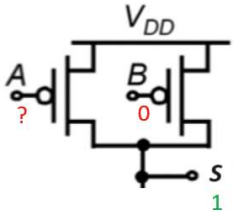
A	B	F
0	0	1
0	1	1
1	0	1
1	1	0

(b) Partie NMOS entrées à '1'



A	B	S
0	0	1
0	1	1
1	0	1
1	1	0

(c) Partie PMOS entrée A à '0'



A	B	S
0	0	1
0	1	1
1	0	1
1	1	0

(d) Partie PMOS entrée B à '0'

FIGURE 1.71 – Établissement de la table de vérité de la fonction selon les états des entrées

5. Sortir l'équation : Depuis la table de vérité il faut essayer de ressortir l'équation qui définit la fonction. Dans notre exemple, la sortie prend '0' lorsque les deux entrées sont à '1'. Donc la sortie inversée est :

   Équation

$$\overline{S} = (A \cdot B) \quad ou \quad S = \overline{(A \cdot B)}$$

   Donc la fonction est une porte NAND à deux entrées.

Dans la démarche d'explication de la rétro-conception, une méthode a été présentée, cependant il ne s'agit pas de l'unique méthode. Chaque expert possède ses propres habitudes et manières de travailler. De même, les exemples utilisés dans cette section, ainsi que pour expliquer le transistor, expose toujours des fonctions à deux entrées. Dans des vrais cas, le nombre d'entrées des fonctions dépendent du besoin. De même, la fonction elle-même n'est pas limitée à un catalogue standard. Il est ainsi possible de retrouver en un seul groupe de cellules des équations alliant à la fois XOR, NAND, NOR et pouvant utiliser de multiples entrées. Pour conclure, ce type d'étude est très complexe et très coûteuse en temps. Il n'est donc pas possible de l'appliquer sur chaque cas et seulement quelques experts dans le monde sont capables de l'effectuer. À l'heure actuelle des outils, basés sur de l'intelligence artificielle, d'aide à la rétro-conception sont disponibles ou en cours de développement. Cependant, leur niveau d'aboutissement n'offre pas les performances nécessaires une automatisation complète. Il faut également rappeler que le but global

de cette démarche, dans un cadre de la forensique numérique, n'est pas d'espionner les fabricants de système, mais reste de prendre la main sur certaines fonctionnalités pour en extraire la donnée légale.

1.4 Présentation des supports MultiMedia Card

Au début du chapitre, j'ai présenté la démarche de sélection des supports sur lesquels mes travaux allaient porter, à savoir les MMC, qui sont basées sur les mémoires de technologie flash. Dans cette section, je vais développer la composition et le fonctionnement de ces composants.

1.4.1 Introduction des supports

Les supports de type MultiMedia Card sont une évolution des mémoires de type NAND classiquement utilisées pour le stockage de la donnée dans les systèmes électroniques embarqués. Jusque dans la fin des années 90, le stockage de la donnée le plus performant était réalisé via des mémoires de type flash. Ces mémoires étaient basées sur les technologies Not-AND (NAND) ou Not-OR (NOR) et présentaient certaines contraintes, introduites dans cette introduction puis développées dans la partie *Protocole de communication interne*.

En 1997, les fabricants Sandisk et Siemens s'associent pour concevoir un système de mémoire plus performante [154]) dite MultiMedia Card (MMC). Il ne s'agit plus d'une mémoire isolée mais d'un système complet, contenant une ou plusieurs mémoires de même technologie et d'un contrôleur. Le rôle du contrôleur est d'architecturer la donnée pour accroître l'espérance de vie des mémoires, et de corriger les erreurs de lecture/écriture. De plus, regrouper plusieurs puces mémoires dans un même package permet de multiplier la capacité de stockage sans augmenter la taille du produit. L'objectif à l'époque est de concevoir des stockages amovibles de plus grande capacité.

À partir de la technologie MMC, plusieurs produits similaires ont été créés. En 2000, Sandisk, Panasonic et Toshiba se sont associés pour fonder la SD Association [155] et développer la carte mémoire Secure Digital (SD), dont le fonctionnement est détaillé dans la partie *La norme SD*.

Cette nouvelle carte mémoire présente la même architecture interne que les cartes précédentes avec un contrôleur spécifique. Celui-ci permet de faire l'interface entre le protocole des puces mémoires et le protocole de l'hôte développé suivant la norme SD. Basé sur la même architecture que le standard SD, le composant embedded-MultiMedia Card (eMMC) est introduit en 2007 par la norme JEDEC JESD84-A41 [156]. Contrairement aux technologies précédentes, le composant eMMC n'a plus vocation d'être un support de stockage mobile, mais présente une solution de stockage à intégrer dans le système. L'objectif est de remplacer les mémoires flash classiques par des composants qui facilites la gestions des données en intégrant un contrôleur, ce qui permet de prendre en charge la gestion des erreurs et l'optimisation des plans mémoires.

Sur la fin des années 2000, les évolutions technologiques ainsi que la multiplication des

équipements mobiles ont favorisés les évolutions des normes SD et eMMC. Les besoins en volume de stockage et en vitesse de transfert ont nécessité d'utiliser des puces mémoires avec des protocoles plus rapides. Une nouvelle famille de mémoire est apparue utilisant un protocole d'échange avec l'hôte différent. Cette technologie appelée Universal flash Storage (UFS) a été normalisée en 2011 sous l'appellation JEDEC JESD220 [157]. Ces dix dernières années, les technologies SD, eMMC et UFS n'ont cessé d'évoluer pour augmenter la vitesse de transfert, débouchant sur une mise à niveau des normes eMMC 5.1 (JEDEC JESD84-B51A [158]) et UFS 3.1 (JEDEC JESD220E [159]).

Dans le domaine de l'expertise judiciaire, il est important de suivre les évolutions technologiques. Le fort développement d'une technologie sur un marché tel que la téléphonie (Figure 1.72) ou les systèmes multimédias embarqués accroît d'autant la probabilité de devoir expertiser de tels supports de stockage.

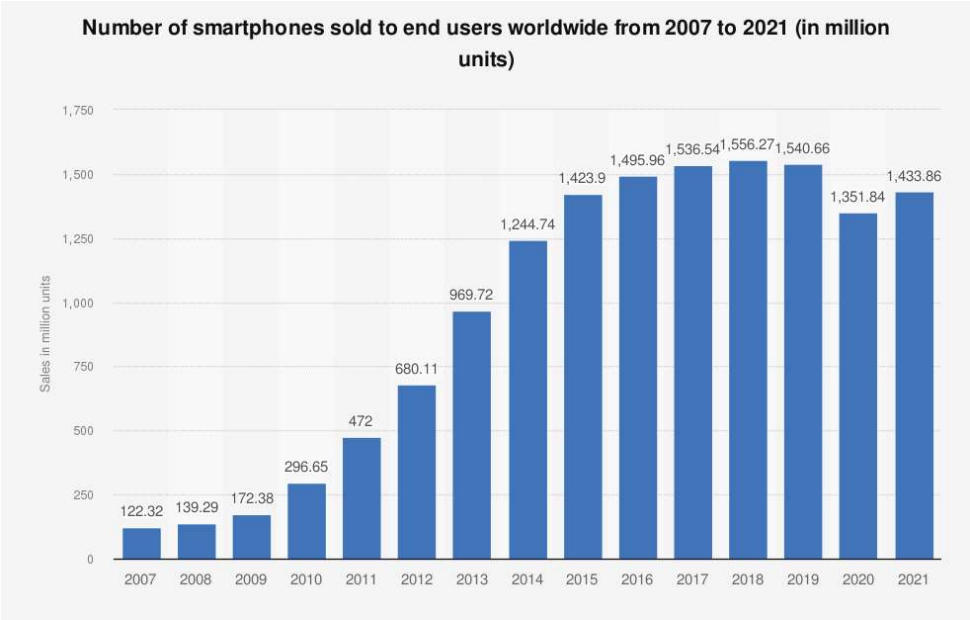


FIGURE 1.72 – Évolution des ventes de smartphones dans le monde entre 2007 et 2021

Un autre paramètre conditionnant l'importance de maîtriser l'expertise des nouvelles technologies est la sensibilité d'un dossier. Prenons l'exemple de l'attaque terroriste de SAN BERNARDINO en décembre 2015 [160], l'un des tireurs de l'attentat possédait un iPhone 5C. Ce téléphone étant sortie en septembre 2013 soit deux ans avant l'attentat, le FBI n'a pas eu l'opportunité de monter en compétence sur le déverrouillage du téléphone et l'extraction des données. Pour traiter le support le FBI a demandé de l'aide auprès d'Apple, qui a refusé prenant le parti de la protection de sa clientèle [51]. L'exemple de l'impossibilité de traiter un support dans un dossier sensible illustre bien l'importance de s'intéresser à une technologie telle que les MMC.

1.4.2 Une MMC particulière, la carte Secure Digital (SD)

Nous l'avons abordé précédemment, les MMC sont une famille de produits de type monolithe caractérisée par l'implémentation d'un contrôleur et d'une ou plusieurs puces mémoires permettant un stockage et une lecture plus rapide de la donnée. Nous l'avons également abordé, l'une des supports standardisés intégrant la famille des MMC est la carte Secure Digital (SD). Elle peut se décliner sous plusieurs tailles avec des capacités de stockage plus ou moins importantes. Les formats que nous pouvons rencontrer sont SD, mini-SD et microSD, comme le montre la Figure 1.73. Proposer plusieurs tailles de supports permet une meilleure adaptabilité et une meilleure intégration dans les systèmes qui vont accueillir ce stockage.

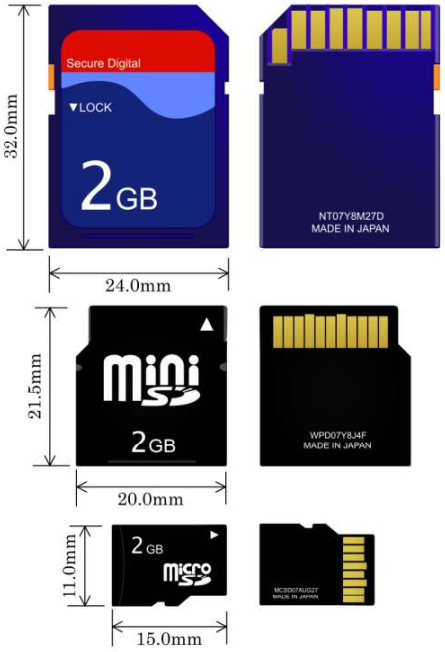


FIGURE 1.73 – Forme et taille standard des cartes SD (de haut en bas : cartes SD, miniSD et microSD)

Le recours à une carte SD amovible, contrairement à une MMC intégrée, permet à l'utilisateur un transfert plus facile de ses données (c'est-à-dire extraire les photos d'un appareil photo ou récupérer des vidéos d'une dashcam). Elle permet aussi de faire évoluer la capacité de stockage d'un appareil à faible coût, en fonction de ses besoins. En complément de la taille de la carte, d'autres paramètres peuvent varier pour s'adapter aux besoins des systèmes. Comme mentionné précédemment, il est possible de choisir une carte de grande capacité, avec des capacités de transfert rapide (Tableau 1.10).

Dans le Tableau 1.10, quatre labels sont donnés aux cartes SD qui dépendent directement de la capacité de stockage. À ces noms et capacités de stockage correspondent également des normes de vitesses de transfert. En effet, les fabricants de cartes ont dû

Tableau 1.10 – Tableau comparatif des différentes normes de carte SD avec leurs capacités et vitesses respectives

Norme		SD SC	SDHC	SDXC	SDUC
		Standard Capacity	High Capacity	eXtended Capacity	Ultra Capacity
Capacité	Min	128Mo	2Go	32Go	2To
	Max	2Go	32Go	2To	128To
Format		FAT12	FAT32	FAT32	exFAT
		FAT16		exFAT	
Norme bus (Vitesse de transfert max en Mb/s)		Défaut (12.5)	Défaut (12.5), High speed (25), UHS-I (50),		
			UHS-II (156 en Full Duplex et 312 Half Duplex)		
		High Speed (25)	(UHS-III,312 en Full Duplex et 624 en Full Duplex)		
			985	1970	3940

faire évoluer les capacités de transfert des cartes pour s'adapter et rester cohérent avec les volumes de données à traiter. Pour donner un ordre d'idée de l'évolution des tarifs, en 2020 le prix d'une carte 400 Go en SDXC au format microSD était d'environ 100€. Aujourd'hui ce tarif correspond à une carte d'une capacité de 1 To.

D'un point de vue de l'activité d'expertise judiciaire, un expert doit s'adapter aux évolutions technologiques [161]. La carte SD est devenue l'objet d'expertises [162] car présent dans presque toutes les preuves judiciaires [139] (notamment des appareils tels que les smartphones, les caméras, les outils d'automatisation, les action-cams, les consoles de jeux, les ordinateurs portables et les véhicules connectés). Ces dispositifs de stockage étant devenus de plus en plus performants, ils permettent de sécuriser les données grâce à diverses options telles que le verrouillage ou le chiffrement. Certains fabricants utilisent même les cartes SD comme magasins de clés pour chiffrer les données des smartphones à très haute sécurité, appelés darkphones, comme le No.1BC [163]. Bien que les cartes SD présentent l'avantage d'être amovibles et facilement transportables, elles ont également l'inconvénient d'être fragiles (facilement endommagées par un choc ou un accident) et facilement dissimulables pour une utilisation illégale (exemple de support contenant des images pédopornographiques, de terrorisme ou de trafic de drogue). Connaissant le contenu de leurs supports de stockage, les individus engagés dans des activités illicites essaient fréquemment de détruire le plus de preuves possibles et donc lors de leur arrestation, ils essayent de détruire physiquement ces supports. La carte SD étant très fragile, les experts peuvent rencontrer régulièrement ce type de support endommagé. Pour cette raison, dans notre étude, il est intéressant de se focaliser sur ce produit particulier de la famille des MMC pour faire nos tests et développer notre processus de diagnostic.

Avant de commencer nos travaux, nous avons recherché si des articles avaient été publiés, traitant des différentes étapes de la récupération des données spécifiquement sur les cartes SD. Nos recherches n'ont pas permis d'identifier de protocole public de diagnostic

pour des cartes endommagées. Le travail le plus proche est le diagramme de décision [51] pour les appareils mobiles (c'est-à-dire les smartphones) endommagés et non endommagés. Dans deux articles [164, 165], les auteurs discutent de la manière d'adapter les techniques d'acquisition et d'analyse pour récupérer des données précises et pertinentes à partir de puces de mémoire flash ; cependant, cela se fait dans l'hypothèse implicite qu'elles ne sont pas endommagées. Dans un article [166], les auteurs expliquent qu'en raison de leur structure par blocs, les mémoires flash deviennent des cibles forensiques, mais ils proposent principalement une technique anti-forensique. Enfin plusieurs articles [167, 168, 169] autour des IoT discutent de la prise en compte des supports dans un cadre forensic. Il s'avère que les cartes SD ne sont que rarement prises en compte dans les enquêtes, ce qui illustre la valeur potentielle de notre protocole de diagnostic forensic pour les cartes SD endommagées et plus globalement de nos travaux sur les MMC.

1.4.3 Architecture d'une MMC

La conception d'un support de type MMC est basée sur une technologie similaire pour l'ensemble des produits SD, microSD, eMMC ou UFS. Ils sont composés d'une ou plusieurs puces de mémoires Not-AND (NAND) flash [170] (description fonctionnelle d'une mémoire flash dans la section *Gestion de la mémoire flash interne*) pour le stockage des données et d'un contrôleur [171] réalisant l'interface entre les mémoires et l'hôte (Figure 1.74).

La puce mémoire et le contrôleur sont standards. Ils sont produits par de nombreux fabricants notamment Samsung, Intel, Toshiba, Phison, Silicon Motion et Sandisk. En dehors de la taille de la carte et de l'interface externe, il n'y a pas de règles pour la conception interne que ce soit en termes d'emplacement des composants ou de leur nombre. Les fondeurs des puces doivent suivre la norme pour les signaux et les fonctions de base, ensuite ils peuvent apporter leurs propres spécifications pour certains paramètres, tels que des commandes spécifiques ou des modes d'adressages plus performant que ceux d'écrits dans les normes. Cette conception est faite pour favoriser l'intégration dans les produits et la multiplicité des applications. Le fabricant d'une MMC, à de rare exception n'est pas le fondeur des puces. Il entre dans la catégorie des intégrateurs, car il achète des puces puis les positionne et les relie entre elles. Il réalise la conception d'une carte électronique pour assurer les communications, comme pour n'importe quel système. La particularité des MMC demande ensuite au fabricant de couler son produit dans de la résine pour ne former qu'un bloc monolithique respectant les standards (eMMC, SD, microSD, UFS). Les intégrateurs qui achètent leurs puces sont par exemple : Kingston, Lexar, PNY. Certains intégrateurs achètent des contrôleurs standards pour utiliser avec leurs puces mémoires comme le fait Toshiba. D'autres encore comme SAMSUNG sont à la fois intégrateurs et fondeurs ce qui leurs permettent de faire entièrement leurs propres produits.

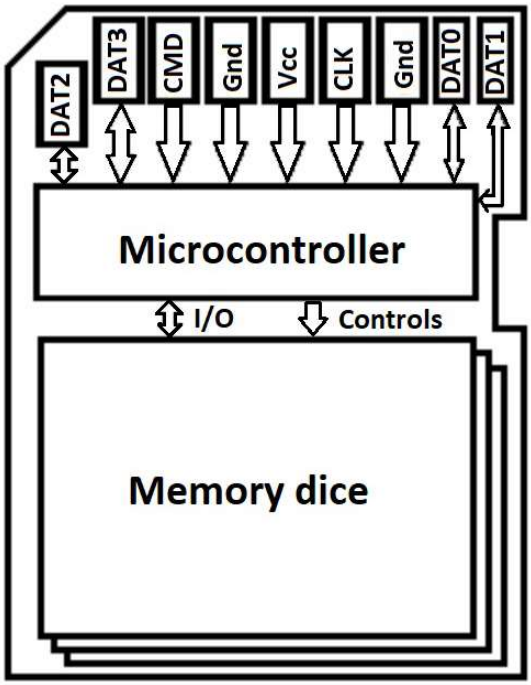


FIGURE 1.74 – Schéma de la composition interne d'une carte SD, comprenant les composants, les signaux et les bus de communication

La Figure 1.75 illustre un exemple de disposition de la puce mémoire et du contrôleur dans une carte microSD. Dans ce cas, la puce mémoire est posée sur la carte électronique et le contrôleur est positionné par-dessus la mémoire. Un autre exemple de carte microSD en vue Rayons-X (Figure 1.76) montre un positionnement différent avec une mémoire plus petite en taille directement posée sur la carte électronique. Dans ce cas, le contrôleur n'est pas placé sur la mémoire mais directement sur la carte électronique, dans le talon [5]. Il est à noter que les exemples de positionnement des puces dans le package sont sur des cartes microSD mais ils sont similaires pour les autres MMC.

Comme l'illustre la Figure 1.74, le contrôleur dispose de deux bus de communication distincts :

— Un bus externe avec le lecteur de carte, c'est-à-dire avec l'hôte qui sera plus amplement développé dans la section *La norme SD* pour les cartes SD et microSD, dans la section *La norme eMMC* pour les eMMC et dans la section *La norme UFS* pour les UFS.

— Un bus interne entre le contrôleur et la puce mémoire, pour lequel il existe plusieurs normes pour les signaux de communication qui seront développés dans la

5. Le terme de talon de la carte microSD sera utilisé pour parler de la partie de la carte qui ressort du lecteur. Cette partie est légèrement plus épaisse pour permettre à l'utilisateur une plus grande facilité d'utilisation.

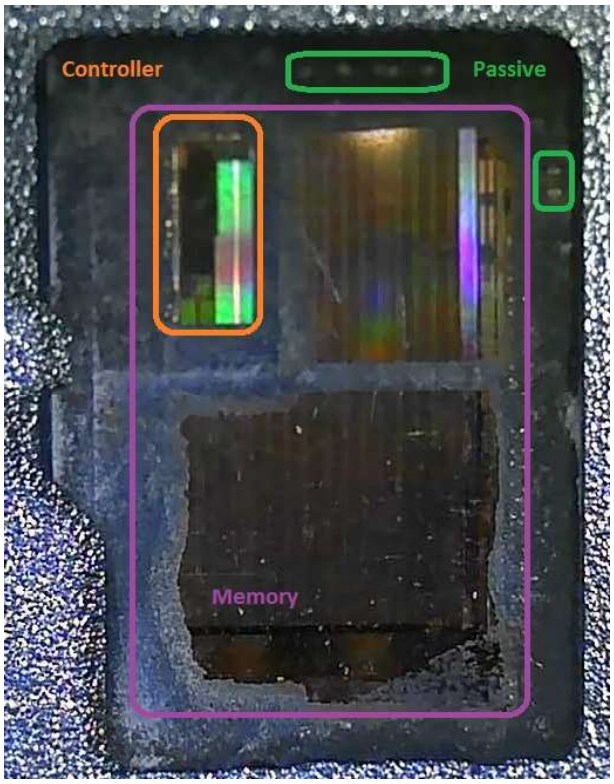


FIGURE 1.75 – Vue optique d'une carte microSD après décapsulation laser et chimique exposant le contrôleur et la puce mémoire

section *Signaux de contrôle de la mémoire flash.*

Le raccordement interne des puces est réalisé par une carte électronique constituée de deux ou quatre couches de cuivre. Dans le cas des supports SD, l'alimentation des puces se fait par le port de communication avec l'hôte, qui utilise une tension de 3.3V. Cette tension est compatible avec l'ensemble des puces de la carte. À l'inverse, pour un support de type eMMC ou UFS, le système peut fournir plusieurs tensions car les puces elles-mêmes peuvent avoir recours à différentes tensions.

Le dernier élément identifiable sur les supports est la présence potentielle de plots de debug. Il s'agit de plots dans le design du PCB permettant les tests ou la programmation des composants lors de la fabrication (Figure 1.77). Il existe différentes matrices pour les plots, mais malgré une forme et un emplacement déterminé, il n'y a pas de normes pour le positionnement des signaux sur les plots. De plus, ils ne sont pas présents sur l'ensemble des supports MMC. Dans ce cas, il faudra trouver une autre solution pour interagir avec les composants internes, par exemple en utilisant les vias du PCB. Cet aspect est plus amplement développé dans la section *Interconnexion.*

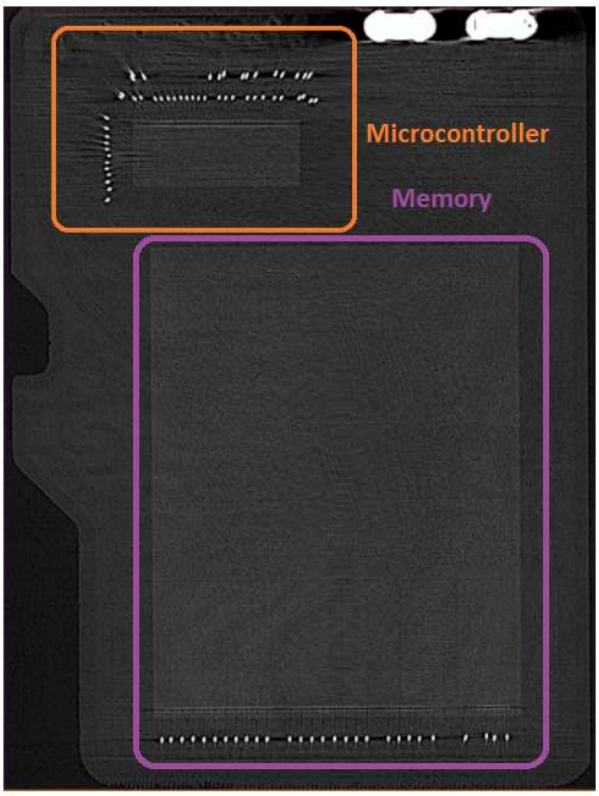


FIGURE 1.76 – Vue aux Rayons-X d'une carte microSD sur laquelle sont mis en évidence le contrôleur et la puce mémoire

1.4.4 Protocole de communication entre la MMC et l'hôte

1.4.4.1 La norme SD

Dans l'introduction des supports de ce chapitre, la norme SD a été introduite comme un consortium ayant créé une association appelée SD Association [155]. L'objectif de ce regroupement de fabricants était de produire un standard pour l'intéropérabilité des supports et des lecteurs.

Le premier paramètre définit par la norme SD est le format. Il existe plusieurs modèles de carte appelés SD et microSD, dont les cotations exactes sont précisées dans des documents. La Figure 1.78 est un exemple des dimensions que doit respecter une carte microSD. Cette illustration peut d'ailleurs être retrouvée dans les documentations techniques de produits finaux à destination des fabricants de lecteurs.

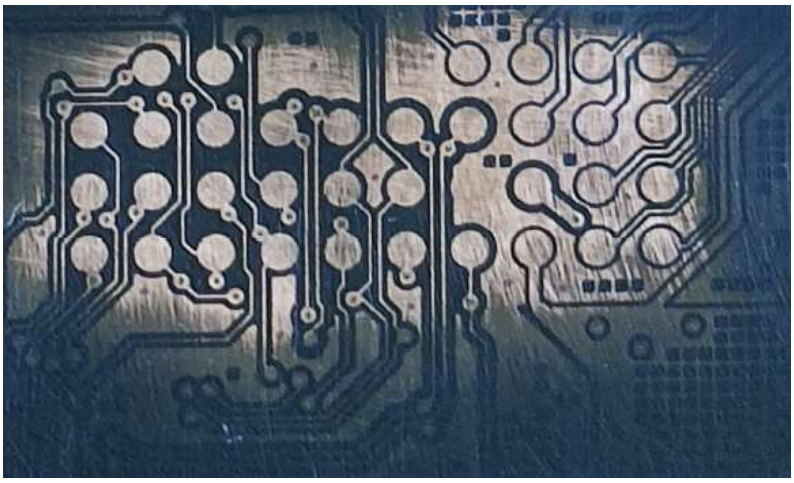


FIGURE 1.77 – Vue optique des plots de debug d'une carte SD après polissage du vernis

Le second paramètre définit par la norme SD est le protocole de communication. Comme l'illustre sur la Figure 1.74, l'interface entre l'hôte et la carte SD utilise des signaux d'alimentation, de contrôle et d'E/S. Il est à noter que les deux formats SD et microSD ne disposent pas des mêmes nombres de signaux. En effet, la carte SD dispose d'une broche d'alimentation de plus destinée à une masse. L'affectation du rôle des broches est définie dans le Tableau 1.11. D'après ce tableau, nous pouvons distinguer des signaux spécifiques de contrôle qui sont constitués d'une horloge (CLK) et d'un signal de commande (CMD). L'horloge est fournie par l'hôte et permet de cadencer les échanges entre les deux parties. Le signal de commande permet de définir les messages à transmettre entre l'hôte et la carte. Les autres signaux présents sur la carte sont des entrées/sorties liés aux échanges de données. Ils sont appelés DATx avec x leur numéro associé.

Tableau 1.11 – Comparaison des signaux entre la carte SD et la carte microSD

Fonction du signal	Nom du Signal	Pinout carte SD	Pinout carte microSD
Alimentation	Vcc	4	4
	Gnd	3, 6	6
Contrôles	CMD	2	3
	CLK	5	5
I/O	DAT0	7	7
	DAT1	8	8
	DAT2	9	1
	DAT3	1	2

Le fonctionnement des cartes SD est basé sur le concept de machine à états. Au début du cycle de démarrage du support, le contrôleur entre dans cette machine à états. Pour passer à l'étape suivante, il faut avoir rempli les conditions requises. Il existe aussi une possibilité d'embranchements dans les séquences qui permettent de basculer dans des

SYMBOL	COMMON DIMENSIONS (mm)			NOTE
	MIN[2]	NOM[2]	MAX[2]	
A	10.90	11.00	11.10	
A1	9.60	9.70	9.80	
A2	-	3.85	-	BASIC
A3	7.60	7.70	7.80	
A4	-	1.10	-	BASIC
A5	0.75	0.80	0.85	
A6	-	-	8.50	
A7	0.90	-	-	
A8	0.60	0.70	0.80	
A9	0.80	-	-	
B	14.90	15.00	15.10	
B1	6.30	6.40	6.50	
B2	1.64	1.84	2.04	
B3	1.30	1.50	1.70	
B4	0.42	0.52	0.62	
B5	2.80	2.90	3.00	
B6	5.50	-	-	
B7	0.20	0.30	0.40	
B8	1.00	1.10	1.20	
B9	-	-	9.00	
B10	7.80	7.90	8.00	
B11	1.10	1.20	1.30	

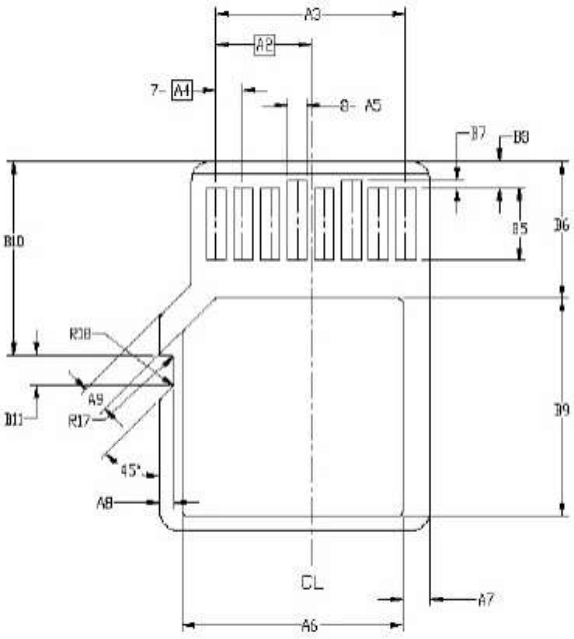


FIGURE 1.78 – Dimensions standard d'un support (carte microSD) référencé dans une datasheet [47] d'après les normes émises par le SD Association

modes particuliers. Le schéma de la machine à états d'initialisation de la carte SD est illustré en Figure 1.79.

Pour aller plus loin dans l'étude de cette machine à états, nous pouvons analyser la mise sous tension de la carte. Cette fonction est d'ailleurs appelée "hardware reset". Lorsque l'électricité parvient à la carte, le contrôleur est dans un état d'inactivité et attend de recevoir des commandes parmi les 64 prédéfinies [49]. La première commande est `CMD0` pour définir le mode du bus. Une carte SD fonctionne suivant deux protocoles possibles que sont SD ou SPI. Lors d'un fonctionnement normal, c'est le protocole SD qui est utilisé car il est plus rapide. Le protocole SPI est plutôt un protocole de debug pour des commandes basiques et nous ne l'aborderons pas dans ce mémoire.

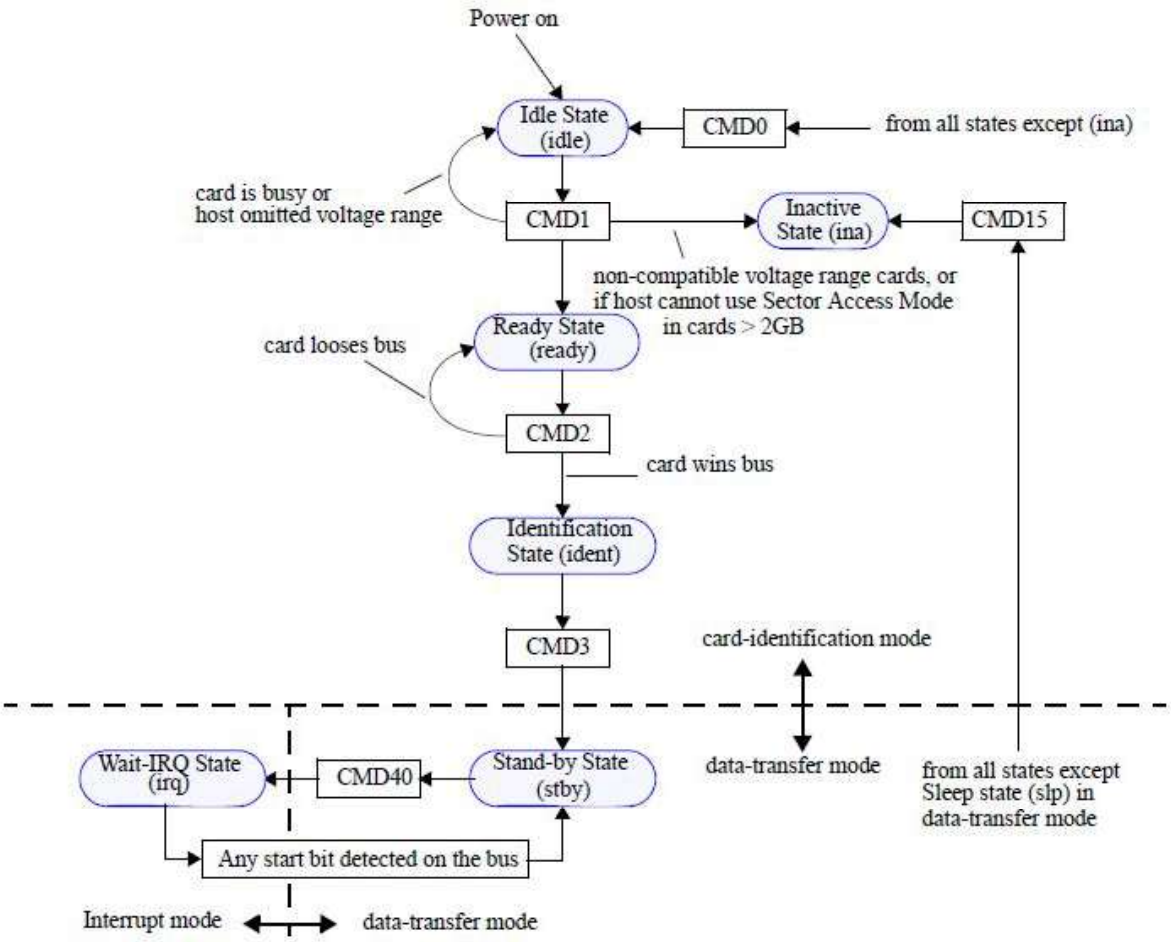


FIGURE 1.79 – Machine à états assurant l'initialisation d'une carte SD d'après la norme JEDEC JESD84-A43 [48]

Au stade de cette première commande, la machine à états est conçue pour fonctionner sur une largeur de bus de 1 bit. Cela signifie que seul DAT0 est utilisé pour les transferts de données. Cependant, lors de la phase de boot initiale un registre est configuré en interne de la carte pour prédéfinir la taille maximum du bus d'I/O. La carte peut utiliser un bus de données de 2 bits (DAT0-DAT1) ou 4 bits (DAT0-DAT3).

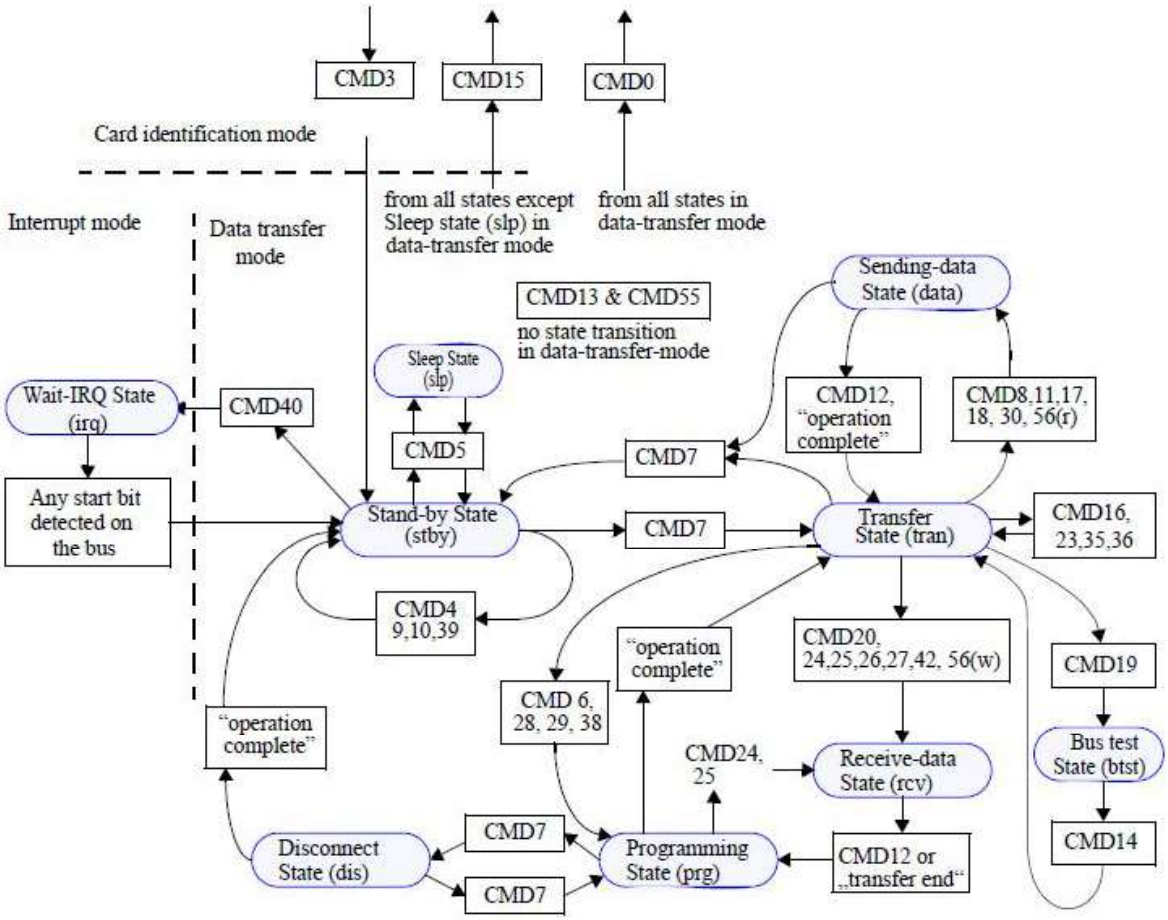


FIGURE 1.80 – Machine à états assurant le transfert des données d'une carte SD d'après la norme JEDEC JESD84-A43 [48]

La machine à états d'initialisation s'inscrit dans une autre plus globale, qui est présentée en Figure 1.80. Pour chacune des commandes utilisées, elle peut être en lecture `read` ou en écriture `write`. L'exemple de trames est visible sur les Figures 1.81 et 1.82. Aux vues de la trame de lecture, l'hôte envoie une commande de lecture, qui est validée par la carte. Ensuite la carte renvoie les trames de données constituées des données en elles-mêmes et d'octets provenant d'un code de détection d'erreurs (Cyclic Redundancy Check ou CRC[6]. Le CRC permet à l'hôte d'ainsi valider l'exactitude de la lecture, ou demander à nouveau la lecture en cas de mauvaise réception. En comparant les courbes de lecture et d'écriture, la différence notable que nous pouvons remarquer se situe dans la présence d'une attente `busy` lors de l'écriture.

6. Le CRC est un algorithme de détection d'erreurs qui prend en entrée des séquences de données et les divisent par un polynôme. Le quotient de cette division est ensuite ajouté à la séquence de données originale. Lors de la vérification des données, la division du polynôme du message reçu est comparée avec celui d'origine pour valider la concordance. S'ils divergent, la récupération de la donnée a été incorrecte. Le calcul exact du CRC d'une carte SD est défini dans la norme JEDEC JESD84-A43 [48].

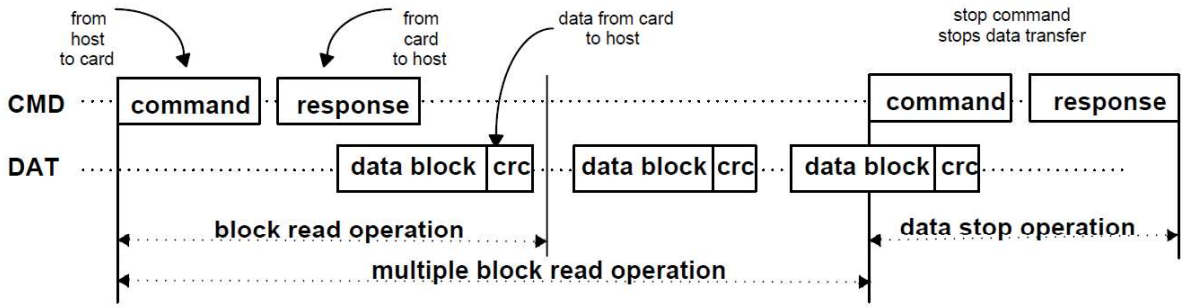


FIGURE 1.81 – Protocole entre l'hôte et le contrôleur pour l'opération de lecture en mode SD [49]

D'après la Figure 1.82 la temporisation est faite pour permettre à la carte de calculer correctement les CRC de la transmission précédente avant que le contrôleur renvoi une nouvelle vague de données.

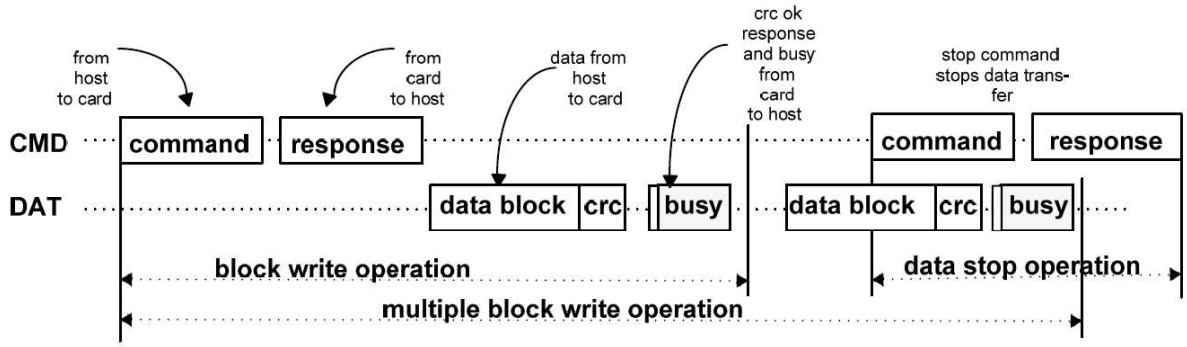


FIGURE 1.82 – Protocole entre l'hôte et le contrôleur pour l'opération d'écriture en mode SD [49]

1.4.4.2 La norme eMMC

Les mémoires eMMC sont similaires aux cartes SD, et elles sont basées sur la norme JEDEC JESD84-A41 [156]. D'un point de vue protocolaire, les supports respectent la même norme JESD84-A43 [48] et elles possèdent les mêmes concepts pour les communications. Alors que le support au format SD ne dispose que d'un maximum de 9 broches, les eMMC peuvent se présenter sous plusieurs packages. Les plus courants sont les BGA153, BGA162 ou BGA221 (Figure 1.83). Le terme BGA signifie Ball Grid Array et représente littéralement un composant équipé d'une matrice de billes. La présence des billes de soudure implique qu'il s'agisse d'une mémoire conçue pour être intégrée dans le système, contrairement à la carte SD. La liaison du composant avec la carte électronique se fait par les billes de soudure, le rendant inamovible à l'exception de faire refondre les billes.

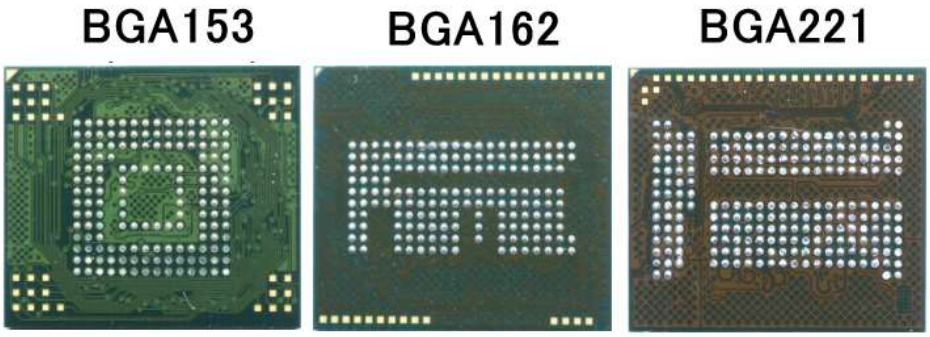
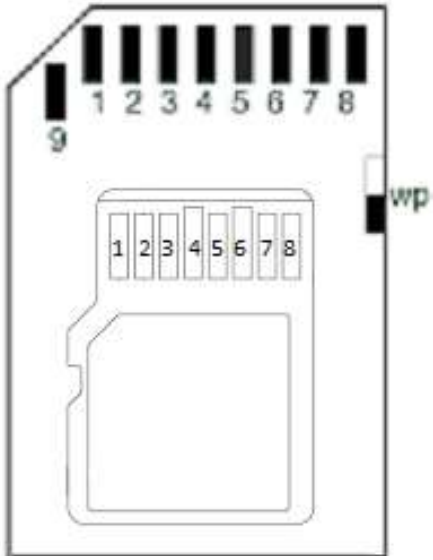
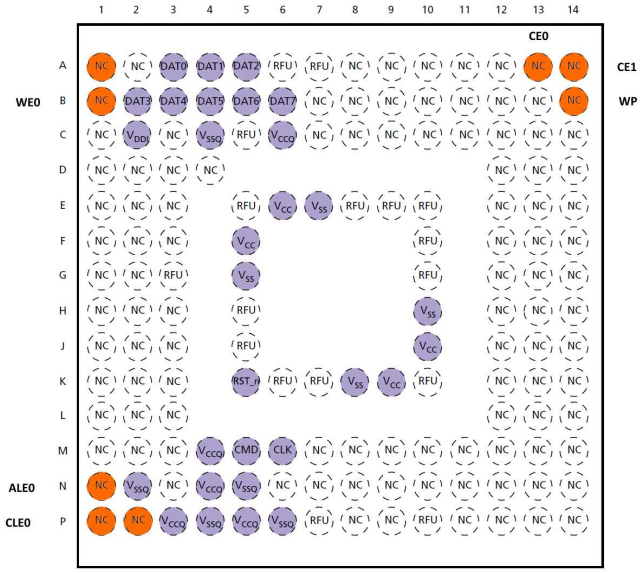


FIGURE 1.83 – Comparaison des pinouts des formats BGA153, BGA162 et BGA221 pour des eMMC

Le nombre de billes présentes n'inclus pas nécessairement une utilisation de chacune d'entre elles. Un parallèle peut être fait entre le brochage des supports SD (Figure 1.84a) et le support eMMC de type BGA153 (Figure 1.84b).



(a) Carte SD et microSD



(b) Mémoire eMMC BGA153 [172]

FIGURE 1.84 – Brochage des supports MMC sur différents formats

En reprenant le Tableau 1.11 créé pour les cartes SD, il est possible de produire le Tableau 1.12. Contrairement aux cartes SD, l'eMMC dispose d'une broche de Reset. Elle possède également plus de signaux d'entrées/sorties, ce qui permet d'avoir un port de communication sur 8 bits, donc une vitesse de transfert accrue.

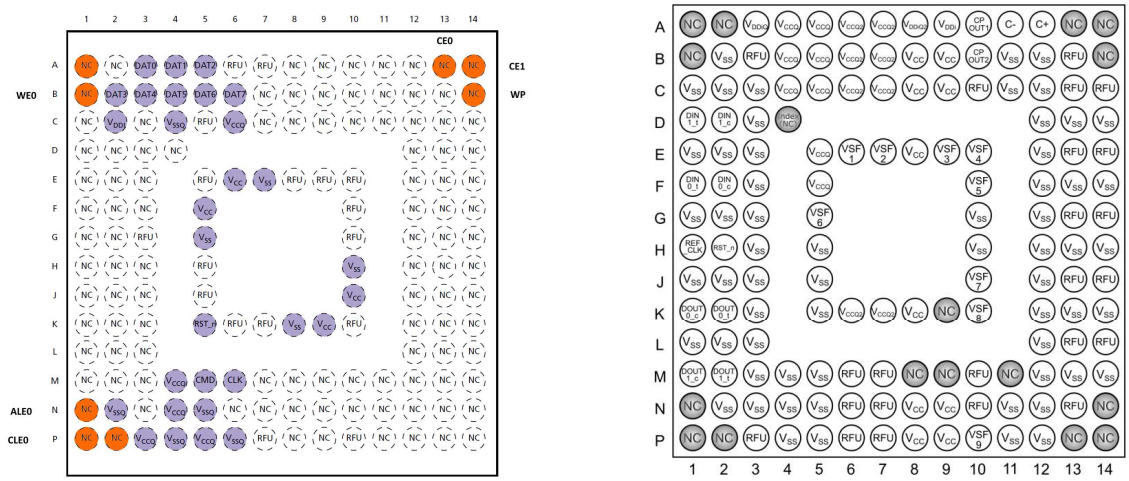
Tableau 1.12 – Comparaison des signaux entre la carte SD, la carte microSD et la mémoire eMMC BGA153

Fonction du signal	Nom du Signal	Pinout carte SD	Pinout carte microSD	Pinout eMMC BGA153
Alimentation	Vcc	4	4	9 pins
	Gnd	3, 6	6	9 pins
Contrôles	CMD	2	3	M5
	CLK	5	5	M6
	RST	**X**	**X**	K5
I/O	DAT0	7	7	A3
	DAT1	8	8	A4
	DAT2	9	1	A5
	DAT3	1	2	B2
	DAT4	**X**	**X**	B3
	DAT5	**X**	**X**	B4
	DAT6	**X**	**X**	B5
	DAT7	**X**	**X**	B6

X : Absents

1.4.4.3 La norme UFS

Les mémoires de types UFS utilisent leurs propres protocoles de communication avec l'hôte, totalement différent des autres supports MMC. Elles sont basées sur l'empreinte BGA153, et des billes initialement vides sur l'eMMC sont utilisées pour l'UFS, comme le montre la Figure 1.85.



(a) Mémoire eMMC en BGA153 [172]

(b) Mémoire UFS en BGA153 [173]

FIGURE 1.85 – Différence de pinout entre une eMMC et une UFS en package BGA153

La technologie UFS est basée sur les signaux en paires différentiels. Cela implique que chaque signal de donnée dispose d'un signal '+' et d'un signal '-'. La principale plus-value lors de l'utilisation de paires différentielles est la capacité à augmenter les vitesses de transfert. En effet, le fait que les signaux soient redondés sur deux lignes limitent la perte de la donnée. De plus, ces signaux sont en opposition de phase et tracés côte à côte ce qui réduit les perturbations électromagnétiques possibles ainsi que les effets capacitifs. Les mémoires UFS fonctionnent avec deux paires différentiels distinctes, elles-mêmes composées d'une ligne d'entrée et d'une ligne de sortie, comme le montre le Tableau 1.13. Contrairement à la mémoire eMMC, il ne s'agit plus d'une seule ligne bidirectionnelle, mais de deux lignes distinctes. Pour commander la mémoire, le signal d'horloge ainsi que le Reset sont toujours présents. Cependant le signal de commande `CMD` n'est plus présent et l'ensemble des commandes passent par l'entrée des paires différentielles.

Tableau 1.13 – Position des signaux de la mémoire UFS en package BGA153

Fonction du signal	Nom du signal	Pinout
Alimentation	Vcc	10 pins
	Vccq	6 pins
	Vccq2	8 pins
	Gnd	61 pins
Contrôles	REF_CLK	H1
	RST_N	H2
I/O	DIN0_N	E1
	DIN0_P	E2
	DIN1_N	D1
	DIN1_P	D1
	DOUT0_N	K1
	DOUT0_P	K2
	DOUT1_N	M1
	DOUT1_P	M2

Sur le plan du protocole de communication, la mémoire UFS fonctionne également sur la base d'une machine à états, mais elle n'utilise pas les mêmes commandes que l'eMMC. Les commandes en elles-mêmes pour piloter la mémoire sont différentes. Un échange entre l'hôte et le contrôleur sur le protocole UFS est composé de deux parties principales : l'en-tête de trame et la charge utile. L'en-tête de trame contient les informations de contrôle nécessaires pour la transmission des données, telles que le type de trame, la longueur de la trame et l'adresse du périphérique (Tableau 1.14). La charge utile contient les données utiles à transférer. Le type de trame est définie par une combinaison d'octets présentés dans le Tableau 1.15. Concernant la longueur de la trame, elle est limitée à 1024 octets.

Tableau 1.14 – Trame de communication pour le protocole UFS entre l'hôte et le contrôleur

Indice d'octet	Champ	Description
0	Type	Indique le type de trame
1	Longueur	Indique la longueur de la trame en octets
2	Adresse	Indique l'adresse du périphérique de destination, défini par l'hôte
3-N	Charge utile	Contient les données réelles à transférer

Tableau 1.15 – Valeur pouvant prendre le champ Type dans la trame de communication

Type	Signification	Description
0x00	Trame de commande	Indique une commande envoyée par l'hôte au contrôleur de mémoire
0x01	Trame de réponse	Indique une réponse envoyée par le contrôleur à l'hôte
0x02	Trame de données	Indique des données envoyées par le contrôleur de mémoire à l'hôte ou vice versa
0x03	Trame de contrôle	Indique une trame de contrôle utilisée pour des tâches telles la reconnaissance de périphérique ou sa configuration

1.4.5 Gestion de la mémoire flash interne

1.4.5.1 Signaux de contrôle de la mémoire flash

La mémoire flash est basée sur deux bus afin d'assurer les communications avec le contrôleur qui lui est associé. Le premier bus est composé de signaux de contrôle qui permettent d'envoyer des commandes à la mémoire et le second bus est dédié aux données. L'ensemble des signaux est défini par la norme ONFI [54] et résumé dans le Tableau 1.16.

Tableau 1.16 – Signaux des mémoires NAND flash référencés dans la norme ONFI avec les fonctions respectives

Nom du pin	Input/Output	Fonction
CEn	Input	Chip Enable
CLE	Input	Command Latch Enable
ALE	Input	Address Latch Enable
WE	Input	Write Enable
RE	Input	Read Enable
IO[7 :0]	Input/Output	Data Input/Output
R/B	Output	Ready/Busy
WP	Input	Write Protect

Pour envoyer une commande à la puce, le contrôleur doit activer la ligne `CEn` en la tirant vers le bas (soit '0' logique). Cette fonctionnalité permet de relier le contrôleur à plusieurs puces mémoires de type flash en utilisant les mêmes signaux de contrôles et de données sous forme de bus. Le seul signal qui permettra au contrôleur de s'adresser à

une puce mémoire précise sera le CEn, où n représente le numéro symbolique de la puce concernée. Lorsque la puce mémoire cible reçoit le signal CE à '0', elle prend en compte les commandes suivantes.

Tableau 1.17 – Commandes référencées dans la norme pour les échanges entre le contrôleur et la mémoire, pour les actions liées au statut ou aux pages

Mode	Fonction	1ère commande	nb adresses	2ème commande
Paramètrage	Reset	FFh		
	Read Status	70h		
Identification	Read ID	90h	1	
	Read Page Parameter	ECh	1	
	Read Unique ID	EDh	1	
Configuration	Set Feature	EFh	1	
	Get Feature	EEh	1	
Pilotage	Page Read	00h	5	30h
	Page Program	80h	5	10h
	Block Erase	60h	3	D0h
	Random Data Input	85h	2	
	Random Data Output	05h	2	E0h

Pour valider une action que la mémoire doit traiter, il faut d'abord choisir une commande parmi une liste normalisée (Tableau 1.17). Pour indiquer qu'il s'agit d'une commande c'est le signal `CLE` qui est activé en le tirant vers le haut (valeur '1' logique). En parallèle, les I/O sont sollicités pour choisir le code de la commande appliquée. Dans la Tableau 1.17, le Reset est défini par "FF" donc les I/O devront être tous à '1' pour former la combinaison. On notera qu'il existe dans le tableau des commandes avec un ou deux codes à composer. Ainsi pour la commande READ_ID, le contrôleur devra actionner `CLE` et afficher sur les I/O la valeur "90". Dans un second temps, il devra actionner un autre signal de commande appelé `ALE`, destiné à renseigner les adresses. Pour le READ_ID, le niveau logique haut de `ALE` valide l'adresse "00" appliquée sur les I/O. En revanche pour d'autres commandes nécessitant plus d'actions, comme par exemple un READ_PAGE qui nécessite d'entrer une adresse sur cinq octets, entre deux valeurs de `CLE`, la commande sera constituée de `CLE` qui se combine avec la valeur "00" sur les I/O, puis `ALE` avec cinq octets d'adresses sur les I/O et enfin `CLE` avec la valeur "30" sur les I/O.

Pour valider chaque élément de la commande, le contrôleur utilise le signal `WE`. Celui-ci doit réaliser un front montant pour que l'information soit actée par la mémoire, qui devra répondre en activant les I/O. La lecture (c'est-à-dire la prise en compte) de chaque octet de la réponse sera validé par le signal `RE`, qui est actionné par le contrôleur et soumis à des timings. Pour faciliter les échanges, le contrôleur dispose d'un signal `R/B` permettant à la mémoire d'indiquer son état, et en particulier lorsque le bus I/O est prêt.

Le dernier signal disponible au contrôleur pour piloter la mémoire est `WP`. Il permet,

lorsqu'il est actif, donc bloqué à l'état bas ('0' logique) de bloquer toute action d'écriture sur la mémoire. Cette fonctionnalité peut être particulièrement intéressante dans un contexte de la forensique numérique, dans l'objectif de la conservation de la preuve.

Les échanges entre le contrôleur et la mémoire peuvent se faire suivant plusieurs vitesses de transfert, qui dépendent du mode de validation de la donnée lors des échanges. Le mode de transfert classique et historique est appelé Single Data Rate (SDR), car la validation de la donnée lors du transfert à lieu sur les fronts montants ou descendants de l'horloge. Pour gagner en vitesse de transfert, les fabricants de composant ont développés deux autres protocoles appelés Toogle mode et Double Data Rate (DDR). Ces deux protocoles de communication entre le contrôleur et la mémoire utilisent les deux fronts de l'horloge (c'est-à-dire le front montant et le front descendant) pour valider la donnée lors des échanges. Ces deux protocoles ont été développés en parallèles, par des associations de fabricants de composants, et ils se différencient par la liste des commandes utilisées. Pour pallier ces différences et conserver une compatibilité entre les différents composants, ils utilisent tous le mode SDR lors de leur initialisation. Par la suite, le contrôleur négocie le mode de transfert avec la mémoire et s'adapte en fonction de la réponse. Mentionnons que dans le contexte d'une expertise judiciaire, la fiabilité de la donnée prime sur la vitesse des opérations. Par conséquent, lors de l'extraction de données d'une mémoire, l'expert privilégiera la configuration initiale (c'est-à-dire le mode SDR) pour effectuer ses opérations.

1.4.5.2 Protocole de communication interne

La mémoire flash contient les données stockées dans ses "cellules". Une cellule de mémoire est essentiellement un transistor à grille flottante, dont l'état est déterminé par sa tension de seuil. La tension de seuil d'un transistor à grille flottante est déterminée par la quantité de charges stockées dans sa grille flottante. Les notions de transistors ont été plus amplement présentées dans la section *Le transistor*.

Pour la mémoire flash SLC (Single Level Cell) NAND, la valeur stockée d'une cellule peut être soit '0', soit '1'. S'il n'y a pas de charge dans la grille flottante, la valeur est de '1'. En revanche, lorsqu'une tension est appliquée à la grille de contrôle, cela entraîne le piégeage de charges dans la grille flottante. Ainsi, de la donnée est stockée prenant la valeur de '0'.

Afin de réduire le coût par bit et de stocker davantage de données dans une matrice de transistors, les technologies MLC (Multi Level Cell) ou TLC (Triple Level Cell) sont aujourd'hui couramment utilisées dans la fabrication des mémoires flash NAND. Les cellules MLC et TLC stockent respectivement 2 (0b00 à 0b11) ou 3 (0b000 à 0b111) bits de données dans une cellule.

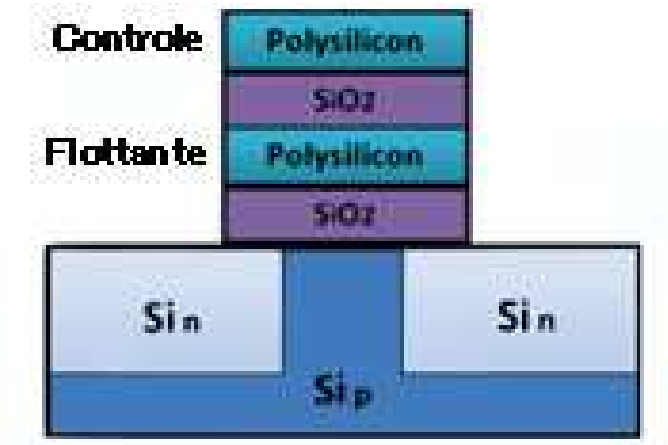


FIGURE 1.86 – Illustration d'un transistor possédant une double grille (contrôle et flottante)

La structure simplifiée d'une cellule de mémoire flash MLC NAND est illustrée Figure 1.87. Une fois que la charge est piégée dans la grille flottante, une tension plus élevée est nécessaire pour activer le transistor. La tension de la grille de contrôle, Vcg, à laquelle le transistor peut être activé (c'est-à-dire que le courant peut circuler entre la source et le drain du transistor, Ids) est appelée tension de seuil (Vth dans la Figure 1.87). Les données stockées peuvent être lues en appliquant la tension entre la tension de seuil de chaque état et en vérifiant si le courant passe. Cette tension est appelée tension de lecture (Vread dans la Figure 1.88).

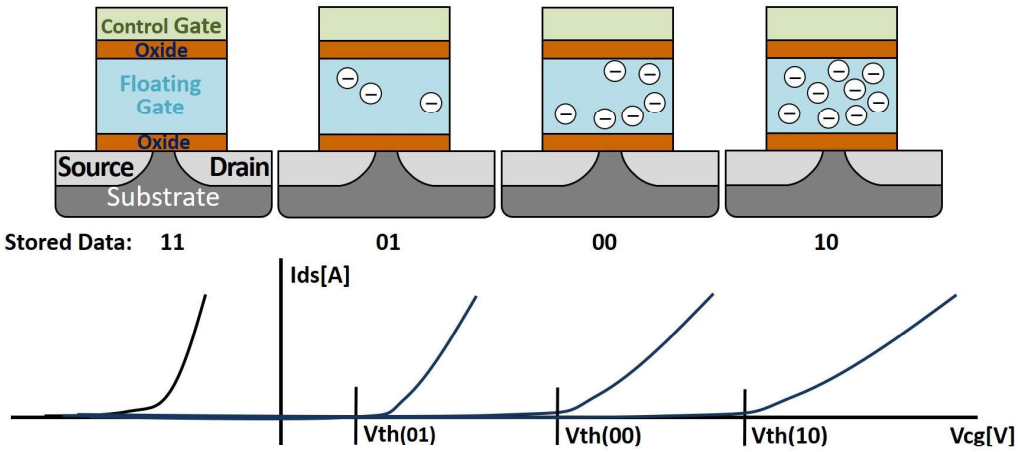
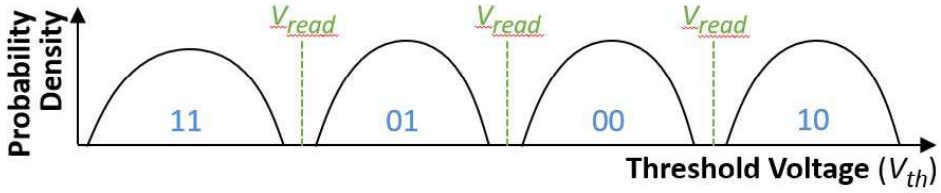
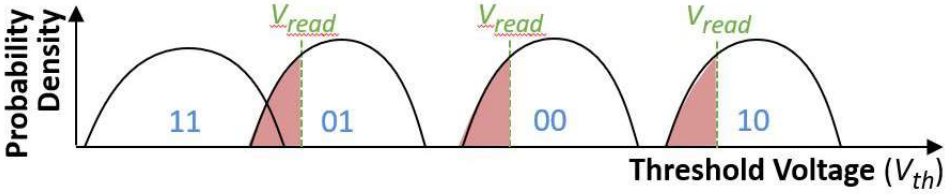


FIGURE 1.87 – Cellule mémoire NAND flash MLC, illustration de l'évolution des charges permettant de charger la grille flottante et ainsi de stocker des données dans la cellule

Dans une mémoire flash, l'opération de lecture ou d'écriture n'est pas effectuée bit par bit, elle est effectuée par *page*. Une page est un groupe de cellules mémoire connectées en série. Bien que la taille de la page varie d'un modèle de mémoire à l'autre, une page se compose généralement de 4k à 16k octets de données dans la mémoire flash moderne.



(a) Distribution des tensions de seuil des cellules de mémoires NAND flash



(b) Distribution des tensions de seuil après fuite des charges

FIGURE 1.88 – Modèle de distribution de tensions de seuil pour une cellule mémoire NAND flash de technologie MLC, les zones colorées représentant de potentielles erreurs de bits

À la notion de page se rajoute la notion de *blocks* (Figure 1.89). Comme nous pouvons le constater, cette mémoire spécifique est conçue à base de 2048 bits par page avec 64 bits en plus pour les méta-données, appelés spares. Les spares regroupent les données utiles au contrôleur pour remettre dans l'ordre les pages, ainsi que les éléments servant à la correction des erreurs de la page. Un groupe de 64 pages forment un bloc, qui est la plus petite unité pouvant être effacée par le contrôleur. Dans la flash d'exemple, les blocs sont au nombre de 2048 pour former une unité logique, aussi appelé *device* dans ce cas. Il arrive que les mémoires regroupent plusieurs unités logiques, ce qui permet de multiplier le nombre de cellules, et donc d'accroître la taille de la mémoire.

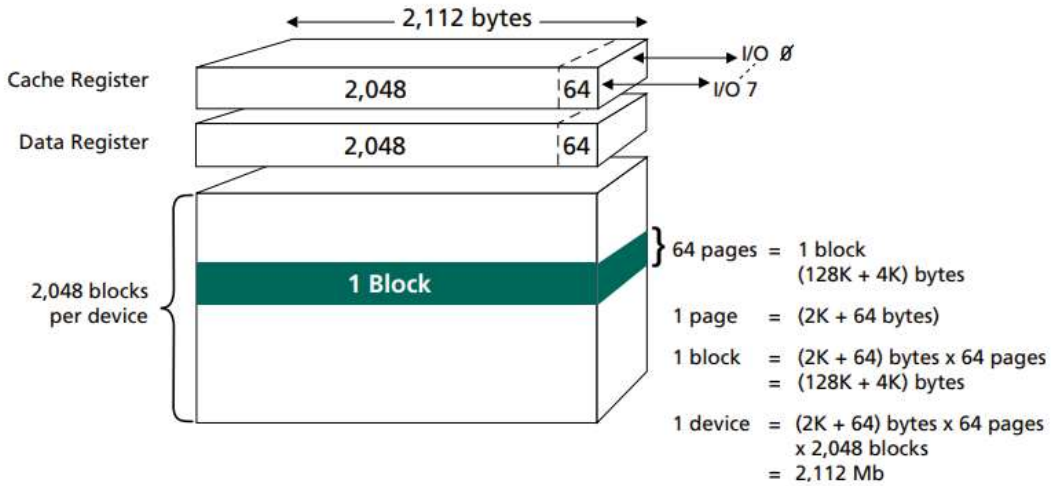


FIGURE 1.89 – Vue de l'organisation d'une mémoire flash Micron [50]

Le contrôleur servant d'interface entre les puces de mémoires flash NAND brute et l'hôte pour offrir un stockage de données géré, est également chargé de l'organisation des données. Il répartit les données dans le plan mémoire des différentes puces pour optimiser la lecture/écriture. Lors des premiers échanges entre le contrôleur et la mémoire, celui-ci identifie les zones mémoires corrompues, ce qui permet de les exclure de la table de gestion et ainsi ne plus les solliciter lors des écritures. En outre, il permet de corriger les erreurs de lecture et la corruption de la mémoire à l'aide du code correcteur d'erreurs (ECC). Le contrôleur effectue également des opérations mathématiques sur les données afin d'accroître la durée de vie des mémoires. Ces deux derniers aspects seront abordés dans la section suivante.

1.4.5.3 Management des erreurs

Dans cette section, nous allons nous attarder sur les opérations réalisées par le contrôleur lors de la lecture de la mémoire. Les opérations d'intérêt sur lesquelles nous allons nous focaliser sont la gestion de la durée de vie de la mémoire et les corrections des erreurs dit Error Correction Code (ECC). La mémoire flash a une durée de vie limitée en raison de l'usure de l'oxyde isolant. En effet, cet oxyde est une couche très fine qui se situe sous les grilles de contrôle et les grilles flottantes (Figure 1.86). Sa permittivité garantit la capacité de piégeage des électrons dans la grille flottante. Chaque fois que les données sont stockées et effacées, les charges traversent la couche d'oxyde. Après de nombreuses opérations répétées, la couche d'oxyde s'abîme et elle assure de moins en moins bien son rôle. Une fois que la couche d'oxyde est abîmée, les charges stockées dans la porte flottante peuvent s'échapper à travers elle. La perte de charges sur une grille flottante entraîne une réduction de la tension de seuil de la cellule. Par conséquent, lorsque la tension de lecture est appliquée, les données sont lues comme une valeur différente (par exemple, de 0b01 à 0b11 comme illustré Figure 1.88), ce qui provoque une erreur de bit.

Pour maintenir l'intégrité des données stockées dans la mémoire flash, les contrôleurs de mémoire flash doivent mettre en œuvre un mécanisme de correction des erreurs. Le code de correction d'erreur (ECC) est la solution la plus couramment utilisée. Pour garantir l'intégrité des données pendant le stockage (ou en tout cas à la relecture), l'ECC est calculé pour chaque bloc de données et stocké avec les données originales dans la mémoire flash. La capacité de correction d'erreurs varie selon le contrôleur, mais la capacité minimale requise est définie par le fabricant de la mémoire flash.

L'un des codes ECC les plus couramment utilisés par les contrôleurs de mémoire flash est le code BCH. Il a été inventé en 1959 par Alexis Hocquenghem, et en 1960 par Raj Chandra Bose et D.K. Ray-Chaudhuri [174, 175]. Le code BCH est un traitement cyclique de la donnée. Il ne traite pas un nombre de donnée fixe mais variable en fonction du

nombre d'erreurs rencontrées. L'objectif est que le nombre d'erreurs soit inférieur ou égal à la moitié de la longueur des données à corriger. Par exemple, pour une mémoire flash avec une taille de page de 2 koctets de données, la taille des spares de 128 octets, contenant les ECC, permet de corriger jusqu'à 48 bits d'erreurs. Cela signifie aussi que si le nombre d'erreurs devient trop important, la séquence de calcul devra être adaptée en conséquence. Le code BCH est connu pour son efficacité dans la réalisation de la capacité de correction d'erreurs requise pour la mémoire flash. Dans des conditions normales d'utilisation, ce système d'ECC corrige les erreurs de bits internes à la mémoire, de manière à ce que l'hôte réceptionne les données lues normalement. Toutefois, si plus de 49 bits de données deviennent erronés parmi les 2 koctets de données codées, les erreurs ne peuvent plus être corrigées, ce qui provoque des erreurs système. En d'autres termes, si les cellules de la mémoire flash s'abîment excessivement et que le nombre d'erreurs dépasse la capacité de correction de l'ECC, ces données ne peuvent plus être corrigées au moyen d'une correction ECC normale (sauf si certaines informations sont connues sur la structure du contenu, comme abordé dans la section *Fiabilisation de la donnée*).

Les ECC sont donc importants pour maintenir l'intégrité des données dans les mémoires. Il existe de multiples sources d'erreurs de bits dans les mémoires flash NAND, notamment les interférences entre cellules, les fuites de charges, les perturbations de lecture et la mauvaise programmation des transistors lors de l'écriture. À chaque accès à une page pour effectuer une lecture, le contrôleur effectue des calculs ECC. Si le processus de correction ECC ne permet pas de récupérer l'intégrité des données, le contrôleur peut éventuellement refaire une tentative de lecture de la page avec les mêmes paramètres ou en les adaptant, comme en changeant l'horloge, par exemple. L'objectif est de transmettre à l'hôte une lecture exempt d'erreurs. Avant d'écrire les données à stocker dans la mémoire, le contrôleur calcule la valeur ECC pour les insérer dans la plage des données de spares.

En parallèle de l'aspect de correction des erreurs dans la mémoire, un autre rôle important que joue le contrôleur réside dans la préservation de la durée de vie de la mémoire. Le contrôleur met en œuvre un algorithme de nivellement de l'usure (appelé wear-leveling) dans les différentes zones de la mémoire, ce qui permet de limiter les répétitions d'écriture dans certaines zones, alors que d'autres sont rarement utilisées. Les cellules de mémoire flash NAND supportent généralement environ 5000 cycles de programmation, paramètre qu'il faut mettre en opposition avec l'utilisation moderne des mémoires flash. Sur les appareils comme les smartphones, le chargement et l'écriture des données est permanent et les appareils fonctionnent sans s'arrêter pendant plusieurs jours, ce qui provoque une utilisation de la mémoire constante.

La Figure 1.90 illustre l'objectif du mécanisme de nivellement de l'usure qui est d'effacer le moins possible dans chaque bloc, en écrivant les nouvelles données en priorité sur les blocs vides les moins utilisés. Il est basé sur le nombre d'effacements dans chaque

bloc, en utilisant un mécanisme de compteur incrémenté.

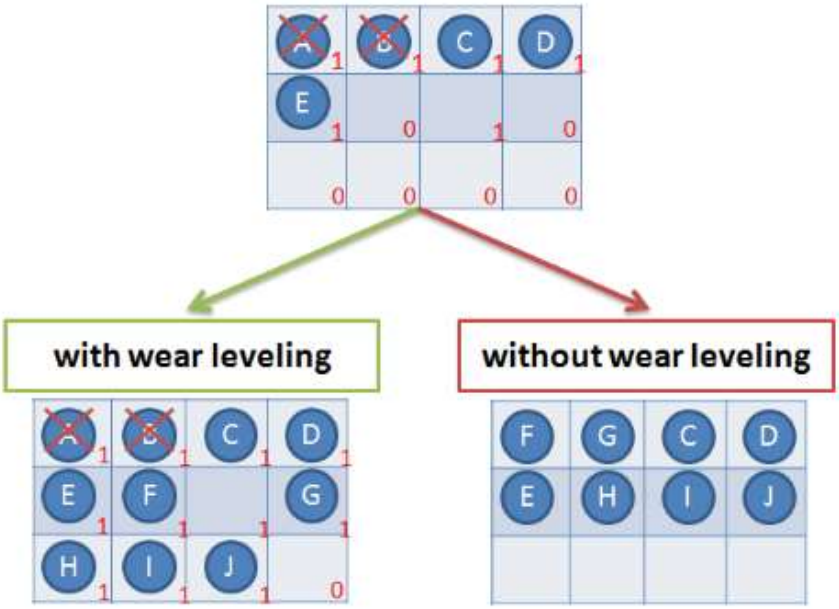


FIGURE 1.90 – Exemple d'écriture de nouvelles données avec et sans wear-leveling dans une mémoire NAND flash [51]

L'exemple présenté dans la Figure 1.90, illustre le comportement du contrôleur avec ou sans l'utilisation du wear-leveling. Supposons une mémoire dont cinq blocs sont remplis de données. Les blocs A et B, possèdent un contenu qui est effacé. Cela signifie que pour un bloc fonctionnel, le contrôleur aura le droit de le réécrire à volonté. À noter que les blocs ne sont pas systématiquement libérés afin d'éviter un changement d'état superflu des cellules mémoires. Pour préserver la durée de vie des mémoires flash, la stratégie utilisée est d'enrichir une table de gestion des pages et des blocs. Cette table permettra au contrôleur de connaître l'état d'utilisation, ce qui favorisera une bonne utilisation des ressources. Dans le cas d'une nouvelle écriture, sans présence de wear-leveling, les nouvelles pages (F et G) sont écrites dans les premiers blocs disponibles. Le contrôleur ne monitorant pas l'usure des blocs, F et G seront écrites à la place des anciennes pages A et B. Si le contrôleur utilise le wear-leveling, les deux premiers blocs étant marqués comme ayant déjà été utilisés une fois, les nouvelles pages seront écrites dans les premiers blocs qui ont le plus faible taux d'utilisation.

Cette gestion faite par le contrôleur a d'autant plus d'importance avec la gestion des zones mémoires défectueuses. Celui-ci disposant d'une table qui gère la répartition des données. La table doit également comporter les informations de l'usure de certains blocs. Ce management des zones abîmées évitera une future écriture dans une zone endommagée. Dans le cas d'une mauvaise gestion de ces zones, l'écriture pourrait connaître des erreurs

irréversibles, et à une future relecture, les données ne seraient probablement pas fiables. En plus du wear-leveling, le contrôleur dispose donc d'un autre mécanisme appelé garbage collector [176]. Il est en charge de gérer l'espace libre. Son rôle est de déterminer les espaces qui ne peuvent plus être utilisés et de les récupérer ensuite. Si des blocs contiennent des pages marquées comme invalides (c'est-à-dire qui ne sont plus utilisées), l'algorithme déplace les pages valides vers un autre bloc, puis libère les blocs initiaux.

En conclusion, en présence du wear-leveling, lorsqu'un bloc doit être modifié, le contrôleur le copie avec les données modifiées ailleurs dans la mémoire. La nouvelle adresse physique est remplacée dans la table de gestion des adresses logiques et le bloc précédent est marqué comme invalide. En utilisant l'interface externe de la mémoire MMC, l'hôte n'aura accès qu'à la donnée la plus récente, même si plusieurs versions sont encore physiquement dans la mémoire. Par conséquent un problème inhérent à une relecture de la mémoire en interne, sans passer par le contrôleur, serait de différentier les différentes versions d'un fichier et le dernier bloc valide. Cette problématique sera d'autant plus complexe, que dans certains cas elle devrait être traité sans l'accès à la table des adresses logiques (car elle se situerait dans une zone inaccessible de la mémoire, ou dans le contrôleur lui-même) et uniquement avec l'étude des spares. Il s'agit d'une étape importante du travail à effectuer par un expert judiciaire, lorsque celui-ci envisage une relecture directe d'une mémoire, sans passer par son composant la pilotant (le contrôleur).

1.5 Présentation et état de l'art de la Google Home

L'une des problématiques de recherche abordée dans ce mémoire dans la partie *Fiabilisation de la donnée* est la fiabilisation de la lecture des mémoires flash. La partie précédente a consisté à présenter des composants MMC qui ont la particularité d'intégrer plusieurs puces aux fonctions différentes dans le même boîtier. Cependant, si cette famille de produits est intéressante à aborder dans le contexte de la recherche pour du diagnostic et de l'extraction de donnée, le fait que tous les éléments soient intégrés posent des difficultés lorsqu'il s'agit de développer et surtout fiabiliser un process complexe. De ce fait, le besoin s'est fait ressentir de travailler sur un système moins intégré et pour cela nous nous sommes intéressés à la Google Home. Elle a déjà été ouverte et étudiée sur plusieurs sites dont IFIXIT [177], ce qui permet de présenter des résultats sans s'interroger sur la divulgation de propriété intellectuelle. La démarche pour l'étude du système a consisté à reprendre les descriptifs du démontage sur les sites puis à le refaire sur notre propre système. Nous avons confirmé les références des composants pour en ressortir les documentations et valider leurs fonctionnalités. Enfin, nous avons localisé la mémoire la plus adaptée à nos expérimentations. Cette partie restant sur l'étude théorique du système, les travaux d'extraction et de lecture de la mémoire seront développés dans la partie *Extraction de la donnée*.

Présenté pour la première fois en 2016, la Google Home est une enceinte intelligente et connectée développée par Google. Fonctionnant en parallèle d'une application, elle permet d'exécuter automatiquement des actions, de faire des recherches et de jouer de la musique. Sa version originale présente un boîtier cylindrique (Figure 1.91) avec des entrées vocales et tactiles, se connectant à divers appareils par Wi-Fi ou Bluetooth. Plusieurs variantes ont depuis été commercialisées, notamment la Google Home mini ou la Google Home max, qui a été abandonnée depuis. L'enceinte dispose de plusieurs concurrents sur le marché dont l'Apple Homepod, les Sonos, la Harman Hardon et sa grande rivale, l'Amazon Alexa.

D'un point de vue recherche, les enceintes intelligentes ont été au centre de plusieurs publications. Ainsi, Chung [178] a étudié l'Amazon Alexa, en examinant les différents appels API et les données locales stockées par l'application smartphone compagnon, liée au haut-parleur intelligent. Engelhardt [179] a étendu la méthodologie à l'application compagnon de Google Home sur le téléphone Android Samsung Galaxy S5. Des approches basées sur le matériel dans le cadre de l'analyse forensique ont été réalisées sur l'Amazon Echo par Youn [180] en 2021. En 2019, Qian a présenté une attaque sur la Google Home à travers une vulnérabilité dans SQLite et curl [181]. Comme première étape de leurs efforts de rétro-ingénierie, ils ont extrait la mémoire de l'appareil pour récupérer le firmware. À cette occasion, ils n'ont fait mention d'aucune méthodologie concernant la correction d'erreurs de lecture dues à des bitflips, objet de notre étude. En 2020, Courk [182, 183] a

FIGURE 1.91 – Image de la Google Home dans sa version 2016

présenté une autre attaque sur la Google Home, avec des étapes initiales de rétro-ingénierie similaires. Courk a réussi à deviner l'algorithme de correction d'erreur du processeur, par une méthode itérative. Bien qu'impressionnant, leurs résultats ne sont malheureusement limités qu'au processeur particulier qui équipe cet appareil spécifique. La Google Home est équipé de plusieurs processeurs qui ne sont pas garantis d'utiliser le même algorithme de correction d'erreur (ECC). Notre analyse va donc en avançant le fait de privilégier une correction des erreurs suivant une démarche mathématique, indépendamment de la technologie utilisée dans un processeur.

Si nous revenons spécifiquement à la Google Home, il est intéressant de constater que fidèle à la philosophie de Google, une grande partie des logiciels sont open source. Cela représente un avantage pour notre démarche. Si nous identifions la version du firmware dont nous disposons sur notre modèle, nous pourrons télécharger son équivalent sur internet et ainsi le comparer avec son implémentation sur la puce mémoire. Naturellement, cette démarche est possible uniquement si le firmware est stocké en clair ou tel que dans la mémoire, et ne subit aucune transformation par le processeur lors de son écriture.

1.5.1 Démontage de la Google Home

Le système retenu est la version de la Google Home construite en juin 2017. En suivant les descriptifs de démontage disponibles sur internet, il est possible d'extraire les différentes cartes électroniques constituant le système, visibles Figure 1.92. En accord avec la figure, le système est divisé en plusieurs éléments. Sur la partie droite sont visibles les haut-parleurs en haut et le support d'une des deux cartes en bas. Sur ces éléments aucun composant électronique n'est à référencer, tout comme le socle en plastique en bas à gauche sur la figure.

Les éléments d'intérêt sont la carte électronique du haut et la carte électronique basse

situées respectivement en haut à gauche et au centre bas de la figure. Les deux cartes électroniques sont reliées par une nappe flexible visible au centre haut de la figure.

FIGURE 1.92 – Principaux composants du Google Home

1.5.2 Étude fonctionnelle

La première carte, appelée carte IO, située dans la partie supérieure du Google Home a une forme circulaire (Figure 1.93). La carte électronique (PCB) comporte 4 couches, visibles sur la Figure 1.94 à l'aide de la tomographie Rayons-X. La face supérieure (couche 4) est composée de 12 LED et d'un réseau de grilles capacitives faisant office d'écran tactile. Cette face est collée au boîtier supérieur et extrêmement délicate à extraire sans endommager le boîtier plastique.

La tomographie Rayons-X montre que cette face ne comporte pas de composants pouvant contenir des données. La face arrière de la carte IO comporte des composants actifs. D'après les marquages des composants, il s'agit de deux contrôleurs LED NXP PCA9956BTW [184] qui permettent de gérer les 12 LED présentent sur la carte. Il y a aussi deux microphones INMP621 [185] permettant une captation des sonorités ambiantes mais présentant une qualité médiocre. Le dernier composant est un micro-contrôleur ATMEL ATSAMD21-G16 Cortex M0+ [186] contenant une mémoire flash interne de 64ko. Cette mémoire a une capacité limitée et elle n'est dédiée qu'à contenir un script de boot équivalent du BIOS dans les ordinateurs. Ce code basic n'a pour vocation que d'exécuter des commandes simples pour initialiser le système et/ou de faire appel à d'autres firmwares

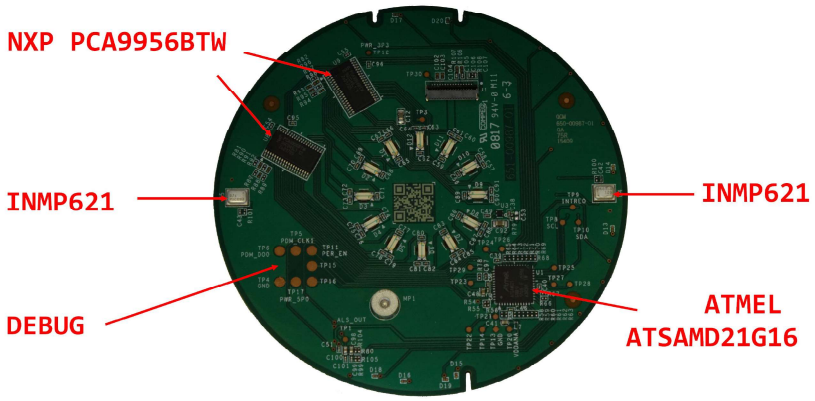


FIGURE 1.93 – Vue de l'arrière de la carte IO

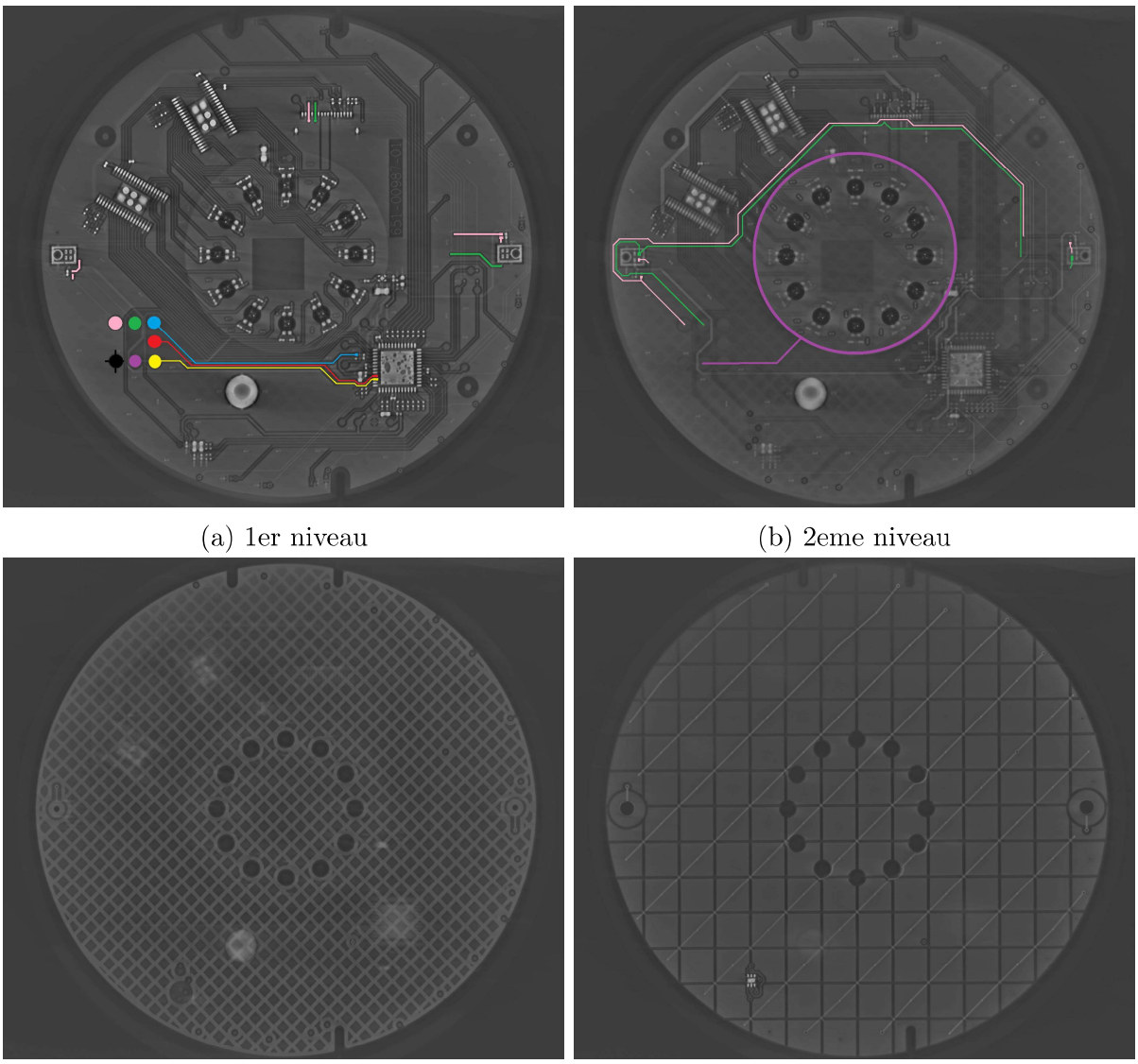
plus conséquent présents dans des mémoires flashs répondant à la norme Serial Peripheral Interface (SPI) [7]. Sur la carte, il est également possible d'observer sept points de test (avec des broches nommées respectivement du haut vers la gauche dans le sens des aiguilles d'une montre sur la Figure 1.94 : `TP6 PDM_DOO`, `TP5 PDM_CLK1`, `TP11 PER_EN`, `TP15`, `TP16`, `TP17 PWR_SPO`, `TP4 GND`). D'autres points de test sont disponibles, qui peuvent être liés à divers composants, mais ils n'ont pas été étudiés dans le cadre de ces travaux, car non pertinent avec nos besoins. En effet, nous souhaitions comparer notre lecture du composant avec une lecture faite depuis un protocole de debug embarqué dans le composant. Pour les opérations de programmation et de débogage, plusieurs protocoles sont utilisés, mais les plus courants sont les protocoles JTAG [187] ou SWD [188].

En regardant la datasheet du micro-contrôleur ATMEL, certains pads correspondent à un bus SWD. Le protocole SWD nécessite deux fils d'alimentation (`GND` et `PWR`) et deux fils de données (`SWDIO` et `SWCLK`). Les fils `GND` et `PWR` permettent respectivement de partager une ligne de masse et d'alimentation commune entre le programmateur et la carte. Certains points de test sur la carte peuvent donc correspondre à une interface SWD. Le premier est un `SWDIO` assurant les échanges de données entre le programmateur et le micro-contrôleur. Le second fil est `SWCLK`, qui est une horloge.

Il est possible d'identifier des points de test correspondant aux signaux du micro-contrôleur à l'aide de la tomographie à rayons X (Figure 1.94) pour confirmer le rôle de TP15 comme `SWCLK`, TP16 comme `SWDIO`, TP4 comme `GND`, TP17 comme `PWR` et TP11 comme `RESET`. La broche RESET étant dans notre cas en permanence à l'état haut ce qui permet de désactiver la possibilité de lancer la commande. Les broches TP6 et TP5 permettent de récupérer les sons acquis par les microphones, sous la forme d'un signal

7. La norme SPI a été créée dans les années 1980 par Motorola. Elle fonctionne sur la base d'une relation maître-esclave avec 4 signaux `SS` pour la sélection de l'esclave, `SCLK` pour l'horloge, `MOSI` comme sortie du maître donc entrée de l'esclave, `MISO` comme entrée du maître donc sortie de l'esclave.

numérique utilisant la *Modulation de densité d'impulsion*, TP6 étant les données, et TP5 le signal d'horloge.

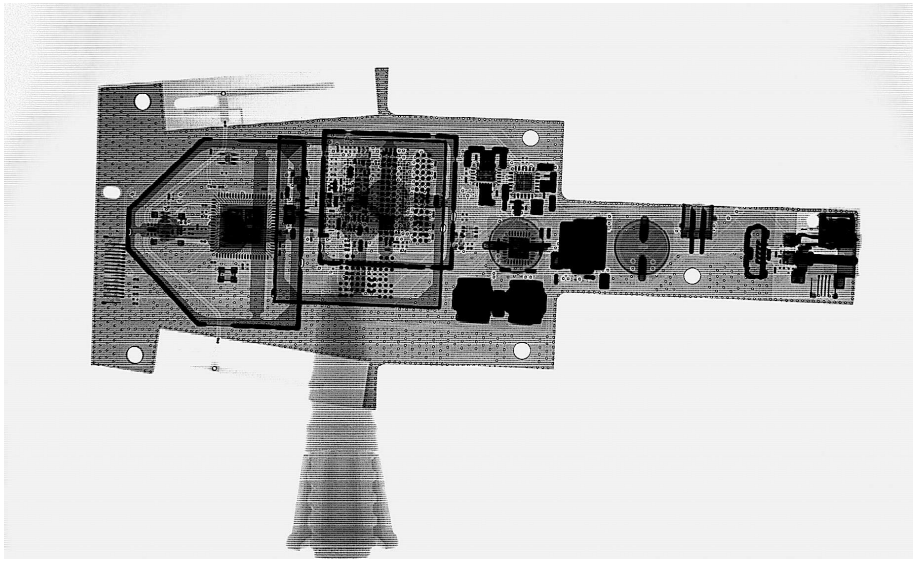


(a) 1er niveau (b) 2eme niveau

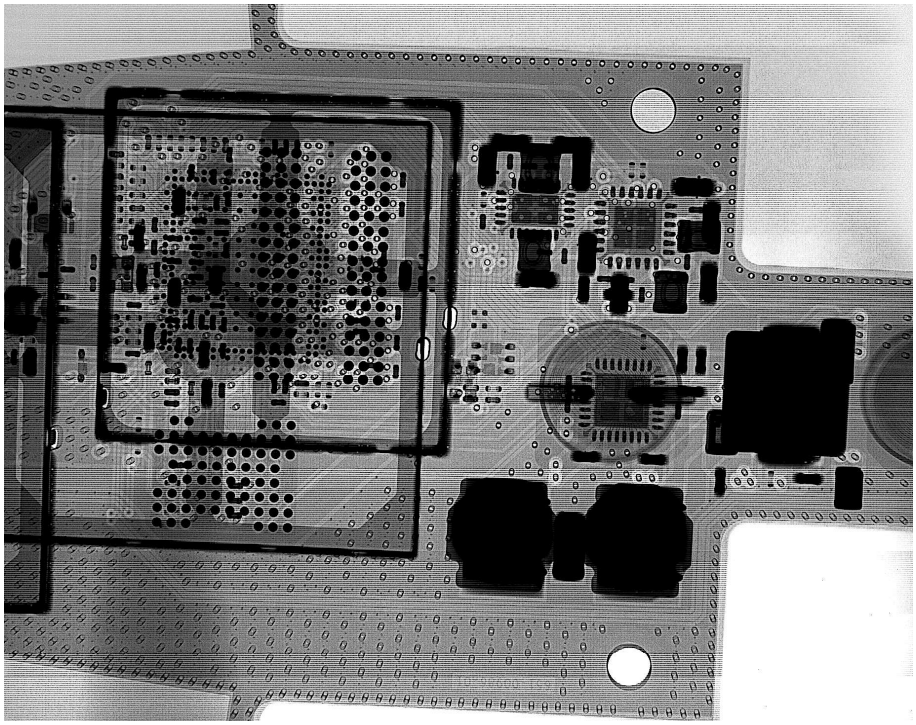
(c) 3eme niveau (d) 4eme niveau (Ce côté est collé au boîtier)

FIGURE 1.94 – Vue Rayons-X de la carte IO supérieure. Le circuit imprimé est composé de quatre couches, chacune donnant une image 2D. Les sept points de test visibles sur la Figure 1.93 sont tracés jusqu'aux composants respectifs

La carte supérieure est reliée à la carte inférieure par un câble plat à 16 broches. La deuxième carte comporte plusieurs blindages Radio-Fréquence (RF) qui cachent les composants situés en dessous. Une vue 2D aux Rayons-X est réalisée pour localiser les composants sous les blindages (Figure 1.95a). Grâce à cette vue, il est possible de déterminer la nature des composants et de savoir s'ils sont actifs ou passifs sans avoir à exposer les puces. Pour rappel, les données sont contenues dans les composants actifs.



(a) Vue aux Rayons-X 2D de la carte inférieure. Les composants actifs peuvent être identifiés derrière les blindages RF

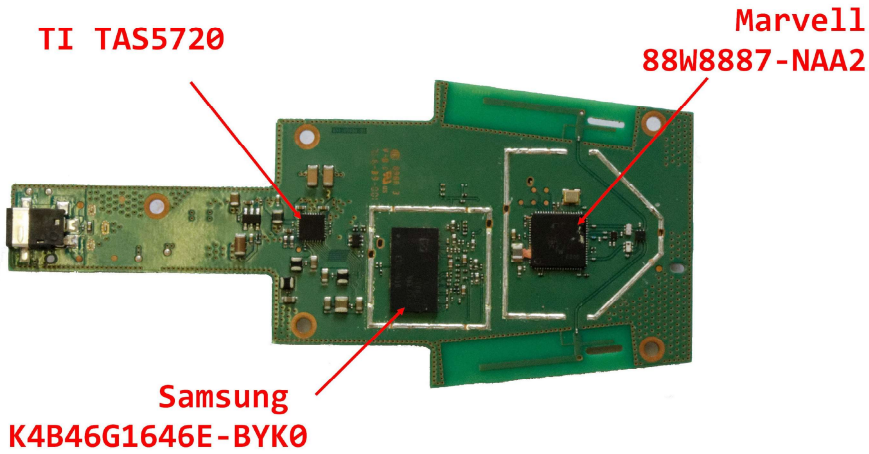


(b) Vue rapprochée aux Rayons-X 2D de la carte inférieure. La puce RAM, la mémoire flash et le CPU sont situées derrière le blindage RF

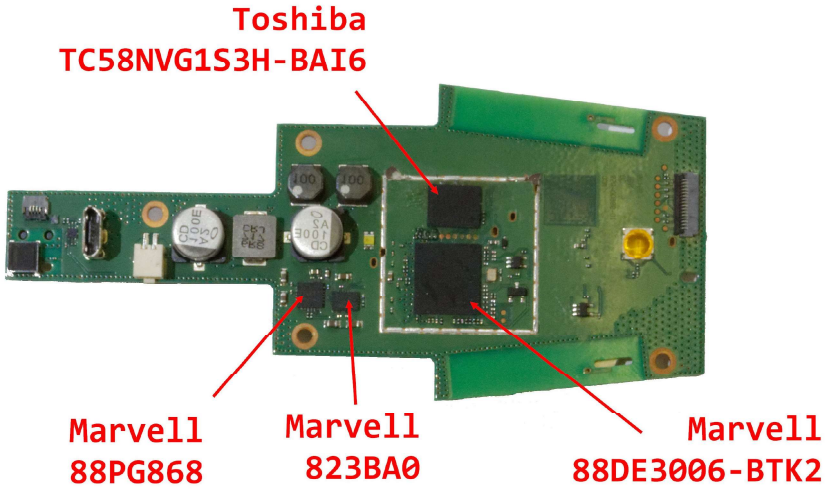
FIGURE 1.95 – Vue aux Rayons-X de la carte inférieure

Il existe plusieurs solutions pour retirer les blindages tout en minimisant le risque d'endommager les composants environnants. Une solution consiste à le dessouder à l'aide d'une machine. Une autre solution consiste à usiner la partie supérieure du blindage avec une micro-fraiseuse. Lors de l'utilisation d'une fraiseuse, il est nécessaire d'employer une fraise de petit diamètre, afin d'être précis et d'éviter de toucher d'autres éléments. Le plus

efficace est d'usiner le bord des boucliers, sans aller trop profond puis en glissant une lame de scalpel, il faut casser la fine couche de métal restante. Il ne faut en aucun cas arracher un bouclier avec une pince, car ceux-ci sont reliés à la carte au niveau du plan de masse et il y aura un risque d'arracher celui-ci en plus d'autres composants environnants.



(a) Vue de dessus de la carte principale



(b) Vue arrière de la carte principale

FIGURE 1.96 – Vue optique de la carte principale avec les composants actifs mis en évidence après retrait des blindages RF

Après avoir retiré les blindages électromagnétiques ou blindages RF, il est possible d'identifier les composants actifs. Sur la face arrière (Figure 1.96a), on retrouve une puce de communication Wi-Fi, Bluetooth et NFC de type Marvell Avastar 88W8887-NAA2 [189]. À côté, on trouve un composant d'amplification audio pour les haut-parleurs référencé TAS5720 [190] et une puce Samsung 512 Mo DDR3 SDRAM référencée K4B4G1646E-BYK0 512MB DDR3 SDRAM [191]. Sur la face avant (Figure 1.96b), on trouve un régulateur de tension I2C DC/DC Marvell 88PG868 [192]. Les deux puces

intéressantes sont le System on Chip (SoC), qui est un ARM Cortex-A7 à 2 cœurs Marvell Armada 1500 Mini Plus [193] connecté à une mémoire flash Toshiba NAND256MB [194] (visible dans la Figure 1.97). La mémoire flash étant le seul composant pouvant contenir une quantité significative de données, l'étude se concentrera sur elle.

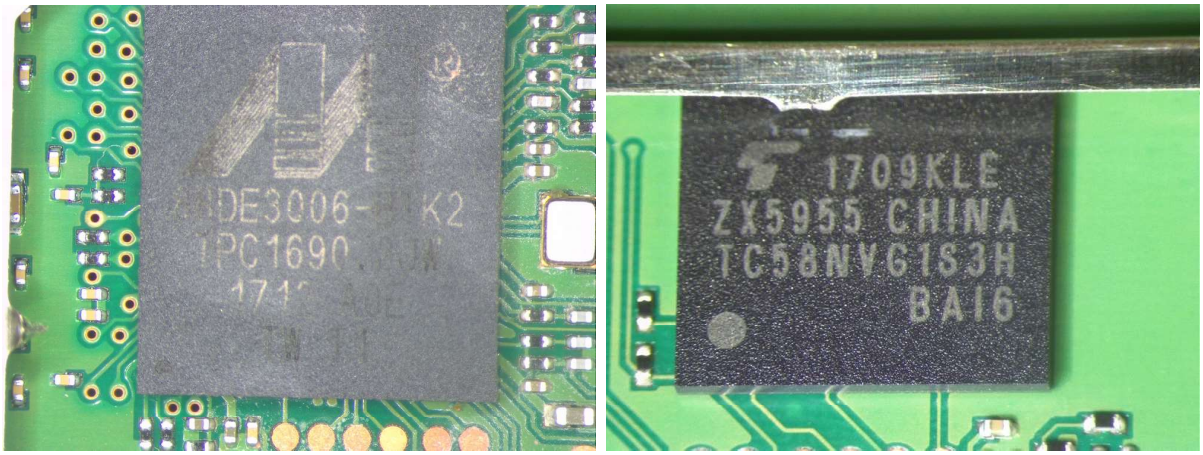
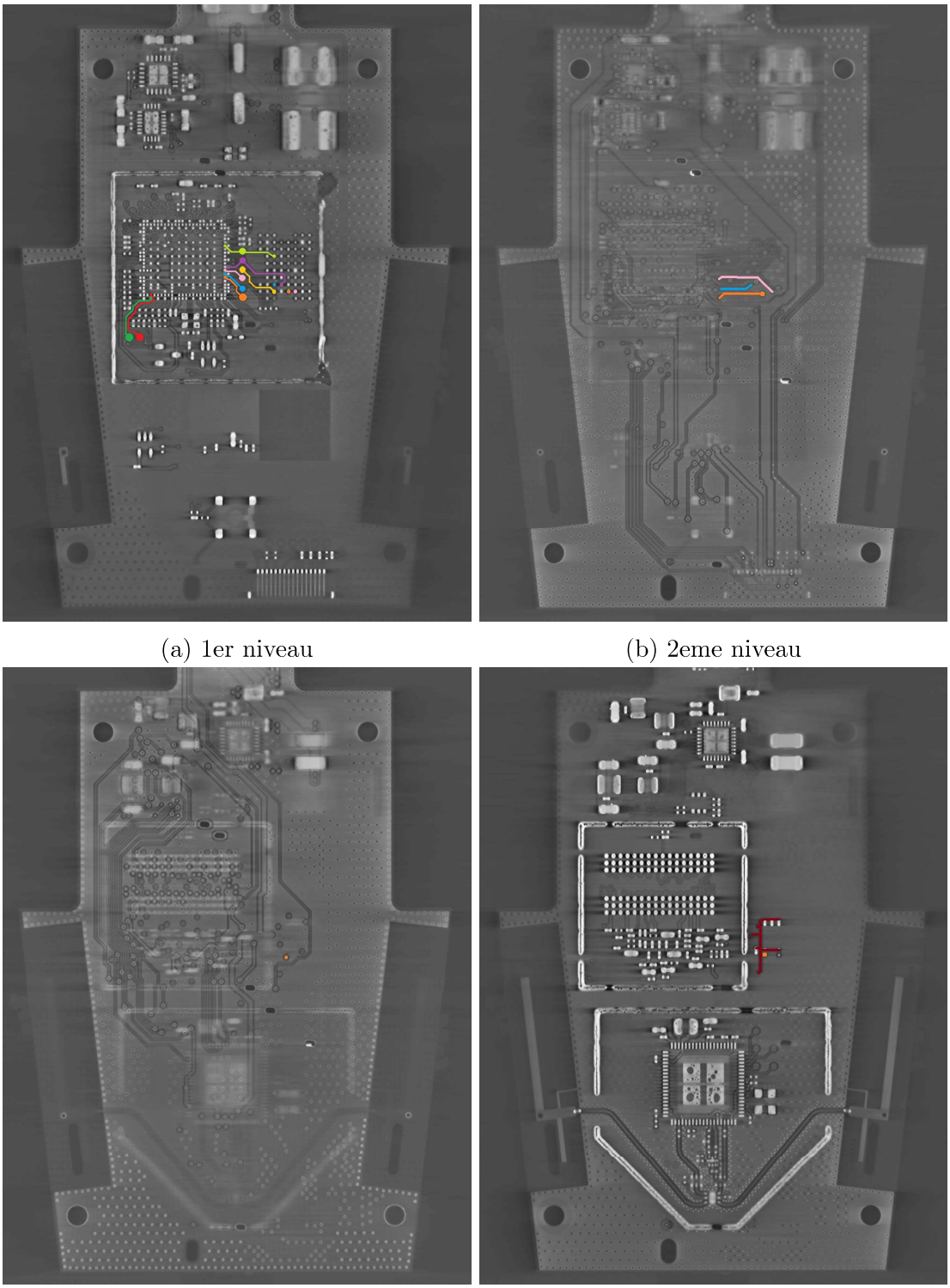


FIGURE 1.97 – Zoom sur le SoC Marvell Armada 1500 Mini Plus (référence : 88DE3006-BTK2) et sa mémoire flash NAND Toshiba 256MB (référence : TC58NVG1S3H-BAI6). Six points de test sont visibles en bas de l'image de gauche

D'après la datasheet, la mémoire Toshiba utilise un protocole SDR (Single Data Rate) respectant la norme ONFI, décrite dans la section *Gestion de la mémoire flash interne*. Cela signifie que cette mémoire utilise le même format que celle étudiée dans la section *Extraction de la donnée*, donc nous pourrons utiliser le même lecteur. Sur le même principe que pour l'autre carte, nous recherchons les points de tests qui nous permettrait de faire une lecture in-situ de la mémoire avant de l'extraire. La tomographie Rayons-X de la Figure 1.98 permet de tracer six broches de test situées entre le SoC et la flash sur la 1ère couche de la Figure 1.98. Elles sont connectées aux `I/O1`, `CLE`, `ALE`, `WE`, `RE` et `CE`. Les signaux de contrôle principaux étant bien présents, uniquement le signal d'entrée/sortie `I/O1` est disponible, ce qui ne permet pas une lecture depuis les points de tests.



(a) 1er niveau (b) 2eme niveau

(c) 3eme niveau (d) 4eme niveau (Vcc identifié en rouge)

FIGURE 1.98 – Vue aux Rayons-X de la carte mère inférieure. Le PCB est composé de quatre couches, chacune donnant une image 2D. Les six points de test sont tracés jusqu'aux composants respectifs. Deux autres points de test ont été tracés jusqu'à des broches non identifiées du SoC. Le trait rouge dans la couche 4 est connecté à VCC et il est utilisé pour tirer le point de test orange (`CE`)

Chapitre 2

Création d'un processus de diagnostic

2.1 Protocole de diagnostic de supports MMC illustré sur carte SD

Cette section va aborder le développement du protocole de diagnostic des supports de type MMC. Comme développé dans la section *Une MMC particulière, la carte Secure Digital (SD)*, ce processus est travaillé sur le support SD qui permet un pilotage plus simple et donc une meilleure répétabilité dans les expérimentations. Toutefois, le but de la démarche reste de développer un processus général pour l'ensemble des supports MMC.

Le diagnostic initial d'une carte SD dans un contexte de la forensique numérique n'est pas fondamentalement différent d'une analyse de défaillance, comme présenté dans la section *Introduction à l'analyse de défaillance*. L'objectif principal est de trouver le défaut présent sur le support qui empêche l'extraction des données, sans l'accentuer. Les premières étapes, après celle de la réception de l'échantillon, consistent à effectuer les manipulations non-invasives, avant de passer éventuellement à celles invasives. En s'inspirant des protocoles utilisés en analyse de défaillance, nous avons proposé le diagramme de décision global suivant est proposé (Figure 2.1).

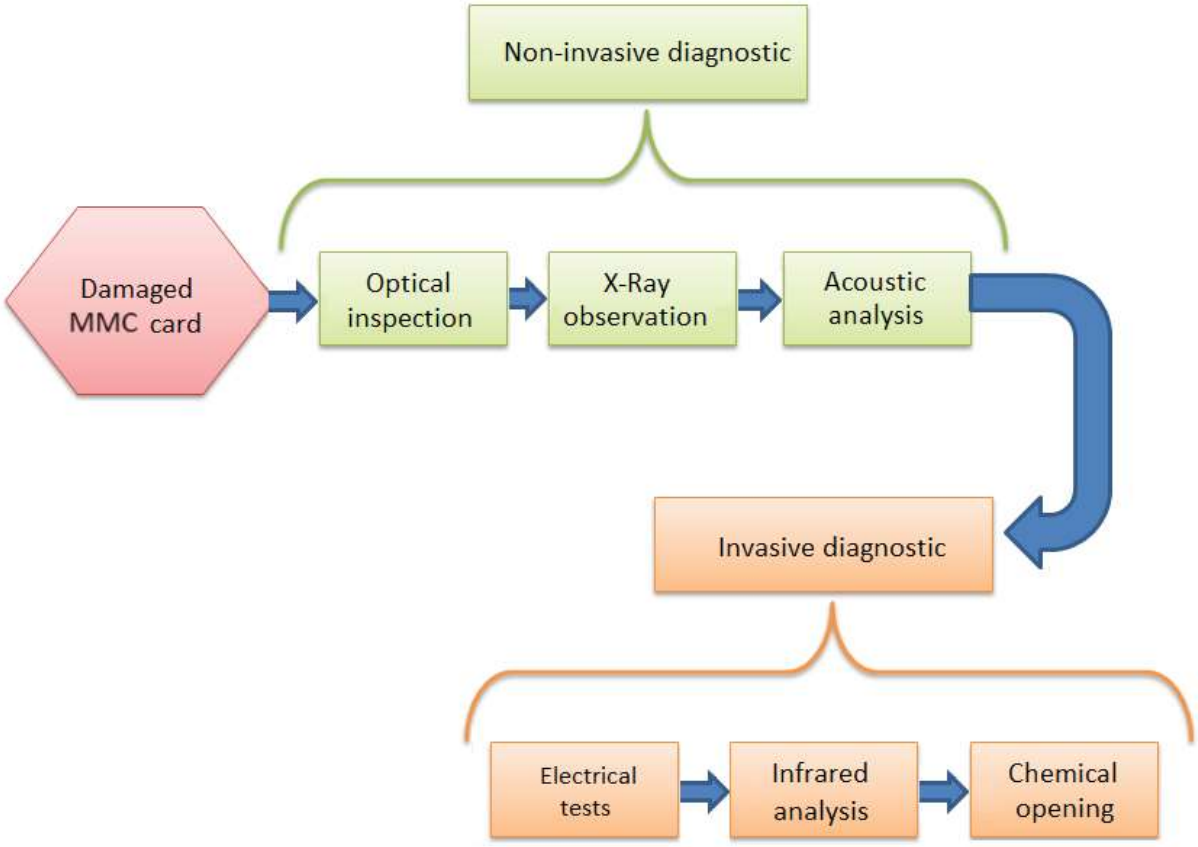


FIGURE 2.1 – Diagramme de décision orienté forensique numérique appliqué sur les MMC endommagées

Pour ce diagramme, les équipements présentés dans la section *Équipements des laboratoires*, classiquement utilisés dans l'univers de la forensique numérique, sont conservés. Les deux équipements (scanner acoustique et caméra thermique) identifiés comme pouvant apporter une plus-value sont ajoutés dans le diagramme. Avant de les incorporer, des tests ont été effectués sur plusieurs échantillons présentant des niveaux de dommages différents et inconnus. Cette démarche a permis de confirmer que l'équipement présentait un réel intérêt dans le protocole, avec une utilisation significative sur une quantité non négligeable d'échantillons. Après avoir confirmé l'utilité des deux équipements, une réflexion a été portée sur la position de celui-ci dans la chaîne de diagnostic. Utilisé trop tard ou trop tôt et l'équipement n'apportait pas son plein potentiel.

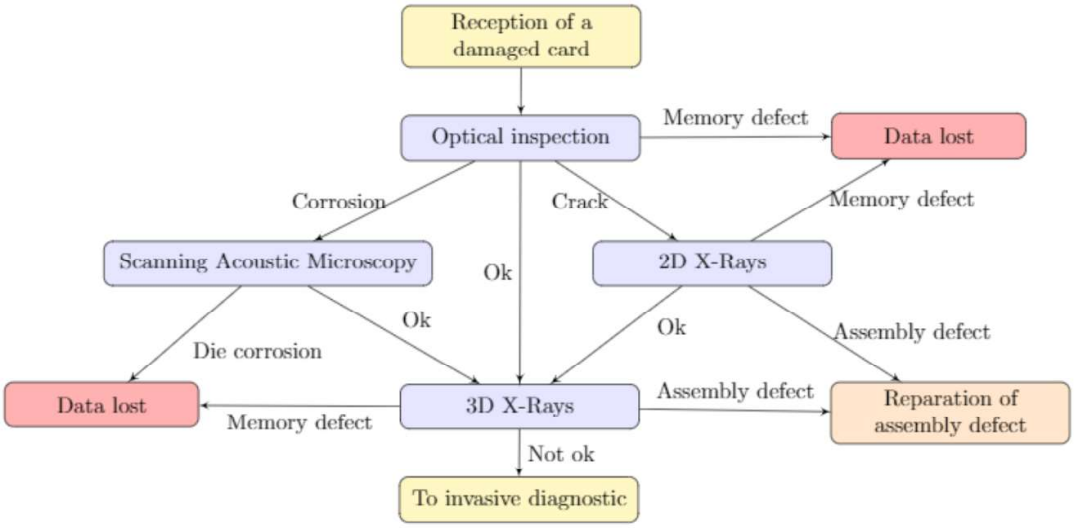


FIGURE 2.2 – Les étapes de la partie non-invasive du diagramme de décision

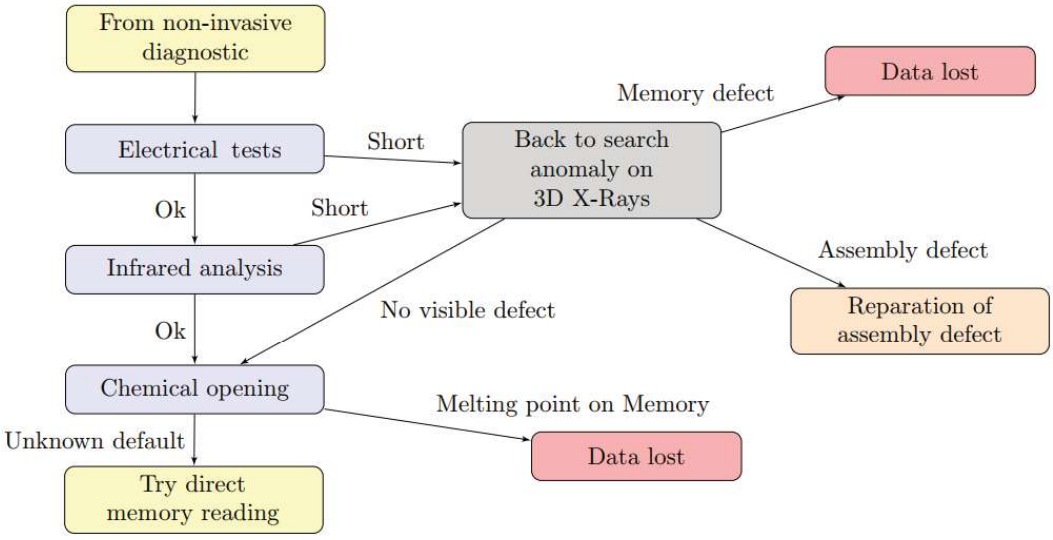


FIGURE 2.3 – Les étapes de la partie invasive du diagramme de décision

Le diagramme de décision (Figure 2.1) peut être développé en deux sous-parties. La partie non-invasive (Figure 2.2) est composée d'étapes qui ne devraient pas modifier les données contenues dans les mémoires, si l'expert judiciaire procède de manière appropriée. En revanche, la partie invasive (Figure 2.3) peut accentuer les défauts et entraîner la perte de données. C'est pourquoi elle est située dans la deuxième partie du diagramme de décision. Cette partie du diagramme n'est appliquée que si la partie non-invasive n'a pas été concluante. Pour chacune des étapes, les options de transition sont présentées ainsi que les réparations possibles. Elles seront plus amplement discutées à la fin de ce chapitre.

2.1.1 Diagnostic non-invasif

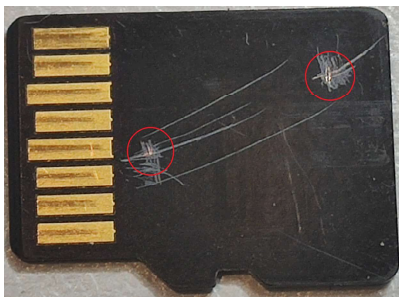
L'objectif principal de l'analyse non-invasive est de localiser les éventuels défauts dans le package de la carte SD sans les accentuer, ni causer de dommages supplémentaires. Plusieurs techniques sont utilisées dans le protocole forensique proposé :

— l'inspection optique ;
— les observations aux Rayons-X 2D et 3D ;
— l'analyse par microscopie acoustique à balayage.

2.1.1.1 Inspection optique

À l'aide d'une binoculaire (Se référer section *Binoculaire*), un expert judiciaire recherche des fissures dans le package comme le montre par exemple la Figure 2.4a. Toute courbure anormale de la carte est également recherchée car elle peut créer des contraintes mécaniques importantes sur les puces. L'inspection des circuits imprimés (PCB) est également effectuée afin de trouver des traces de coupure. Un tel défaut pourrait couper une piste, bloquant ainsi la communication interne entre le contrôleur et les puces mémoires, comme illustré sur la Figure 2.4b. Si des défauts sont localisés, il est possible de les caractériser afin de déterminer s'ils sont juste superficiels ou s'ils affectent l'intégrité de la carte.

(a) Fissure sur le package montrant la puce en silicium



(b) Rayure sur le côté piste de la carte

FIGURE 2.4 – Vues optiques de cartes microSD avec différents types de dommages visibles

Un autre aspect recherché dans l'inspection optique est la présence de corrosion. Lorsque ces supports ont été en contact prolongé avec l'eau, les éléments métalliques exposés sont attaqués. Les zones de la carte SD sous le vernis ou avec une couche d'or sont noramelement protégées. Toutefois, l'un des objectifs de l'inspection optique est de déterminer si de l'humidité est présente et d'étudier comment elle a pénétré dans le package. Si la présence d'humidité est suspectée, l'utilisation d'un microscope acoustique à balayage (SAM) permettra de vérifier l'hypothèse et de déterminer la propagation de la corrosion afin d'en estimer les dommages. Cette étape sera plus amplement détaillée dans la section *Analyse par microscopie acoustique à balayage*.

2.1.1.2 Observations aux Rayons-X 2D et 3D

En complément de l'observation optique, l'inspection par Rayons-X permet d'approfondir le diagnostic interne. La réalisation d'une vue 2D depuis le dessus de l'échantillon, puis en vue profil, permet à l'expert judiciaire de rechercher des anomalies structurelles telles que des bondings endommagés ou manquants au niveau de la puce. Cependant, ce type d'observation ne permet pas toujours de différencier correctement les éléments et leurs couches. Il est donc préférable de réaliser une acquisition et une reconstruction 3D. Cela permet aux experts judiciaires d'identifier les niveaux entre le PCB et les bondings, et ainsi de mieux localiser les éventuels défauts [195]. La Figure 2.5 montre une fissure dans le silicium à travers la zone active (zone contenant les pistes de cuivre et les transistors) des puces de mémoire. Ce défaut n'est pas toujours visible lors de l'étape d'inspection optique car la texture de surface d'une MMC, carte microSD comprise, est rugueuse et inhomogène. Grâce à l'analyse aux Rayons-X, l'expert forensique dispose d'informations supplémentaires pour identifier les défauts dans le but de réparer l'échantillon.

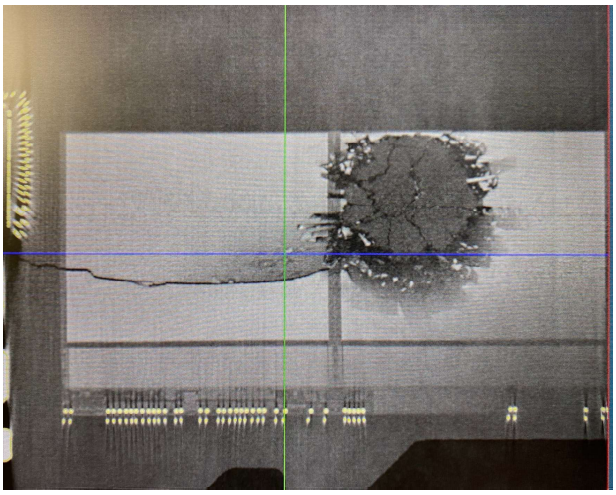
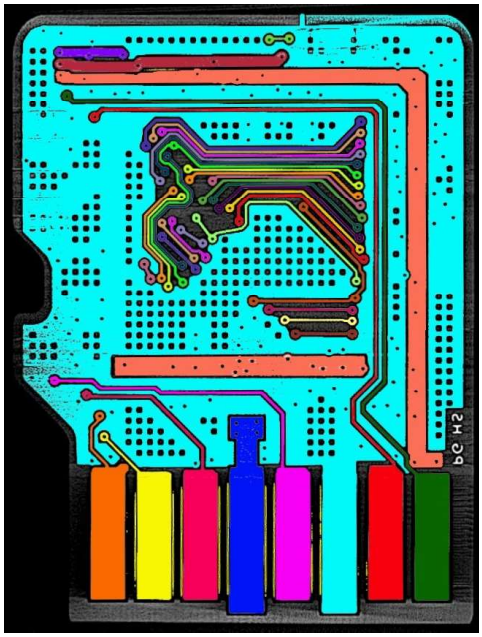


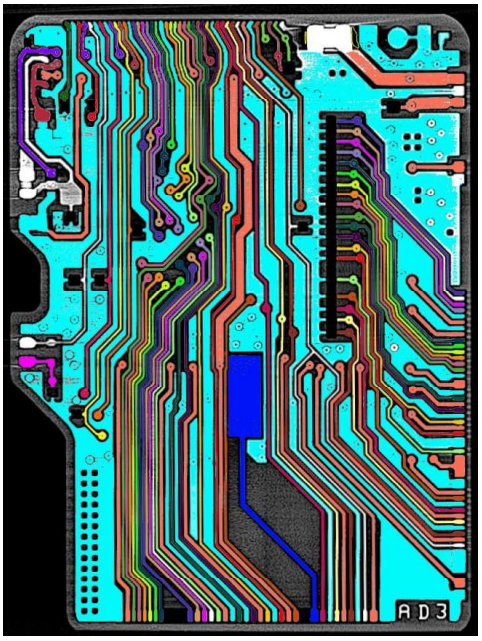
FIGURE 2.5 – Vue aux Rayons-X de cartes microSD présentant des défauts structurels : fissure dans la puce mémoire

L'acquisition d'une image 3D permet d'observer les différentes couches de l'échantillon sur chaque axe. À partir des images obtenues en 3D, un expert forensique peut effectuer une rétro-ingénierie des différents signaux en utilisant un outil de dessin, ou un logiciel métier pour coloriser les pistes de cuivre :

— Entre le contrôleur et les broches externes de la carte SD (c'est-à-dire celles qui sont en contact avec le lecteur de l'hôte).
— Entre le contrôleur et la puce mémoire (Figures 2.6 et 2.7).



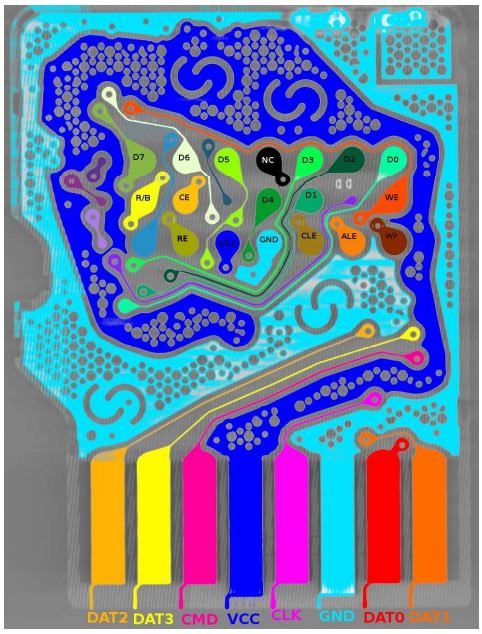
(a) Slice des broches externes



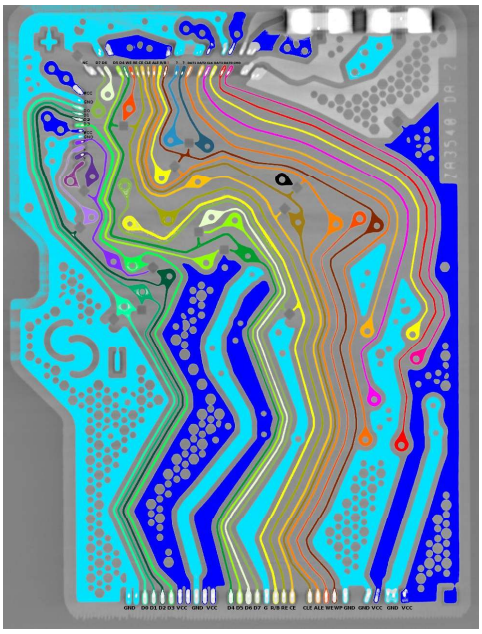
(b) Slice au niveau des bondings des puces

FIGURE 2.6 – Radiographie 3D provenant d'une carte SD avec identification des pistes après une étude de rétroconception

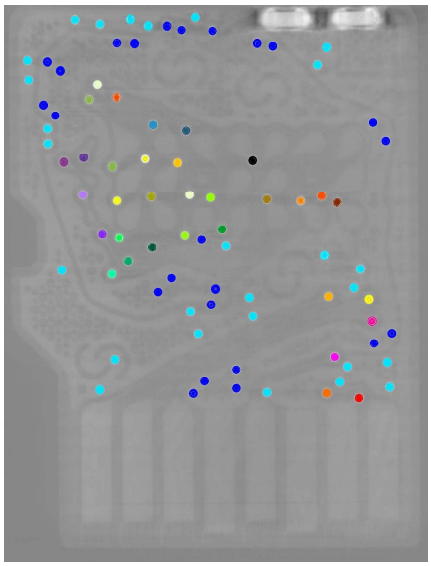
L'étape suivante de l'analyse consiste à attribuer une fonction à chaque couleur. Dans le but d'identifier les signaux, les experts forensiques peuvent comparer les traces identifiées avec les bases de données existantes. Par exemple, la base de données "PC-3000 Flash" [196] (de ACE Lab [197]) peut aider à rendre les opérations d'identification et de rétro-ingénierie beaucoup plus rapides. Pour une marque et un modèle de carte SD, le site internet donne le pattern des plots permettant le debug pour les fabricants. Ils permettent de s'interconnecter et de communiquer directement avec les puces. Cependant, même si le pattern est connu dans la base de données, l'attribution du rôle de chaque plot n'est pas garantie.



(a) Slice de brochage SD



(b) Slice coté bondings



(c) Slice de vias

FIGURE 2.7 – Radiographie 3D provenant d'une autre carte SD après une étude de rétro-ingénierie et l'identification des signaux

Dans l'exemple présenté dans la Figure 2.7, une comparaison du niveau de cuivre d'une carte inconnue est faite avec la base de données "PC-3000 Flash" (Figure 2.8a). Cela permet à l'expert d'obtenir très rapidement une description du rôle des plots de debug, y compris l'ordre du bus interne entre le contrôleur et les puces mémoires (Figure 2.8b).

(a) Identification des plots de la carte SD à partir de la base de données "PC-3000 Flash". [196]

PIN DESCRIPTION

	A	B	C	D	E	F	G
1		RE	Vcc	GND	CLE	ALE	
2	R/B	CE	Vcc	D4	D1		WE
3	D7	D6	D5		D3	D2	D0

(b) Description des signaux pour les plots identifiés dans la Figure 2.8a

FIGURE 2.8 – Identification du rôle des signaux de la carte SD

Lorsque la topologie des plots de debug n'existe pas dans une base de données, l'expert devra rétro-concevoir le PCB lui-même pour trouver la fonctionnalité de chaque plot. Il peut également utiliser une carte similaire comme comparaison. Il faudra toutefois être vigilant car des cartes de la même marque et du même modèle peuvent être extérieurement identiques mais intérieurement différentes. Pour compléter l'étude, un analyseur logique sera nécessaire, mais l'opération sera abordée plus en détail dans la section *Confirmation du comportement et des signaux*.

Après avoir trouvé une description des fils de bondings reliés au contrôleur [1], il est également possible de le schématiser comme illustré dans la Figure 2.9 pour aider au processus de diagnostic.

En résumé, les observations par Rayons-X, en particulier les images de tomographie (imagerie en 3D), sont très puissantes lorsque la carte à diagnostiquer est d'un modèle inconnu, car il est essentiel de comprendre le design de celle-ci et les liaisons internes. Cependant, les experts doivent être conscients de la possibilité d'introduire des erreurs binaires [198] lors de l'utilisation de Rayons-X sur des mémoires flash [199]. Comme pour toute méthode, les experts doivent maîtriser le procédé et doivent pouvoir évaluer les avantages et les inconvénients avant de l'utiliser.

1. Il s'agit du contrôleur de la carte présentée dans les Figures 1.76 et 2.7

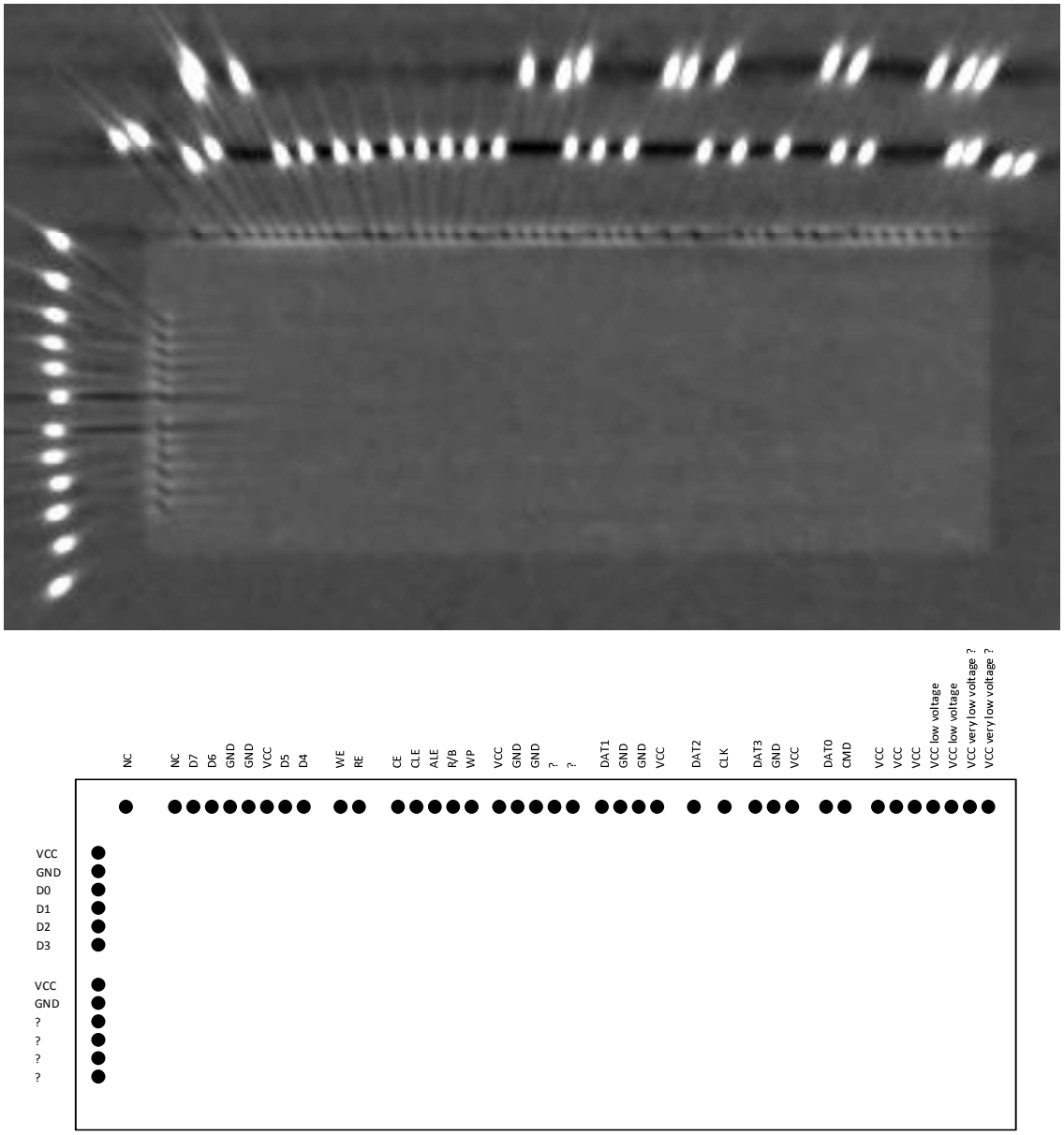


FIGURE 2.9 – Identification des signaux (image du bas) d'après les bondings du contrôleur (image du haut) après une étude de rétroconception avec des slices d'une radiographie en 3D

2.1.1.3 Analyse par microscopie acoustique à balayage

L'analyse par microscope acoustique est une technique d'observation qui permet de déterminer la présence d'air dans un package de composant, comme décrit dans la section *Scanner à balayage acoustique (SAM)*. Cette technique est largement utilisée dans les laboratoires d'analyse des défaillances pour la recherche et le diagnostic de plusieurs défauts structurels [140]. C'est un moyen supplémentaire de diagnostic non-invasif pour

observer la propagation de l'humidité dans le composant. Une carte SD a un package en résine et vernis, ne laissant apparaître que les broches métalliques pour la communication avec l'hôte. Ces broches sont recouvertes d'une fine couche d'or, appelée cotting, servant à les protéger de la dégradation. Les autres parties métalliques sont protégées par le package. Si une fissure ou une rayure apparaît dans la résine ou le vernis, l'humidité peut s'infiltrer et créer une zone de corrosion sur la puce. Dans ce cas, une partie significative des pistes du composant peuvent être attaquées, provoquant des discontinuités électriques. Ce défaut peut, dans un contexte de la forensique numérique, empêcher la récupération des données. En effet, si la corrosion se trouve sur une piste en cuivre du PCB, celle-ci peut être dégradée, comme l'illustre la Figure 2.10.

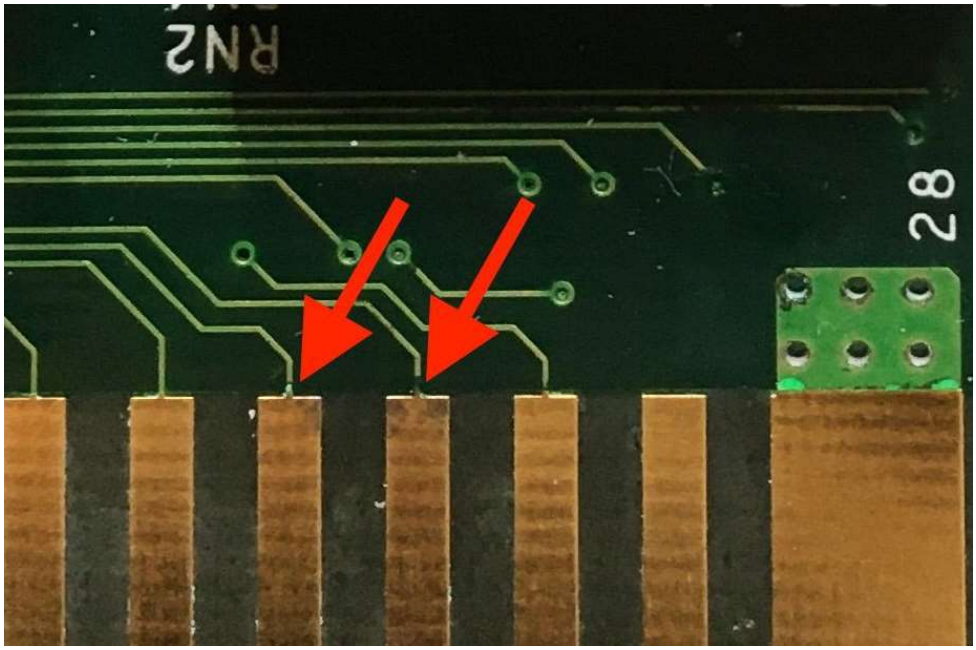


FIGURE 2.10 – Exemple de corrosion suite à une infiltration d'humidité, entraînant une coupure de la continuité électrique [52]

Le scanner acoustique peut permettre sans alimenter le composant, de localiser une zone de délamination, pouvant provoquer une corrosion. L'équipement sert à identifier une zone, qui couplée à l'étude d'images obtenues par Rayons-X 3D, permet de juger de la réparabilité. Une dégradation des pistes de cuivre offre une plus grande réparabilité qu'une dégradation au niveau de la puce, car il est techniquement plus facile d'agir sur le PCB que dans une puce. À ce stade du diagnostic, il est déjà possible de tirer certaines conclusions sur la possibilité de réparer le support. La partie non-invasive du diagramme de décision (Figure 2.2) a normalement permis d'identifier des défauts structurels liés à l'assemblage entre les composants et la carte électronique. Dans le cas contraire, il est nécessaire de continuer l'investigation grâce à des opérations dites invasives.

2.1.2 Diagnostic invasif

Les diagnostics invasifs ne sont pas sans risque pour l'échantillon. Une technique invasive peut altérer ou détruire une information en accentuant ou en créant un défaut. Pour cette raison, elle doit toujours être pratiquée et maîtrisée de manière approfondie. Dans le cadre d'une expertise judiciaire, il est important que la nature et la traçabilité des preuves soient garanties. Aussi, préalablement à leur réalisation, les travaux font l'objet d'une information auprès du magistrat en charge du dossier, afin qu'il puisse décider si le risque peut être pris et donner son autorisation. Les techniques invasives retenues pour notre protocole sont les suivantes :

— les tests électriques de base ;
— l'analyse infrarouge ;
— l'ouverture de l'échantillon chimique.

2.1.2.1 Tests électriques de base

Le but de cette analyse n'est pas d'étudier la carte pendant son fonctionnement mais de rechercher des défauts potentiels dans les jonctions au niveau des signaux d'entrée/sortie des composants. La notion de diode a été abordée dans la section *Notions de la rétro-conception hardware*. Il s'agit de jonctions PN qui laissent passer un courant lorsque la tension appliquée est suffisante. Sachant que les composants actifs sont basés sur les transistors, il est possible de contrôler certaines de ces jonctions et ainsi d'identifier des défauts électriques. En positionnant les sondes d'un multimètre [200] entre un signal et la masse, il est possible d'observer soit une diode qui fonctionne (ce qui signifie un fonctionnement correct), soit un court-circuit ou un circuit ouvert (ce qui signifie une défaillance du signal). En scannant ainsi chaque entrée/sortie de chaque composant de la carte SD, c'est-à-dire le contrôleur et la puce mémoire, l'élément défectueux de la chaîne peut être localisé. En suivant le protocole de la Figure 2.3, un expert peut vérifier la puce touchée en recherchant les anomalies avec les Rayons-X 3D pour décider du type de réparation à effectuer.

2.1.2.2 Analyse par caméra infrarouge

Une caméra infrarouge, également appelée caméra thermique, enregistre le rayonnement infrarouge d'un composant électronique en fonctionnement, comme développé dans la section *Caméra thermique*. En général, l'étude d'un échantillon est réalisée en comparaison avec un échantillon témoin (c'est-à-dire un produit fonctionnel similaire). Ce principe permet de comparer les points chauds et froids pour identifier les différences de comportement entre les deux échantillons. La caméra thermique met en évidence des effets transitoires, qui sont normalement difficiles à détecter (Figure 2.11).

En suivant le protocole de la Figure 2.3, l'identification de ces problèmes, l'expert judiciaire pourra investiger plus en profondeur les défaillances pertinentes à l'aide d'images radiographiques 3D, afin de décider ensuite, si et comment ces défaillances peuvent être réparées.

Dans l'exemple d'acquisition d'images à l'aide d'une caméra infrarouge de la Figure 2.11, la carte microSD est détectée par l'ordinateur mais les processus de lecture et d'écriture ne sont pas possibles. L'ordinateur offre seulement la possibilité de formater la carte. Dans cet état initial, la carte microSD est mise sous tension (Figure 2.11a), puis la carte est sollicitée en lecture par l'hôte. Comme le montrent les Figures 2.11b, 2.11c et 2.11d, la chaleur s'accumule très rapidement dans la moitié du contrôleur. Afin de préserver la carte, l'expert qui observe ce phénomène doit être prêt à arrêter immédiatement l'expérience en coupant l'alimentation.

Une différence de coloration globale des Figures 2.11a, 2.11b et 2.11c peut être observée en raison de l'auto-calibrage de la caméra. La différence de coloration entre les Figures 2.11c à 2.11g est due à la propagation et à la dissipation de la chaleur dans le boîtier de la carte microSD.

Avec une telle analyse, il est difficile d'identifier avec précision le point de départ du défaut et l'évolution de la température. Il est possible que :

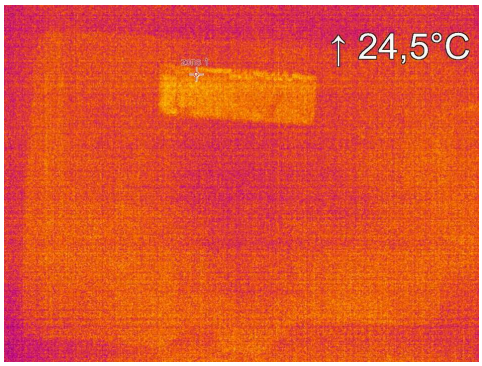
— La température continue d'augmenter jusqu'à atteindre un seuil dangereux pour l'intégrité des matériaux de la puce. Dans ce cas, l'expert judiciaire doit être prêt à arrêter le processus, c'est-à-dire arrêter l'alimentation de la carte, pour laisser le contrôleur refroidir. L'expérience aura permis d'identifier la puce défectueuse mais pas son emplacement précis. Il n'y a pas d'état stabilisé qui pourrait être qualifié d'état final.

— La température va cesser d'augmenter, ce qui permet à la caméra de s'adapter et donc de fournir une image plus précise de la zone où se trouve le défaut. Il existe un état stabilisé que l'on peut qualifier d'état final. C'est le moment où le système a atteint un équilibre thermique, permettant à l'expert de faire une observation précise sans risque de dégradation de l'échantillon.

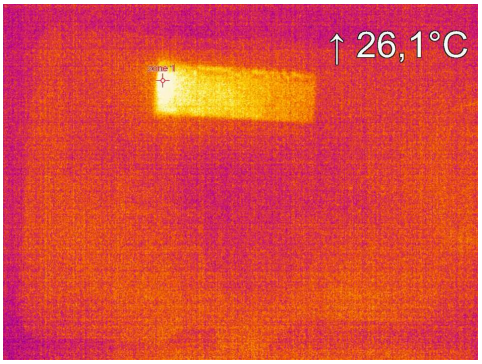
Lors de l'utilisation d'une caméra infrarouge, un défi pour l'expert est de déterminer si l'échantillon va atteindre un état final (et donc un état stabilisé). Suivant une démarche expérimentale, l'expert devra donc lancer plusieurs acquisitions d'images pour valider l'hypothèse, chaque fois sur une base de temps légèrement plus longue, jusqu'à ce qu'un état stabilisé soit éventuellement atteint. On décide d'arrêter les opérations, car l'échantillon est dans un état dangeureux pour lui-même.

Pour revenir à notre exemple, la température de la carte microSD cesse d'augmenter. La caméra parvient donc à définir la zone de chaleur intense, comme le montrent les Figures 2.11e et 2.11f. Dans l'état final (Figure 2.11g), l'expert peut distinguer un

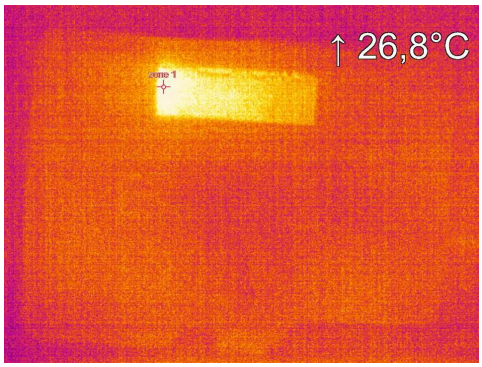
point d'échauffement sur la gauche de la carte, non loin de la rangée de bondings. En comparant le moment de l'acquisition et les opérations effectuées sur la carte microSD, il est possible de montrer que la connexion de la carte microSD à l'ordinateur (et donc la mise sous tension) n'a pas provoqué de défaut de fonctionnement. En revanche, il est établi qu'il existe un défaut interne dans les transistors du contrôleur, ce qui empêche l'expert judiciaire d'accéder aux données. En effet, même si des opérations sont réalisables techniquement, elles nécessite un temps de réalisation qui est incompatible avec le temps judiciaire et par ailleurs, elles sont très onéreuses. Comme expliqué précédemment, suivant le protocole (Figure 2.3), l'expert doit vérifier, à l'aide d'une analyse 3D par Rayons-X, si la défaillance est visible. Cela lui permettra de décider de passer soit à une phase de réparation, soit à une ouverture chimique de l'échantillon pour rechercher la défaillance interne.



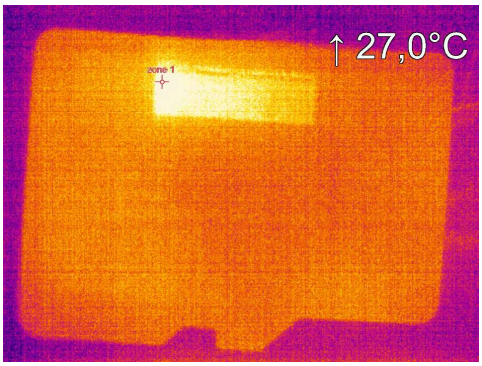
(a) Carte à l'état initial



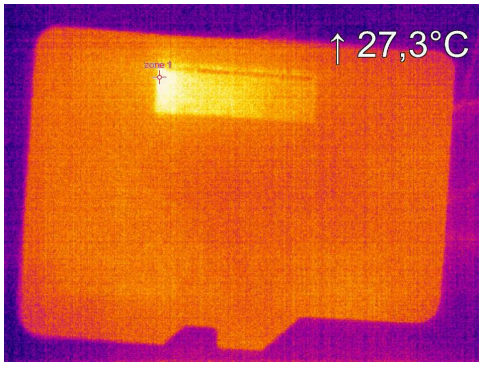
(b) Carte durant la lecture à t = 1s



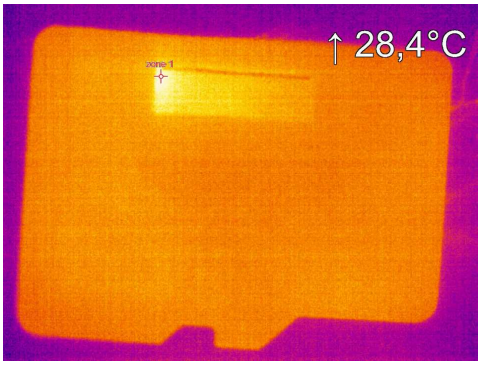
(c) Carte durant la lecture à t = 2s



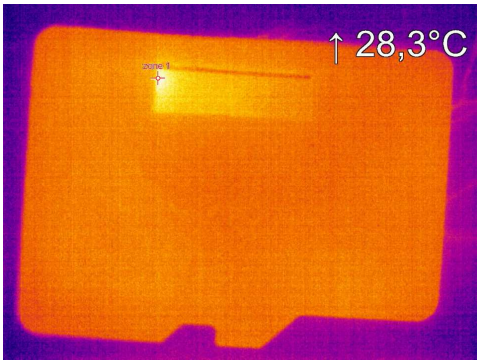
(d) Carte durant la lecture à t = 5s



(e) Carte durant la lecture à t = 7s



(f) Carte durant la lecture à t = 8s



(g) Carte durant la lecture à l'état final

FIGURE 2.11 – Acquisition infrarouge sur une carte microSD pendant les phases normales de mise sous tension et de lecture

2.1.2.3 Ouverture chimique de l'échantillon

Il s'agit de la technique la plus destructive qui puisse être utilisée pour diagnostiquer un défaut car elle enlève la résine protectrice des puces pour les exposer. Il existe plusieurs solutions chimiques pour y parvenir, mais la plus courante consiste à déposer localement des gouttes d'acide nitrique fumant 100 % préalablement chauffé à 90 °C pour effectuer une attaque localisée des puces [201]. L'utilisation de cette technique comporte plusieurs contraintes. Tout d'abord, la zone d'attaque doit être identifiée par une vue aux Rayons-X, puis l'acide concentré doit être appliqué au bon endroit. L'attaque doit également être contrôlée pour n'exposer que le silicium sans surexposer d'autres éléments, tels que les bondings ou le PCB en cuivre, qui seraient gravement endommagés. Pour éviter ce problème, il est possible de changer le procédé en modifiant la température d'attaque, la nature du produit chimique, ou la nature d'un éventuel mélange. La solution la plus couramment utilisée est un mélange d'acide nitrique fumant 100 % dilué à 60 %/40 % dans de l'acide sulfurique chauffé à seulement 40 °C [202]. Cette attaque chimique, bien qu'elle soit plus longue à mettre en place, permet de préserver les éléments en cuivre et donc de garder la carte SD fonctionnelle [203]. Une alternative à cette technique appelée la gravure manuelle, consiste à utiliser une machine d'ouverture chimique décrite dans la section *Chimie humide* et de préalablement amincir la carte SD avec un laser d'ablation comme présenté dans la section *Laser d'ablation*. L'acide appliqué sera dirigé et centralisé dans le trou créé par ablation laser. Ainsi, le temps d'exposition aux acides sera considérablement réduit, afin d'augmenter les chances de réussite [204].

En conclusion, l'élaboration du protocole nous a permis d'effectuer des expérimentations sur deux nouveaux équipements rarement utilisés dans les laboratoires de forensique numérique. De plus, ces travaux nous ont permis de réfléchir sur le rôle de chaque manipulation faite sur la carte. Afin de juger si cette technique posait un risque potentiel pour le support ou si elle était transparente. Nous avons également pu étudier la logique d'ordonnancement de passage sur les différents équipements. Nous avons d'ailleurs constaté que la pratique appliquée dans les process de l'analyse de défaillance, qui consiste à effectuer une acquisition aux Rayons-X pour figer la situation était intéressante. Ainsi, dans notre protocole, nous avons décliné cette idée en recommandant de faire une acquisition aux Rayons-X 2D et 3D pour également figer l'état du support. Cela permettra de faire une recherche approfondie en cas de résultat positif lors des tests électriques, tests à la caméra thermique ou scan au microscope acoustique. Un retour sur la vue 2D ou 3D permettra de faire une première tentative de localisation de défauts. Pour un résultat plus complet, une seconde acquisition aux Rayons-X 2D et 3D pourra être pratiquée, permettant une comparaison de l'état avant et après les tests effectués. Grâce à cette nouvelle acquisition, une comparaison pourra être faite ce qui indiquera si les défauts

étaient présents à la réception du support ou ont été induits par les expérimentations.

Après avoir développé notre protocole sur un plan théorique et avec quelques illustrations, nous l'avons utilisé sur des supports aléatoires. Notre but était de valider que pour chaque cas abordé, un chemin était applicable permettant une conclusion. Dans la section suivante, nous développerons l'exemple d'un des supports que nous avons utilisé et notre cheminement dans le processus pour le traiter.

2.2 Cas d'étude

L'étude du cas présentée est relative à une carte SD non fonctionnelle. Avant de présenter le travail effectué sur ce support, il est important de rappeler le contexte lors de la réception d'un échantillon.

2.2.1 Contexte

En France, le chemin d'un scellé n'est pas une ligne continue passant par des acteurs identiques. La répartition des forces de l'ordre sur le territoire, apporte des spécificités. Pour rappel, le partage entre police et gendarmerie en termes de juridiction des affaires dépend de la densité de population du territoire concerné. La police est responsable des villes de plus de 20000 habitants, en opposition, la gendarmerie est responsable d'environ 95% de la superficie de la France. Cette opposition a un effet simple, chaque force de l'ordre est responsable de la moitié de la population Française. La même démarche de juridiction est appliquée pour un scellé. Lorsque celui-ci est confectionné par la police, l'enquêteur s'adresse d'abord à ses points de contacts cyber locaux, avant de s'adresser à l'échelon national puis de s'adresser à d'autres entités. Le fonctionnement est le même pour la gendarmerie. L'effet de cette situation est que les laboratoires centraux peuvent recevoir un scellé qui a déjà connu plusieurs traitements mais sans savoir lesquels. En raison de la pluralité des acteurs, l'état de réception du support est considéré comme l'état d'origine. Toute fissure, rayure ou courbure de celui-ci doit être considérée comme originale et traitée comme tel.

2.2.2 Présentation de l'échantillon

L'échantillon de l'étude de cas est une carte SD (Figure 2.12). La première constatation que nous pouvons faire est qu'une partie du vernis de protection du PCB a été retirée sur une zone. Comme expliqué précédemment, il n'est pas possible de savoir s'il s'agit d'un défaut d'origine ou engendré par une expertise précédente. Ensuite nous ne constatons aucune écriture visible sur le PCB ou sur la résine. Il n'est donc pas possible d'obtenir directement le fabricant, le modèle ou la taille de la mémoire de la carte. Cependant, certaines informations peuvent être déduites. Par exemple, la topologie du bus de l'interface SD est celle d'une carte UHS-II, ce qui suggère une carte récente conçue pour une communication rapide, avec une taille mémoire conséquente.

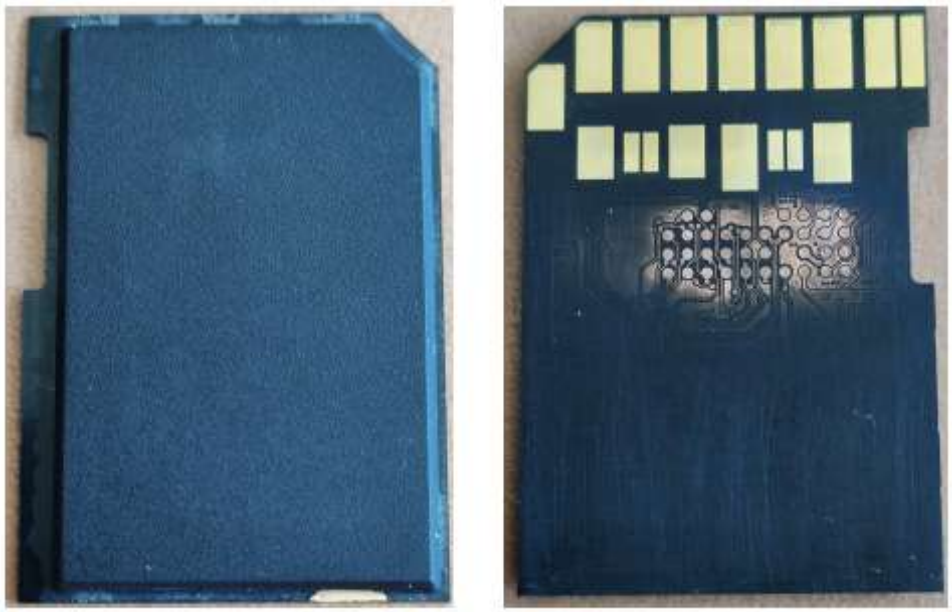


FIGURE 2.12 – Vue optique des faces avant et arrière d'une carte SD provenant d'un cas réel, dans l'état dans lequel elle a été réceptionnée

Selon les informations du demandeur, la carte SD est reconnue par l'hôte lorsqu'elle est insérée dans un lecteur. L'hôte demande un formatage, et l'accès aux données n'est plus possible. L'objectif de l'analyse est d'accéder aux données contenues dans cette carte SD. Pour ce faire, le protocole décrit dans la section *Protocole de diagnostic de supports MMC illustré sur carte SD* est strictement appliqué pour initier la phase de diagnostic et orienter l'expertise en fonction des résultats obtenus. Ensuite, le protocole de réparation nécessaire sera appliqué pour récupérer les données, si le cas le permet.

2.2.3 Analyse non-invasive de l'échantillon

2.2.3.1 Inspection optique

Selon le diagramme de décision orienté forensique numérique proposé en Figure 2.1, une inspection optique est effectuée (Figure 2.12). En ce qui concerne la résine, aucune fissure, délamination ou tout autre défaut ne peut être observé. En regardant le PCB, un polissage a été effectué au niveau des plots de debug de la mémoire (Figure 2.13). Ce polissage peut avoir plusieurs origines, soit accidentelles, soit délibérées par un autre laboratoire lors d'une tentative de diagnostic. Compte tenu de la forme et de la position de ce polissage, l'hypothèse du diagnostic est privilégiée. De plus, il a été correctement réalisé car aucune piste n'a été endommagée.

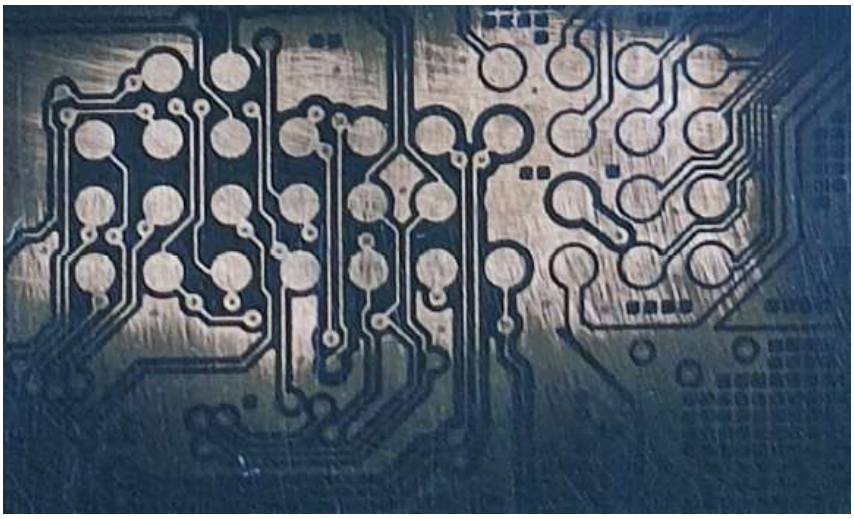


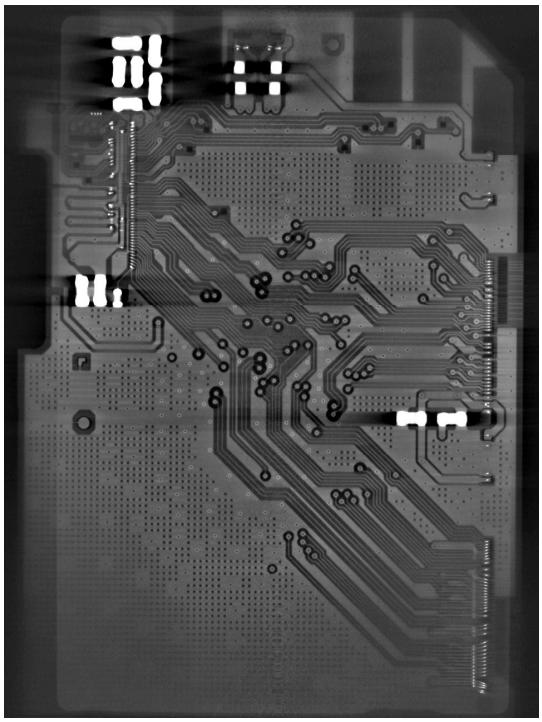
FIGURE 2.13 – Diagnostic initial, à l'aide d'un microscope binoculaire, d'une partie de la carte SD étudiée : aucun défaut visible constaté

L'inspection optique n'ayant pas fourni d'information sur le défaut de la carte, nous passons à l'étape suivante du diagramme de décision (Figure 2.2). En l'absence de délamination visible et sans indication d'immersion, la branche basée sur l'utilisation du scanner acoustique peut être omise pour se concentrer sur l'étape suivante : les observations aux Rayons-X 2D et 3D.

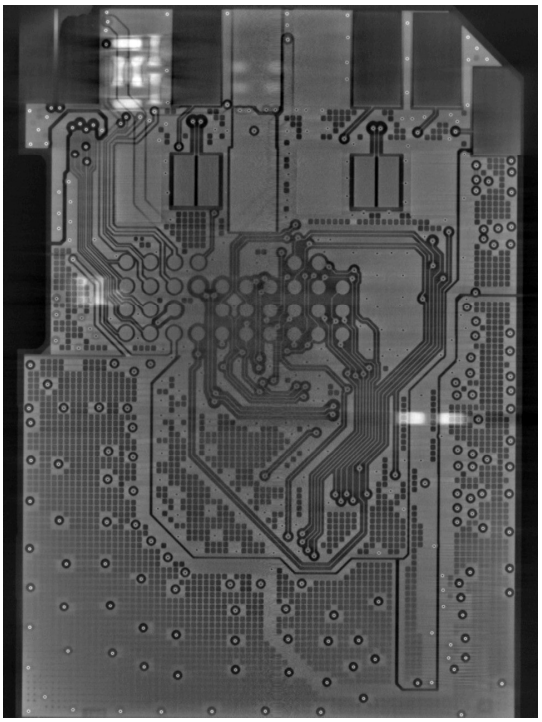
2.2.3.2 Observations aux Rayons-X

Aucune anomalie n'ayant été observée lors de l'inspection optique, une observation aux Rayons-X est effectuée. Dans un premier temps, l'observation se fait en deux dimensions, pour la recherche de défauts identifiables. En raison de la densité des éléments constituant cette carte SD, certaines zones des images sont difficiles à interpréter. L'analyse en deux dimensions ne montrant aucun dommage visible, un examen en trois dimensions est effectué pour recueillir davantage d'informations. Comme mentionné précédemment, la tomographie 3D est le moyen le plus efficace pour localiser une anomalie structurelle dans un empilement technologique complexe.

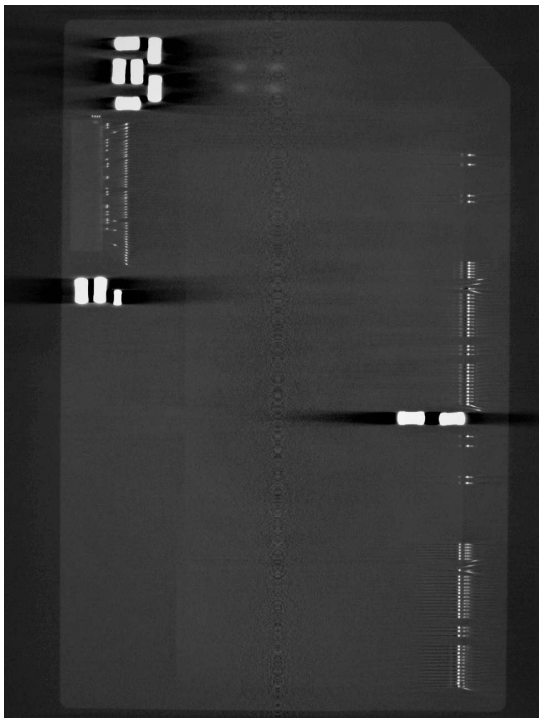
La Figure 2.14 montre les couches d'intérêt dans la carte SD de notre cas d'étude. La Figure 2.14a représente la slice du PCB du côté des puces. La Figure 2.14b représente le coté du PCB au niveau des plots de debug. Les autres slices d'intérêt sont les puces (Figure 2.14c) et leurs bondings (Figure 2.14d). Cependant, les images ne montrent aucun défaut et l'observation aux Rayons-X étant la dernière étape non-invasive du diagramme de décision (Figure 2.2), la phase suivante est le diagnostic invasif.



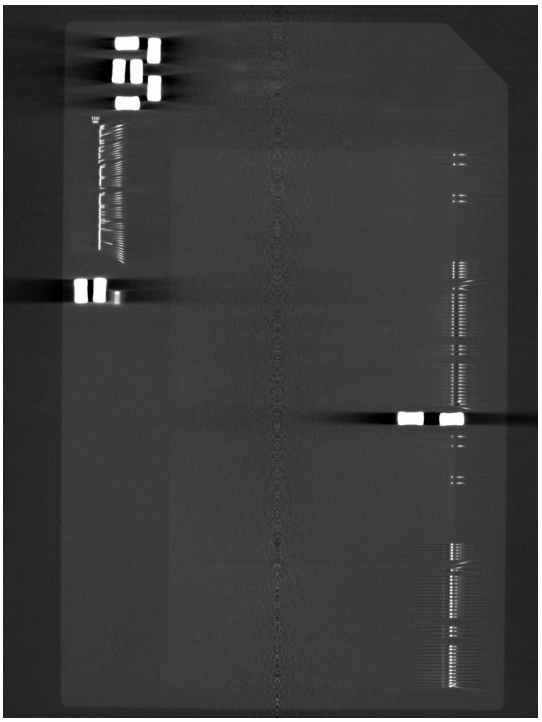
(a) Slice du PCB coté puces



(b) Slice du PCB coté plots de debug



(c) Slice des puces



(d) Slice des bondings

FIGURE 2.14 – Vue radiographique 3D des différentes couches d'intérêt de la carte SD étudiée : aucun défaut détecté

2.2.4 Analyse invasive de l'échantillon

Comme décrit dans la Figure 2.3, la première étape consiste à effectuer des tests électriques.

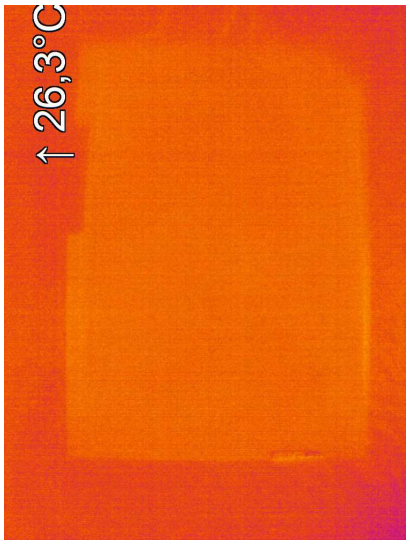
2.2.4.1 Tests électriques

Le comportement de la carte SD décrit dans la section 2.2.2 indique une reconnaissance par l'hôte de la carte SD mais pas du système de fichiers. Cette information indiquerait que le comportement électrique du contrôleur est normal. Pour vérifier cela, un test de diode avec un multimètre est effectué sur les plots externes du bus SD. Ce test étant concluant, une seconde analyse est effectuée au niveau des plots de debug présents entre la mémoire et le contrôleur. Ce test étant également concluant, il n'y a pas de court-circuit entre le signal et l'alimentation de la carte SD. Cette conclusion permet à l'expert de passer à l'étape suivante du diagramme de décision (Figure 2.3), c'est-à-dire l'analyse de la caméra infrarouge.

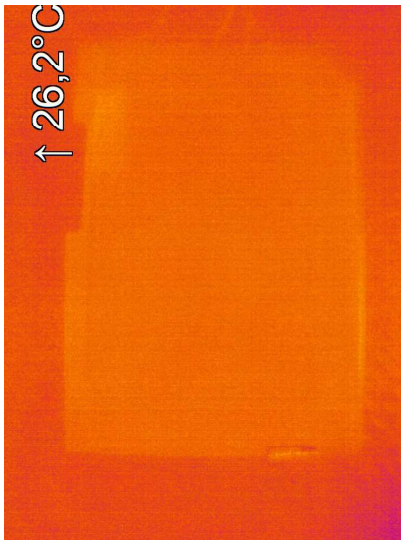
2.2.4.2 Analyse infrarouge

Pour évaluer les défauts potentiels reflétés par les températures mesurées à l'aide d'une caméra infrarouge, une analyse thermique comparative est effectuée sur le cas d'étude (Figure 2.16) et sur un échantillon de contrôle (Figure 2.15). Pour exécuter le test, la carte SD est connectée à un hôte par un lecteur de carte contrôlé par un script, mettant sous tension la carte puis lisant 500 Mo de données à une adresse aléatoire. Cette phase de pilotage, qui prend quelques secondes, est réalisée alors que la carte est placée sous la caméra infrarouge.

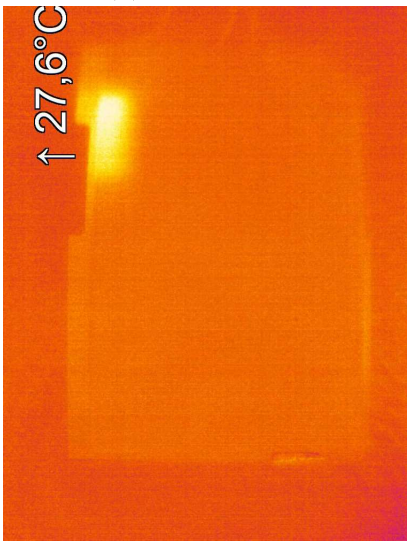
Dans l'état initial, la carte n'est pas pilotée et elle est au repos. L'ensemble de la carte a une coloration homogène et donc une température homogène de 26°C (Figure 2.15a). Dès que le script est lancé, l'hôte met la carte sous tension. Un changement de couleur minime est observé dans le coin supérieur gauche (Figure 2.15b), correspondant à la position de la puce du contrôleur selon les Rayons-X (Figure 2.14c). Ensuite, l'hôte passe en mode lecture de données et exécute plusieurs requêtes successives. Cette action a pour effet de solliciter d'avantage le contrôleur (Figure 2.15c). La température du contrôleur passe à 27°C et continue à augmenter comme le montre la Figure 2.15 après 2 secondes (Figure 2.15d), 3 secondes (Figure 2.15e) et 20 secondes (Figure 2.15f). La lecture est terminée après 20 secondes, et sur cet échantillon, seule l'activité du contrôleur est observable, c'est-à-dire qu'il n'y a pas d'émission de chaleur sur la mémoire ou ailleurs. L'étape suivante va consister à reproduire la manipulation puis de comparer les résultats.



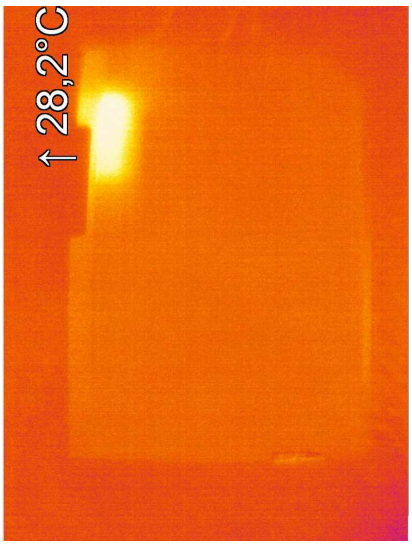
(a) État initial



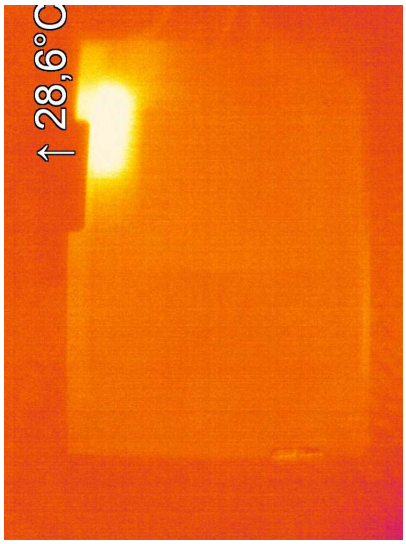
(b) Mise sous tension



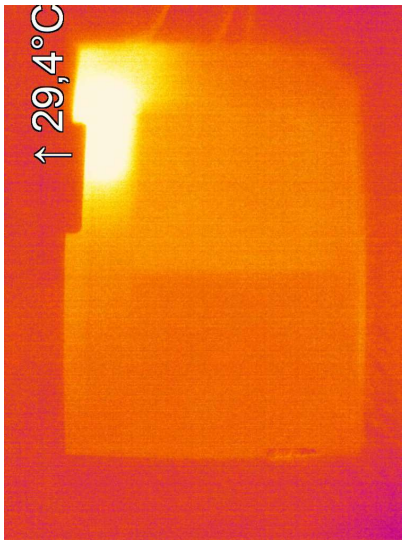
(c) Début de la lecture



(d) Après 2s de lecture



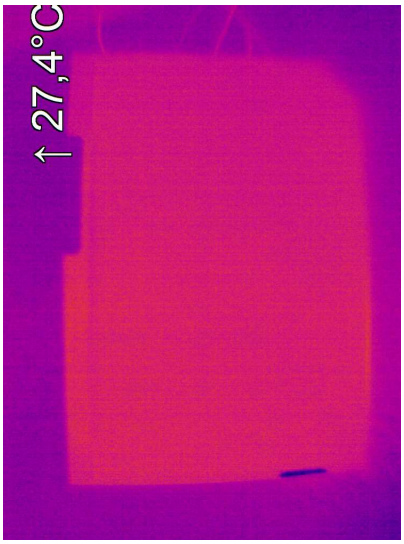
(e) Après 3s de lecture



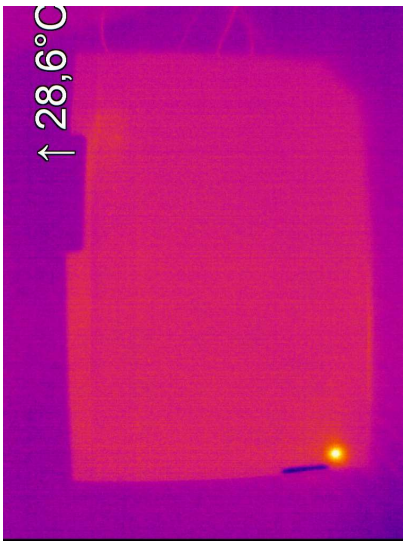
(f) Après 20s de lecture

FIGURE 2.15 – Vue infrarouge de la carte SD témoin étudiée pendant les phases de mise sous tension et de lecture

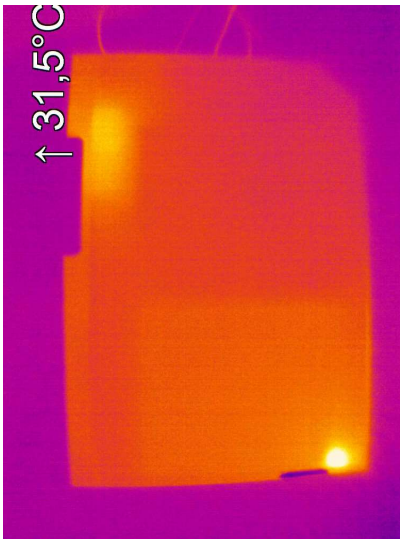
Contrairement au comportement de l'échantillon témoin, la carte de l'étude de cas montre une augmentation de la température au niveau de la mémoire à partir de la phase d'initialisation (Figure 2.16b). Il s'agit du point chaud en bas à droite. Lorsque le script passe en phase de lecture, l'augmentation de la température au niveau de la mémoire est encore plus importante (Figure 2.16c) et augmente avec le temps (Figure 2.16d). Au vu de ce résultat, l'analyse est arrêtée afin d'éviter d'endommager davantage la carte.



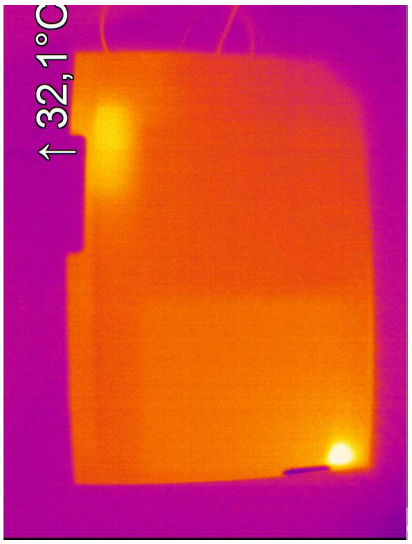
(a) État initial



(b) Mise sous tension



(c) Début de la lecture



(d) Après 3s de lecture

FIGURE 2.16 – Vue infrarouge de la carte SD étudiée pendant les phases de mise sous tension et de lecture : un défaut est détecté en bas à droite

L'analyse des images de la caméra infrarouge (Figure 2.16) et des images Rayons-X (Figure 2.14c) confirme la position du défaut dans la mémoire, au niveau d'une rangée de bondings. Compte tenu du fait que le composant se trouve dans un boîtier rigide, il est normalement impossible que les bondings bougent et se touchent. Il y a donc deux

hypothèses qui peuvent expliquer le phénomène. Le défaut peut se situer au niveau des bondings, et dans ce cas la température a suffisamment augmenté pour faire fondre la résine et permettre aux bondings de se rejoindre. Le second cas, un point de fusion s'est produit à l'intérieur de la puce (fusion du silicium, des oxydes de silicium et des pistes).

Nous l'avons évoqué précédemment, l'intérêt de faire une acquisition aux Rayons-X 3D est de figer la situation puis de pouvoir revenir analyser les images par la suite du process. Le cas se présente pour notre support. Nous constatons avec la caméra infrarouge une élévation de la température au niveau d'une des puces et des bondings. Si nous reprenons la vue des bondings (Figure 2.14d), nous ne voyons aucun défaut. De plus, si nous poursuivons l'observation nous pouvons voir en combinant les vues du PCB (Figure 2.14a) et de la puce du contrôleur (Figure 2.14c) que le défaut se localise directement dans la puce. D'un point de vue purement recherche, il y aurait un intérêt à faire une ouverture chimique de la carte pour observer avec un microscope la puce du contrôleur. Cependant, nous évoluons en corrélation avec les pratiques des laboratoires de forensique numérique donc il n'est pas possible d'effectuer des manipulations superflues. Nous l'avons mentionné dans la section *Contexte*, les actions sont effectuées sous l'accord préalable d'un magistrat et elles ont un coût. Dans les cas similaires à notre exemple, les expertises se concluent sur la non-possibilité d'extraction des données et le dossier est clôturé.

Bien que le dossier ait été clôturé sans pouvoir extraire les données, la démarche n'a pas été un échec, au contraire. Le protocole de diagnostic a permis de faire une recherche méthodique du défaut permettant d'éliminer les différentes options, pour se focaliser sur les étapes apportant réellement une information. Un autre point positif du protocole réside dans l'ajout de la caméra thermique pour effectuer le diagnostic. Une caméra proposant une bonne résolution et un temps d'échantillonnage rapide, permet de localiser les effets transitoires dans les supports. Sans ce type d'équipement, l'expert ne dispose que de la consommation de courant du support pour estimer un défaut et n'a aucune information de localisation. En enregistrant les expérimentations avec la caméra thermique, il est possible de figer des points de chauffes furtifs, puis de revenir dessus en l'associant avec de l'imagerie (Rayons-X, optique, SAM,). En complément de la conclusion par rapport à notre protocole, nous allons mener une discussion sur les différentes suites pouvant être données.

2.3 Discussion

Les deux parties du protocole de diagnostic que nous avons développé présentent plusieurs chemins, débouchant sur plusieurs issues. Nous allons faire un état des lieux de ces situations. Elles sont au nombre de trois d'après les deux branches non-invasives et invasives du protocole :

1. Data lost (données perdues) : il n'est plus possible de lire le contenu de la puce mémoire car elle est trop endommagée. Les facteurs qui peuvent en être la cause sont les fractures suite à un stress mécanique trop important, une corrosion suite à une délamination dégradant une piste ou un point de fusion suite à un stress électrique.
2. Reparation of assembly defect (Réparation d'un défaut d'assemblage) : le PCB servant à relier les puces présente un défaut qui peut être une corrosion suite à une délamination, une fissure dans le package dû à un stress mécanique. La corrosion et la fissure peuvent provoquer la coupure d'une piste. Le stress mécanique peut également couper un fil de bonding. Il est possible de réparer une piste ou un bonding coupé pour restaurer les communications entre les composants. Pour cela, plusieurs solutions existent dont l'utilisation de colles conductrices pigmentées telles que présentées dans des travaux [139, 51]. Ayant participé à ces travaux, je recommande donc cette technique pour la réparation des pistes et pour reformer des bonding cassés.
3. Try direct memory reading (Tentative de relecture de la mémoire) : un des composants est défectueux ce qui empêche l'accès aux données. À ce stade nous ne savons pas s'il s'agit du contrôleur ou de la mémoire. Par conséquent il nous faut travailler sur les suites à donner à notre protocole.

Le cas d'étude est l'exemple parfait de la première situation. À la fin du processus de diagnostic, nous arrivons à la conclusion que la puce mémoire est défectueuse, mais ce n'est pas toujours le cas. Pour beaucoup de support, nous arrivons dans la troisième situation. Il fallait donc trouver une solution pour aller plus loin dans le diagnostic, pour viser l'extraction des données. Dans un premier temps une question se pose sur l'élément défectueux dans la MMC. Pour résumé, si c'est la mémoire, comme pour la première situation, les données sont définitivement perdues ; si c'est le contrôleur, il reste une possibilité d'extraction. En effet, même si nous arrivons à nous substituer au contrôleur, les données ne seront pas forcément exploitables directement. Plusieurs opérations réalisées par le contrôleur seront à inverser et il faudra également compenser les corrections d'erreurs de lecture que peut apporter le contrôleur. Deux étapes se détachent donc pour la suite des travaux. La première consistant à pousser le diagnostic en interne

de la MMC pour déterminer quelle puce est défectueuse, puis à relire la mémoire sans passer par le contrôleur. La seconde pour corriger les erreurs de lecture qui peuvent avoir plusieurs causes. Ces deux étapes seront abordées dans le prochain chapitre *Extraction et fiabilisation de la donnée.*

Chapitre 3

Extraction et fiabilisation de la donnée

Lors des discussions dans le chapitre précédent, nous avons abordé plusieurs points restant à traiter après l'utilisation de notre protocole de diagnostic. Dans un premier temps, nous devons entrer en communication avec le support pour comprendre quelle puce est défectueuse, le contrôleur ou la mémoire, ce que nous aborderons dans la section *Extraction de la donnée*. Pour réaliser cette opération, nous avons besoin d'une solution polyvalente (applicable à l'ensemble des MMC) et fiable (réduisant les risques d'introduction d'erreurs de lecture). Dans un second temps, après avoir réussi la lecture de la donnée, il faudra réaliser les opérations de corrections d'erreurs et de transformations (c'est-à-dire XOR, agencement des pages) normalement effectuées par le contrôleur. Nous avons choisi de nous focaliser sur la correction des erreurs dans la section *Fiabilisation de la donnée*, car les autres opérations sont plus facilement prises en charge par des outils commerciaux. Si nous prenons l'exemple de la solution "PC3000 flash", dans le cas où l'association du contrôleur et de la mémoire de la MMC est connue, les opérations sont préprogrammées et le logiciel propose de faire la relecture de la mémoire, la correction des erreurs et applique automatiquement les opérations mathématiques (comme un XOR). En revanche si l'association du contrôleur et de la mémoire de la MMC n'est pas connue, il est plus compliqué de faire la lecture, la correction des erreurs et de retrouver l'éventuel XOR, car les paramètres ne sont pas dans la base. Toutefois de nombreux travaux étant conduits sur la recherche du XOR par des sociétés comme Rusolut, nous nous sommes focalisés sur la partie relecture et correction des erreurs.

3.1 Extraction de la donnée

Dans cette section, nous allons décrire la méthode que nous avons utilisée pour effectuer l'extraction des données des puces mémoires de MMC. Cette étape intervient à l'issue de notre protocole de diagnostic, lorsque l'ensemble des opérations de diagnostic ont conduit l'opérateur à la dernière étape du protocole, c'est-à-dire "Try direct memory reading". Il nous faut à présent identifier la puce qui présente un défaut, vu qu'il ne s'agit pas d'un défaut d'assemblage. Il existe deux possibilités :

— Un défaut de la puce mémoire : Ce défaut s'avère actuellement irréversible pour un laboratoire de forensique numérique. En effet, les puces mémoires qui contiennent la donnée sont des circuits complexes, sensibles aux stress électriques et mécaniques. À notre connaissance et à l'heure actuelle, dans un contexte d'expertise judiciaire, il n'est pas possible de réparer un défaut électrique ou mécanique intervenant dans les puces électroniques, compte tenu de la taille micrométrique des éléments. Dans la mesure où il n'est pas possible de communiquer avec la mémoire, une solution consisterait à aller lire la donnée cellule par cellule au niveau des transistors. Des travaux expérimentaux ont été effectués pour cette méthode relecture et ils seront

abordés dans la section *Cas des mémoires défectueuses.*

— Un défaut sur le contrôleur : Cela empêche l'hôte d'établir une communication avec la MMC, entraînant l'inaccessibilité des données bien qu'elles soient toujours "physiquement" présentent sur le support. Comme nous avons eu l'occasion de l'introduire, il existe des solutions commerciales telles que celles de "Acelab" ou de "Rusolut" permettant de récupérer les données. Cependant, ces solutions ne couvrent pas tous les supports et demandent d'avoir un minimum d'informations sur les références des puces utilisées. Régulièrement, dans les expertises judiciaires, les supports étant dégradés, les références sont difficilement lisibles, voire absentes. Dans ce cas, l'utilisation de solutions commerciales devient compliqué.

Nous allons donc présenter la méthodologie que nous avons développé pour effectuer les opérations d'identification du composant défectueux, puis si la mémoire est fonctionnelle, les opérations de relecture sures et efficaces.

3.1.1 Rétro-ingénierie d'une MMC

La lecture *in situ* de la mémoire implique un certain travail préparatoire qui peut être chronophage, mais compte tenu de l'importance des données, le processus est payant. Avant de débuter, il est intéressant de connaître l'architecture interne du support concerné (section *Gestion de la mémoire flash interne*) ainsi que les protocoles utilisés (section *Protocole de communication interne*).

La rétro-conception du support MMC peut être découpée en trois étapes :

— le travail préparatoire (présenté en section *Travail préparatoire*) consistant à une étude initiale du support avec des techniques non-invasives (c'est-à-dire imageries Rayons-X, optique). À partir d'une tomographie 3D aux Rayons-X, il est possible d'étudier la présence et le raccordement de plots de debug ainsi que le positionnement des bondings. Cette technique est présentée dans la section *Machine à Rayons-X.* Le but de cette étape est de préparer des scenarii pour s'interconnecter efficacement sur le bus de communication entre le contrôleur et la puce mémoire.

— l'interconnexion (présentée en section *Interconnexion*) sur le support. Cette étape est la suite de l'étude précédente. Elle a pour but de se raccorder physiquement sur les plots présentant un intérêt. L'interconnexion doit pouvoir permettre plusieurs interactions, à savoir écouter les échanges ou communiquer. Ces deux techniques n'ont pas recours aux mêmes sondes ou aux mêmes câblages. Nous avons donc besoin d'une solution polyvalente.

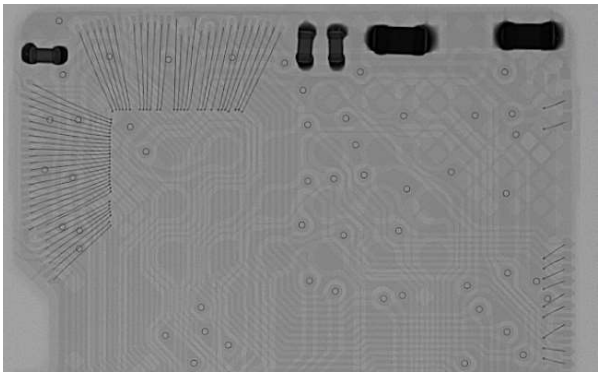
— l'extraction et l'exploitation (présentées en section *Diagnostic des puces*) faite sur le support. Au début de cette étape, nous ignorons toujours si la mémoire

est fonctionnelle ou non. Le premier objectif sera donc de statuer sur l'état de la mémoire. Pour cela, une solution efficace consiste à étudier les échanges internes du support MMC. Une fois cette vérification faite, si la mémoire est toujours fonctionnelle, il sera possible d'en effectuer l'extraction de son contenu.

3.1.2 Travail préparatoire

Comme énoncé précédemment, le but du travail préparatoire est de définir le meilleur point d'accès possible pour identifier les échanges avec la mémoire. Dans un premier temps, il faut observer s'il y a des plots de debug ou non. Pour cela, la manière la plus rapide consiste à utiliser une binoculaire avec une lumière directe ou rasante ; afin de voir si des reliefs sont identifiables (Figure 3.1a). Dans le cas contraire, il est possible que le vernis ou la résine soit trop épaisse pour pouvoir identifier un relief du cuivre en dessous. Dans certains cas, il n'y a tout simplement pas de plots de debug sur lesquels s'interconnecter. Il est également possible de rechercher les plots grâce à une observation aux Rayons-X 2D (Figure 3.1b).

(a) Vue optique



(b) Vue aux Rayons-X

FIGURE 3.1 – Identification des plots de debug de cartes microSD

Si les plots de debug ne sont pas présents ou en nombre insuffisant, il faut rechercher un autre moyen de s'interconnecter. Le PCB d'un support MMC étant composé classiquement de deux couches de cuivre (des pistes et des vias) et les puces étant situées du même côté, il est fortement probable que l'ensemble des signaux se retrouvent sur une surface accessible.

La dimension des éléments est aussi importante. Une piste possède une dimension qui est beaucoup moins importante qu'un via, celui-ci mesurant environ 0,3 mm. Il est évident que pour des opérations manuelles, quelle que soit la technique utilisée, une plus grande surface de travail sera privilégiée. Par conséquent, l'ordre de priorité sera de favoriser : les plots puis à défaut les vias et en dernier recours les pistes.

Une fois localisés les points d'intérêt sur lesquels nous allons effectuer nos interconnexions, il faut identifier la structure interne du support MMC. La méthode la

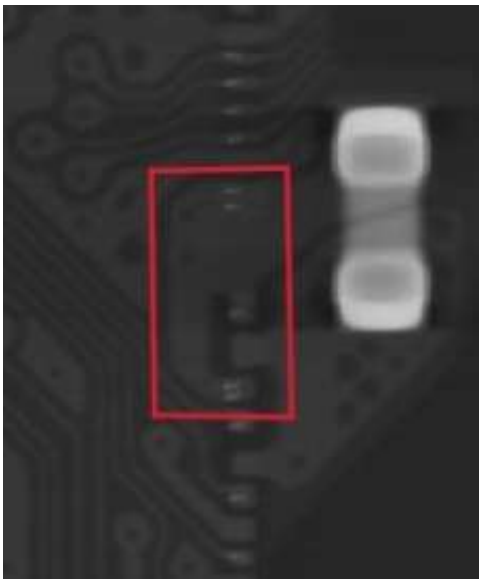
plus simple est de procéder à une acquisition du support en Rayons-X 3D (par exemple par tomographie) comme décrit dans la section *Machine à Rayons-X*. Il faut regarder la position des puces et surtout la disposition des bondings. Dans la mesure où le contrôleur permet les échanges entre l'hôte et les mémoires, une partie des bondings de celui-ci est destinée aux ports de communication externe comme décrit dans les sections *La norme SD*, *La norme eMMC* et *La norme UFS*. Pour la communication interne, dont le protocole est décrit dans la section *Protocole de communication interne*, nous devons retrouver un nombre identique de bondings sur le contrôleur et la mémoire. Ce sont ces bondings qui vont nous intéresser et sur lesquels nous allons porter notre attention lors de la rétro-conception du PCB.

Ainsi voici les trois types de signaux que nous allons rechercher sur le PCB lors de la rétro-conception :

1. Les alimentations qui permettent de fournir les différentes tensions à la puce mémoire, ainsi que le référentiel appelé ground ou masse. Ces signaux sont facilement identifiables car ils sont reliés à plusieurs points, donc sur plusieurs bondings. Sur les PCB, ils sont reliés à des plans. Lors de la phase d'identification des signaux, il sera aisé de définir les bondings pour les éliminer.
2. Les signaux de données qui sont généralement regroupés sous forme de bus de quatre ou huit lignes. Ils sont également entourés par les alimentations car lors du fonctionnement du composant mémoire, la phase d'écriture nécessite une consommation non négligeable de courant. Il faudra rechercher des groupes de quatre bondings avec une forte concentration de bondings d'alimentation (tension et masse).
3. Les signaux de contrôle qui sont moins exigeants dans le positionnement. Ils sont au nombre minimum de sept mais peuvent être en nombre supérieur en fonction de la vitesse de transfert et de la version de la norme. L'ordre et la position des signaux de contrôle sont certes moins contraints par le fonctionnement intrinsèque de la puce mémoire mais comme nous le verrons par la suite, une certaine logique est généralement utilisée.

Pour la suite de la déclinaison de notre méthodologie, nous allons utiliser un support MMC de type carte microSD. Il s'agit d'un support générique acheté pour les tests. Même si ce n'est pas un scellé, nous ferons en sorte de toujours l'utiliser dans les mêmes conditions et de ne pas réaliser d'étapes allant à l'encontre de la préservation de la preuve. La première étape que nous réalisons sur ce support est d'effectuer une acquisition aux Rayons-X 3D (Figure 3.2a). Cela nous permet d'effectuer la rétro-conception du PCB et de tenter d'identifier le rôle de chacun des fils de bonding de la puce mémoire.

(a) Vue globale

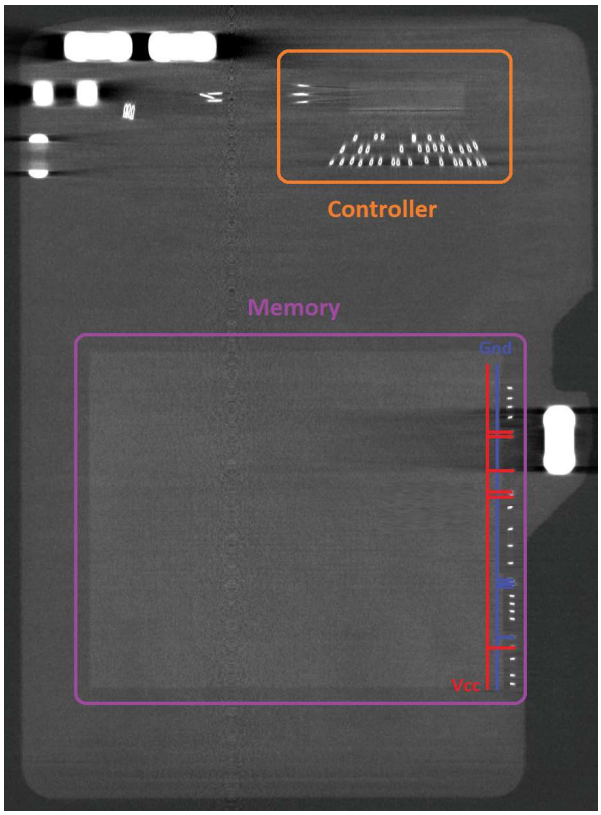


(b) Zoom sur une partie de la zone de bondings

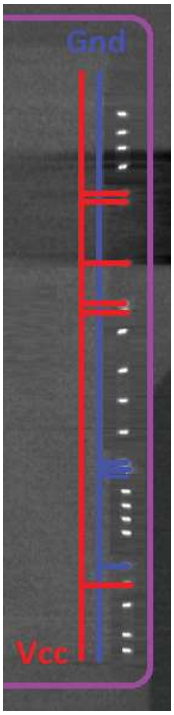
FIGURE 3.2 – Vue aux Rayons-X de la carte microSD étudiée

En se basant sur les trois points mentionnés précédemment, en premier lieu il convient d'identifier les signaux d'alimentation. Il faut donc rechercher les bondings qui ont la même piste ou le même plan d'origine. La Figure 3.2b qui est un zoom de notre image d'origine, illustre bien l'exemple de plusieurs fils de bondings qui prennent leur source sur la même piste. Les fils sont les cinq traits blancs encadrés en rouge. En regardant plus en détail le design du PCB, ils sont reliés à la tension d'alimentation de la carte, donc fournissent l'alimentation de la puce mémoire. Maintenant que nous avons localisé une première piste servant à l'alimentation, nous pouvons la suivre au travers du PCB pour voir si elle couvre d'autres bondings de la puce mémoire, ce qui est le cas.

En ce qui concerne la masse, par construction elle est commune pour toute la carte. Nous partons donc de la broche de masse de la communication avec l'hôte dont la position est normée. Ensuite, nous suivons cette piste pour identifier les bondings de la puce mémoire qui y sont reliés. Sur notre exemple (Figure 3.2b), avec cette démarche nous identifions 3 bondings pour la masse et six bondings pour la tension. Ils sont présentés sur la Figure 3.3 de couleur bleu pour la masse (Gnd) et rouge pour la tension (Vcc).



(a) Mise en évidence des bondings servant à l'alimentation de la puce mémoire



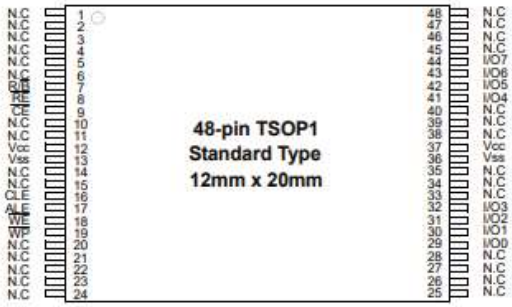
(b) Zoom sur les bondings

FIGURE 3.3 – Vue aux Rayons-X de la carte microSD étudiée (bleu = masse et rouge = tension)

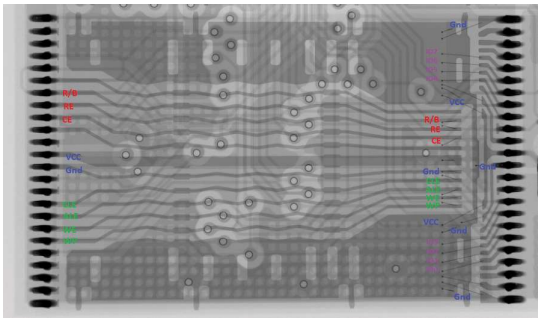
Sur la Figure 3.5a, nous pouvons clairement voir des groupes de bondings qui se détachent. Il est possible de distinguer trois groupes de quatre bondings ainsi qu'un groupe de trois bondings. Par rapport à la description des signaux faite précédemment en termes de nombre et de dépendances, le groupe de trois doit faire partie des signaux de contrôle. Deux groupes de quatre bondings au centre sont probablement des données par la proximité avec les alimentations. Cela impliquerait que le dernier groupe en haut soit les contrôles manquants. Il est possible de mettre à jour les hypothèses sur la localisation des signaux (Figure 3.5b).

Pour corroborer nos méthodologies déductives, nous pouvons essayer de voir si elle peut s'appliquer sur des mémoires de même type utilisées en dehors des MMC. En effet, comme abordé dans la section *Architecture d'une MMC*, les puces flash qui sont intégrées dans les MMC puisent leurs origines dans le catalogue de fabricants. Il s'agit de puces standards qui peuvent être utilisées pour des MMC mais qui peuvent également être commercialisées dans d'autres packages. Une mémoire flash est traditionnellement commercialisée sous forme d'un composant en boîtier Thin Small Outline Package (TSOP) de 48 broches. Sur la Figure 3.4a, il est possible de voir qu'un composant en package a des broches de chaque

côté. Les contrôles se situent sur la gauche et les I/O sur la droite. Instinctivement, il peut être envisagé qu'à l'intérieur du package, les bondings soient disposés de la même manière. Cela rendrait toute comparaison avec notre mémoire de MMC impossible. Cependant, lorsqu'une vue aux Rayons-X est réalisée, il est possible de constater que les bondings au niveau de la mémoire sont tous situés du même côté. Il est aisé de suivre les liaisons entre les broches du composant et les bondings pour leur attribuer un rôle (Figure 3.4b). Sur cette figure, le nom des broches a été rapporté en corrélation avec la Figure 3.4a. Les tensions et masses ont été identifiées en bleu. Les deux groupes d'I/O qui sont situés à droite sont repérés en violet. Nous pouvons voir que les broches sont raccordées au plus court sur la mémoire. Deux autres groupes sont identifiables. Un groupe de trois contrôles est repéré en rouge et un second groupe de quatre contrôles est repéré en vert sur la gauche de la figure. Nous pouvons voir qu'ils traversent pour prendre attache sur la puce du même côté que les signaux d'I/O.



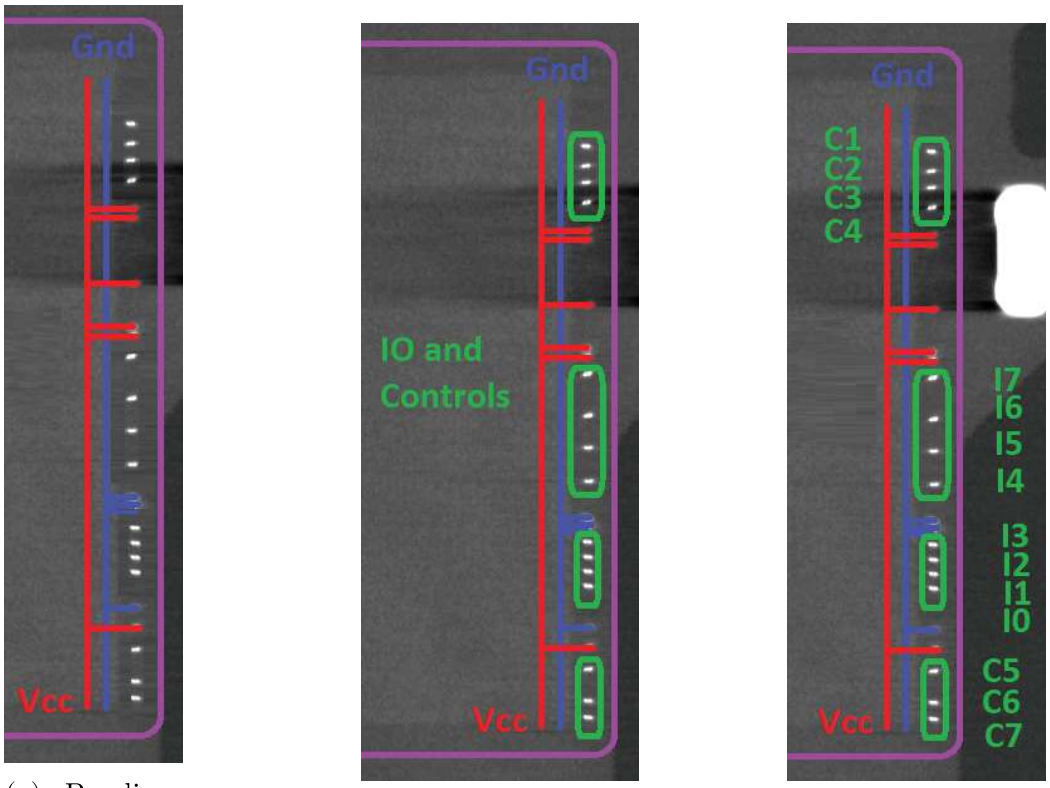
(a) Pinout d'une NAND Flash en boitier TSOP provenant d'une datasheet [205]



(b) Vue aux Rayons-X d'une NAND flash avec la correspondance des bondings

FIGURE 3.4 – Comparaison entre la datasheet d'une mémoire flash et son implantation réelle dans un package

Dans cet exemple, les signaux d'I/O sont situés sur l'extérieur et les signaux de contrôles sont regroupés au centre. Nous avons constaté, lors des observations aux Rayons-X, qu'en fonction des marques des mémoires cela pouvait être l'inverse.



(a) Bondings d'alimentations

(b) Signaux de contrôle et I/O

(c) Proposition du rôle des bondings

FIGURE 3.5 – Les différentes étapes d'identification des bondings de la puce mémoire (bleu = masse, rouge = tension et vert = signal)

Dans l'exemple de notre carte microSD, contrairement au boîtier TSOP présenté dans la vue aux Rayons-X, les signaux de contrôles semblent être aux extrémités et les I/O au centre. Le résultat de la rétro-ingénierie et de nos premières hypothèses est illustré sur la Figure 3.5c.

Le travail ne s'arrête pas là, car il faut proposer des solutions pour établir une connexion. Les bondings sont alors suivis pour voir leurs propagations sur le PCB. Dans cet exemple il n'y a pas de plots de debug. En accord avec l'hypothèse émise dans la partie *Travail préparatoire*, il faut donc se focaliser sur les vias. Il est possible d'identifier un via pour tous les signaux d'intérêt sauf pour un des signaux de contrôle, comme le montre la Figure 3.6. D'après notre hypothèse, il s'agit du signal R/B, qui n'est pas nécessaire pour la lecture *in situ*. Par conséquent, nous pourrons réaliser nos travaux avec uniquement les six contrôles pour lesquels nous avons identifié les vias.

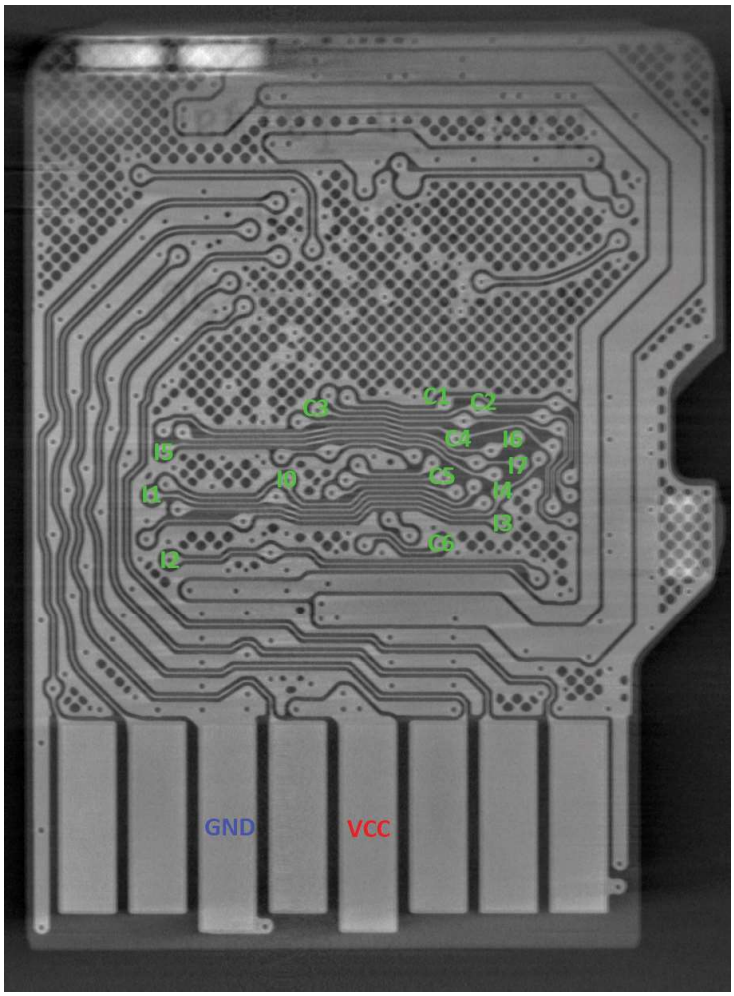


FIGURE 3.6 – Report des noms attribués à chacun des bondings sur les vias correspondants afin de s'interconnecter dessus

À ce stade, il n'est pas encore possible de savoir si nos hypothèses sont valdies. Pour déterminer si c'est le cas, il va falloir s'interconnecter sur les vias identifiés puis essayer, soit de communiquer, soit d'intercepter des communications.

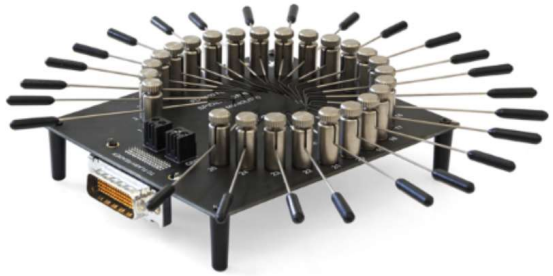
3.1.3 Interconnexion

Après avoir identifié les pads ou vias sur lesquelles s'interconnecter, il faut réaliser physiquement les liaisons. Pour cela, il existe plusieurs solutions commerciales dont l'utilisation est perfectible. Nous avons donc développé une solution qui a pour but d'être polyvalente et fiable, car nous avons recours à un PCB sur mesure.

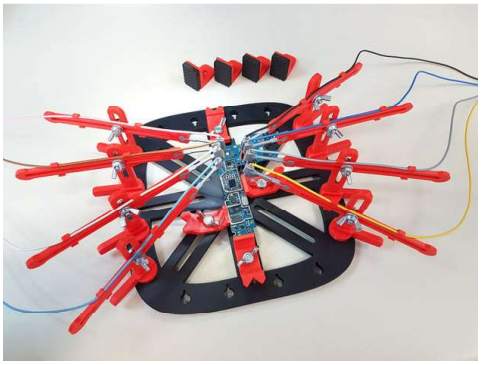
3.1.3.1 Solutions commerciales

Il existe plusieurs solutions commerciales qui peuvent être utilisées pour intercepter les signaux entre le contrôleur et la mémoire flash. Parmi les dispositifs couramment utilisés,

figurent les adaptateurs monolithiques microSD/SD/UFD de type Spiderboard [206], PCBite [53], Rusolut [207] et Multi-com [208]. Si nous prenons l'exemple de la Spiderboard, un technicien peut modifier la position des aiguilles comme le montre la Figure 3.7a. Le réglage de chacune des pointes de touche est fait indépendamment pour garantir une polyvalence de la solution, par rapport à la multitude des supports MMC disponibles sur le marché. Les aiguilles sont faites pour venir toucher les plots de debug, cependant leurs dimensions peut rendre la solution plus complexe à utiliser lorsqu'il faut se connecter à des vias. Les utilisateurs peuvent rencontrer un autre problème pour l'utilisation de cette solution. Les pointes étant placées en périphérie, il peut s'avérer complexe de les positionner sur des motifs matriciels. Il faudra réfléchir en avance de phase aux pointes à positionner en priorité, pour ne pas se bloquer l'accès aux autres plots de debug. La flexibilité de ce genre de solution est donc limitée. Cette solution commercialisée par ACELab étant relativement onéreuse, ce concept a été reproduit en impression 3D puis mis à disposition sur le site Thingiverse [209]. Cela permet de réaliser des opérations similaires (Figure 3.7b), mais pour un coût bien moindre (une bobine d'impression et de quelques vis et aiguilles).



(a) La Spiderboard par ACELab [210]



(b) Produit équivalent réalisé en impression 3D

FIGURE 3.7 – Exemple de tables à base d'aiguilles mobiles permettant la lecture des supports MMC

Une solution qui parait plus polyvalente est commercialisée par la société Sensepeek [53]. La gamme des produits permettant l'interconnexion est appelé PCBite, avec un exemple visible sur la Figure 3.8. Le catalogue de produits PCBite est assez conséquent, prévoyant une couverture large des équipements pouvant être utilisés, comme le montre la Figure 3.9. Le support qui nous intéresse est muni de bras articulés et aimantés qui se posent à volonté sur un plateau magnétique. Une fois en place, la liaison du bras est forte, ce qui ancre bien le support de la pointe de test. À l'usage, cette solution règle le problème des pointes à déposer sur une zone matricielle, cependant l'ajout de sondes supplémentaires peut s'avérer compliqué. En effet, cette solution est parfaite lorsqu'il faut

appliquer un petit nombre de sondes, mais la solution pour articuler le bras demande une force qui peut faire trembler et bouger les autres sondes. Il peut donc s'avérer difficile de déposer une vingtaine de sondes comme le demande une mémoire flash de MMC.

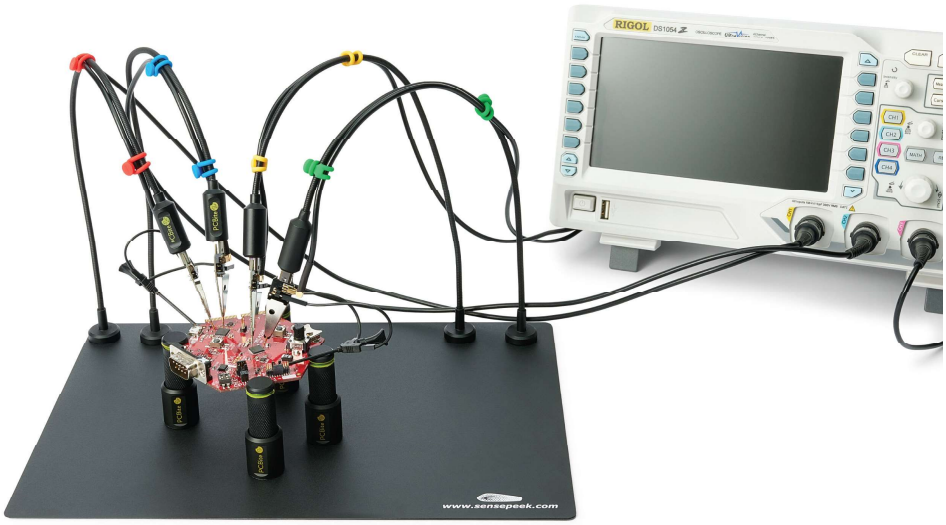


FIGURE 3.8 – Solution PCBite de la société Sensepeek [53] pour s'interconnecter sur des cartes électroniques

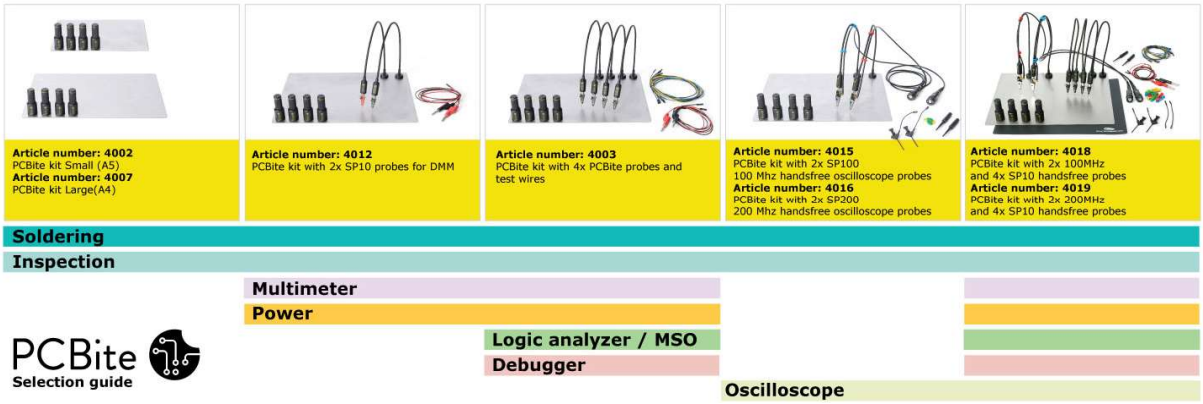
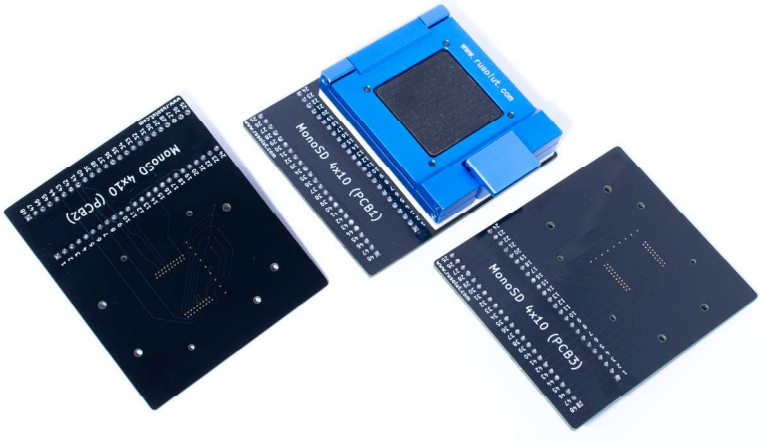


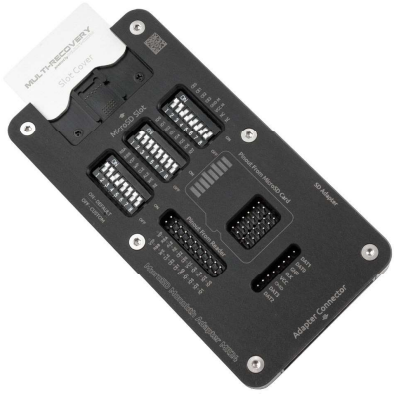
FIGURE 3.9 – Catalogue des solutions PCBite en fonction des applications

Il existe en plus des solutions polyvalentes, des solutions qui sont spécifiques à chaque type de MMC. La première d'entre elles est commercialisée par Rusolut [207]. Le système de lecture est nommé Visual NAND Reconstructor (VNR) visible sur la Figure 3.10a. Il est composé d'un lecteur et d'adaptateurs qui doivent être changés en fonction de la MMC ciblée. Cela signifie que la MMC doit être dans leur catalogue pour être traitée. Le prix de ces adaptateurs est généralement compris entre 300 et 600 euros, ce qui est conséquent vue le nombre de MMC différentes sur le marché. Le principal atout de cette solution réside dans le logiciel (Figure 3.11) qui permet d'appliquer les opérations mathématiques à la suite d'une extraction brute des données d'une mémoire flash. L'interface étant conviviale,

il est facile de retrouver les opérations pouvant être appliquées. Cette solution propose également un large catalogue de MMC déjà maîtrisées, ce qui facilite grandement le traitement pour les techniciens.



(a) Solution Rusolut [207] pour les cartes SD de type 4x10



(b) Solution Multi-com [208] modèle MR24 pour les cartes microSD de type 4x6

FIGURE 3.10 – Exemple d'adaptateurs permettant de s'interconnecter sur les plots de debug de supports MMC

Un autre exemple de solution basée sur des adaptateurs spécifiques est commercialisée pour le site Multi-com [208]. Ces adaptateurs sont conçus pour embarquer une MMC de type carte microSD. Ils utilisent un système de pins réglables qui viennent contacter les plots de debug. Les liaisons sont ensuite faites vers des borniers plus facilement utilisables pour des équipements de mesure ou de programmation. Le modèle présenté en Figure 3.10b est nommé MR24. Il permet de s'interconnecter sur des cartes microSD disposant de plots de debug en matrice de 4x6. Il s'agit de l'adaptateur que nous avons utilisé pour réaliser plus facilement certaines de nos expérimentations dans la section *Confirmation du comportement et des signaux*.

En conclusion, les solutions commerciales présentent des défauts lors de leurs utilisations. Les solutions composées d'aiguilles sont polyvalentes mais elles manquent de fiabilité. À l'inverse, les adaptateurs sont fiables mais il faut en acheter pour chaque design de MMC différent et pour un coût important. Nous avons donc décidé de développer une autre solution qui réponde aux critères de polyvalence et de fiabilité souhaités. Pour cela, nous avons basé notre solution sur l'utilisation d'un PCB et de colle conductrice.

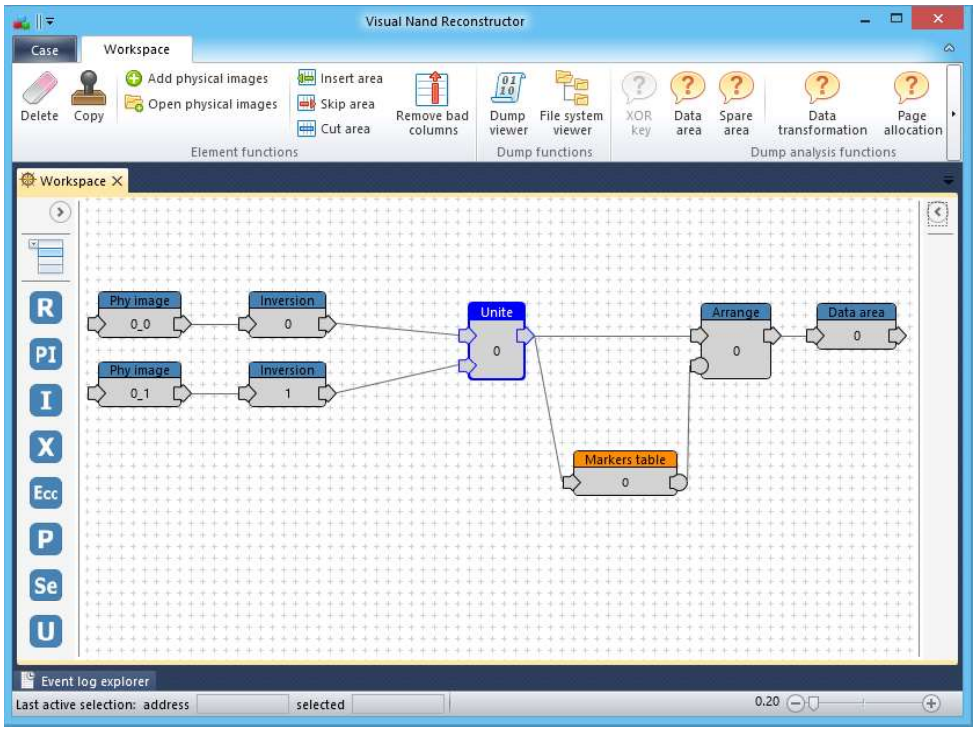


FIGURE 3.11 – Logiciel VNR de la société Rusolut permettant d'appliquer les opérations logiques pour les relectures brutes des mémoires flash

3.1.3.2 Solution non-commerciale

Dans la section précédente, nous avons mis en évidence des problèmes inhérents à chaque solution commerciale. Ce que nous pouvons retenir, c'est que des adaptateurs sont pratiques parce qu'ils sont stables et fiables, alors que des tables sont polyvalentes. Le cadre de travail dans les laboratoires de forensique numérique est également un axe de réflexion pour l'établissement du cahier des charges de notre solution. Les scellés reçus par les laboratoires de forensique numérique sont variés. Le cahier des charges de notre solution doit être axé sur la polyvalence. Notre solution doit être réalisable rapidement avec un minimum d'achats pour s'affranchir des délais de livraison. De plus, les laboratoires de forensique numérique suivent des protocoles strictes qui nécessites de ranger les scellés entre chaque opérations. Une solution comme la Spiderboard ou le PCBite ; basée sur des points de contacts flottants, nécessitent un repositionnement des contacts pour chaque utilisation. Cela implique une grosse perte de temps pour le technicien et une incertitude sur le positionnement des pointes, donc un impact sur la fiabilité. Notre démarche pour fabriquer un moyen d'interception polyvalent et fiable a donc été de s'orienter sur un adaptateur plutôt qu'une table avec des pointes. Le cahier des charges retenu pour le développement de la solution était le suivant :

— Les points de contact doivent être fixes pour garantir la fiabilité de la solution lors de déplacements. Nous n'utilisons pas des pins de contact avec ressorts (pogopins)

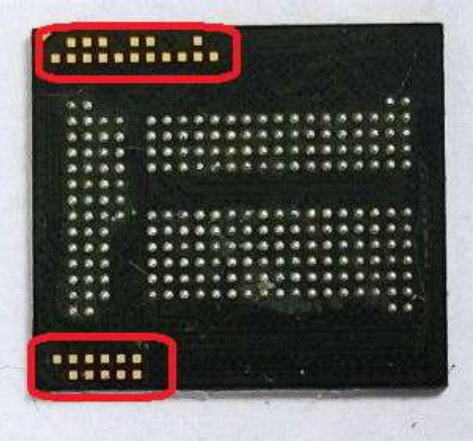
car ils sont trop sensibles aux vibrations et risques de sauter en cas de mouvement.
— Il doit être possible d'appliquer notre solution aussi bien sur des plots de debug que sur des vias, voire des pistes. Notre solution doit avoir une dimension en conséquence et ne doit pas être liée à une matrice prédéfinie, pour être polyvalente.
— Comme il n'est pas possible que la solution soit universelle et utilisable sur n'importe quel support MMC comme pour les adaptateurs VNR ou Multi-com, le design de l'adaptateur devra être capable de changer pour chaque support. Ainsi, la conception des adaptateurs doit être facile et "industrialisable" afin de s'adapter à chaque nouveau support rencontré.
— Les fils "volants" étant rarement une bonne alternative lorsqu'il s'agit d'acheminer un signal électrique en raison des interférences générées, notre solution doit donc intégrer un maximum de pistes routées sur une carte électronique. Si le fait d'élaborer nos propres cartes peut sembler une perte de temps par rapport à la soudure directe de fils, la stabilité et la fiabilité gagnées sont considérables. De plus, avec de bons choix lors de la conception, il est possible de trouver une solution capable de s'adapter aux différents supports rencontrés. Pour le routage des cartes électroniques, il existe des règles et des conseils qui peuvent être retrouvés sur différents sites, dont celui de la société Proto-electronics.com [211].

Le cahier des charges élaboré doit tenir compte des différentes exigences pour concevoir un adaptateur polyvalent, permettant d'être modifié en fonction de chaque support MMC à traiter. Pour que le système soit fiable, l'adaptateur doit également être conçu pour réduire les interférences extérieures qui peuvent perturber la lecture des données.

Pour répondre au cahier des charges, notre solution consiste à réaliser une carte électronique sur mesure. Elle est constituée d'ouvertures sur le support MMC (dans le package) à l'endroit des points de contact (plots de debug, vias, ...) et de pistes permettant de faire la liaison électrique avec des borniers. L'intérêt de faire des ouvertures à l'endroit exact des points de contacts réside dans l'utilisation de colles conductrices pour faire la liaison entre le support MMC et la carte électronique. Cela réduit le nombre de fils "volants" et permet de diminuer la perturbation des signaux. Le support doit subir une préparation car les vias ne sont jamais exposés et dans beaucoup de cas, les plots de debug non plus. Par exemple sur une carte SD ou microSD, il faut donc retirer la fine couche de vernis de façon localisée pour empêcher les courts-circuits lors de l'utilisation de la colle conductrice. Les étapes de notre solution sont donc :

1. Préparation du support : Cette étape est à réaliser en fonction de l'état des contacts sur lesquels nous souhaitons nous raccorder. Si le support MMC possède déjà des pads sous forme de matrice avec un cotting en or comme le port de communication avec l'hôte, cette étape est superflue (Figure 3.12a). Au contraire, s'il y a une couche de vernis ou si nous devons nous raccorder sur les vias, elle est obligatoire.

La couche de vernis est isolante et il n'est pas possible d'interagir avec la mémoire sans cette préparation. Pour rappel, le support que nous avons pris en exemple ne possède pas de plots de debug (Figure 3.12b).



(a) eMMC avec 2 matrices de plots sans vernis

(b) Carte microSD avec vernis utilisé comme cas d'exemple

FIGURE 3.12 – Comparaison entre une eMMC BGA221 et une carte microSD avec plots de debug apparents et recouverts de vernis

Nous devons nous connecter sur des vias donc cette étape est indispensable. Il existe plusieurs solutions pour retirer la couche de vernis située au-dessus des vias :

— Le ponçage : Réalisé avec du papier de verre aux grains très fins, il faut frotter doucement le vernis jusqu'à voir la surface cuivrée. Cette technique ne demande pas beaucoup d'investissements financiers car le papier de verre fin (exemple : 2400, 4000) se trouve dans tous les magasins de bricolage. Le temps nécessaire pour réaliser l'opération sans risque est d'environ 30 à 60 minutes et la difficulté est jugée faible, car la vitesse d'ablation du vernis est assez lente. L'opérateur a donc le temps de s'arrêter en surface des plots sans les endommager. Les avantages de cette technique sont la simplicité et l'homogénéité de la préparation. Le principal inconvénient est que l'ensemble du vernis est retiré sur la zone, donc les pistes ne sont plus protégées ou isolées. Il faudra faire attention aux courts-circuits lors des manipulations et l'absence de vernis favorise la dégradation des pistes dans le temps.

— Le grattage : Réalisé avec un scalpel, le but est de gratter le vernis pour le retirer. Beaucoup plus sélectif que le papier de verre, le scalpel permet de dégager précisément des pistes ou des vias en gardant le reste de la surface intacte. Cependant, les risques sont plus grands car il est possible de retirer trop de matière et d'arracher le cuivre. Le niveau de difficulté est donc jugé intermédiaire. Le coût d'un scalpel est faible et ils sont commercialisés sur internet ou en magasins de bricolage. L'avantage de cette technique est une

bonne sélectivité des éléments. Les inconvénients sont la technicité et le temps du procédé car il faut s'attaquer à chaque via ou piste un à un.

— L'attaque chimique : Réalisée avec de l'acide, cette technique permet d'attaquer un élément avec une assez grande vitesse. Ce procédé nécessite d'avoir de bonnes connaissances dans le domaine. De savoir quel produit utiliser et comment le manipuler en sécurité. Il faut en plus des produits, des éléments de verrerie, de mesure et de chauffe, donc cette technique n'est pas low-cost. Il faudra également bien choisir le produit qui est utilisé pour limiter l'attaque au vernis en préservant le PCB du support MMC (la colle epoxy fixant la fibre de verre), ainsi que les pistes de cuivre. L'avantage de cette technique est la rapidité, alors qu'il y a plusieurs inconvénients dont la sélectivité de l'attaque et le niveau de qualification demandé à l'opérateur.

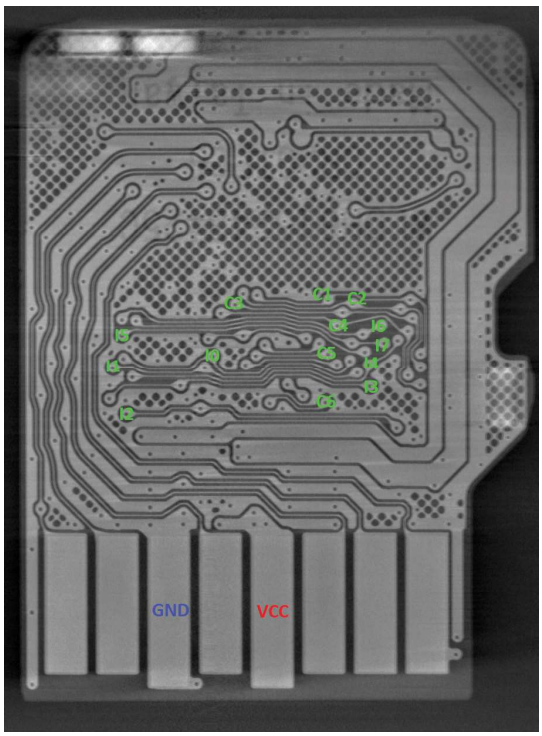
— L'ablation : Réalisée avec un laser, l'objectif est de vaporiser une zone. La précision de l'attaque dépend des paramètres du laser (taille du faisceau, pas de balayage). Cette technique est onéreuse car elle nécessite une machine comme celle présentée dans la partie *Laser d'ablation*. Il s'agit d'un équipement standard dans les laboratoires d'analyses de défaillances ou de forensique numérique. Il est rapide à mettre en œuvre, d'autant plus que l'opérateur est aidé pour le positionnement des zones de gravure. En effet, il est possible de superposer l'échantillon avec une acquisition aux Rayons-X 2D. La vue permet de positionner rigoureusement les points d'usinage sur le support MMC, ce qui accentue la fiabilité de la technique. Le principal inconvénient de cet équipement est donc le prix. Cependant s'il est disponible, il est très avantageux de l'utiliser pour faire les ouvertures sur les points d'intérêt.

Tableau 3.1 – Tableau comparatif des solutions pour dégager les points d'intérêt sur un support MMC

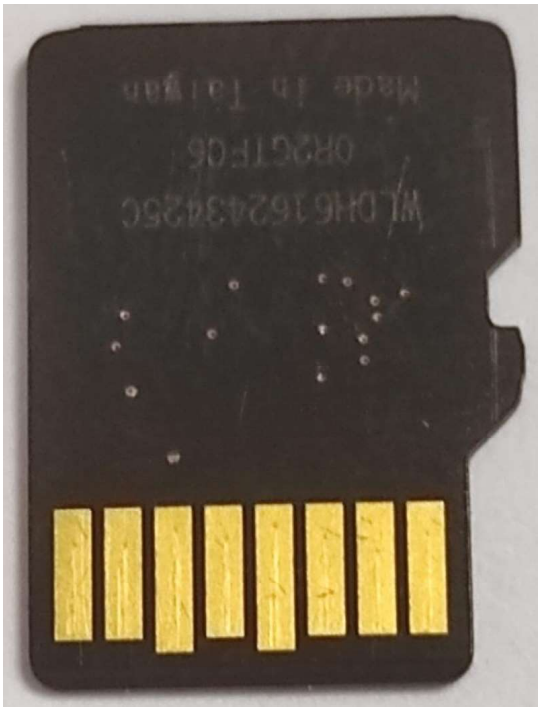
Technique	Outil	Prix (en €)	Temps (en min)	Difficulté	Inconvénients	Avantages
Ponçage	Papier de verre ou stylo fibre de verre	10	30-60	Novice	Exposition complète de la zone	Simple et homogène
Grattage	Scalpel	10	60-120	Intermédiaire	Technicité et temps	Sélectivité
Attaque chimique	Produits chimiques	2-5k	20	Confirmé	Technicité et homogénéité	Rapidité
Ablation	Laser	200k	10	Novice	Prix	Rapidité et sélectivité

Sur la base du Tableau 3.1, nous nous sommes orientés vers une ouverture par laser. Cela nous permet d'avoir une ouverture propre de chacun des vias sans

risque de courts-circuits avec l'utilisation de la colle conductrice pour recréer des continuités électriques. Nous disposons d'une vue aux Rayons-X en 2D pour nous aider au positionnement des ouvertures, ce qui nous fait gagner beaucoup de temps dans la procédure. Concrètement, pour réaliser cette ouverture, nous utilisons un laser de la marque CLC. La source est de longueur d'onde de 1064nm donc dans l'infrarouge, avec une puissance de 30W. Cet équipement est spécialement conçu pour effectuer des ouvertures sur des composants électroniques. Il est donc parfait pour dégager précisément les vias d'un diamètre de 300μm, avec son faisceau d'un diamètre de 50μm. Pour notre application, nous n'avons même pas besoin de dégager complètement les vias. Une simple ouverture de 100 à 150μm suffit (Figure 3.13b).



(a) Vue Rayons-X préparatoire



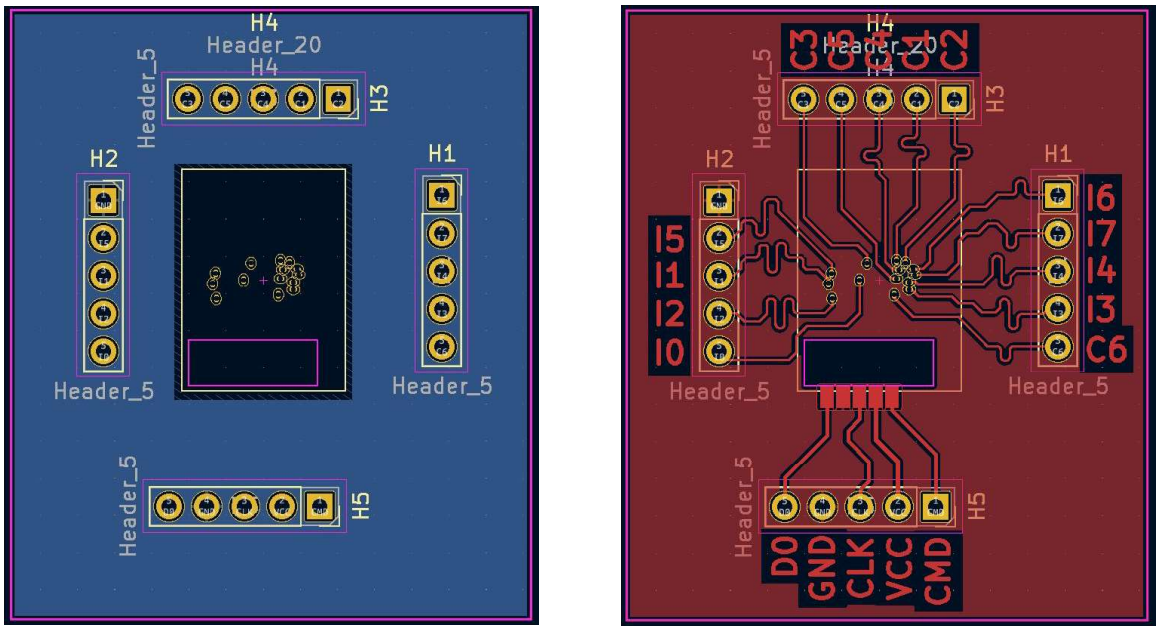
(b) Vue réelle de la carte microSD

FIGURE 3.13 – Parallèle entre la vue Rayons-X prévoyant les ouvertures et la vue réelle après ablation laser du vernis

2. Prise des dimensions : Pour concevoir le PCB avec le positionnement exact des ouvertures au niveau des vias, il faut commencer par prendre les dimensions du support. La taille globale du package du support MMC est standard, qu'il s'agisse d'une eMMC, d'une carte SD ou d'une UFS. La position des contacts pour les communications avec l'hôte sont également standard et référencée dans la norme de référence du support MMC. À l'inverse des autres dimensions de la carte, les positions de la matrice de plots de debug et encore plus des vias ne sont pas normées

et doivent être mesurées. Il faut faire les mesures sur les axes X et Y en visant le centre des vias ou des plots. L'idéal est de faire les mesures avec deux référentiels pour confirmer les résultats. Il existe plusieurs solutions pour faire les mesures. Il est possible d'utiliser un pied à coulisse sur le support physique ou de faire des mesures sur une image agrandie en optique ou aux Rayons-X. Pour cette deuxième solution, il existe des logiciels open-sources pour nous assister.

3. Conception du PCB : À partir des mesures préalablement réalisées, une carte électronique est développée. Elle servira à faire la liaison entre les vias du support MMC ou le port de communication avec l'hôte et les équipements que nous y connecterons (analyseur logique, ...) pour l'écoute ou l'envoi de commandes vers la mémoire interne. Elle doit donc disposer de borniers permettant de se connecter sur le port de communication interne au niveau des vias. La carte est dessinée à partir d'un logiciel de CAO (Conception Assistée par Ordinateur) dédié. Lors de cette étape, il faut prendre en compte la façon de fixer le support MMC à la carte, ainsi que les raccordements. Pour rappel, les liaisons électriques seront faites avec de la colle conductrice. Des trous seront faits dans le PCB et dans le package du support, à la position exacte des vias, ce qui permettra de couler la colle conductrice. Par conséquent, il faut que la face comportant les vias du support MMC soit en contact avec la carte développée. De plus, la taille des trous sera assez restreinte. Pour garantir que la colle conductrice fasse bien la liaison, il faut usiner notre PCB avec une plaque de cuivre d'épaisseur fine. Si nous réalisons notre carte électronique sur une plaque de 0,4mm, le résultat sera suffisamment rigide pour être manipulé par un opérateur sans risque de dégradation. Pour faciliter l'utilisation de la colle conductrice, l'emplacement du support MMC pourra être aminci d'environ 0,25mm d'épaisseur. Il restera donc une épaisseur de 0,15mm. La Figure 3.14a montre la face arrière de la carte électronique dessinée sur mesure pour le support MMC de notre exemple. Il n'y a pas de piste sur cette face, mais juste une ouverture permettant d'insérer la carte microSD. Les pistes sont tracées sur la Figure 3.14b, qui montre la face avant de la carte électronique. Elles relient les trous de liaison par colle aux borniers permettant l'écoute et le pilotage de la mémoire interne. Elle comporte aussi le bornier pour qu'un hôte discute avec la carte microSD.
4. Usinage du PCB : Le PCB est usiné avec une prototypeuse sur une plaque d'une épaisseur de 0,4mm. Cet équipement n'est pas standard dans les laboratoires de forensique numérique, cependant il est possible de commander le PCB directement sur internet pour quelques euros. Pour cela, il faut exporter les fichiers d'usinage du logiciel de CAO. Ces fichiers sont appelés Gerbers (une partie d'entre eux sont visibles dans la Figure 3.14). Ils sont composés au minimum de la face de cuivre avant (Figure 3.14b), de la face arrière (Figure 3.14a), des découpes de contour et

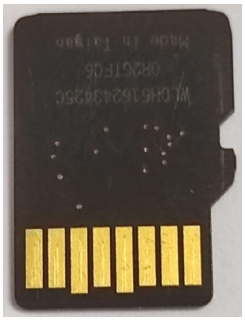


(a) Face arrière du PCB

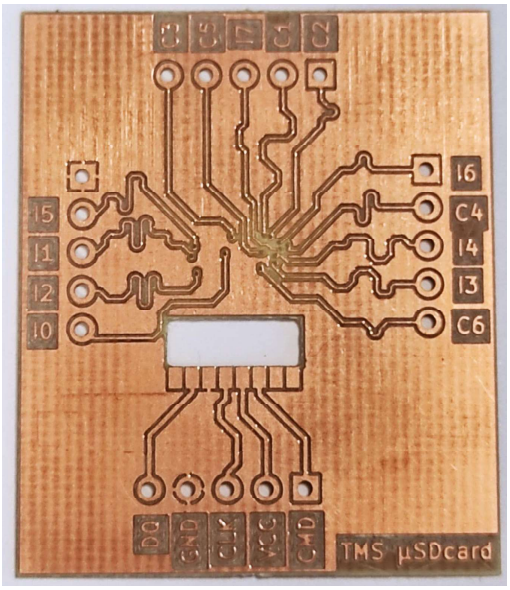
(b) Face avant du PCB

FIGURE 3.14 – Carte électronique dessinée sur mesure en fonction de la carte microSD

des perçages. Lorsque le PCB est réalisé, il peut être laissé avec le cuivre apparent. Il peut également être enduit d'un vernis de protection, classiquement de couleur vert ou bleu. Dans notre cas, le PCB est laissé avec le cuivre exposé. Sur la Figure 3.15, il est possible de voir le coté des vias après usinage (Figure 3.15a), à côté de la face avant du PCB (Figure 3.15b).



(a) Carte microSD



(b) Vue du PCB dessiné sur mesure

FIGURE 3.15 – Carte microSD et PCB correspondant, avant assemblage

5. Fixation du support MMC sur le PCB : le circuit imprimé et le support MMC sont assemblés. Pour ce faire, la face comportant les vias est collée sur la face arrière du PCB avec de la colle isolante de type superglue. Cette colle est intéressante parce qu'elle a une température de dégradation proche de 90°C. Pour restituer le scellé, il suffit d'appliquer une légère chaleur pour décoller le support du PCB après traitement.
6. Liaison électrique : Une fois le support fixé sur le PCB, la dernière étape de la préparation consiste à réaliser les connexions électriques. Pour atteindre cet objectif, la solution retenue est un adhésif conducteur tel qu'étudié dans la publication [212]. Les trous du PCB forment un réceptacle à la base duquel se trouvent les vias qui nous intéressent. L'utilisation d'une colle conductrice de viscosité moyenne, environ 5000 mPa.s, permet de confiner la colle à proximité du via. L'objectif est de couvrir les parois du via et la piste de cuivre (Figure 3.16). La colle doit être séchée thermiquement, mais avec une température inférieure à 90°C pour ne pas dégrader la superglue. Si besoin, l'étape peut être réalisée par plusieurs itérations de chauffage et de dépôt de colle.

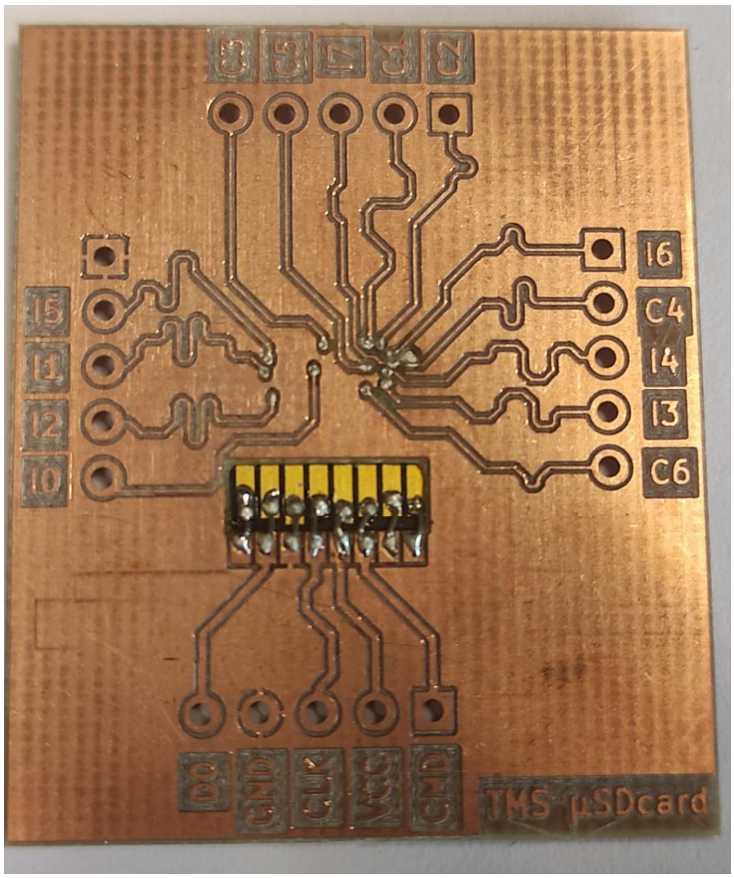


FIGURE 3.16 – Vue de la carte microSD après fixation sur le PCB et établissement des connexions électriques avec les vias

7. Validation électrique : Une validation finale de chaque connexion doit être effectuée en vérifiant les courts-circuits et les diodes entre les pistes et la masse, comme expliqué dans la section *Notions de la rétro-conception hardware*. Après avoir vérifié les connexions, les borniers sont ajoutés au PCB.

L'adaptateur, comportant le port au format SD ainsi que les liaisons entre le contrôleur et la mémoire, peut avoir plusieurs utilisations. Il offre plusieurs possibilités :

— Le pilotage de la MMC par un lecteur du commerce.
— Le diagnostic en branchant un analyseur logique entre les deux puces (contrôleur et mémoire).
— La lecture directe de la mémoire.
— Le raccordement d'un contrôleur d'une MMC similaire.

L'adaptateur est donc polyvalent, tel que requis dans notre cahier des charges. Comme il est constitué d'un PCB et de colle conductrice, il est ne perturbe pas les échanges entre le contrôleur et la mémoire lors du diagnostic et il permet une lecture stable et fiable de la mémoire.

3.1.3.3 Lecteurs

Il existe de nombreux lecteurs commerciaux capables de gérer des mémoires avec des protocoles de type MMC (eMMC, UFS, SD). Pour le protocole NAND, le choix est déjà plus limité. La box commerciale ESAYJTAG présentée dans la section *Box de lecture* est capable de communiquer à la fois avec le protocole eMMC/SD et UFS mais aussi avec le protocole NAND. De plus, elle est très réputée dans les laboratoires de forensique numérique. Nous allons donc nous baser sur cette box pour effectuer nos tests. Pour rappel, il convient de noter que si les protocoles SD et eMMC présentent quelques différences durant la phase d'initialisation, leurs cadres principaux sont largement similaires. Au lieu d'utiliser des solutions commerciales et en fonction des besoins, il est possible de mettre en œuvre un lecteur capable de gérer les deux protocoles (interne et externe) de la MMC. Un tel lecteur devrait gérer à la fois les protocoles standardisés eMMC, SD, UFS et NAND. Une cible idéale pour implémenter ce lecteur universel est une carte FPGA (field-programmable gate array). L'utilisation d'une carte FPGA, ayant recours à nos propres implémentations des protocoles, nous offrira la possibilité d'ajouter des signaux de synchronisation (trigger), simplifiant l'utilisation des équipements (analyseur logique) durant les manipulations [1].

1. Les travaux de développement du lecteur universel à base de FPGA n'est pas couvert par cette thèse mais fait partie d'autres travaux menés en partenariat avec plusieurs laboratoires dans un cadre professionnel.

3.1.4 Diagnostic des puces

3.1.4.1 Hypothèse de travail

La phase précédente consistait à préparer le support MMC pour cette nouvelle étape de diagnostic dédié au fonctionnement interne de la MMC. La démarche consiste à lancer une phase d'initialisation du support, tout en monitorant les échanges en interne avec un analyseur logique. Pour rappel, à l'heure actuelle nous n'avons qu'une supposition du rôle de chaque fil de bonding. Si l'étape de diagnostic le permet, nous pourrons en profiter pour confirmer ces rôles. Le process que nous allons appliquer sera fait comme suit. Le support sera alimenté par un lecteur commercial compatible avec la norme du MMC (un analyseur logique sera raccordé pour visualiser les échanges entre la MMC et l'hôte). Après la phase d'alimentation, une initialisation et une requête de lecture sera faite sur le support. Nous avons déjà réalisé cette opération lors du diagnostic global du support, lors de l'application de notre process (Section *Protocole de diagnostic de supports MMC illustré sur carte SD*). À ce moment-là, ces opérations ont été effectuées sous caméra thermique afin de visualiser le comportement interne du support et de repérer une éventuelle chauffe anormale. Dans cette section, nous allons nous concentrer sur le comportement interne de la MMC en effectuant des relevés avec les deux analyseurs logiques. Le comportement attendu sur une carte saine lors de ces trois actions est le suivant :

— Alimentation : la carte est mise sous tension par l'hôte. Cette alimentation est partagée à l'ensemble des puces mais aucune action n'est attendue en interne, hormis le passage de certains signaux à l'état haut ('1' logique) lorsqu'ils sont raccordés à une pull-up (se référer à la section *Les résistances de tirage* pour la description d'une pull-up). Cette étape ayant été validée lors de l'application du protocole de diagnostic global, nous ne nous attendons pas à découvrir un défaut d'ordre électrique.

— Initialisation : Le contrôleur reçoit un ordre suivant un des protocoles décrits dans la section *Protocole de communication entre la MMC et l'hôte*. En fonction de la nature du support MMC, il peut s'agir du protocole SD, eMMC ou UFS. Cet ordre a pour action de réveiller le contrôleur qui entre dans une série de questions-réponses avec l'hôte. Ces échanges peuvent être capturés et analysés, ce qui permet de constater que le protocole attendu est bien respecté et que le contrôleur fonctionne parfaitement au niveau de l'interface avec l'hôte. Après s'être lui-même initialisé, le contrôleur va lancer des échanges successifs avec les différentes puces mémoires, s'il y en a plusieurs. En accord avec le protocole flash décrit dans la section *Gestion de la mémoire flash interne*, plusieurs commandes d'initialisation peuvent être utilisées. Il est possible de retrouver des READ_STATUS, READ_ID, READ_PAGES ou des configurations pour basculer

vers des modes de communication plus rapides. Lors de l'initialisation avec l'hôte, nous nous attendons à observer des trames connues sur le bus interne puis d'observer des informations cohérentes sur le bus externe.

— Lecture : Le contrôleur a réussi à passer sa phase d'initialisation et celle des puces mémoires. Il va recevoir de l'hôte une demande de lecture pour un fichier précis correspondant à une plage d'adresse. Cet ordre va être décliné dans le protocole flash aux adresses correspondant physiquement dans les mémoires. Pour rappel, en accord avec la section *Protocole de communication interne*, une mémoire flash fonctionne avec un système de pages. Ainsi, pour un fichier, il faut s'attendre à un nombre de requêtes multiple de sa taille divisée par la taille d'une page. Par exemple, un fichier de 9ko, sur une mémoire de 2048 octets de taille de pages, nécessitera l'utilisation de 5 pages [2]. Durant la phase de lecture d'un fichier, même petit, nous nous attendons à observer des commandes READ_PAGES entre le contrôleur et la mémoire. En retour, la mémoire doit répondre avec le contenu de chaque page. Plusieurs lectures du même fichier doivent donner le même résultat pour l'ordre et le contenu des pages.

Nous avons décrit le comportement attendu dans le cas où le support MMC est fonctionnel. Dans le cas où le support est défectueux, les comportements peuvent varier, donnant des indications sur son état interne :

1. L'hôte envoie des requêtes mais il ne reçoit pas de réponse. L'analyseur logique raccordé sur le bus externe confirme qu'il n'y a aucune trame de réponse. Sachant qu'un diagnostic externe a déjà été réalisé, le défaut est identifié au niveau du contrôleur. À ce stade, il n'est pas possible de statuer sur l'état de la mémoire, donc les données peuvent être encore considérées comme récupérables.
2. L'hôte envoie des requêtes et reçoit des réponses de la part du contrôleur. À son tour le contrôleur interroge la mémoire qui ne lui répond pas. Il est possible de conclure que le contrôleur est fonctionnel mais pas la mémoire, donc les données ne sont plus récupérables avec les moyens actuels.
3. L'hôte envoie des requêtes et reçoit des réponses de la part du contrôleur. À son tour le contrôleur interroge la mémoire qui donne une première réponse. Lors des échanges d'initialisation, le contrôleur pose à plusieurs reprises la même question, généralement le READ_ID. Les trames observées sur l'analyseur logique au niveau du bus interne montrent que la mémoire change de réponse pour une

2. Il faut rappeler qu'il n'est pas possible d'utiliser une demi-page pour les mémoires flash. Toute page commencée est entièrement utilisée, même si son utilisation n'est que de 5%. Dans ce cas, le reste sera rempli de "dummies" (pattern de valeur logique d'octets à "00" ou "FF") ce qui peut réduire la durée de vie de la mémoire. Pour contrer ce vieillissement prématuré, les contrôleurs n'écrivent pas les pages en clair mais les chiffrent avec un XOR ou une autre opération logique. Cela évite des zones entières de "00" ou "FF".

même question. Il est possible de conclure que le contrôleur est fonctionnel mais la mémoire a un comportement instable, plutôt liée à l'exécution de la machine à état interne qu'au stockage des données a proprement parlé.

4. L'hôte envoie des requêtes et reçoit des réponses de la part du contrôleur. À son tour le contrôleur interroge la mémoire qui répond correctement. Le contrôleur relaie les réponses à l'hôte mais le résultat de la réponse est incohérent. Par incohérence de la réponse, nous entendons que la phase d'initialisation ou de lecture est aberrante. Face à ce comportement, il est possible de statuer sur le bon fonctionnement de la mémoire, mais le contrôleur défectueux, donc les données peuvent être récupérables.

Nous venons de décrire les quatre comportements possibles que l'on peut rencontrer lors de l'exécution de notre scénario. Sur ces quatre cas de figure, les comportements 2 et 3 mettent fin à nos travaux. Pour le comportement 1, il s'agit de la pire situation pour effectuer une relecture de la mémoire. Elle se fera selon l'hypothèse sur l'ordre des signaux estimé depuis la vue Rayons-X et la rétro-conception du support (sauf à disposer d'une carte "témoin"). Il ne sera pas possible d'appliquer l'intégralité du processus qui suit, mais de le substituer par un balayage exhaustif des différentes combinaisons d'ordre des signaux grâce à la commande READ_ID. Cela produira une liste de réponses (valeurs d'ID), qu'il faudra ensuite comparer par rapport à la liste des ID de fabricants de composants pour déterminer la combinaison la plus probable des signaux. Une fois l'ordre des signaux le plus probable déterminé, une lecture de la mémoire pourra être tentée (section *Lecture de la mémoire*). Le comportement 4 est plus favorable, car il va permettre une étude poussée des échanges. Cela permet de confirmer les hypothèses sur l'ordre des signaux faites avec la vue Rayons-X. Il s'agit de l'objet de la section suivante.

3.1.4.2 Confirmation du comportement et des signaux

Lors de l'étape précédente, nous avons décrit les comportements que pouvaient prendre le support MMC. Nous en avons identifié deux pour lesquels une relecture de la mémoire reste possible, donc qui permet une étude de l'ordre des signaux internes. Cela évitera de lancer des commandes de lecture aléatoires, basées seulement sur les hypothèses d'observation hardware. Notre démarche pour mettre au point la méthodologie d'identification et/ou de confirmation des signaux a été d'utiliser une carte microSD avec une matrice de plots de debug. Elle a été positionnée dans un adaptateur commercial MR24 distribué par Multi-com (Figure 3.10b) pour faciliter les tests. Ce boîtier possède un port qui permet de faire la liaison entre la carte et un lecteur de carte. À la surface du boîtier, sont disposés des borniers, sur lesquels nous positionnons des analyseurs logiques. Les deux équipements que nous utilisons sont de la marque Saleae [213]. Ils sont portatifs et conçus pour être utilisés directement sur un ordinateur sous Windows ou

Linux au travers d'un logiciel. Cela permet de pouvoir exploiter les trames directement avec des scripts ou de télécharger de nouveaux plugins, pour l'interprétation de nouveaux protocoles par exemple. Les deux analyseurs utilisés sont différents. Celui raccordé au bus (externe) de communication avec le lecteur SD est un modèle 8 bits, tandis que celui raccordé sur le bus (interne) flash est un modèle logique pro 16 bits. Le setup des expérimentations est visible sur la Figure 3.17. Si nous avons développé la méthodologie sur un adaptateur commercial, elle a également été validée avec notre adaptateur, comme nous le montrons par la suite avec notre exemple, et comme nous l'avons fait avec des nombreux échantillons.

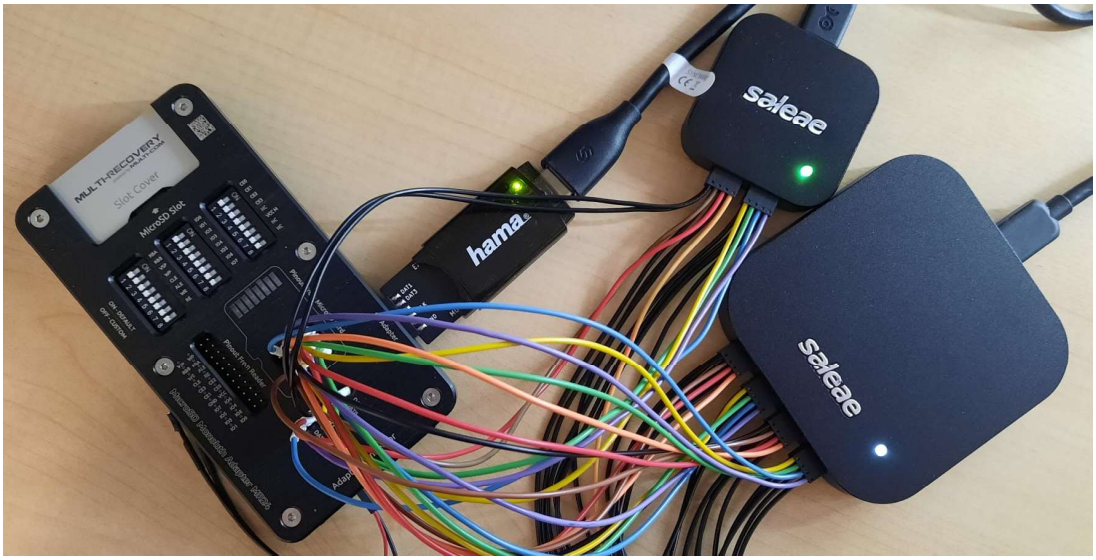


FIGURE 3.17 – Photo du montage utilisé pour effectuer la capture des trames entre l'hôte et la carte microSD ainsi qu'avec la mémoire

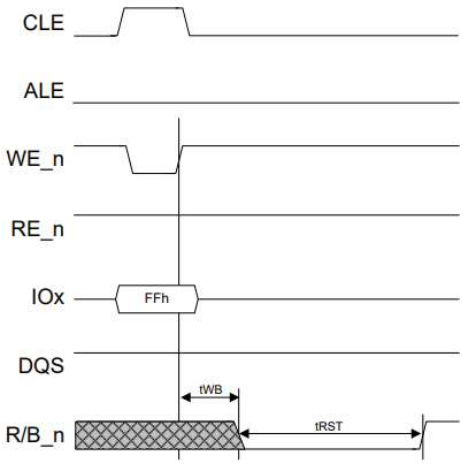
D'après le travail préparatoire effectué sur l'acquisition Rayons-X 3D, les signaux de contrôle et d'entrée/sortie (I/O) peuvent être renseignés dans le logiciel de pilotage de l'analyseur raccordé à la mémoire (celui à 16 bits). Le scénario décrit dans la section *Hypothèse de travail* est lancé, ce qui permet d'enregistrer des captures, à la fois pour l'hôte et pour la mémoire. Sur la capture d'écran réalisée au niveau de la mémoire (Figure 3.18), les I/O sont positionnés en bas (D8 à D15) et les contrôles sont situés en haut. Pour le moment, le rôle de chaque ligne n'est pas encore renseigné car cela va être fait en accord avec le chronogramme observé.

FIGURE 3.18 – Vue du chronogramme de début des échanges entre le contrôleur et la mémoire avec l'analyseur logique Saleae

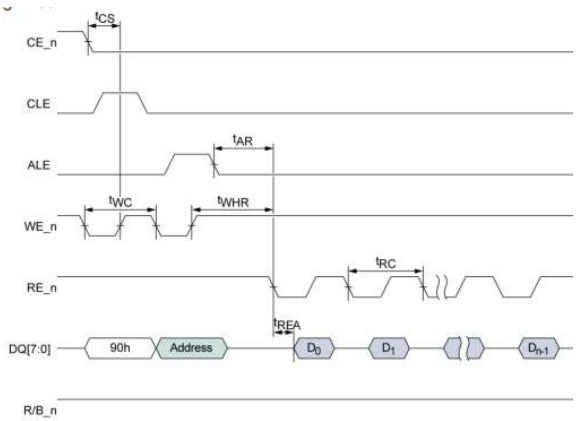
En navigant sur l'axe temporel du chronogramme, il est possible d'identifier des comportements spécifiques de certains signaux. Le signal Chip Enable (CE) qui valide l'activité d'une puce mémoire doit basculer au niveau bas avant tout envoi de commande. D'après les normes, ce signal doit être bas durant la totalité des échanges entre le contrôleur et la mémoire. Ainsi, sur l'étude des trames (Figure 3.19), il est possible d'identifier le signal CE sur la ligne D7.

FIGURE 3.19 – Zoom sur le chronogramme permettant d'identifier les signaux Vcc et le Chip Enable (CE)

L'étape suivante consiste à rechercher, soit la fonction RESET (Figure 3.20a), soit la fonction READ_ID (Figure 3.20b) dans le chronogramme. Généralement la chaîne d'initialisation de la mémoire par le contrôleur utilise les deux fonctions successivement.



(a) Trame de RESET



(b) Trame de READ_ID

FIGURE 3.20 – Chronogramme des fonctions RESET et READ_ID d'après la norme ONFI 4.1 [54]

Les deux trames étant localisées, il est maintenant possible de les étudier pour valider le rôle des signaux. Le fonctionnement du protocole flash est basé sur une machine à états. Pour valider des commandes, les signaux sont sollicités dans un ordre précis et à un état précis. Lorsque la mémoire reçoit une commande, si la combinaison n'est pas intelligible, elle est abandonnée en attente d'une nouvelle commande. Pour la commande RESET, la combinaison correspondant à la trame (Figure 3.20a) est résumée dans le Tableau 3.2. La confirmation du rôle de certains signaux est faite sur le chronogramme (Figure 3.21).

Tableau 3.2 – Interprétation du round unique de la trame de RESET

Commande	Valeur logique des controles				I/O
	CLE	ALE	WE	RE	7-0
Round 1	1	0	↑	1	FFh

'1' Niveau haut, '0' Niveau bas, ↑ Front montant

FIGURE 3.21 – Zoom sur la commande RESET permettant d'identifier les signaux Command Latch Enable (CLE) et Write Enable (WE)

La fonction RESET a permis de confirmer les signaux de contrôle Write Enable (WE) et Command Latch Enable (CLE), mais pas Address Latch Enable (ALE) et Read Enable (RE) qui sont repérés en provisoire, car le fonction les initialise mais ne les actionne pas. Les signaux de données, quant à eux, sont tous au niveau haut pour former la valeur logique “FFh”, donc il n’est pas possible de confirmer l’ordre du bus. Pour déterminer la fonction des autres signaux, la commande READ_ID va être plus efficace. La combinaison correspondant à la trame (Figure 3.20b) est résumée dans le Tableau 3.3 permettant de mettre à jour le chronogramme (Figure 3.22).

Tableau 3.3 – Interprétation des rounds de la trame de READ_ID

Commande	Valeur logique des contrôles				I/O			
	CLE	ALE	WE	RE	7	6-5	4	3-0
Round 1	1	0	↑	1	1	0	1	0
Round 2	0	1	↑	1	0	0	0	0

’1’ Niveau haut, ’0’ Niveau bas, ↑ Front montant

FIGURE 3.22 – Zoom sur la commande READ_ID permettant d’identifier l’ensemble des signaux

Contrairement à la fonction RESET qui ne permet pas de valider les principaux signaux de contrôle, la fonction READ_ID le permet, car WE et CLE sont associés à la valeur logique “FFh”, puis ALE et WE sont associés à la valeur logique “00h”. La réponse quant à elle se fait en suivant le signal RE. De plus, cette fonction permet de confirmer la position des I/O 7 et 4, donc de mieux comprendre l’ordre du bus de données. Toutefois, même si deux des 8 I/O se démarquent, il n’est pas possible d’être catégorique

sur leur fonction ni sur celle des six autres. Pour cela, il va falloir étudier la réponse de la mémoire, si elle est correcte.

Cette expérimentation nous a donné l'opportunité de définir l'ordre des signaux de contrôle et deux I/O et de confirmer ou d'infirmer nos hypothèses émises dans la section *Travail préparatoire*. Pour rappel, elle n'est possible et utile que pour le comportement 4, car pour le comportement 1 il n'y a pas de communication entre la mémoire et le contrôleur. À la place, il serait possible d'envoyer la commande READ_ID en testant chaque combinaison possible des signaux, mais en priorisant l'ordre établi durant nos hypothèses. Nous allons passer à l'étape suivante, qui consiste à étudier les réponses aux commandes pour connaître les paramètres de la mémoire.

3.1.5 Lecture de la mémoire

Avant de procéder à la lecture de la donnée contenue dans la mémoire, il faut poursuivre les investigations. En effet, chaque puce mémoire dispose de ses propres paramètres de lecture. Il s'agit des tailles des pages, des blocks, des spares décrits dans la section *Protocole de communication interne*. Ces informations peuvent être retrouvées dans la réponse de la mémoire pour la commande READ_ID. Si le contrôleur est capable d'envoyer les commandes (comportement 4), ou une source extérieure (comportement 1), et que les acquisitions contiennent la requête, il est possible de mener l'étude depuis cette acquisition.

La Figure 3.22 présente la commande READ_ID et la réponse de la mémoire pour notre cas d'étude, capturé avec l'analyseur logique. Il est possible de distinguer 8 curseurs. Les curseurs 0 et 1 sont respectivement la validation de la commande "FFh" et "00h". Les curseurs 2 à 8 représentent chaque octet de réponse de la mémoire, dont l'ID du fabricant pour le numero 2. En effet, chaque fabricant dispose d'un code unique disponible dans la norme [214], ce qui va servir pour essayer de déterminer l'identité de chaque I/O encore indéterminés. Il faut considérer les différentes combinaisons possibles, en se basant sur des groupes de quatre I/O, conformément à l'hypothèse que les I/O ont un ordre logique. Un Tableau 3.4 récapitulatif peut être fait afin de mieux traduire les combinaisons de l'ID fabricant (manufacturer ID).

En croisant le Tableau 3.4 et la liste des manufacturer ID [214], il existe deux combinaisons plausibles. Dans notre exemple, l'ID serait "98h", correspondant au cas 1 et 3. La marque de la mémoire serait alors Toshiba. Dans notre cas d'étude, le code "98h" est défavorable car il n'apporte que très peu d'informations par rapport à la commande READ_ID. Il faut poursuivre l'étude de la réponse avec les autres rounds pour confirmer l'ordre exacte des signaux. Ces rounds donneront les informations de modèle de la mémoire ainsi que les différentes tailles et nombre de pages et de blocks. Des ID de mémoire

Tableau 3.4 – Tableau comparatif des combinaisons possibles pour les ID relevés lors des échanges

Ordre	D15	D14	D13	D12	D11	D10	D9	D8	Valeur Hexadécimal
	1	0	0	1	1	0	0	0	
Cas 1	I/O7	I/O6	I/O5	I/O4	I/O3	I/O2	I/O1	I/O0	98h
Cas 2	I/O7	I/O6	I/O5	I/O4	I/O0	I/O1	I/O2	I/O3	91h
Cas 3	I/O4	I/O5	I/O6	I/O7	I/O3	I/O2	I/O1	I/O0	98h
Cas 4	I/O4	I/O5	I/O6	I/O7	I/O0	I/O1	I/O2	I/O3	91h

courantes sont référencées sur certains sites permettant de retrouver la référence boîtier de la mémoire et ainsi de retrouver la datasheet de celle-ci. Le but est de prendre connaissance des paramètres de la mémoire afin de configurer correctement le lecteur.

Le Tableau 3.5 présente l'étude du second round permettant de valider l'ordre des signaux, toujours en respectant l'hypothèse que les signaux sont regroupés dans l'ordre. En se référant à la liste des manufacturer ID, seul le cas 1 possède une valeur correspondant à une mémoire. Cela signifie que l'ordre des signaux est tel que supposé sur la Figure 3.22.

Tableau 3.5 – Tableau comparatif du second round de l'ID relevés lors des échanges

Ordre	D15	D14	D13	D12	D11	D10	D9	D8	Valeur Hexadécimal
	1	1	0	1	1	1	0	0	
Cas 1	I/O7	I/O6	I/O5	I/O4	I/O3	I/O2	I/O1	I/O0	DCh
Cas 2	I/O4	I/O5	I/O6	I/O7	I/O3	I/O2	I/O1	I/O0	BCh

Une fois la confirmation de l'ordre des signaux, le Tableau 3.6 représente la lecture de la réponse de la mémoire, correspondant aux curseurs 2 à 8 sur la Figure 3.22.

Tableau 3.6 – Interprétation des différents rounds en hexa de l'ID de la mémoire

Curseur	I/O								Hex
	7	6	5	4	3	2	1	0	
2	1	0	0	1	1	0	0	0	98h
3	1	1	0	1	1	1	0	0	DCh
4	1	0	0	0	0	1	0	0	84h
5	1	0	1	0	0	1	0	1	A5h
6	0	1	1	0	0	0	0	0	60h
7	0	0	0	1	0	0	1	0	12h
8	0	0	0	0	1	1	0	0	0Ch

D'après des recherches internet sur la marque et l'ID de la mémoire, il est possible de retrouver sa référence complète et de la documentation. Avec la datasheet, nous pouvons traduire les rounds qui donnent des informations de lecture (Tableau 3.7).

Tableau 3.7 – Interprétation des différents rounds en hexa de l'ID de la mémoire

Round	ID	Signification
1	98h	Manufacturer
2	DCh	Device
3	84h	Nb Cell and chip
4	A5h	Block and Pages size
5	60h	Nb plane

En complément de la réponse à la commande READ_ID, il est possible de trouver ces informations d'après la référence complète de la mémoire. Normalement, chaque partie de la référence donne une information d'après la base du fabricant. Dans notre exemple, il s'agit d'une NAND flash Toshiba TC58NVG2D4CTG00 dont les informations peuvent être interprétées dans le Tableau 3.8.

Tableau 3.8 – Signification des différents rounds en hexa de l'ID de la mémoire

Référence	Signification		
TC58	Single Chip memory		
N	NAND flash		
V	3.3V		
G2	4GB		
D	2 bits per cell		
4	bus size	page size	block size
	8 bits	2ko	256ko

Nous disposons à présent des paramètres physiques de raccordement de la mémoire (brochage minimum nécessaire pour relire la mémoire). Nous avons également les informations d'organisation interne de la mémoire et surtout une confirmation du bon fonctionnement de celle-ci. La dernière étape consiste à paramétrer la box de lecture et à lire la mémoire. Comme nous l'avons expliqué, ce travail de lecture, sans passer par le contrôleur, entraîne une phase de post-traitement de la donnée extraite. Il faut prendre en compte les erreurs de lecture et tenter de les corriger mathématiquement. Cette opération sera abordée dans la section *Fiabilisation de la donnée*. D'autres tâches à effectuer a posteriori consisteront à compenser un éventuel XOR appliqué par le contrôleur sur les données, puis à analyser les spares des pages pour retrouver leur ordre et remonter un

système de fichiers cohérent. Ces travaux peuvent être réalisés manuellement mais il existe également des outils forensiques permettant de faciliter le travail.

Ce process a été développé et orienté sur les supports MMC qui regroupent les mémoires embarquées ou externes, composées d'une puce mémoire flash et d'un contrôleur, le tout dans un package monolithique. Cependant, il existe d'autres types de supports monolithiques qui n'ont pas été développés lors de nos travaux, il s'agit par exemple des clés USB. Elles sont également composées d'une puce mémoire flash et d'un contrôleur, mais elles ont recours à un protocole d'échange différent avec l'hôte. Une autre différence réside dans les tensions appliquées sur les puces. Contrairement aux MMC, les clés USB ne fonctionnent pas en 3.3V. Les ports USB délivrent 5V, ce qui implique des adaptations de tensions en interne. Malgré la prise en compte de cette contrainte supplémentaire, des tests ont été effectués sur ce type de support et le process de diagnostic global présenté en section *Protocole de diagnostic de supports MMC illustré sur carte SD*, ainsi que celui décrit dans ce chapitre fonctionnent parfaitement. Nos travaux peuvent donc être utilisés en veillant à adapter les niveaux de tension attendus.

3.2 Fiabilisation de la donnée

L'un des challenges lors de la lecture d'une mémoire flash directement sans passer par le contrôleur, consiste à réaliser toutes ses fonctions et pas uniquement la lecture. Parmi ses fonctions, il y a des opérations mathématiques sur les pages ou sur des blocs d'octets. Il peut aussi y avoir des opérations de type ou-exclusif (XOR) permettant de rendre la donnée moins homogène et donc d'allonger la durée de vie de la mémoire. Une fonction notable du contrôleur lors de la lecture consiste à s'assurer que les données sont correctement lues. Il doit donc effectuer des corrections d'erreurs (Error correction code ou ECC), comme décrit dans la section *Management des erreurs*.

Sachant que dans la section précédente, nous nous sommes substitués au contrôleur, il faut que notre méthodologie intègre les opérations de correction d'erreurs. Nous l'avons abordé dans la partie *Présentation et état de l'art de la Google Home* sur la présentation de la Google Home, un système multi-composants est plus simple pour effectuer des travaux de recherche. Pour cette raison, la détection et la correction d'erreurs de la mémoire flash vont être abordées sur la mémoire du firmware de la Google Home. De ce fait, il est possible de simplifier au maximum le setup de lecture pour écarter les potentielles erreurs introduites par notre montage. De plus, il sera possible de répéter plusieurs lectures successives rapidement, ce qui permet de gagner du temps sur cette phase de développement de la méthodologie.

Avant de développer notre démarche sur la correction d'erreurs, intéressons-nous aux travaux préalablement réalisés dans le domaine. En particulier ceux sur les données compressés, comme nous aurons à les traiter dans le cas du firmware de la Google Home. La réparation des données compressées n'a pas fait l'objet de recherches importantes et les outils se concentrent principalement sur l'extraction de fragments non corrompus d'archives corrompues. Une méthode permettant de récupérer des parties d'un fichier corrompu compressé avec Deflate[3] a été publiée par Park en 2008 [215].

Leur méthode exploite le codage de Huffman dans DEFLATE pour supprimer les préfixes des données irréparables jusqu'à ce que la zone corrompue n'ait plus d'influence sur le reste du fichier. Les résultats de cette opération donnent plusieurs morceaux de données non corrompues mais non contiguës. Un autre travail publié par Wang en 2019 [216] explique comment modifier l'algorithme de compression LZSS (Lempel-

3. Il s'agit d'un format de compression de données sans perte basé sur deux autres algorithmes de compression qui sont LZ77 et le codage de Huffman. Le premier est une compression par dictionnaire qui consiste à établir un dictionnaire évolutif, supprimant les redondances de séquences de caractères les plus longues possibles. Le stockage est fait sous forme de groupe (indice dictionnaire, longueur du motif trouvé, caractère suivant). Le second codage est basé sur un arbre statique ou adaptatif qui permet également de supprimer les occurrences identiques dans une suite de données. Deflate est un algorithme de compression par dictionnaire par codage de longueur variable.

Ziv-Storer-Szymanski) [4] pour ajouter de la redondance avec un impact minimal sur les performances, sans modifier l'algorithme de décompression. Nous notons que la réparation des erreurs doit toujours être effectuée avec un algorithme personnalisé. Contrairement aux travaux existants, la méthode présentée vise à réparer les parties corrompues des données, en s'appuyant uniquement sur la redondance déjà existante qui y est intégrée et imaginant ne pas avoir pu faire de relecture (par exemple : le support ne peut pas être relu, corruption d'un bit provoquant toujours la même erreur).

3.2.1 Préparation du composant

Pour effectuer la lecture de la mémoire de la Google Home, nous avons besoin de l'extraire de son système et de venir s'interconnecter directement dessus. Il existe plusieurs solutions pour extraire la mémoire. Nous pouvons procéder par un jet d'air chaud appliqué par une machine ou manuellement. La température à appliquer pour dessouder le composant va dépendre de la nature de la soudure utilisée. Pour les applications commerciales, nous pouvons retrouver un mélange au plomb (Étain 63% - Plomb 37% ou Sn63-Pb37) ou avec les nouvelles normes environnementales un mélange sans plomb dit SAC (Silver Alloy Copper pour Étain-argent-cuivre ou Sn-Ag-Cu). La nature de l'alliage de soudure a une influence sur les températures à utiliser lors du process de soudure ou de dessoudage. Ainsi, le Sn63-Pb37 présente une température de fusion de 183°C. Sachant qu'il faut chauffer le composant en entier pour atteindre la soudure située dessous, la température utilisée dans les process est plutôt située autour de 250°C-280°C. De même pour l'alliage Sn-Ag-Cu, dont plusieurs variations existent, les températures de fusion varient de 217°C à 227°C. Cela implique une utilisation de températures plus élevées dans les process, entre 320°C et 380°C. D'importants travaux ont été réalisés sur les températures et les alliages de soudure. Ils ont eu pour but d'optimiser les process de chauffe et de changer la nature des alliages. Certains équipements sont également développés dans ces articles [51, 217].

Si nous revenons aux équipements à air chaud permettant un dessoudage de notre mémoire, nous retrouvons :

— Le pistolet à air chaud (Figure 3.23a) : Il s'agit d'un pistolet qui souffle un flux d'air chaud à une température pouvant aller de 100 à 400°C. Le flow est également réglable en fonction de la puissance de l'équipement. Le diamètre de la buse varie entre 0,3mm et 3cm, selon la gamme du pistolet. C'est un équipement a visé manuel qui n'est pas guidé. Il est donc difficile d'estimer la zone chauffée tant qu'aucun effet n'est observable.

4. Il s'agit d'un format de compression de données sans perte avec dictionnaire similaire sur le principe à LZ77 mais dont la forme du stockage de la donnée est différente. LZSS utilise un couple (indice dictionnaire, longueur de la redondance).

— La machine Zevac (Figure 3.23b) : L'équipement utilise un flux d'air chaud dont la température et le flow sont réglables. Contrairement à la technique manuelle, dans cette machine, les programmes sont enregistrables. La buse de sortie de l'air peut être changée avec des modèles permettant d'épouser la forme des composants standards. L'équipement dispose également d'un plateau de chauffe pour préchauffer l'ensemble de la carte électronique à une température proche de 100°C. Cela diminue le stress mécanique de celle-ci autour du composant d'intérêt, diminuant les risques de dégradation de la carte et du composant. L'intérêt fondamental de cet équipement est la précision du process. En effet, il dispose d'une visée et d'un positionnement de la buse réglable au millimètre, ce qui diminue considérablement les risques d'échec ou de dégradation.

(a) Pistolet à air chaud de la marque JBC [218]

(b) Zevac modèle Onyx24 [219]

FIGURE 3.23 – Deux équipements fonctionnant à base d'air chaud pour dessouder des composants

L'avantage de l'équipement réside dans la précision du flux d'air qui va être concentré sur le composant désiré, sans surexposer inutilement les composants autour. À contrario, l'avantage du pistolet à air chaud est le faible coût d'utilisation et la possibilité d'avoir une action mécanique (par exemple : levier) sur le composant en cas de difficulté d'extraction.

Une autre technologie qui existe pour dessouder un composant est l'infrarouge. Cette technique est très fiable et pour un prix intermédiaire par rapport aux deux solutions à air chaud présentées précédemment. Il s'agit d'un canon infrarouge qui est positionné sur le composant cible, permettant de le faire monter à la température de refonte des billes de soudures. Un équipement réalisant cette fonction est la IR E6 de la marque PDR (Figure 3.24). Il s'agit d'une colonne équipée d'une lampe infrarouge qui est focalisable sur la surface d'un composant. Le diamètre de chauffe est également réglable. Cela permet de ne chauffer que la zone précise autour du composant d'intérêt. Comme la Zevac, cet

équipement dispose d'un plateau de chauffe réglable jusqu'à 100°C.

FIGURE 3.24 – Station de dessoudage PDR modèle IR E6 [55]

Pour extraire le composant de la Google Home, nous avons eu recours à la PDR. Ensuite nous utilisons un lecteur pour relire son contenu. Ne disposant pas d'adaptateur pour cette mémoire spécifique, la liaison entre le lecteur et la mémoire est réalisée avec des fils (Figure 3.25). Idéalement, le ressoudage de la puce sur un PCB personnalisé est plus pratique et fiable. Cependant, lors de ces travaux, nous ne disposions plus de l'accès à l'équipement permettant d'imprimer un PCB personnalisé, et ni du temps nécessaire pour en faire produire un. Pour pallier le montage moins fiable que celui présenté dans la section *Solution non-commerciale*, la vitesse de lecture est réduite pour minimiser les erreurs pouvant survenir au cours de la lecture.

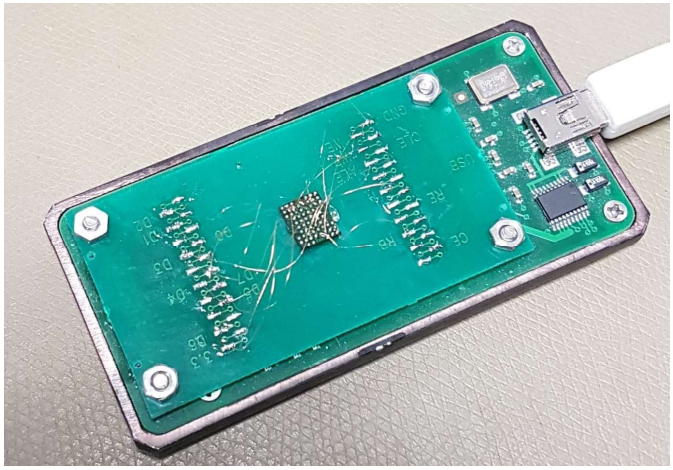


FIGURE 3.25 – Vue optique de l'assemblage de lecture de la mémoire, avec la connexion fil à fil entre la puce mémoire et une carte de lecture

3.2.2 Lecture de la mémoire flash

L'image brute extraite fait 285212672 octets (272MiB), segmentée en 2176 *pages de mémoire*. Chaque page de mémoire comporte 2048 octets de données et 128 octets de spares. Nous avons eu l'occasion de l'aborder dans la section *Protocole de communication interne* les spares contiennent des méta-données telles que l'indication que la page de mémoire est endommagée et ne doit pas être utilisée ou des codes de correction d'erreurs, ajoutant une redondance aux données stockées en cas d'erreurs matérielles. Selon la datasheet, lors de la lecture le processeur effectue directement la correction d'erreur et elle indique la présence d'un code Bose-Chaudhuri-Hocquenghem [175, 174]. Il s'agit d'un code de correction d'erreurs fonctionnant sous forme de blocs de données. Le message d'origine est découpé en blocs associés à une séquence de contrôle appelée "polynôme générateur". Le calcul forme des bits de redondances qui sont ajoutés au message d'origine pour permettre une vérification ultérieure. À ce stade, la mémoire contient la donnée d'une page ainsi que les bits de redondances associés. Lorsque la mémoire est relue, le processeur effectue la vérification. Pour cela, il applique de nouveau le "polynôme générateur" à la donnée lue, pour recalculer les bits de redondances. Ils sont comparés avec ceux reçus de la mémoire et doivent être identiques pour que la lecture soit considérée comme valide. D'après la documentation, notre processeur utilise donc un code Bose-Chaudhuri-Hocquenghem avec le triplet (17360, 16640, 97). Cela correspond respectivement à :

— 17360 : C'est la longueur totale du code comprenant les données originales et les bits de redondances.
— 16640 : C'est la longueur des données utiles du message. Étant donné que la longueur totale est 17360, cela signifie qu'il y a 720 bits de redondances.
— 97 : C'est le nombre maximum d'erreurs que ce code est capable de détecter et de corriger.

Des tentatives d'interpolation du polynôme à l'aide de l'algorithme Berlekamp-Massey [220] ont échouées. Selon toute vraisemblance, certaines opérations non linéaires sont effectuées sur les données avant le calcul du syndrome. Ces opérations sont détaillées dans la datasheet du Marvell Armada 1500 Mini Plus, qui est seulement disponible aux personnes développant des solutions avec ce processeur. Par conséquent, une autre méthode est nécessaire pour corriger les erreurs matérielles en se basant uniquement sur l'image principale obtenue en retirant les octets de spares de l'image brute.

Une analyse de l'entropie de Shannon [221] [5] de l'image de la Figure 3.26, met en évidence deux types de segments. Soit une entropie nulle (correspondant à des octets

5. L'entropie de Shannon mesure l'incertitude dans un ensemble de données. Elle atteint son minimum lorsque toutes les valeurs de la variable aléatoire ont une probabilité de 1. Dans ce cas, il n'y a pas d'incertitude. A l'inverse, son maximum est atteint lorsque les probabilités sont uniformes, c'est-à-dire quand toutes les valeurs ont la même probabilité créant le plus grand degré d'incertitude.

nuls), soit une entropie élevée. Les segments à forte entropie possèdent plusieurs causes. Une entropie comprise entre 0,99980 et 0,99983 caractérise des données chiffrées (encadrées en bleu sur la Figure 3.26) alors qu'une entropie entre 0,998 et 1,000 avec des chutes qui vont jusqu'à 0,95 est plutôt caractéristique de segments compressés [222, 223] (encadrée en vert sur la Figure 3.26).

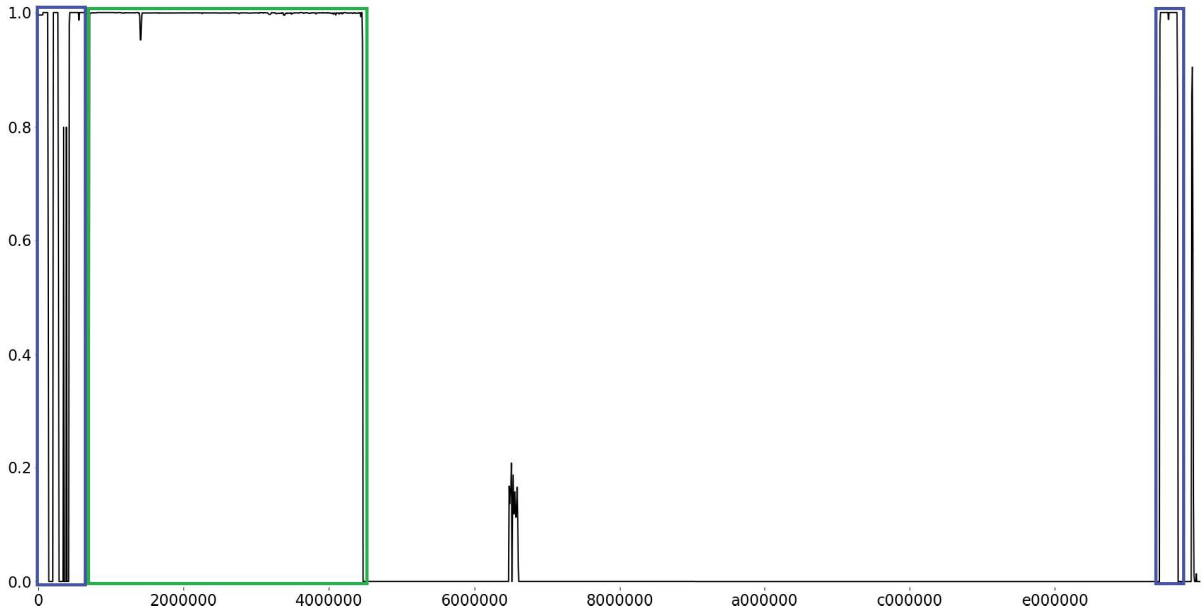


FIGURE 3.26 – Analyse de l'entropie de Shannon (normalisée) de l'image principale en utilisant `binwalk`. L'axe des x désigne le décalage par rapport au début de la lecture, tandis que l'axe des y montre l'entropie d'une petite région centrée sur un décalage donné

L'exécution de binwalk[6] en mode d'analyses de signature fournit des informations supplémentaires sur le partitionnement des données dans la mémoire, telle que le montre le Tableau 3.9. Le partitionnement est significatif d'un système Android. Le processus de démarrage commence par l'exécution du code de démarrage contenu dans une mémoire de type ROM, située directement dans le SoC. Ce code initialise le matériel et vérifie l'intégrité et l'authenticité du bootloader situé dans la mémoire flash, avant de l'exécuter. Le bootloader vérifie l'intégrité et l'authenticité de la flash, et appelle un petit utilitaire qui décompresse le noyau Linux (connu sous le nom de *zImage*) dans la RAM. Le noyau appelle ensuite le processus `init`. Les étapes supplémentaires d'initialisation des éléments de sécurité (Secure Monitor, TrustZone, ...) ne sont pas détaillées.

6. Binwalk est un outil en ligne de commande fonctionnant sous Linux et permettant de faire l'extraction de firmware ainsi que son analyse et de la rétro-conception basique. L'outil est classiquement utilisé en première analyse dans une phase de rétro-conception pour identifier rapidement des partitions de boot ou la nature d'un firmware.

Tableau 3.9 – Plan mémoire de l'image

adresse début	adresse fin	description
0x0	0x120000	unknown
0x120000	0x260000	unknown encrypted
0x260000	0x360000	null bytes
0x360000	0x4A0000	unknown encrypted
0x4A0000	0x5A0000	null bytes
0x5A0000	0x5C0000	SecureMonitor et bootloader
0x5C0000	0x640000	null bytes
0x640000	0x660000	SecureMonitor et bootloader
0x660000	0x6E0000	null bytes
0x6E0000	0xAB6840	[corrupt] mkbootimg zImage
0xAB6840	0xB60000	null bytes
0xB60000	0x4780000	[corrupt] SquashFS
0x4780000	0x67A0000	null bytes
0x67A0000	0x69A1A00	unknown
0x69A1A00	0xF720000	null bytes
0xF720000	0xFB18500	[corrupt] android boot zImage
0xFB20000	0xFE20000	null bytes-
0xFE20000	0xFEA1A00	YAFFS overlayfs
0xFF20000	0xFF300C0	crash dumps
0xFF300C0	0xFF34000	ECC
0xFF34000	0xFFC0000	null bytes
0xFFC0000	0xFFE0800	Bad Block Table
0xFFE0800	0xFFFFFFF	null bytes

La comparaison de deux sections chiffrées de la mémoire flash montre des différences mineures qui sont incompatibles avec l'effet d'avalanche du chiffrement [7]. En effet, une modification d'un bit sur un chiffré provenant d'un algorithme fort n'est pas plausible. Ces différences ne peuvent donc apparaître qu'après le chiffrement, c'est-à-dire pendant le stockage. Ces erreurs de mémoire sont appelées *bitflips*. Elles se produisent naturellement lors de l'écriture, bien que certaines méthodes visent à les provoquer délibérément. La comparaison faite des deux zones mémoires de 1310720 octets, avec un logiciel, a mis en évidence 11 différences, ce qui donne une proportion d'un bitflip tous les $(2 \times 1310720)/11 = 238312$ octets. Une analyse préliminaire informelle ne montre pas de schéma évident dans l'occurrence des bitflips.

7. L'effet d'avalanche est une propriété introduite dans les algorithmes de chiffrement par blocs. L'algorithme de chiffrement est conçu pour que toute modification mineure (changement d'un bit) en début d'exécution d'un chiffrement provoque une avalanche changeant radicalement le rendu final. Cela permet de complexifier l'attaque du chiffrement en diffusant largement les modifications, ne laissant pas à l'attaquant la possibilité d'observer directement les changements.

Dans la suite des travaux, un modèle d'erreurs de Bernoulli[8] de paramètre p est utilisé pour quantifier plus précisément les bitflips. Plus formellement, nous supposons que chaque bit de la mémoire flash se retourne suivant une séquence de variables aléatoires *indépendantes, identiquement distribuées.* (IID) dont la distribution de probabilité est une distribution de Bernoulli de paramètre p.

Bien que le taux de bitflip mesuré semble raisonnablement faible, il a été suffisant pour corrompre trois sections importantes du dump, à savoir le zImage `mkbootimg`, le système de fichiers SquashFS, et le zImage de démarrage Android. Le premier et le dernier sont compressés avec LZMA [224], tandis que le second utilise gzip [225, 226, 227]. Sans correction des bitflips, la récupération des données est impossible. Les deux algorithmes de compression appartiennent à deux familles différentes : LZMA est un algorithme de compression de flux, pour lequel un bitflip corrompt l'ensemble du flux suivant, tandis que gzip utilise un algorithme de compression de blocs, pour lequel un bitflip n'a d'impact que sur le bloc dans lequel il se produit.

D'une manière générale, étant donné la rareté des bitflips, il est réaliste de penser que les algorithmes de compression par blocs peuvent bruteforcer un ou deux bitflips dans chaque bloc jusqu'à ce qu'ils soient réparés. Pour les algorithmes de flux, le flux est décompressé jusqu'à ce qu'une erreur irrécupérable soit atteinte. À partir de là, le bitflip précédent est bruteforcé, ce qui maximise la longueur du flux décompressé avec succès. Cependant, cette dernière méthode nécessite une intervention manuelle importante pour sortir l'algorithme des minima locaux, ce qui nuit à sa reproductibilité dans d'autres cas d'utilisation. Nous avons donc décidé de baser notre recherche uniquement sur la compression de blocs. Le but est de détailler le processus de réparation du système de fichiers SquashFS corrompu.

3.2.3 Récupération de données pour la lecture de la SquashFS corrompu

Cette section détaille les étapes suivies pour corriger les bitflips sur le dump SquashFS corrompu. SquashFS est un système de fichiers en lecture seule, souvent utilisé pour stocker le système d'exploitation de périphériques embarqués. Une configuration commune le combine avec une autre partition inscriptible sur le même point de montage, appelée le système de fichiers superposés, dont les fichiers ont la priorité sur le SquashFS sous-jacent. Cela facilite les réinitialisations d'usine des dispositifs embarqués, car l'effacement du système de fichiers superposés ramène le dispositif à son état d'origine, sans aucune donnée utilisateur stockée à l'intérieur.

8. Le modèle de Bernoulli permet de classer des résultats en les catégorisant en succès ou échec, représentés par un '0' ou un '1'. Cela permet une représentation binaire d'une probabilité, pouvant être ensuite réutilisée.

Une image SquashFS est divisée en neuf parties au maximum [228], en commençant par un *superblock*, dont la disposition est illustrée dans le Tableau 3.10. Dans la Google Home, la taille du bloc est définie sur 128 ko et la méthode de compression est gzip. Chaque fichier ou répertoire est référencé à l'aide d'un *inode*, une structure spéciale contenant les méta-données du fichier. Pour améliorer l'efficacité du stockage, SquashFS compresse ses inodes en les regroupant en *blocs de méta-données* de taille 8 ko, qui sont ensuite compressés avec gzip et stockés dans la *table des inodes*. De même, chaque fichier est également compressé en le divisant en *fragments* d'au plus 128 ko, qui sont ensuite compressés avec gzip.

Tableau 3.10 – Plan des superblock de la SquashFS

<table>
<tr><td colspan="6">128 bits</td></tr>
<tr><td>0x73717368</td><td colspan="2">inode count</td><td colspan="2">timestamp</td><td>blocksize</td></tr>
<tr><td>fragment entry count</td><td>compression algo.</td><td>block size (log)</td><td>flags</td><td>id count</td><td>version</td></tr>
<tr><td colspan="3">root directory mode</td><td colspan="3">archive size (bytes)</td></tr>
<tr><td colspan="3">id table start offset</td><td colspan="3">xattr id table start offset</td></tr>
<tr><td colspan="3">inode table start offset</td><td colspan="3">directory table start offset</td></tr>
<tr><td colspan="3">fragment table start offset</td><td colspan="3">export table start offset</td></tr>
</table>

L'utilitaire `squashfs-tools`, qui est un utilitaire destiné à extraire, monter ou vérifier les images de type SquashFS, échoue à décompresser 204 des 920 fragments soit 22% du système de fichiers. Cela correspond à 111 des 1139 fichiers répertoriés dans la table des inodes. Heureusement, la table des inodes n'est pas corrompue. Cette information permet d'affiner l'estimation du taux de bitflip p, en modélisant la corruption de chaque fragment i par une variable aléatoire Y_i égale à '0' si le fragment n'est pas corrompu et à '1' si le fragment est corrompu. Ainsi, Y_i est une variable de Bernoulli de paramètre $1-(1-p)^{\text{length}_i}$ (où length_i est la longueur du fragment i).

Le nombre attendu de fragments corrompus peut être estimé en additionnant toutes les variables aléatoires Y_i. La valeur de l'espérance est ensuite égale au nombre observé de fragments corrompus (*i.e.*, 204). Cela donne un p égal à $5,03 \times 10^{-7}$ ou, de manière équivalente, un bitflip tous les 248253 octets.

$$204 = \mathbb{E}\left(\sum_{i=1}^{920} Y_i\right) = \sum_{i=1}^{920} \mathbb{E}(Y_i) = \sum_{i=1}^{920} 1-(1-p)^{\text{length}_i} \tag{3.1}$$

$$p = 5,03 \times 10^{-7} \tag{3.2}$$

En utilisant l'inégalité de Hoeffding [229], l'écart par rapport à l'espérance peut être limité comme suit :

$$P\left(\left|\sum_{i=1}^{920} Y_i - \mathbb{E}\left(\sum_{i=1}^{920} Y_i\right)\right| \geq t\right) \leq 2\exp\left(-\frac{2\,t^2}{\sum_{i=1}^{920} 1 - 0}\right) \tag{3.3}$$

En résolvant t pour une probabilité de 10^{-2}, on obtient $t = 50$. En remplaçant le côté droit de l'équation (3.1) par $204 \pm t$, on obtient que le taux de bitflip p est dans la plage $[\,3,66 \times 10^{-7}; 6,53 \times 10^{-7}\,]$ avec une probabilité de 99% ou, de manière équivalente, un bitflip tous les 191255 à 341937 octets. Cette fourchette est cohérente avec l'analyse manuelle préliminaire, confirmant l'hypothèse d'un taux de bitflip identique dans toutes les sections de la flash [9].

D'après la documentation, la méthode de compression gzip [227], basée sur l'algorithme DEFLATE, est une enveloppe autour des données compressées par la librairie zlib [225]. Les données compressées DEFLATE [226] sont concaténées entre elles avec quelques méta-données supplémentaires, comme le montre l'illustration des *fragments compressés* présentés dans le Tableau 3.11.

Tableau 3.11 – Structure d'un fragment compressé avec zlib

Header	Deflate block	...	Deflate block	Deflate block	Checksum

La somme de contrôle (checksum) est calculée sur les données décompressées à l'aide de l'algorithme Adler-32 [10]. Outre le fait qu'Adler-32 n'est pas destiné à la correction des erreurs, un bitflip sur des données compressées peut entraîner une propagation importante du nombre de bitflips dans les données décompressées. Cela rend toute tentative de correction après décompression peu pratique. À l'inverse, une approche boîte noire semble plus adéquate, en modélisant la vérification Adler-32 comme un oracle, en l'interrogeant avec un *candidat de réparation* qui correspond à un fragment compressé auquel un bitflip est appliqué. Cela permet de déterminer si le candidat de réparation est *valide* ou *invalide*. Un candidat valide peut ensuite être décompressé en utilisant `gzip` pour produire un *candidat cible*.

9. L'utilisation de l'inégalité de Bienaymé-Chebyshev (avec une variance égale à 160) donne des limites moins précises pour la même probabilité 10^{-2}.

10. L'algorithme Adler-32 est une fonction de hachage sur 32 bits qui prend chaque octet d pour lui apposer les opérations suivantes : $A = (A + d)$ et $B = (B + A)$. Cela permet à la fin du traitement de former deux valeurs A et B qui sont ensuite concaténées pour former un mot de 32 bits $(B << 16)|A$. Il a l'avantage d'être rapide en calcul, donc performant pour les vérifications d'erreurs de copie.

3.2.4 Génération de candidats cibles

Pour affiner cette stratégie, une estimation plus fine du nombre de bitflips dans les fragments corrompus doit être effectuée. En utilisant le taux p calculé précédemment, il est maintenant possible de modéliser le nombre de bitflips dans chaque fragment i en utilisant une variable binomiale Z_i de paramètres (length_i, p). Il est alors possible de calculer le nombre attendu de fragments qui ont k bitflips comme suit, où δ est le delta de Kronecker, $i.e., \delta^k_{Z_i} = \begin{cases} 1, Z_i = k \\ 0, Z_i \neq k \end{cases}$

$$\mathbb{E}\left(\sum_{i=1}^{920} \delta^k_{Z_i}\right) = \sum_{i=1}^{920} \mathbb{E}(\delta^k_{Z_i}) = \sum_{i=1}^{920} \binom{\text{length}_i}{k} p^k \left(1-p\right)^{\text{length}_i - k} \tag{3.4}$$

Sur les 204 fragments corrompus, on s'attend donc à ce que $175,22$ aient un seul bitflip, $25,78$ deux bitflips et $2,75$ trois. Les fragments avec plus de 4 bitflips sont presque inexistants. Dans ce qui suit, les réparations se concentrent uniquement sur les bitflips simples et doubles. Pour commencer, les fragments corrompus sont provisoirement réparés en utilisant un modèle d'erreurs de bitflip simple. Pour chacun des 204 fragments compressés corrompus f, l'ensemble associé de candidats à la réparation C_f est généré en mutant f avec un seul bitflip. Trois critères sont utilisés pour distinguer les candidats à la réparation et générer l'ensemble de candidats cibles T_f :

1. L'un des blocs DEFLATE du fragment est corrompu et ne peut être majoré.
2. L'Adler-32 des données décompressées n'est pas correct.
3. La longueur du fragment décompressé dépasse 128ko.

On dit que la réparation est réussie si la cardinalité de T_f est de '1', donc il y a exactement un candidat cible. La génération des candidats à la réparation peut être optimisée. Lors de la tentative de décompression à l'aide de zlib, le nombre d'octets n lus à partir du fragment compressé fn est comparé par rapport à la longueur de f. Si elle est inférieure, cela signifie qu'un bitflip s'est produit dans les n premiers octets de f. Il est ainsi possible de réduire l'ensemble des candidats à la réparation à ceux qui ont un bitflip dans leurs n premiers octets. Cette optimisation réduit considérablement l'intervalle de recherche pour 5 fragments sur 204, tandis que pour tous les autres, la donnée complète est lue.

3.2.5 Oracle basé sur une table d'inodes supplémentaires

Pour les fragments ayant plusieurs candidats à la réparation, il est possible de réduire ce nombre aux valides, en utilisant la longueur du fragment décompressé. Comme la longueur de chaque fichier est stockée dans la table des inodes, seuls les candidats cibles dont la longueur après décompression est compatible avec la longueur des fichiers associés sont conservés. Pour des raisons de simplicité, une approche par essai et erreur est réalisée, en supposant que tous les fragments restants ont une longueur de 128 ko.

Après la décompression du SquashFS, la longueur de chaque fichier est comparée à sa longueur dans la table des inodes. Dans notre cas, les longueurs correspondent pour tous les fichiers, validant l'hypothèse initiale sur la longueur des 29 fragments. Si un fichier avait été de longueur incorrecte, seules les combinaisons de candidats cibles dont la somme des longueurs est égale à la longueur du fichier auraient dû être conservées. Ceci peut être implémenté comme une variante du problème de la somme des sous-ensembles [230]. Ce filtre supplémentaire permet de réduire considérablement le nombre de candidats cibles, comme le montre la colonne #cibles du Tableau 3.12.

Tableau 3.12 – Liste des fragments (identifiés par leur hash) avec de multiples candidats cibles et leur nombre de candidats respectifs

Nom fichier	Hash du fragment	#cibles	Indéterminés	
			#bits	#octets
/bin/bluetoothtbd	heNYlKQRQ8pfXf3Z3PPPrTiGCnkbaLLai2lenD8qRzA	2	10	3
/bin/wpa_supplicant	92bEmBqIKN9dGW%AtlCg3fWYGgsYhTJ5DHuenvz8dbY	105	3961	1136
/boot/recovery.img	256HgEHVU@6U0uNouwruyGDWO%2jTniABl%NEEhWKRI	40717	80984	59421
	1QCNtpab0aCWKV68Ydo2IWnoo5IqLN4zYy3vezSCdzE	2	2	2
/chrome/assets/cast_shell.pak	Sh43xfhLF3@Remh2coYSxiChVxt2SqW0iyLw%o9ApGs	2	247123	58624
/chrome/icudtl.dat	Wnu5X5DpQtyOHAgAdOJOnZ0@k8xUVu8w5Yc7TLatcY4	2337	257725	64282
	i3LU8g00MdGpitYFOsNAVaI4M%Hjb2lJ6Odhjwnxgs4	6	430705	94562
	r2DiXJjXryJsggIHr1Ca4HXGdgXg3j3Tnloza9bynCM	2	6144	1558
/chrome/lib/libassistant.so	t2hs5Z71xQbRDW1LjNMPHvtyLoP%jC3voPG%R@nhD1c	2	18050	4935
	Km21LAN6wnDRqmpBA@RMXTUQmaQ9fSHhXDXWrR9cHoM	24709	93454	39408
/chrome/cast_shell	wC8p%RucvcX4EDStclRmSsO5a7CVA1W6WHrUFcrJKVo	1354	30713	8456
	JOw2De0T4V3G@0vSQFrp6Ie6%7myxs%iHJjQpMl0lTI	3	999	245
	D2dCzirIrlRGNTIKjCMn2sIJyquiLNs8guKlHCQNfRU	394	13671	4033
	wOhHT5XDso@EZ7kkp39lcyEOyNKXo1BC7DsT2h6EUZc	3	400268	104706
	fstWXSWTHt2jVMNr0C1lU@qNAEntfS@BQD%XV3WjDCE	124	10501	2778
	GVioeSeF8NRKMMULiTs0Ns8xQr2J9ytABwuIRSwbquI	2	296963	73781
	4jQJy1mkwBhbDEuGGH28WdzPSWswwaTFkq5fhiyujVE	414	19355	5076
	b1VT5jiuhOqxRX%xa7INu52iYt%t9bpL2aVe7nfp7os	59	8163	2224
	r1zrx7VtnidJz6ohWtwyDILTc2x1h4cZ3Y%yVcg8@Zg	8	387421	99010
	JHMZLlzG%FqGyCYFV2fVxL3@lqLZq1e3lKsU7%0ZtxA	2	19	7
/chrome/libffmpeg.so	WHi3paAUS9t6DdQ2Ka2CxkcRyTLhnTiSztpftJ%3kzs	5	318888	81323
/lib/libfreeblpriv3.so	nD4ME7GTBAsBjKfVIC7YprIeYNT%4Kru1%4RDinT3aA	6	397451	99523

3.2.6 Résultats et discussion

Le processus de réparation d'un bitflip prend 73 minutes sur une machine Intel i7-8700 (6 cœurs / 12 threads). Sur les 204 fragments corrompus, 172 ont un ensemble de candidats cibles de cardinalité '1'. Sur les 32 restants, 29 ne peuvent pas être réparés avec un seul bitflip. La cardinalité des candidats cibles est de '0', tandis que 3 ont des cibles multiples. Au total, 102 des 111 fichiers corrompus du système de fichiers ont été réparés en utilisant un modèle d'erreurs à un bitflip. Les neuf fichiers restants sont listés dans le Tableau 3.12, avec le nom des fragments associés au nombre de candidats cibles pour chaque fragment.

Pour les 29 fragments restants, un modèle d'erreurs à double bitflip est utilisé pour générer les candidats à la réparation. Le processus prend plusieurs mois par fragment sur une machine Intel i7-8700. Tous les fragments ont été réparés : le plus petit prend 22 jours, tandis que le plus grand prend plus d'un an. Lors de nos opérations, la tâche est répartie sur 40 ordinateurs afin de réduire le temps d'exécution à une semaine par fragment. Le nombre de candidats cibles pour chaque fragment varie de 1 à 40717 (Tableau 3.12). Les paragraphes suivants détaillent la manière de gérer les candidats cibles multiples.

3.2.6.1 Fusionner plusieurs candidats cibles

Deux méthodes de fusion sont utilisées pour produire le résultat final. Si le nombre de candidats cibles pour un fragment est faible (typiquement 2), un fichier par candidat cible est généré, et analysé manuellement à l'aide de l'outil d'analyses de binaire : `ghidra` [231]. L'outil met en évidence toutes différences entre les candidats cibles, afin d'éliminer les aberrants. Ce processus est entièrement manuel et prend du temps. Il doit être effectué pour chaque fragment. À titre d'exemple, la Figure 3.27 détaille ce processus pour le fragment `heNYlKQRQ8pfXf3Z3PPPrTiGCnkbaLLai2lenD8qRzA`. La liste complète est disponible dans le Tableau 3.12, en comparant deux versions de `/bin/bluetoothtbd`. Il existe deux cibles candidates, chacune correspondant à un fichier binaire. L'outil repère alors les différences entre les deux fichiers, et affiche le code binaire associé. Les candidats qui présentent un code aux comportements aberrants sont alors écartés. Les résultats présentés dans la section *Ratios de récupération* ne prennent pas en compte les fragments réparés à l'aide de cette méthode. Son efficacité dépend fortement de l'expertise humaine pour discriminer les cibles, ce qui ne peut être mesuré avec précision.

```
                    FUN_0001fd98                          XREF[3]:     FU
                                                                       FU
                                                                       FU
0001fd98 2d e9 f0 4f     push      { r4, r5, r6, r7, r8, r9, r10, r11, lr }
0001fd9c 81 b0           sub       sp,#0x4
0001fd9e 04 46           mov       r4,param_1
0001fda0 0d 46           mov       r5,param_2
0001fda2 6f f0 11 00     mvn       param_1,#0x11
0001fda6 1f 46           mov       r7,param_4
0001fda8 34 1b           subs      r4,r6,r4
0001fdaa 90 42           cmp       param_1,param_3
0001fdac 54 d3           bcc       LAB_0001fe58
0001fdae 20 78           ldrb      param_1,[r4,#0x0]
0001fdb0 dd f8 28 a0     ldr.w     r10,[sp,#param_5]
0001fdb4 c0 07           lsls      param_1,param_1,#0x1f
0001fdb6 0c bf           ite       eq
0001fdb8 60 1c           add.eq    param_1,r4,#0x1
0001fdba a0 68           ldr.ne    param_1,[r4,#0x8]
0001fdbc 00 90           str       param_1,[sp,#0x0]=>local_28
0001fdbe 4f f6 e6 70     movw      param_1,#0xffe6
```

```
                    FUN_0001fd98                          XREF[3]:     FU
                                                                       FU
                                                                       FU
2d e9 f0 4f              push      { r4, r5, r6, r7, r8, r9, r10, r11, lr }
81 b0                    sub       sp,#0x4
04 46                    mov       r4,param_1
0d 46                    mov       r5,param_2
6f f0 11 00              mvn       param_1,#0x11
1f 46                    mov       r7,param_4
40 1b                    subs      param_1,param_1,r5
90 42                    cmp       param_1,param_3
54 d3                    bcc       LAB_0001fe58
20 78                    ldrb      param_1,[r4,#0x0]
dd f8 28 a0              ldr.w     r10,[sp,#param_5]
c0 07                    lsls      param_1,param_1,#0x1f
0c bf                    ite       eq
60 1c                    add.eq    param_1,r4,#0x1
a0 68                    ldr.ne    param_1,[r4,#0x8]
00 90                    str       param_1,[sp,#0x0]=>local_28
4f f6 e6 70              movw      param_1,#0xffe6
```

FIGURE 3.27 – Différences apparaissant dans le fichier `/bin/bluetoothtbd` des deux candidats cibles pour le fragment `heNYlKQRQ8pfXf3Z3PPPrTiGCnkbaLLai2lenD8qRzA`. Le candidat de gauche présente une instruction (en vert) utilisant un registre indéfini `r6`, alors que le candidat de droite semble valide. Par conséquent, le candidat de gauche n'est pas valide, il est écarté

L'autre méthode fusionne indistinctement tous les candidats cibles en utilisant une logique à trois valeurs, où un bit est de valeur *true* (ou *false*) si et seulement si ce bit est égal à *true* (ou *false*) dans tous les candidats cibles. Sinon il est de valeur indéterminée. Pour cela, l'utilitaire `sasquatch` est patché pour générer deux variantes de chaque fichier, l'une dans laquelle tous les bits indéterminés sont à *true*, et l'autre dans laquelle tous les bits indéterminés sont à *false*. La comparaison des deux fichiers de sortie à l'aide de l'outil `ghidra` ou `bindiff` permet de mettre en évidence toute section qui n'a pas été bien réparée.

3.2.6.2 Ratios de récupération

Pour rappel des sections précédentes, l'utilitaire `squashfs-tools` actuellement disponible ne parvient à décompresser que 1028 fichiers sur les 1139 fichiers de la table inode. Cela correspond à seulement 9806355 octets sur un total de 117873827 octets de données décompressées. Le taux de récupération est de $8,32\%$. Après le processus de réparation, il reste 3022570 bits indéterminés. Cela équivaut à $0,32\%$ de données corrompues au niveau du bit. Si l'on considère les octets dans lesquels au moins un bit indéterminé est corrompu, on obtient 805093 octets corrompus, soit un ratio de $0,68\%$.

Tableau 3.13 – Taux de récupération au niveau du bit, de l'octet et du fichier avant et après la réparation du bitflip.

Méthode de réparation	Bits (ratio)	octets (ratio)
`squashfs-tools`	$78,450,840$ (8.32%)	$9,806,355$ (8.32%)
Réparation Bitflip	$939,968,046$ (99.68%)	$117,068,734$ (99.31%)
Total	$942,990,616$	$117,873,827$

Dans l'ensemble, le processus de réparation parvient à augmenter le ratio de données récupérées de $8,32\%$ à $99,68\%$, comme le montre le Tableau 3.13, ce qui facilite considérablement tout effort d'investigation.

3.3 Conclusion

Les travaux décrits dans cette section ont eu pour but de répondre à la problématique des erreurs de lecture. Pour réaliser ces expérimentations, la recherche et la correction d'erreurs a été réalisée sur un système de fichiers (SquashFS). Cela a permis de rechercher une méthode visant à réparer les données compressées par gzip, en exploitant la redondance résiduelle intégrée dans les données. Sous l'hypothèse d'un faible taux d'altération des bits, la plupart des données peuvent être récupérées, au prix de plusieurs mois de calcul. Cette approche basée sur l'oracle peut être facilement reproduite pour d'autres systèmes de fichiers SquashFS corrompus. Dans le cadre de travaux futurs, cette méthodologie peut être étendue à d'autres algorithmes de compression, en particulier la compression de flux comme `lzma`. Les efforts de recherche préliminaires visant à récupérer le `zImage` donnent des résultats prometteurs qui doivent être généralisés pour être reproductibles avec une intervention humaine minimale. Sur un plan plus généraliste, avec l'avancée des travaux, le traitement se fait à partir du système de fichier, et non directement sur le binaire et nécessite des connaissances pointues.

Ces derniers travaux s'inscrivaient en bout de notre méthodologie globale, permettant à partir d'un support MMC non fonctionnel au travers d'un diagnostic de plus en plus fin de trouver l'origine du défaut. Le but ultime étant de localiser l'élément défaillant dans la chaîne pour soit corriger le défaut, soit s'il n'est pas réparable, le compenser pour extraire les données. Nous rappellerons à cette occasion que nous évoluons dans le domaine de la forensique numérique et que nous intervenons dans un cadre d'examens ou d'expertises judiciaires. Nous ne recherchons pas à rendre notre support fonctionnel durablement, mais à le rendre suffisamment fonctionnel pour l'exploiter et si ce n'est pas possible, uniquement pour récupérer son contenu afin de l'analyser. Outre la possibilité d'appliquer presque directement les travaux présentés dans ce mémoire sur des supports similaires aux MMC, ils ont fait émerger de nouvelles idées ou problématiques qui nous offrent une base de réflexion pour de nouvelles recherches, dont certaines idées seront développées dans la partie *Conclusion et perspectives*.

Chapitre 4

Conclusion et perspectives

Pour conclure ce mémoire, je vais décrire un bilan de la thèse ainsi que de ses apports dans le contexte de la forensique numérique. Comme mentionné précédemment dans le mémoire, ma carrière avant la thèse a cheminé entre plusieurs secteurs d'activité. J'ai eu l'occasion d'évoluer dans trois domaines totalement différents, que sont l'analyse de défaillance dans le milieu du semi-conducteur, la rétro-conception matérielle, et la forensique numérique. Comme évoqué dans la section décrivant le matériel de laboratoire (section *Équipements des laboratoires*), les trois secteurs d'activités, bien que différents dans leurs objectifs, ont recours à des techniques et des équipements communs. Ainsi par l'apprentissage de la rigueur et de la méthodologie indispensable au traitement des supports en analyse de défaillance. Ma transition vers la forensique numérique a été facilitée. En effet, les procédures judiciaires sont dépendantes des pièces qui la composent et une erreur dans une pièce peut entraîner une annulation de poursuites judiciaires, empêchant d'aboutir à un verdict. Lors d'une expertise scientifique, il faut donc être rigoureux à la fois dans le traitement du scellé, dans les opérations techniques, mais aussi dans la rédaction du rapport.

La seconde activité que j'ai pratiquée est l'étude de conception de systèmes électronique dans un laboratoire national. Pour des raisons évidentes de confidentialité, je ne développerais pas mes acquis de compétences lors de cette expérience longue de neuf ans, mais j'affirmerais simplement que ces compétences ont été progressivement transposées dans le domaine de la forensique numérique. Durant cette période, j'ai eu l'occasion de participer aux travaux de recherche de mon co-directeur de thèse, qui ont débouchés sur de nombreuses publications et un brevet.

Ainsi mes expériences passées au sein d'une entreprise de fabrication de composants électroniques puis dans un laboratoire de recherche de l'état, m'ont donc apporté une plus-value non négligeable dans les capacités de traitement des supports pour la forensique numérique puisque, grâce à ces expériences professionnelles, je dispose d'une vision très précise de la composition et du fonctionnement des composants, ce qui est facilitateur pour trouver des solutions différentes lors d'un diagnostic d'un scellé.

Le basculement dans le secteur de la forensique numérique, moins contraint en termes de confidentialité des techniques, m'a donné l'opportunité de concrétiser des projets de recherche sur les supports de stockages de données. Fort de mes expériences précédentes, l'objectif principal de mes travaux de thèse était d'apporter de nouvelles techniques pour le diagnostic et d'extraction de données sur des supports de stockage endommagées. La première phase de la thèse a consisté à faire un bilan des technologies de stockages ainsi que de leur utilisation. Cela m'a permis de déterminer que les supports de type MMC étaient les plus utilisés. Ensuite, j'ai recherché les conditions pour lesquelles le diagnostic de ces supports était abandonné dans les laboratoires de forensique numérique. Après un inventaire des équipements généralement à disposition dans ces laboratoires,

ainsi que des équipements utilisés dans le secteur de l'analyse de défaillance, avec mon équipe de recherche, nous avons élaboré un protocole de diagnostic des supports MMC. Ce protocole basé sur des techniques non-invasives puis invasives permet d'identifier des défauts structurels des supports MMC et il oriente sur une solution de réparation. Cependant, sur certains supports, le déroulé du protocole ne permet pas d'aboutir à sa réparation. Par conséquent, nous avons cherché des solutions permettant de poursuivre les travaux de récupération de la donnée par une relecture *in situ* de la mémoire. Après un état des lieux des solutions commerciales, nous avons conclu qu'aucune d'entre elles n'était à la fois polyvalente et fiable. Par conséquent, nous avons décidé de concevoir notre propre solution, basée sur la conception d'un PCB raccordé directement sur les points de debug ou les vias. Cette solution nous permettant d'effectuer l'extraction de la mémoire, nous avons fait le choix de recourir aux logiciels commerciaux pour la remise en forme des données. Cependant, nous avons constaté que les logiciels possédaient des limitations dans la correction des erreurs après la lecture des données. Les algorithmes utilisés par les supports MMC ne permettent de corriger qu'une quantité limitée d'erreurs. Si les données extraites en comportent trop, les algorithmes ne sont plus suffisants. Connaissant un autre groupe de recherche travaillant sur cette problématique, j'ai eu l'opportunité de leur apporter mes compétences pour effectuer ces travaux, pour lesquels nous avons eu des résultats encourageants. L'ensemble des résultats obtenus ont menés à plusieurs publications listées dans la section *Contributions*.

Mes travaux se poursuivent et donnent des perspectives qui ont été imaginées pendant les phases expérimentales ou celles d'analyses ou même celles de rédaction. Naturellement, le cadre de la forensique numérique est resté un pilier de cette réflexion. Si certaines perspectives sont encore de l'ordre de l'état de l'art, d'autres sont déjà plus avancées et notre objectif principal restera d'essayer de proposer une transposition à des cas concrets. Avec mon équipe de recherche, nous souhaitons maintenant nous attacher à développer les sujets suivants :

1. La continuité des travaux : Comment remplacer les lecteurs commerciaux ? À quoi ressemble un firmware de contrôleur ? Y a-t-il une similitude dans les firmwares d'une même marque ? et de marques concurrentes ?
2. Le cas des mémoires défectueuses : Comment continuer l'investigation en cas de puce mémoire défectueuse ? Est-il possible de relire directement la mémoire au niveau des transistors ? Est-ce applicable dans un cas de la forensique numérique ?
3. L'élargissement à d'autres supports : Existe-t-il d'autres équipements intéressants ? Peut-on ajouter d'autres étapes au protocole de diagnostic ? Comment modifier le protocole par rapport aux autres supports ?
4. Les coûts de réalisation : Notre activité est-elle réalisable dans d'autres conditions

que le laboratoire ? Peut-on réduire les coûts des équipements pour nos laboratoires sans réduire la qualité des résultats ? Par soucis de transmission des compétences, une université ou école peut-elle acheter des équipements pour se rapprocher d'une qualité professionnelle ?

Nous allons donc à présent développer plus en détails chacun des points énumérés pour répondre aux questions posées.

4.1 Suite des travaux

Nous avons eu l'occasion de l'aborder dans le chapitre *Extraction et fiabilisation de la donnée*, il existe plusieurs solutions commerciales pour s'interconnecter avec un support MMC de type carte microSD ou SD. Toutefois lorsque l'on souhaite travailler sur un autre support comme une eMMC, le choix se réduit car la clientèle pour ces produits est moindre. Pour les communications avec l'hôte, le panel des lecteurs est très large, alors que pour les communications des protocoles internes la quantité est drastiquement plus faible. De plus, les lecteurs commerciaux sont des produits figées. Leur comportement interne n'étant pas maîtrisé par l'utilisateur, l'accès aux fonctions et aux logs est bridé par les fabricants des solutions. Cela signifie qu'en cas de problème lors de l'utilisation de la box de lecture, un code défaut sera remonté, mais la raison du défaut sera compliquée à identifier précisément. Dans la plupart des applications, un expert judiciaire travaille sur un support avec un process standard. Pour un support courant, une box commerciale apporte le degré d'information de dysfonctionnement suffisant pour que l'expérience de l'expert permette de corriger le défaut. Cependant, lorsque l'expert doit traiter un support plus atypique ou sur un support plus instable, il doit avoir un meilleur contrôle des outils qu'il utilise pour comprendre ce qu'il fait. Une solution pour résoudre ce problème est la maîtrise du développement d'une solution, comme la création des cartes électroniques d'interconnexion.

Ainsi, disposer d'un lecteur maîtrisé permettrait de combler plusieurs défauts des lecteurs commerciaux. Nos objectifs derrière cette démarche sont de répondre à trois problématiques :

— La polyvalence : un lecteur doit pouvoir traiter différents protocoles, et être le plus polyvalent possible. L'utilisateur doit pouvoir changer facilement de protocole. De même, le lecteur doit être associé à un logiciel assez simple et ouvert, ce qui permet des changements de paramètres sans être enfermé dans des processus fermés (suite de fenêtres qui demandent d'être renseignée avec une validation obligatoire).

— Le debug : Lancer une action avec comme seul retour, un succès ou un échec est frustrant pour un opérateur, d'autant plus qu'en fonction des applications, les défauts peuvent avoir plusieurs raisons. L'exemple le plus simple est la relecture

d'une mémoire provenant d'un scellé. Si en cas d'échec, un seul debug existe, l'opérateur n'a aucun moyen de savoir si le logiciel a un problème de communication avec la box, ou si c'est la box qui rencontre un problème, ou si c'est le composant qui est défectueux ou si le problème vient de la liaison entre le composant et la box. Cet exemple illustre la complexité face à laquelle se retrouve un expert en forensique numérique lorsqu'il doit relire une mémoire MMC et que le lecteur qu'il utilise lui retourne simplement les mots : échec lecture.

— La disponibilité : la multitude de lecteurs implique d'importantes commandes pour les acquérir ou d'avoir du délai d'approvisionnement au fil de l'eau. À l'inverse, une solution générique et simple à acheter, évite les pertes de temps dans les commandes et les problèmes de stockages. Une carte standard, sur laquelle il est possible de charger des scripts semble plus facile à utiliser et plus durable.

Pour répondre à ces trois points, le support qui nous semble idéal sera une carte FPGA. Il s'agit d'une carte de développement basée sur des langages de programmation propre. Il existe le Very High speed hardware Description Language (VHDL) qui est le plus bas niveau, et le Verilog qui reste le plus haut niveau. Ces deux langages sont très descriptifs dans leurs programmation. Ils permettent de gérer des registres et de configurer à volonté des cellules de composants électroniques de base. Modifier les liaisons internes du FPGA permet de modifier les combinaisons de portes logiques et donc de modifier le résultat final. Avec ce type de carte, il serait possible de programmer une relecture de mémoires de type eMMC ou SD. Ensuite l'opérateur pourrait basculer sur des protocoles plus bas niveaux tels que le protocole des mémoires flash, ce qui répond à la question de la polyvalence. D'un point de vue du debug, comme il s'agirait d'une solution maîtrisée, lors de la rédaction des codes de pilotage, le développeur pourrait ajouter autant de codes erreur qu'il le souhaite pour augmenter la précision des diagnostics des supports. Enfin, le COVID a mis en avant la difficulté d'approvisionnement de certains équipements électroniques. Si un expert en forensique numérique a besoin d'une box de lecture pour un protocole précis, mais qu'il ne peut pas se la procurer à temps, la justice en pâtie. À l'inverse, s'il disposait d'un lecteur générique à base de FPGA, diffusé à la communauté et dont les scripts sont accessibles en open-source, il serait plus facile pour lui de travailler. En effet, en cas de difficultés avec un nouveau protocole, si celui-ci a déjà été traité par un autre laboratoire, il pourrait uniquement solliciter un partage de script. L'échange serait quasi instantané et il n'aurait pas besoin d'attendre un délai d'approvisionnement.

Lors de plusieurs échanges en conférence, avec des experts de différents pays, l'idée a été proposée. Elle a été reçue favorablement, d'autant plus que la philosophie courante dans les laboratoires de forensique numérique est la mise en commun des outils autour de l'open-source. L'ensemble de ces raisons nous ont motivé à lancer une étude de faisabilité par des étudiants auprès d'une école partenaire.

Un autre point d'intérêt, qui a été identifié lors de nos travaux, consisterait à faire l'étude des contrôleurs de supports MMC. Nous entendons par là, l'extraction et la rétro-conception de leur firmware. Qu'ils soient d'eMMC, de carte SD ou même d'autres applications plus complexes, les contrôleurs ne disposent pas d'une programmation figée en sortie de chaîne de fabrication. Ils disposent d'un code générique permettant leurs initialisations internes qui déclenchent le boot réel en fonction de l'application. Ce code de boot se localise dans une mémoire embarquée de type flash, ce qui permet une réécriture, et donc une reconfiguration au besoin. Pour se faire, les contrôleurs doivent disposer d'un accès physique de programmation. Il s'agit de broches dédiées ou non, qui peuvent au besoin être raccordées à un programmateur. Les protocoles les plus courants pour la programmation de contrôleurs se nomment Joint Test Action Group (JTAG) et Universal Asynchronous Receiver/Transmitter (UART). Une fois la programmation initiale effectuée, les ports peuvent être reconfigurés et utilisés pour d'autres actions. Cependant, il est possible de les réactiver, ce qui permet à un développeur ou à un attaquant de venir relire le firmware embarqué. Pour un attaquant, qu'il soit légitime ou non, l'accès au firmware sera une source d'informations importantes, car il permettra de comprendre les subtilités de fonctionnement du contrôleur.

Si nous revenons à notre application spécifique des supports MMC, les informations qui nous intéressent concernent les XOR et la répartition de la donnée dans les puces mémoires. L'objet de l'étude pourrait être de retrouver un accès au firmware de plusieurs contrôleurs de supports MMC, et de plusieurs types (eMMC, SD, microSD). Suite à ces extractions, une analyse fonctionnelle pourrait être faite afin de comprendre les mécanismes d'intérêt. En appliquant une méthodologie adaptée, consistant à répertorier les marques, modèles, et autres informations trouvées pour chacun des contrôleurs étudiés, une base de données pourrait être créée. Cette base servirait ensuite pour estimer des similitudes et des statistiques sur l'utilisation de contrôleurs. Ainsi, il serait peut-être possible de ressortir un biais dans des associations entre les fabricants de MMC et les fabricants de composants. Le but final de cette étude serait de proposer une base, pouvant être en libre accès, pour les professionnels de l'expertise judiciaire dans le monde.

4.2 Cas des mémoires défectueuses

Un second axe de réflexion porte sur la fin de notre protocole de diagnostic développé en section *Protocole de diagnostic de supports MMC illustré sur carte SD*, ainsi que lors de l'observation de certains comportements à l'application de la méthodologie de la section *Hypothèse de travail*. Nous avons mis en avant que la mémoire d'un support MMC peut être défectueuse, ce qui en rend l'extraction des données impossible. La question que nous souhaitons nous poser est : est-ce réellement le cas ? Naturellement, le contexte du

traitement du support dans le domaine de l'expertise judiciaire impose des contraintes de temps et de conservation de la preuve. Cependant, est-ce qu'en dehors de ce contexte, c'est-à-dire en pouvant se permettre d'altérer la donnée ou avec un temps de traitement illimité, il serait possible d'effectuer la relecture d'une mémoire qui ne répond pas ? Pour cela, il faut imaginer aller plus loin que simplement envoyer des requêtes à une puce par un protocole prédéfini. Il faut imaginer que nous puissions interagir directement avec les bits de la mémoire, en allant les consulter directement sur les transistors.

Dans une présentation datant de 2016 [232], une équipe de l'université de Cambridge a proposé une méthodologie pour relire le contenu de mémoire de type EEPROM. Dans un premier temps, le travail consiste à préparer l'échantillon pour avoir accès à la face arrière de la puce, qui est composé uniquement du silicium. Dans le cas d'un composant en package, il est nécessaire de retirer la résine et tous les éléments qui peuvent se trouver au niveau de la face arrière de la puce. Pour une MMC, il faut faire de même et donc extraire la puce mémoire. Ensuite, il convient d'amincir le substrat de la puce pour arriver au plus proche des transistors. Un substrat d'un composant ancienne génération pouvait mesurer 350μm, alors que pour un processeur de technologie récente, l'épaisseur serait plutôt de quelques dizaines de micromètres. Lorsque les auteurs expliquent qu'il faut être au plus près des transistors, il est question d'un ordre d'échelle de la dizaine de nanomètre. Il est donc essentiel de procéder à un amincissement du substrat, et pour cela il existe plusieurs techniques :

— La chimie : En utilisant de l'acide fluorhydrique, il est possible d'attaquer le substrat. Au contact d'oxygène, de l'oxyde de silicium se forme à la surface du silicium. Celui-ci est attaqué par l'acide fluorhydrique, ayant pour effet un amincissement progressif du substrat. Cette attaque est lente et comme pour toute attaque chimique par bain, le résultat est assez irrégulier. Pour une exploitation ultérieure nécessitant une surface d'observation propre, la technique n'est pas recommandée.

— Le plasma : L'équipement est décrit dans la section *Graveur plasma* pour effectuer la préparation de surface et la destratification des composants. Dans le cas de l'étude, l'équipement permet de faire une attaque isotropique de la surface du silicium à l'aide d'un gaz fluoré. Il s'agit d'un procédé très lent qui peut prendre une demi-journée pour un retrait de 300μm. L'avantage de cette méthode est donc un excellent contrôle de l'attaque, contrebalancé par un effet néfaste des ions pour la programmation de la mémoire. L'un des effets de l'équipement est de faire fuiter les électrons qui sont stockés dans les grilles flottantes des mémoires, donc d'effacer celles-ci.

— Le polissage : L'équipement est également présenté pour son utilisation dans les laboratoires d'analyses de défaillances en section *Polissage*. Pour rappel, il est

utilisé pour faire des sections de la tranche des composants ou pour planariser des surfaces dans le but de rechercher des défauts ou de mesurer des épaisseurs. Dans le cas de l'article, la technique du polissage permet d'éliminer le substrat progressivement. Il est possible de faire varier le type de tapis afin d'avoir un process rapide au début puis plus lent et précis vers la phase finale. Cela a aussi pour effet de gommer les rayures pouvant être provoquées et d'avoir un effet semblable à un miroir, optimal pour de l'observation.

Pour ces trois techniques, la plus fiable et la moins risquée pour les données reste le polissage. Après avoir effectué l'amincissement du substrat, il faut procéder à l'observation des bits de mémoire. Pour cela, les auteurs utilisent la technique de contraste de potentiel au Microscope Électronique à Balayage (voir section *Microscope électronique à balayage (MEB)*). Cette technique consiste à utiliser le faisceau d'électrons de la colonne pour charger (emmagasiner des électrons) localement les cellules de mémoire. Pour cela, l'opérateur va lancer un balayage lent sur une zone réduite de l'échantillon, qui est reliée à la masse globale. Cette méthode d'observation permet de faire ressortir un changement de comportement entre les cellules programmées avec un '0' ou un '1'. Ce changement de comportement ce traduit par une couleur plus claire ou plus foncée de la cellule mémoire, donnant une relecture bit à bit de la programmation. Dans l'étude, les auteurs montrent qu'avec les bons paramètres, cette technique est très efficace. Cependant, elle reste très lente, car il faut être focalisé sur une matrice réduite à quelques cellules mémoires et prendre le temps d'atteindre l'effet de charge pour effectuer l'observation.

Ces travaux datent de presque dix ans et ont été réalisés avec les équipements et techniques contemporaines. Notre idée est de reprendre cette étude pour essayer de l'appliquer avec des équipements plus récents, puis de voir les limites technologiques. Une prise de contact a d'ailleurs été initiée avec l'un des contributeurs principaux afin d'échanger sur les limitations qui auraient pu être identifiées lors des premiers travaux. Dans cette nouvelle étude, nous ne rechercherons pas une application directe sur des supports d'expertises judiciaires, mais plutôt à reprendre et à poursuivre des travaux fondamentaux pour en déterminer les limites courantes.

4.3 Élargissement à d'autres supports

Un troisième axe de réflexion a été abordé précédemment en conclusion de la section *Lecture de la mémoire*, il s'agit de l'élargissement du périmètre de notre protocole. Dans un premier temps, nous avons abordé la possibilité d'utiliser le protocole de diagnostic ainsi que la méthode de relecture *in-situ* sur d'autres supports que des MMC. Nous avons déjà mentionné la possibilité de les transposer sur les supports USB. Nous pouvons également imaginer utiliser nos travaux sur des supports plus complexes tels que des

disques durs SSD. Pour cela, il faudra probablement retravailler sur plusieurs aspects, car si certains tests peuvent être utilisés directement, comme par exemple l'observation optique ou aux Rayons-X, les tests électriques sous caméra thermique demanderont une adaptation, surtout pour être capable de piloter le disque. De même, le comportement de ce type de support dans un Scanner Acoustique à Balayage sera à évaluer car la présence de nombreux passifs et composants sous capots métalliques pourrait dégrader certains résultats [1]. Il faudra donc reprogrammer une phase de tests pour valider l'utilité et la nature des défauts localisés, ainsi que les conclusions apportées sur ces nouveaux supports.

Par ailleurs, nous avons abordé la possibilité de transposer notre travail à des supports de conception similaire aux supports MMC, mais les systèmes conçus différemment peuvent aussi connaître leur évolution. Nous pouvons prendre l'exemple de smartphones ou de tablettes, qui sont des systèmes basés sur une carte électronique, accueillant des centaines de composants de natures différentes. Chacun des composants possède sa propre structure et sa propre routine de défaillance. Le développement d'un process demandera beaucoup de réflexions dans l'utilisation des équipements de diagnostic ou d'observation, pour éviter de faire des étapes inutiles ou pas assez précises. L'exemple qui peut être apporté est l'observation optique. Rechercher un défaut visuel sur une carte microSD n'a pas la même amplitude que rechercher le même défaut sur 200 composants. Pour répondre à notre besoin, il faudra peut-être se tourner vers des techniques couramment utilisées dans les entreprises faisant de la fiabilité tel que l'utilisation d'AMDEC [2]. Cela permettra d'identifier les composants les plus fréquemment défectueux pour se focaliser prioritairement dessus. L'adaptation du protocole sur des smartphones est actuellement en cours en partenariat avec des services de forensique numérique européens.

Un autre aspect de l'évolution du process qui peut être travaillé est la mise évidence de nouvelles techniques entraînant l'ajout de nouvelles étapes. Lors de la création de notre protocole de diagnostic, nous nous sommes basés sur des techniques ou équipements dont l'utilisation avait fait leurs preuves dans les laboratoires d'analyse de défaillance et pour auxquels nous avions accès suffisamment longtemps pour mener notre campagne de tests. Le critère de la disponibilité n'a exclu aucun équipement, cependant le critère de la maturité en a exclus un certain nombre. Dans de futurs travaux, nous souhaitons

1. L'utilisation de résine implique une fermeture hermétique de la puce électronique, car la résine est injectée dans un moule sous pression et à haute température. Dans le cas d'un composant sous capot métallique, celui-ci est collé sur les bords, avec généralement une liaison entre la puce et le capot par de la pâte thermique afin d'optimiser la dissipation thermique. Le fait que seuls les bords du capot soient refermés et que la puce soit entourée d'air et de pâte thermique changera le comportement de l'onde permettant de faire les mesures acoustiques.

2. L'AMDEC ou l'Analyse des Modes de Défaillances, de leurs Effets et de leur Criticité est un outil prenant en compte la fréquence, la gravité et la criticité des défaillances afin de prédire les voies de défaillances du système global [233].

prendre en compte des techniques plus atypiques telles que de l'imagerie par perturbation laser ou de l'imagerie photonique, pour accroître l'efficacité du diagnostic. Seulement ces techniques sont très coûteuses. Par ailleurs, pour qu'elles soient applicables, les composants cibles doivent subir des préparations. Il sera donc impératif d'évaluer le niveau de préparation et de l'opposer aux risques encourus pour l'échantillon, dans le but de garantir au maximum la préservation de la preuve.

4.4 Coûts de réalisation

La dernière perspective qui sera développée réside dans le coût des équipements utilisés dans les laboratoires. Dans le contexte européen et d'entités étatiques, nous avons la chance d'évoluer avec des financements provenant à la fois de nos pays respectifs mais également de l'union européenne à travers la participation à des projets de recherche et d'innovation. Cependant, dans le paysage de l'expertise judiciaire, les laboratoires étatiques ne représentent qu'une partie des acteurs et il faut compter également des laboratoires privés. N'ayant pas autant d'appuis des gouvernements et des institutions, ils doivent recourir à des moyens moins importants. Partant de ce constat, il faut les considérer lors du développement d'une solution, et pour qu'elle soit profitable au plus grand nombre, il convient d'éviter le recours à des équipements hors de prix. Par exemple, les universités ou les écoles d'ingénieurs ont souvent un budget limité. Pourtant, notre secteur d'activité nécessite la transmission de compétences, passant par l'enseignement dans des cursus spécialisés ou généralistes. Ce passage de témoin envers les nouvelles générations ne peut pas se faire que sur des aspects théoriques. Pour que l'enseignement soit de la meilleure qualité possible, il faut que les étudiants aient la possibilité d'appliquer sur des cas concrets leurs apprentissages. La possibilité d'utiliser des équipements semblables à ceux des professionnels, accompagnés par les experts qui les utilisent, leurs permettra d'acquérir les compétences et savoir-faire. Pour ces deux raisons, nous avons décidé de mettre au point un laboratoire constitué d'équipements low-cost, qui se substitueront aux équipements classiques. Le mot d'ordre de notre recherche, qui est déjà en cours depuis plusieurs mois, est de trouver un substitut bas coût pour chacun des équipements du laboratoire. Ce substitut doit être testé dans des conditions d'utilisation identiques à une analyse judiciaire classique, et il doit proposer un résultat similaire.

Pour valider notre laboratoire, nous avons sélectionné des opérations de base, appliquées au quotidien dans les laboratoires de forensique numérique, sur la thématique de la remise en état de supports pour effectuer de l'extraction de données. Ensuite, nous avons identifié deux cas de figures pour lesquelles l'opération n'est pas réalisée par un professionnel en laboratoire (contexte d'une zone NRBC et manipulation par un acteur moins expérimenté). Enfin, nous allons éprouver notre setup low-cost sur ces deux cas de

figure.

Le premier cas que nous avons identifié est le contexte des menaces nucléaires, radiologiques, biologiques et chimiques (NRBC). L'intervention sur un théâtre NRBC est très particulière car il n'est pas possible de faire circuler les objets en dehors de cette scène. Supposons qu'un expert judiciaire ait à analyser un objet avec un lecteur du commerce. L'expert doit entrer dans la zone avec une combinaison spéciale limitant grandement les mouvements, comme le montre la Figure 4.1a. Il doit prendre en charge l'objet qui n'a pas le droit de sortir de la zone, et doit le traiter sur place. À l'issue des opérations, l'expert doit abandonner sur place à la fois l'objet, mais aussi le lecteur qui lui a permis de travailler. Chaque intervention dans cette zone entraîne la perte des équipements. Pour cette raison, les niveaux d'interventions sont très limités car il n'est pas envisageable de perdre un équipement binoculaire à 2500€ ou une caméra thermique à 5000€ sur chaque intervention NRBC. Si nous sommes capables de sélectionner des équipements pour un montant global de 2000 à 3000€, il sera beaucoup plus facilement envisageable de les abandonner à l'issue des opérations. C'est ce que nous appellerons le risque acceptable de perte qui devra initialement être accepté par le magistrat en charge des opérations judiciaires. Naturellement les experts intervenants sur site devront être de plus en plus formés à des actes complexes malgré la combinaison contraignante. La Figure 4.1b présente un exemple d'expérimentation faite en laboratoire, dans des conditions identiques à celles d'une zone NRBC. Cette opération consistait à effectuer un diagnostic puis une réparation d'une carte SIM ayant un fil de bonding sectionné. Il s'agissait dans un premier temps d'une preuve de concept, validant que l'opération était bien réalisable par un expert judiciaire, avant de pouvoir le transposer directement dans une zone contaminée.

Le second cas que nous avons identifié pour valider notre setup réside dans la facilité de reproduire des actes complexes. Pour un expert de haut niveau, travailler avec des équipements moins performants est réalisable. Mais comment être sûr que notre choix est judicieux ? Ainsi, nous allons choisir de regrouper un panel d'étudiants et de jeunes diplômés ayant un cursus d'ingénieur en informatique et/ou électronique. Ces étudiants n'ayant pas de prédispositions spécifiques en micro-électronique ou en forensique numérique, la première étape consiste à leur donner des notions de base sur les techniques des experts en forensique numérique. Dans un second temps, nous leur apprendrons les étapes des manipulations ainsi que le fonctionnement des équipements. En dernière phase, nous leur montrerons les expérimentations pour qu'ils puissent les prendre en main à leur tour. L'objectif sera de relever le temps nécessaire d'apprentissage ainsi que la qualité du rendu final par ces personnels juniors. S'ils sont capables de prendre en main facilement les équipements et de reproduire fidèlement les résultats, cela nous permettra de tirer des conclusions favorables pour notre combinaison d'équipements de laboratoire low-cost. Dans le cas contraire, nous pourrons retravailler notre configuration pour l'améliorer.

(a) Tenue utilisée en zone NRBC

(b) Ouverture et réparation d'une carte SIM endommagée.

FIGURE 4.1 – Développement et validation d'une preuve de concept de manipulation sur des supports en zone NRBC

Notre projet final sera de proposer en libre accès à des universités ou à des écoles, notre configuration d'équipements low-cost. Nous pourrons également accompagner des étudiants ou jeunes diplômés souhaitant découvrir notre cœur de métier. Enfin pour les professionnels de la forensique numérique, notre laboratoire sera facilement accessible. Nous pourrons les accompagner au travers des médias ou des formations pour une prise en main des outils dans des conditions NRBC.

4.5 Perspective personnelle

Sur un plan personnel, à l'issue de la thèse, j'ai pour objectif de poursuivre les différents travaux de recherche qui ont été initiés, mais qui par faute de temps ou d'accès aux équipements n'ont pas pu aboutir. Je souhaite également explorer les quatre perspectives que j'ai précédemment identifiées. Mon objectif est de fédérer dans un groupe de recherche, des personnes en cours de formation, des ingénieurs juniors et seniors et des doctorants. Je souhaite poursuivre les démarches de communication au travers des publications scientifiques, des conférences publiques ou restreintes, des cours et des masterclasses, comme celles qui ont déjà été initiées au profit de plusieurs MSc, masters et licences. Mon but a moyen terme sera de passer l'Habilitation à Diriger des Recherches, tout en restant dans le domaine de la rétro-conception matérielle ou la forensique numérique pour l'État français. Cependant, j'envisage de trouver une affectation compatible avec l'encadrement des travaux de recherche et qui m'accordera la liberté de procéder à des interventions régulières dans des cursus de formation universitaire ou ingénieur. Cette transition permettra de capitaliser et d'anticiper une reconversion en fin de carrière militaire, m'offrant les qualifications et les expériences nécessaires pour m'orienter, à terme, vers un poste d'enseignant-chercheur.

Bibliographie

[1] "Cycle pdca / la roue de deming," 2023. [Online]. Available : https://www.certification-qse.com/cycle-pdca-roue-de-deming/

[2] "Les défis de la préparation d'échantillons de composants microélectroniques," 2023. [Online]. Available : https://www.struers.com/fr-FR/Knowledge/Materials/Microelectronics#defis

[3] "Lynx evo," 2022. [Online]. Available : https://www.visioneng.fr/produits/microscope-stereo-sans-oculaire/lynx-evo-dynascope/

[4] "Easytom s," 2023. [Online]. Available : https://www.rx-solutions.com/en/products/easytom-s-1270

[5] Q. CLEMENT, *Rapport de stage de fin d'étude entreprise eshard.* Laval : ESIEA / ESHARD, 2022.

[6] "Corrosion mechanism of au balls and al pad." [Online]. Available : https://www.researchgate.net/figure/Corrosion-mechanism-of-Au-balls-and-Al-pad-at-the-a-initiation-stage-b-propagation_fig2_242013902

[7] "warpage induced die crack." [Online]. Available : https://www.semlab.com/wp-content/uploads/2019/07/warpage-induced-die-crack.png

[8] "Tutorial cw305-4 voltage glitching with crowbars," 2018. [Online]. Available : https://wiki.newae.com/Tutorial_CW305-4_Voltage_Glitching_with_Crowbars

[9] A. GRASSET, *Legal implication of hardware reverse engineering for law enforcement agencies.* Melun : CREOGN / EM Lyon, 2022.

[10] "Site internet des disques durs toshiba," 2023. [Online]. Available : https://toshiba.semicon-storage.com/us/storage.html

[11] "Site internet recuperer-cle-usb.fr présentant des visuels de clés usb," 2023. [Online]. Available : https://recuperer-cle-usb.fr/comment-choisir-cle-usb

[12] "Les principes de la microscopie," 2023. [Online]. Available : https://www.naturoptic.com/comment-choisir/microscopes/microscope.php

[13] "Binoculaire leica," 2023. [Online]. Available : https://www.leica-microsystems.com/products/light-microscopes/stereo-microscopes/p/ivesta-3/

[14] "Microscope leica," 2023. [Online]. Available : https://www.leica-microsystems.com/products/light-microscopes/p/leica-dm2700-m/

[15] "Couche électronique," 2023. [Online]. Available : https://fr.wikipedia.org/wiki/Couche_\unhbox\voidb@x\bgroup\let\unhbox\voidb@x\setbox\@tempboxa\hbox{e\global\mathchardef\accent@spacefactor\spacefactor}\let\begingroup\endgroup\relax\let\ignorespaces\relax\accent19e\egroup\spacefactor\accent@spacefactorlectronique

[16] H. Berek, M. Oppelt, and C. G. Aneziris, *X-Ray Computer Tomography for Three-Dimensional Characterization of Deformation and Damage Processes.* Cham : Springer, 2020, vol. 298, pp. 1–20.

[17] "High-end industrial x-ray & ct inspection systems," 2023. [Online]. Available : https://www.rx-solutions.com/en/x-ray-systems-1199

[18] "Iphone 12 and 12 pro teardown," 2023. [Online]. Available : https://www.ifixit.com/Teardown/iPhone+12+and+12+Pro+Teardown/137669

[19] "Scanning electron microscopy (sem)," 2023. [Online]. Available : https://warwick.ac.uk/fac/sci/physics/current/postgraduate/regs/mpagswarwick/ex5/techniques/structural/sem3/

[20] "Electron backscatter diffraction," 2023. [Online]. Available : https://en.wikipedia.org/wiki/Electron_backscatter_diffraction

[21] "Zeiss evo family," 2023. [Online]. Available : https://www.zeiss.com/microscopy/en/products/sem-fib-sem/sem/evo.html

[22] "Zoom into a microchip video," 2023. [Online]. Available : https://www.nisenet.org/catalog/media/zoom_microchip_video

[23] "Combinaison des ondes lumineuses," 2023. [Online]. Available : https://fr.science-questions.org/comment_ca_marche/155/Interferences_et_diffraction_d_une_onde/

[24] "Interféromètre à lumière blanche," 2023. [Online]. Available : https://www.keyence.eu/frfr/ss/products/microscope/roughness/equipment/surface_03.jsp

[25] "Microscope interférométrique bruker contourx 100," 2023. [Online]. Available : https://www.bruker.com/fr/products-and-solutions/test-and-measurement/3d-optical-profilers/contourx-100.html

[26] "Exemple d'image sur un composant électronique avec un microscope interférométrique," 2023. [Online]. Available : http://www.optique-ingenieur.org/fr/cours/OPI_fr_M03_C04/co/Contenu42.html

[27] "Schéma de fonctionnement d'un microscope confocal," 2023. [Online]. Available : https://www.keyence.fr/ss/products/microscope/glossary/cat2/confocal_microscope/

[28] "Microscope confocal zeiss lsm900," 2023. [Online]. Available : https://www.zeiss.com/microscopy/en/products/light-microscopes/confocal-microscopes/lsm-900-for-materials.html

[29] "Exemple d'images produites avec un microscope confocal keyence vk-x3000," 2023. [Online]. Available : https://www.keyence.com/products/microscope/laser-microscope/vk-x3000/

[30] H. Yu, "Scanning acoustic microscopy for material evaluation," *Applied Microscopy*, vol. 50, p. 25, 2020.

[31] "Intérieur de chambre de sam," 2023. [Online]. Available : https://www.mtalabs.com/scanning-acoustic-microscopy

[32] "Spectre de l'infrarouge," 2023. [Online]. Available : https://www.alpha-cure-france.fr/lampes-ir/technologie-ir/

[33] "Inductively coupled plasma – reactive ion etching (icp-rie)," 2023. [Online]. Available : https://corial.plasmatherm.com/en/technologies/icp-rie-inductively-coupled-plasma-reactive-ion-etching

[34] "Focused ion beam," 2023. [Online]. Available : https://en.wikipedia.org/wiki/Focused_ion_beam

[35] D. Gäbler, A. Zimmer, and M. Krojer, "Thin film lens made in cmos process," 2019.

[36] IC-Crack, "Break ic, recover mcu, microcontroller reverse engineering," *IC-Crack Blog*, 2023. [Online]. Available : https://www.ic-crack.com/page/5/

[37] "Schéma de principe d'une polisseuse," 2023. [Online]. Available : https://www.researchgate.net/figure/Schematic-of-chemical-mechanical-polishing_fig1_230932096

[38] "Site internet de la polisseuse ultrapol," 2023. [Online]. Available : https://www.ultratecusa.com/product/ultrapol-advance/

[39] "Microsection d'une puce électronique," 2020. [Online]. Available : https://www.emsdiasum.com/docs/technical/brochures/2020/EMS_LatticeGear.pdf

[40] "Site interent présentant la vr table," 2023. [Online]. Available : https://vr-table.com/

[41] "Site internet présentant des probes précises," 2023. [Online]. Available : https://imina.ch/en/products/micro-robotics-solutions-optical-microscopes

[42] "Exemple d'utilisation de probes sur une sram," 2023. [Online]. Available : https://imina.ch/en/applications/transistor-characterization-5nm-sram-die

[43] "Box de lecture riffbox," 2023. [Online]. Available : https://www.riffbox.org/category/riff-box-version-2/

[44] "Box de lecture easyjtag," 2023. [Online]. Available : https://easy-jtag.com/easyjtag-in-steel-case/

[45] "Box de lecture octoplus," 2023. [Online]. Available : https://octoplusbox.com/products/products/

[46] "Wafer de silicium," 2023. [Online]. Available : https://hightechcompany.fr/materiaux-terres-rares/plaquettes-wafer-de-silicium/

[47] "Slc industrial microsd memory card engineering specification," 2014. [Online]. Available : https://docs.rs-online.com/5cbd/0900766b8165024a.pdf

[48] "Jesd84-a43 embedded multimediacard (emmc) emmc/card product standard," 2007. [Online]. Available : https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/lpc/27039/1/JESD84-A43.pdf

[49] SD Card Association, "Physical Layer Specification Version 3.01," 2010. [Online]. Available : https://community.nxp.com/pwmxy87654/attachments/pwmxy87654/imx-processors%40tkb/3706/1/Part_1_Physical_Layer_Specification_Ver3.01_Final_100218.pdf

[50] "Datasheet de la mémoire micron mt29f2g08aabwp," 2004.

[51] T. Heckmann, "Reverse engineering secure systems using physical attacks," Theses, Université Paris sciences et lettres, Jun. 2018. [Online]. Available : https://theses.hal.science/tel-01990062

[52] Seb, "Dodonpachi dai-ou-jou - cave/pgm," 2020. [Online]. Available : https://www.rep-arcade.com/2020/09/dodonpachi-dai-ou-jou-cave/pgm.html

[53] "Pcbite," 2022. [Online]. Available : https://sensepeek.com/

[54] "Onfi 4.1 gold," 2017. [Online]. Available : https://media-www.micron.com/-/media/client/onfi/specs/onfi_4_1_gold.pdf?la=en&rev=12146b4f212046448d1a2c42bff13a62

[55] "Pdr ir e6," 2023. [Online]. Available : https://www.pdr-rework.com/pdr-ir-e6-rework-station

[56] "Code de la sécurité intérieure," 2023. [Online]. Available : https://www.legifrance.gouv.fr/loda/id/LEGITEXT000030879456

[57] "article 56-1 du code de procédure pénale," 2022. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044568203

[58] "article 77-1 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047052930

[59] "article 100-1 du code de procédure pénale," 2019. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311520

[60] "article 706-95 du code de procédure pénale," 2022. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000044568177

[61] "Article 706-102-1 du code pénal," 2019. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624

[62] Ur-Nammu, *Code d'Ur-Nammu*. Musée archéologique d'Istanbul, 2112-2095 av. J.-C. [Online]. Available : https://fr.wikipedia.org/wiki/Code_d%27Ur-Namma

[63] J. Gaudemet, *Les institutions de l'Antiquité 5e edition*, ser. Domat Droit public. Montchrestien, 1998.

[64] A. Schiavone, *l'invention du droit en Occident*. Belin, 2008.

[65] "Article 427 à 457 du code pénal," 1993. [Online]. Available : https://www.legifrance.gouv.fr/codes/id/LEGISCTA000006182908

[66] "Article 323-1 du code pénal," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047052655

[67] "Article 323-2 du code pénal," 2015. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939443

[68] "Article 323-3 du code pénal," 2015. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939448

[69] "Article 323-3-1 du code pénal," 2013. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000028345220

[70] "Article 323-4 du code pénal," 2004. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418325

[71] "Article 323-5 du code pénal," 1994. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418326

[72] "Article 226-4-1 du code pénal," 2020. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193593

[73] J. P. pour 20 Minutes, "Usurpation d'identité : Comment les victimes de ce cauchemar moderne doivent-elles réagir ?" 2022. [Online]. Available : https://www.20minutes.fr/economie/3348599-20220912-l-usurpation-d-identite-le-cauchemar-moderne

[74] "Article 226-1 du code pénal," 2020. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000042193566

[75] "Article 441-1 du code pénal," 2002. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006418753

[76] "Article 227-23 du code pénal," 2021. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043409170

[77] "Article 421-2-5 du code pénal," 2014. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000029755573

[78] Wikipedia, "Centre de lutte contre les criminalités numériques," 2023. [Online]. Available : https://fr.wikipedia.org/wiki/Centre_de_lutte_contre_les_criminalit\unhbox\voidb@x\bgroup\let\unhbox\voidb@x\setbox\@tempboxa\hbox{e\global\mathchardef\accent@spacefactor\spacefactor}\let\begingroup\

endgroup\relax\let\ignorespaces\relax\accent19e\egroup\spacefactor\accent@spacefactors_num\unhbox\voidb@x\bgroup\let\unhbox\voidb@x\setbox\@tempboxa\hbox{e\global\mathchardef\accent@spacefactor\spacefactor}\let\begingroup\endgroup\relax\let\ignorespaces\relax\accent19e\egroup\spacefactor\accent@spacefactorriques

[79] CNIL, "Nos missions et nos valeurs," 2023. [Online]. Available : https://www.cnil.fr/fr/nos-missions-et-nos-valeurs

[80] "Convention de budapest," 2023. [Online]. Available : https://www.coe.int/fr/web/cybercrime/the-budapest-convention

[81] "Cerberus," 2023. [Online]. Available : https://www.civipol.fr/en/projects/cerberus

[82] "Eu device-cracking platform to receive major upgrade," 2021. [Online]. Available : https://therecord.media/eu-device-cracking-platform-to-receive-major-upgrade

[83] "Exfiles europe fights against crime and terrorism," 2023. [Online]. Available : https://exfiles.eu/

[84] ANSSI, "L'Édito du directeur gÉnÉral," 2023. [Online]. Available : https://www.ssi.gouv.fr/agence/missions/ledito-du-dg/

[85] P. Nationale, "La police scientifique," 2021. [Online]. Available : https://www.sarthe.gouv.fr/IMG/pdf/la_police_scientifique.pdf

[86] "Code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/texte_lc/LEGITEXT000006071154

[87] "article 156 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575748

[88] "article 157 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575366

[89] "article 157-1 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575367

[90] "article 157-2 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575368

[91] "article 97 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038312157

[92] "article 163 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032655631

[93] "article 158 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575368

[94] "article 159 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575751

[95] "article 162 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575376

[96] "article 162 du code de procédure pénale," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006575383

[97] "Site d'accès à la norme iso9001," 2023. [Online]. Available : https://www.iso.org/fr/standard/62085.html

[98] "History of nokia bell labs," 2023. [Online]. Available : https://www.bell-labs.com/about/history/

[99] "About asq walter a. shewhart," 2023. [Online]. Available : https://asq.org/about-asq/honorary-members/shewhart

[100] W. E. Company, *Statistical Quality Control Handbook*. Indianapolis : Western Electric Company, 1956.

[101] "About asq w. edwards deming," 2023. [Online]. Available : https://asq.org/about-asq/honorary-members/deming

[102] "Iso about us," 2023. [Online]. Available : https://www.iso.org/about-us.html

[103] "Principes de management de la qualité," 2023. [Online]. Available : https://www.iso.org/files/live/sites/isoorg/files/store/fr/PUB100080_fr.pdf

[104] J. E. Breneman, C. Sahay, and E. E. Lewis, *Introduction to reliability engineering*. John Wiley & Sons, 2022.

[105] H. Kaufman, "Mathematical theory of reliability. by re barlow and f. proschan, with contributions by lc hunter. wiley, new york (1965). xiii+ 256 pp." *Canadian Mathematical Bulletin*, vol. 13, no. 2, pp. 288–288, 1970.

[106] M. Rausand and A. Hoyland, *System Reliability Theory : Models, Statistical Methods, and Applications*, ser. Wiley Series in Probability and Statistics - Applied Probability and Statistics Section. Wiley, 2003. [Online]. Available : https://books.google.fr/books?id=gkUWz9AA-QEC

[107] A. Birolini, *Reliability engineering*. Springer, 2007, vol. 5.

[108] "Life test : test de vieillissement accéléré de composants électroniques," 2023. [Online]. Available : https://www.tame-component.com/fr/c-problematique/fiabilite/life-test

[109] "Analyseur paramétrique keithley 4200a-scs," 2023. [Online]. Available : https://www.tek.com/fr/products/keithley/4200a-scs-parameter-analyzer

[110] "L'association anadef notre expertise," 2023. [Online]. Available : https://www.anadef.org/

[111] "Welcome page of meeting," 2023. [Online]. Available : https://esref2023.sciencesconf.org/

[112] "Istfa 2023," 2023. [Online]. Available : https://www.asminternational.org/istfa-2023/

[113] E. Committee, *Microelectronics Failure Analysis : Desk Reference*, ser. Microelectronics Failure Analysis : Desk Reference. ASM International, 2004. [Online]. Available : https://books.google.fr/books?id=MyVHpqi1SXwC

[114] "Niveaux msl, délamination, effet popcorn..." 2022. [Online]. Available : https://www.tame-component.com/fr/c-espace-experts/niveau-msl

[115] A. Fukami and K. Nishimura, "Forensic analysis of water damaged mobile devices," *Digital Investigation*, vol. 29, pp. S71–S79, 2019. [Online]. Available : https://www.sciencedirect.com/science/article/pii/S1742287619301586

[116] Wikipédia, "Rétro-ingénierie — wikipédia, l'encyclopédie libre," 2021. [Online]. Available : http://fr.wikipedia.org/w/index.php?title=R%C3%A9tro-ing%C3%A9nierie&oldid=184803032

[117] O.THOMAS, "Advanced ic reverse engineering techniques : In depth analysis of a modern smart card," 2015. [Online]. Available : https://hardwear.io/document/Advanced-IC-Reverse-Engineering-Techniques-In-Depth-Analysis-of-A-Modern-Smart-Card-by-Olivier-THOMAS.pdf

[118] "Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information," 2019. [Online]. Available : https://www.legifrance.gouv.fr/loda/id/LEGITEXT000005632663

[119] "The common criteria," 2023. [Online]. Available : https://www.commoncriteriaportal.org/

[120] "CritÈres et mÉthodologies d'Évaluation," 2022. [Online]. Available : https://www.ssi.gouv.fr/entreprise/produits-certifies/cc/criteres-et-methodologies-devaluation/

[121] "Banc d'émission électromagnétique ledger donjon," 2023. [Online]. Available : https://donjon.ledger.com/

[122] "Banc d'attaque laser alphanov," 2023. [Online]. Available : https://www.alphanov.com/en/products-services/laser-solutions-for-testing-integrated-circuits

[123] "confidentialité," 2023. [Online]. Available : https://www.apple.com/fr/privacy/

[124] "Remote exploitation of an unaltered passenger vehicle," 2015. [Online]. Available : https://www.blackhat.com/us-15/briefings.html#remote-exploitation-of-an-unaltered-passenger-vehicle

[125] "Pwn2own vancouver 2023," 2023. [Online]. Available : https://www.zerodayinitiative.com/blog/2023/3/23/pwn2own-vancouver-2023-day-two-results

[126] "Un regulation no. 155 - cyber security and cyber security management system," 2021. [Online]. Available : https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

[127] "Article 1112-2 du code civil," 2016. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032007140/

[128] "Loi n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires," 2018. [Online]. Available : https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037262111/

[129] "Article 706-102-3 du code pénal," 2019. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311620

[130] "Article 706-102-5 du code pénal," 2019. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311615

[131] "Article 230-1 du code pénal," 2023. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000047053056

[132] "Article 230-2 du code pénal," 2018. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037289946

[133] "Article 230-3 du code pénal," 2017. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032656013

[134] "Article 434-15-2 du code pénal," 2016. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032654251

[135] F. Thomas-Brans, T. Heckmann, K. Markantonakis, and D. Sauveron, "New diagnostic forensic protocol for damaged secure digital memory cards," *IEEE Access*, vol. 10, pp. 33 742–33 757, 2022.

[136] H. Barral, G.-A. Jaloyan, F. Thomas-Brans, M. Regnery, R. Géraud-Stewart, T. Heckmann, T. Souvignet, and D. Naccache, "A forensic analysis of the google home : Repairing compressed data without error correction," *Forensic Science International : Digital Investigation*, vol. 42, p. 301437, 2022.

[137] F. Thomas-Brans, A. Fukami, Q. Clement, T. Heckmann, and D. Sauveron, "Case of study for in situ memory reading on damaged multimedia card," *Forensic Science International : Digital Investigation*, vol. 48, p. 301698, 2024. [Online]. Available : https://www.sciencedirect.com/science/article/pii/S2666281724000076

[138] "Stéréomicroscope lynx evo," 2023. [Online]. Available : https://www.visioneng.fr/produits/microscope-stereo-sans-oculaire/lynx-evo-dynascope/

[139] T. Heckmann, T. Souvignet, D. Sauveron, and D. Naccache, "Medical equipment used for forensic data extraction : A low-cost solution for forensic laboratories not provided with expensive diagnostic or advanced repair equipment," *Forensic Science International : Digital Investigation*, vol. 36, p. 301092, 2021. [Online]. Available : https://www.sciencedirect.com/science/article/pii/S2666281720303942

[140] S. Atkins, L. Teems, W. Rowe, P. Selby, and R. Vaughters, "Use of c-sam acoustical microscopy in package evaluations and failure analysis," *Microelectronics Reliability*, vol. 38, no. 5, pp. 773 – 785, 1998. [Online]. Available : http://www.sciencedirect.com/science/article/pii/S0026271497002205

[141] "Caméra thermique de la marque voltcraft modèle wbp-120," 2023. [Online]. Available : https://www.amazon.fr/thermique-VOLTCRAFT-WBP-120-20-appareil-num%C3%A9rique/dp/B0BM3X7KSS

[142] "Caméra thermique de la marque flir modèle ets320," 2023. [Online]. Available : https://www.es-france.com/landing_page/flir-ETS320/index.html

[143] "Caméra thermique de la marque flir modèle t865," 2023. [Online]. Available : https://www.flir.eu/products/t865_science/

[144] "Article l4412-1 du code du travail," 2022. [Online]. Available : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043893972

[145] "Article r4412-1 à 160 du code du travail," 2008. [Online]. Available : https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006072050/LEGISCTA000018490321/#LEGISCTA000018530960

[146] "Laser d'ablation de la marque clc," 2023. [Online]. Available : https://www.controllaser.com/products/falit-failure-analysis-laser-inspection-tools-for-laser-decap-cross-sectioning-delidding/

[147] "Laser d'ablation de la marque digit concept," 2023. [Online]. Available : http://www.digit-concept.com/equipment/sesame-laser/

[148] A. Sarangan, *Nanofabrication*. New York : Springer, 2016, pp. 1–20.

[149] "Site raspberry," 2023. [Online]. Available : https://www.raspberrypi.org/

[150] "Site arduino," 2023. [Online]. Available : https://www.arduino.cc/

[151] W. contributors, "Apple a13," 2021. [Online]. Available : https://en.wikipedia.org/w/index.php?title=Apple_A13&oldid=1029842498

[152] D. Bushnell, *Essentials of computational linguistics*. Oxford, UK : Blackwell Publishing, 2004.

[153] K. Shirriff, "Nand gate cell," 2021. [Online]. Available : https://twitter.com/kenshirriff/status/1369344203214499843

[154] J. M. Frederic P. Miller, Agnes F. Vandome, *MultiMediaCard*. Alphascript Publishing, 88 pages, ISBN 978-6134094238, 2010.

[155] SDAssociation, "About the sd association," 2022. [Online]. Available : https://www.sdcard.org/about-sda/

[156] JEDEC, "Embedded multimediacard (emmc) product standard, standard capacity," *JESD84-A41, Jul*, 2007.

[157] "Storage, jedec universal flash," 2011.

[158] JEDEC, "Embedded multi-media card (emmc) electrical standard, version 5.1," *JESD84-B51A, Jan*, 2019.

[159] "Universal flash storage (ufs), version 3.1," 2020.

[160] A. Nagourney, I. Lovett, and R. Pérez-Peña, "San bernardino shooting kills at least 14 ; two suspects are dead," *The New York Times*, 2015.

[161] M. Breeuwsma, M. De Jongh, C. Klaver, R. Van Der Knijff, and M. Roeloffs, "Forensic data recovery from flash memory," *Small Scale Digital Device Forensics Journal*, vol. 1, no. 1, pp. 1–17, 2007.

[162] R. V. D. Knijff, "Embedded systems analysis," in *Chapter 11 of Handbook of Computer Crime Investigation : Forensic Tools and Technology, E. Casey (Ed.)*, 2002.

[163] N. BC, "No.1 bc home page," 2022. [Online]. Available : https://no1bc.com/

[164] J. P. van Zandwijk and A. Fukami, "Nand flash memory forensic analysis and the growing challenge of bit errors," *IEEE Security Privacy*, vol. 15, no. 6, pp. 82–87, 2017.

[165] A. Fukami, S. Ghose, Y. Luo, Y. Cai, and O. Mutlu, "Improving the reliability of chip-off forensic analysis of nand flash memory devices," *Digital Investigation*, vol. 20, pp. S1–S11, 2017. [Online]. Available : https://www.sciencedirect.com/science/article/pii/S1742287617300415

[166] N. Y. Ahn and D. H. Lee, "Forensics and anti-forensics of a nand flash memory : From a copy-back program perspective," *IEEE Access*, vol. 9, pp. 14 130–14 137, 2021.

[167] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (iot) forensics : Challenges, approaches, and open issues," *IEEE Communications Surveys Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.

[168] J. Hou, Y. Li, J. Yu, and W. Shi, "A survey on digital forensics in internet of things," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 1–15, 2020.

[169] S. Amiroon and C. Fachkha, "Digital forensics and investigations of the internet of things : A short survey," in *2020 3rd International Conference on Signal Processing and Information Security (ICSPIS)*. IEEE Computer Society, 2020.

[170] R. Bez, E. Camerlenghi, A. Modelli, and A. Visconti, "Introduction to flash memory," *Proceedings of the IEEE*, vol. 91, no. 4, pp. 489–502, 2003.

[171] S. Fiorillo, "Theory and practice of flash memory mobile forensics," in *Australian Digital Forensics Conference,* 37 pages, 2009.

[172] C.-K. Hsieh, "Flash memory controller, sd card device, method used in flash memory controller, and host device coupled to sd card device," Jun. 23 2020, uS Patent 10,691,589.

[173] "Ufs memory device datasheet," 2021. [Online]. Available : https://www.glynshop.com/erp/owweb/Daten/IMS/Kioxia/Products/Specifications/Data%20Sheets/KIOXIA_THGJFGT1E45BAIP_BiCS5_256GB_UFS_Ver_3_1_E_Rev1_00.pdf

[174] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffres*, pp. 147–158, 1959.

[175] R. C. Bose and D. K. Ray-Chauduri, "On a class of error correcting binary group codes," *Information and Control*, vol. 3, no. 1, pp. 68–79, 1960. [Online]. Available : http://www.sciencedirect.com/science/article/pii/S0019995860902874

[176] M.-C. Yang, Y.-M. Chang, C.-W. Tsao, P.-C. Huang, Y.-H. Chang, and T.-W. Kuo, "Garbage collection and wear leveling for flash memory : Past and future," in *2014 International Conference on Smart Computing*. IEEE, 2014, pp. 66–73.

[177] "Google home teardown." [Online]. Available : https://www.ifixit.com/Teardown/Google+Home+Teardown/72684

[178] H. Chung, J. Park, and S. Lee, "Digital forensic approaches for Amazon Alexa ecosystem," *Digital Investigation*, vol. 22, 2017. [Online]. Available : https://www.sciencedirect.com/science/article/pii/S1742287617301974

[179] S. Engelhardt, "Smart speaker forensics," Honors Thesis, 2019. [Online]. Available : https://scholarsarchive.library.albany.edu/honorscollege_business/56/

[180] M.-A. Youn, Y. Lim, K. Seo, H. Chung, and S. Lee, "Forensic analysis for AI speaker with display Echo Show 2nd generation as a case study," *Forensic Science International : Digital Investigation*, vol. 38, 2021. [Online]. Available : https://www.sciencedirect.com/science/article/pii/S2666281721000287

[181] W. Qian, Y. Li, and H. Wu, "Breaking Google Home : Exploit it with SQLite (Magellan)," 2019. [Online]. Available : https://media.defcon.

org/DEF%20CON%2027/DEF%20CON%2027%20presentations/DEFCON-27-Wenxiang-Qian-Yuxiang-Li-Huiyu-Wu-Breaking-Google-Home-Exploit-It-with-SQLite-Magellan.pdf

[182] Courk, "Running custom code on a Google Home Mini (part 1)," 2020. [Online]. Available : https://courk.cc/running-custom-code-google-home-mini-part1

[183] "Running custom code on a Google Home Mini (part 2)," 2020. [Online]. Available : https://courk.cc/running-custom-code-google-home-mini-part2

[184] N. Semiconductors, "Pca9956b 24-channel fm+ i2c-bus 57 ma/20 v constant current led driver," 2020. [Online]. Available : https://www.nxp.com/products/analog/interfaces/ic-bus/ic-led-controllers/24-channel-fm-plus-ic-bus-57-ma-20-v-constant-current-led-driver:PCA9956BTW

[185] I. InvenSense, "Inmp621 wide dynamic range microphone with pdm digital output," 2014. [Online]. Available : https://invensense.tdk.com/products/digital/inmp621/

[186] Microchip, "Sam d21/da1 family low-power, 32-bit cortex-m0+ mcu with advanced analog and pwm," 2021. [Online]. Available : https://www.microchip.com/en-us/product/ATsamd21g18

[187] I. S. 1149.7-2009, "IEEE standard for reduced-pin and enhanced-functionality test access port and boundary-scan architecture," 2009. [Online]. Available : https://ieeexplore.ieee.org/document/5412866

[188] A. Limited, "Arm debug interface architecture specification," 2018. [Online]. Available : https://developer.arm.com/documentation/ihi0031/latest

[189] Marvell, "Marvell Avastar 88W8887 WLAN/Bluetooth/NFC/FM receive single-chip SoC," 2015. [Online]. Available : https://static6.arrow.com/aropdfconversion/fba1353dcf30160996b8e8cb8411c6759e29c02e/8501596417286692marvell_avastar_88w8887_soc-01_pb_v5.pdf

[190] T. Instruments, "Tas5720x digital input mono class-d audio amplifier with tdm support up to 8 channels," 2015. [Online]. Available : http://www.ti.com/lit/gpn/tas5720m

[191] Samsung, "4Gb E-die DDR3L SDRAM datasheet," 2016. [Online]. Available : https://semiconductor.samsung.com/resources/data-sheet/DS_K4B4G1646E_BY_M_Rev1_11-0.pdf

[192] Marvell, "Dc/dc power regulators product portfolio," 2016. [Online]. Available : https://dtsheet.com/doc/1459945/dc-dc-power-regulators-product-portfolio

[193] Google, "Arm marvell socs," 2016. [Online]. Available : https://kernel.googlesource.com/pub/scm/linux/kernel/git/jszhang/linux-berlin/+/refs/heads/master/Documentation/arm/Marvell/README

[194] Toshiba, "TC58NVG1S3HBAI6 datasheet," 2013. [Online]. Available : https://z3d9b7u8.stackpathcdn.com/pdf-down/T/C/5/TC58NVG1S3HBAI6-Toshiba.pdf

[195] R. Gordon, R. Bender, and G. T. Herman, "Algebraic reconstruction techniques (art) for three-dimensional electron microscopy and x-ray photography," *Journal of theoretical Biology*, vol. 29, no. 3, pp. 471–481, 1970.

[196] ACE Lab, "PC-3000 Flash Solution Center," 2021. [Online]. Available : http://www.pc3000flash.com/solbase/monochips.php?lang=eng

[197] "ACE Lab," 2021. [Online]. Available : https://www.acelaboratory.com/

[198] S. Gerardin, M. Bagatin, A. Paccagnella, A. Visconti, S. Beltrami, M. Bertuccio, and L. Czeppel, "A study on the short-and long-term effects of x-ray exposure on nand flash memories," in *2011 International Reliability Physics Symposium*. IEEE, 2011, pp. EX–1.

[199] M. J. Gadlage, M. J. Kay, J. D. Ingalls, A. R. Duncan, and S. A. Ashley, "Impact of x-ray exposure on a triple-level-cell nand flash," *IEEE Transactions on Nuclear Science*, vol. 60, no. 6, pp. 4533–4539, 2013.

[200] A. Terao, D. Flandre, E. Lora-Tamayo, and F. Van de Wiele, "Measurement of threshold voltages of thin-film accumulation-mode PMOS/SOI transistors," *IEEE Electron Device Letters*, vol. 12, no. 12, pp. 682–684, 1991.

[201] F. Kerisit, B. Domenges, and M. Obein, "Comparative study on decapsulation for copper and silver wire-bonded devices," in *40th International Symposium for Testing and Failure Analysis, ASM International*, 2014, pp. 87–93.

[202] E. D. R. Committee *et al.*, *Microelectronics Failure Analysis : Desk Reference*. ASM International, 2011.

[203] Y. S. H.B Kor, Q. Liu and C. Gan, "Laser focus adaptation for decapsulation of copper wirebonded devices," in *40th International Symposium for Testing and Failure Analysis, ASM International*, 2014, pp. 94–99.

[204] M. J. Lefevre, F. Beauquis, J. Yang, M. Obein, P. Gounet, and S. Barberan, "New method for decapsulation of copper wire devices using laser and sub-ambient temperature chemical etch." in *2011 IEEE 13th Electronics Packaging Technology Conference*, 2011, pp. 769–773.

[205] SAMSUNG, "K9f2g08u0c advance 2gb c-die nand flash single-level-cell (1bit/cell)," 2010.

[206] "Pc3000 flash memory reader," 2023. [Online]. Available : https://www.acelab.eu.com/pc3000flash.php

[207] "Rusolut nand reader," 2023. [Online]. Available : https://rusolut.com/emmc-nand-reconstructor/

[208] "microsd nand monolithic mr24 adapter (diagram 6x4)," 2023. [Online]. Available : https://multi-com.eu/,details,id_pr,21962,key,adapter-nand-microsd-mr24.html

[209] "Pcb workstation with nano-probes," 2019. [Online]. Available : https://www.thingiverse.com/thing:3615910

[210] "Pc-3000 flash spider board adapter. how to use it ?" 2017. [Online]. Available : https://blog.acelab.eu.com/pc-3000-flash-spider-board-adapter-how-to-use-it.html

[211] "Protonews," 2023. [Online]. Available : https://www.proto-electronics.com/fr/blog

[212] T. Heckmann, T. Souvignet, and D. Naccache, "Electrically conductive adhesives, thermally conductive adhesives and uv adhesives in data extraction forensics," *Digital Investigation*, vol. 21, pp. 53–64, 2017. [Online]. Available : https://www.sciencedirect.com/science/article/pii/S1742287616301347

[213] "Saleae logic specification," 2022. [Online]. Available : https://www.saleae.com/#section-tech-specs

[214] B. Norris, "Nand flash support table," 2011. [Online]. Available : http://www.linux-mtd.infradead.org/nand-data/nanddata.html

[215] B. Park, A. Savoldi, P. Gubian, J. Park, S. H. Lee, and S. Lee, "Data extraction from damage compressed file for computer forensic purposes," *International Journal of Hybrid Information Technology*, vol. 1, no. 4, 2008. [Online]. Available : http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.180.3061&rep=rep1&type=pdf

[216] G. Wang, H. Peng, and Y. Tang, "Repair and restoration of corrupted LZSS files," *IEEE Access*, vol. 7, pp. 9558–9565, 2019. [Online]. Available : https://ieeexplore.ieee.org/document/8606930

[217] M. Breeuwsma, M. de Jongh, C. Klaver, R. van der Knijff, and M. Roeloffs, "Forensic data recovery from flash memory," *Small Scale Digital Device Forensics Journal*, vol. 1, 2007. [Online]. Available : http://www.foo.be/cours/mssi-20072008/SSDDFJ_V1_1_Breeuwsma_et_al.pdf

[218] "Tese station precision hot air," 2023. [Online]. Available : https://www.jbctools.com/tese-precision-hot-air-station-product-1255.html

[219] "Zevac onyx 24," 2023. [Online]. Available : https://www.zevac.ch/products/smt-rework/onyx-24

[220] E. R. Berlekamp, *Algebraic coding theory.* McGraw-Hill, 1968. [Online]. Available : https://books.google.fr/books?id=nIIpAQAAMAAJ

[221] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, pp. 379–423, 1948. [Online]. Available : http://pespmc1.vub.ac.be/books/Shannon-TheoryComm.pdf

[222] C. Heffner, "Differentiate encryption from compression using math," 2013. [Online]. Available : http://www.devttys0.com/2013/06/differentiate-encryption-from-compression-using-math/

[223] "Encryption vs compression, part 2," 2013. [Online]. Available : http://www.devttys0.com/2013/06/differentiate-encryption-from-compression-using-math/

[224] I. Pavlov, "Lzma SDK (software development kit)," 2007. [Online]. Available : https://www.7-zip.org/sdk.html

[225] L. P. Deutsch and J. loup Gailly, "Zlib compressed data format specification version 3.3," 1996. [Online]. Available : https://tools.ietf.org/html/rfc1950

[226] L. P. Deutsch, "Deflate compressed data format specification version 1.3," 1996. [Online]. Available : https://tools.ietf.org/html/rfc1951

[227] "Gzip file format specification version 4.3," 1996. [Online]. Available : https://tools.ietf.org/html/rfc1952

[228] L. K. Documentation, "SquashFS 4.0 filesystem," 2020. [Online]. Available : https://www.kernel.org/doc/Documentation/filesystems/squashfs.txt

[229] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *Journal of the American Statistical Association*, vol. 58, no. 301, pp. 13–30, 1963. [Online]. Available : http://repository.lib.ncsu.edu/bitstream/1840.4/2170/1/ISMS_1962_326.pdf

[230] S. Martello, *Knapsack problems : algorithms and computer implementations.* Wiley, 1990. [Online]. Available : http://www.math.nsc.ru/LBRT/k5/knapsack_problems.pdf

[231] National Security Agency, "Ghidra," 2019. [Online]. Available : https://ghidra-sre.org/

[232] F. Courbon, S. Skorobogatov, and C. Woods, "Reverse engineering flash eeprom memories using scanning electron microscopy," in *International Conference on Smart Card Research and Advanced Applications.* Springer, 2016, pp. 57–72.

[233] "Analyse des modes de défaillance, de leurs effets et de leur criticité," 2023. [Online]. Available : https://fr.wikipedia.org/wiki/Analyse_des_modes_de_d%C3%A9faillance,_de_leurs_effets_et_de_leur_criticit%C3%A9

Diagnostic et réparation de supports électroniques chiffrés et endommagés

Résumé :
La forensique numérique est la science forensique qui consiste à rechercher et récupérer des données dans des supports numériques. Le terme de supports numériques recouvre l'ensemble des équipements permettant d'acquérir, manipuler ou stocker de la donnée sous forme d'encodage numérique. Les supports rencontrés peuvent être des ordinateurs, des consoles de jeu ou des smartphones, qui se sont largement répandus ces vingt dernières années. Toutefois depuis 2015, les supports sont plus divers et complexes avec la numérisation croissante des objets du quotidien (par exemple : les ampoules, les télévisions, les jouets, l'électroménager). L'évolution du volume global des supports, ainsi que leur complexité sont devenus une problématique importante pour les laboratoires de forensique numérique. Dans ce contexte, ces laboratoires doivent s'adapter pour que les experts soient en mesure d'assurer leurs missions dans des temps compatibles avec le temps judiciaire. Cette adaptation passe par la formation et le développement de nouvelles techniques. C'est dans l'optique de répondre à ces derniers, que les travaux présentés dans le cadre de ce mémoire, ont été réalisés.

La première partie du document présente les trois secteurs d'activités qui ont été une source d'inspiration pour les travaux. Dans un premier temps, la forensique numérique est présentée, car il s'agit de l'activité pour laquelle les travaux sont réalisés. Suivent l'analyse de défaillance, ainsi que la rétro-conception matérielle, car il s'agit de deux secteurs moteurs dans le domaine de l'interaction avec les composants électroniques.

La seconde partie du document traite tout d'abord de la démarche qui a conduit à sélectionner des composants MultiMedia Card (MMC) comme supports cibles pour nos travaux. La seconde partie fait également un état des lieux des équipements présents dans les laboratoires de forensique numérique, ainsi que ceux supplémentaires dans les laboratoires d'analyse de défaillance et qui pourront être utilisés par la suite.

La troisième partie décrit le protocole de diagnostic des MMC qui a été développé dans le but d'harmoniser des procédures de recherche de défaut dans les laboratoires de forensique numérique. Ce protocole a été réalisé en prenant en compte l'ensemble des équipements présentés. Dans ce protocole, nous avons ajouté deux équipements provenant de l'analyse de défaillance et ayant démontré leur utilité dans le diagnostic des supports de forensique numérique : La caméra thermique et le microscope acoustique à balayage.

Le protocole développé dans la troisième partie permettant d'effectuer un diagnostic menant à une réparation structurelle, la continuité des travaux a consisté à la récupération des données. Ainsi, la partie quatre présente tout d'abord un état des lieux des solutions commerciales existantes pour effectuer une extraction des données. Toutefois, beaucoup de MMC n'étant pas supportées par les outils commerciaux, une démarche complète pour le traitement de ces supports a été développée (de l'étude de la composition du support, à la lecture, puis à la fiabilisation de la donnée).

La dernière partie du mémoire présente quatre perspectives identifiées durant l'ensemble des travaux.

Mots clés : Forensique numérique, Diagnostic, Extraction de données, MultiMedia Card, Protocole, Caméra thermique

Diagnosis and repair of damaged and encrypted electronic media

Abstract :
Digital forensics is the science of investigating and recovering data from digital media. The term digital media covers all equipment used to acquire, manipulate or store data in the form of digital encoding. These devices can be computers, games consoles or smartphones, which have become very common over the last twenty years. However, since 2015, the media have become more diverse and complex, with the increasing digitisation of everyday objects (e.g. lights, televisions, toys, home appliances). The growth in the overall volume and complexity of media has become a major issue for digital forensics laboratories. In this context, these laboratories must adapt to ensure that the experts are able to carry out their assignments in a legally-compatible timeframe. This requires training and the development of new techniques. The work presented in this thesis was carried out in response to these requirements.

The first part of the thesis presents the three sectors of activity that were a source of inspiration for the work. Firstly, digital investigation is presented, as this is the focused activity of this work. This is followed by failure analysis and hardware reverse engineering, as these are two key activities in the field of interaction with electronic components.

The second part of the thesis deals firstly with the approach that led to the selection of MultiMedia Card (MMC) components as the target media for our work. The second part also provides an overview of the equipment available in digital investigation laboratories, as well as additional equipment in failure analysis laboratories, which could be used in the future.

The third part describes the MMC diagnostic protocol, which was developed with the aim of standardizing fault detection procedures in digital investigation laboratories. This protocol has been produced taking into account all the equipment presented. In this protocol, we have added two equipment systems from failure analysis that have demonstrated their usefulness in the diagnosis of digital forensic media : the thermal camera and the scanning acoustic microscope.

Since the protocol developed in part three allowed a diagnosis to be performed leading to structural repair, the work continued with data recovery. Part four therefore begins with an overview of existing commercial solutions for data extraction. However, as many MMCs are not supported by commercial tools, a complete approach to processing these media has been developed (from studying the composition of the media to reading and then making the data reliable).

The final part of the thesis presents four perspectives identified during the course of the work.

Keywords : Digital investigation, Diagnostics, Data extraction, MultiMedia Card, Protocol, Thermal camera.

XLIM - UMR CNRS n° 7252
123, avenue Albert Thomas - 87060 LIMOGES Cedex