


THÈSE DE DOCTORAT DE
l'UNIVERSITÉ PIERRE ET MARIE CURIE

Spécialité

Informatique

École doctorale Informatique, Télécommunications et Électronique (Paris)

Présentée par

Kaushik Chakraborty

Pour obtenir le grade de

DOCTEUR de l'UNIVERSITÉ PIERRE ET MARIE CURIE

Sujet de la thèse :

Cryptography with Spacetime Constraints

Soutenue le 12 Octobre 2017
Devant le jury compose de :

Jean-Pierre Tillich	Inria Paris	Directeur de thèse
Anthony Leverrier	Inria Paris	Directeur de thèse
Stephanie Wehner	TU Delft	Rapporteur
Jérémie Roland	Université Libre de Bruxelles	Rapporteur
Frédéric Magniez	Université Paris Diderot	Examinateur
Frédéric Grosshans	Université Paris Sud	Examinateur
Omar Fawzi	ENS Lyon	Examinateur
Jean-Claude Blajard	Université Pierre et Marie Curie	Examinateur.

Cryptography with Spacetime Constraints

Kaushik Chakraborty

Sous la direction de Jean-Pierre Tillich et Anthony Leverrier

Équipe-Projet SECRET
Inria de Paris,
2 rue Simone IFF,
75 012 Paris

Acknowledgements

I am grateful to everyone who guided and supported me during my PhD thesis in Paris. First of all, I would like to cordially thank my supervisors Anthony Leverrier and Jean-Pierre Tillich for giving me the opportunity to conduct the PhD training on relativistic cryptography. I am thankful to André Chailloux for his expert advice and encouragement throughout my training. The countless hours of discussions (both scientific and non-scientific) I had with Anthony and André inspired me a lot to go through the ups and downs of my PhD life. I would like to thank Nicolas Sendrier for introducing me to our research group SECRET and helping me to get the funding for my PhD.

I want to thank Subhamoy Maitra for being a friend, philosopher and guide throughout my research career. Without his inspiration and guidance it was almost impossible for me to start research in quantum information.

I enjoyed being a PhD student in this well organised research group. I thank our group leader Anne Canteaut and other researchers Nicolas, Maria, Gaëtan, Pascale for creating such a good environment for research. I want to thank Pascale for organising the group seminars.

Living in Paris as a student is always exciting. The experience is more exciting when you get the opportunity to discuss with theoretical physicists, mathematicians and experimentalists who work together under the same hood to solve interesting problems on quantum information. I would like to thank Paris Centre for Quantum Computing (PCQC) for providing such a common platform in Paris. I would like to thank all the PCQC members, specially Eleni, Frederic, Damian Marc, Elham, Iordanis, Sophie, Frederic Magniez, Romain, Isabelle for creating a dynamic and versatile research environment. I want to thank all of my friends and the student PCQC members (quantum musketeers), specially Leo, Adel, Niraj, Ruben, Alex, Antoine, Vivien, Xavier, Remi, Bill for making the research life in Paris more enjoyable. I want to thank my colleagues, specially Julia, Antoine, Joëlle, Virginie, Sebastien, Yann, Xavier, Kevin, Rodolfo for supporting me greatly, who were always willing to help me. Special thanks to Julia, Antoine, Rodolfo, Joëlle for being good friend and for their support regarding French administrative system. I am thankful to Christelle for her assistance and guidance on handling the administrative issues. Her continuous support allowed me to focus more on research.

I want to thank Omar Fawzi for having insightful discussions regarding the subject of my thesis. I want to thank Serge Fehr, Christian Schaffner for inviting me to visit CWI, Amsterdam. I have spent a wonderful week at there. I want to give special thanks to Stephanie for inviting me to visit TU Delft and giving me an opportunity to work with her.

I want to thank Jeremie Rolland, Stephanie Wehner, Frederic Magniez, Frederic Grosshans, Omar Fawzi, Jean-Claude Bajard for agreeing to be jury members for my thesis.

I want to thank the collaboration related to "Cryptography & Cryptanalysis: How far can we bridge the gap between Classical and Quantum Paradigm", No: 21/11/2015-BRNS/35038, a project awarded by BRNS to Prof. Subhamoy Maitra at Indian Statistical Institute, Kolkata for supporting my visit at Indian Statistical Institute.

Last but not least, I want to express my gratitude to my family for their immense love and support from the distance. I am infinitely grateful for the great childhood they gave me which was and still is an invaluable source of self-confidence for me.

Abstract

In this thesis we have studied how to exploit relativistic constraints such as the non-superluminal signalling principle to design secure cryptographic primitives like position-verification and bit commitment. According to non-superluminal signalling principle, no physical carrier of information can travel faster than the speed of light. This put a constraint on the communication time between two distant stations. This delay in transferring information can be used for cryptography. For example, by computing the roundtrip communication time one can get an upper bound on the distance between two spatially separated agents. Beside this, one can consider the delay in information transfer as a temporal non-communication constraint. In multi-party cryptography, many cryptographic primitives like bit-commitment, oblivious transfer can be implemented with perfect secrecy under such non-communication assumption between the agents.

In the first part of this thesis we will study how non-signalling constraints can be used to verify securely the position of an agent. Here, we will discuss about a strategy which can attack any position verification scheme. Then we will discuss about a new position verification scheme which is practical for the honest parties and immune against ours attack strategy.

In the next part of this thesis we are going to discuss about the nonlocal games. Such games are relevant for studying of relativistic bit commitment protocols. We have established an upper bound on the classical value of such family of games.

The last part of this thesis discusses about two relativistic bit commitment protocols and their security against classical adversaries. Though both of the protocols are practical for implementation but the first one is not robust against losses. The second protocol is designed to be robust against the presence of losses in the channel. We have exploited the upper bound on the nonlocal games for the security analysis of both of these protocols, .

We conclude this thesis by giving a brief summary of the content of each chapter and mentioning interesting open problems. These open problems can be very useful for better understanding of the role of spacetime constraints such as non-superluminal signalling in designing perfectly secure cryptographic primitives.

Contents

1 Introduction

Cryptography is the practice and study of techniques for secure communication in the presence of third parties called *adversaries*. Historically, the term cryptography is associated with schemes that provide secret communications over an insecure channel. Its history can be traced back to 1500 BCE in the Mesopotamian civilization. Back then, people used it to protect information about craftsman's recipes for pottery glaze. At the nascent stage of its evolution (called the *classical era*), cryptography was limited to hiding information through *encryption* schemes. For example, in the Roman Empire, Julius Caesar used a special type of substitution cipher, now called *Caesar cipher*, to encrypt his messages to communicate with his generals: to produce an encrypted text (*ciphertext*), each letter in the message (*plaintext*) is substituted with a letter corresponding to a certain number of letters up or down in the alphabet. At that time, cryptography was mostly used to provide *privacy* for communication and confined to the military, the diplomatic service and government. We recommend reading [Kah96] for a detailed history of cryptography. More recently, with the rapid evolution of electrical machines, computers and communication technology, applications of cryptography have spread from secret military communication to everyday life. To satisfy security demands in various public domains, the goal of cryptography has expanded from *privacy* or (*confidentiality*) to *data integrity* and *authentication*.

Ideally, from a designer's perspective, the construction of a cryptographic scheme is such that it doesn't lose its prescribed and desired functionality even under incessant malicious attempts to break it. To achieve such security goals, one should not put any assumption on the operational environment of the system, nor be satisfied with the security of a scheme that only resists to some specific attacks. Often, cryptographic schemes which are claimed to be secure under the assumption that the adversary can only perform a certain type of attacks turn out to be insecure against more general attacks. For instance, the Caesar cipher is easily broken by a frequency analysis. This motivates the interest for defining security notions based on firm mathematical foundations.

From the classical era of cryptography until 1949, almost all cryptographic schemes were based on heuristics and ad hoc approaches. The notion of mathematical cryptography was first introduced by Claude Shannon, back in 1949 [Sha49]. He developed a systematic approach to cryptography where definitions and proofs play a visible role. His seminal work was concerned with two main goals: *secrecy* and *authenticity*. Informally, the concept of *secrecy* is concerned about the fact that only a

legitimate user can access the message, whereas *authenticity* ensures that only a legitimate source can create a message that cannot be altered by other parties. Shannon further defined two levels of security: information-theoretic and computational. We review them below.

1 Information-theoretic and computational security

Informally, a cryptosystem is called *perfectly secure* if the adversary can't gain any information about the secret even if they have unlimited computational power. Such a cryptosystem is called *cryptanalytically unbreakable*. Sometimes we call this type of security notion *perfect security*. *One-time pad* is one of the most commonly used examples of information theoretically secure cryptographic schemes: in this scheme, two parties share a secret key which has the same length as a message they want to safely send. Encryption and decryption of this message simply consist in XORing the key to the message. This security comes at a price, however: one needs long secret key that cannot be reused. For this reason, one is interested in finding more efficient cryptosystems. Also, many cryptographic tasks cannot be done with such a strong notion of security.

A cryptosystem is called *computationally secure* if an adversary with limited computational resources cannot get any information about the secret. Generally, to establish computational security, one reduces the problem of breaking the cryptosystem to the problem of solving a computationally hard problem. Security is then implied by the fact that the underlying computationally hard problem cannot be solved with limited computational resources, that is in polynomial time (in the size of the input parameter). It is usually extremely hard to prove that a problem cannot be solved in polynomial time and we will therefore rely on computational assumptions. For example, the security of the RSA cryptosystem [RSA78] is based on the assumption that finding the prime factors of a large number is a difficult problem. Even if it looks easier to design cryptosystems with computational security, one should be cautious with the choice of hard problems. For instance, the Merkle-Hellman public key cryptosystem [MH06] based on the knapsack problem has been broken by several attacks [Sha82, Adl83]. Besides this, improvement of technology and of computational models make some cryptosystems obsolete. One well-known example is the RSA cryptosystem: while no efficient classical algorithm can, as of today, break this scheme; it is vulnerable against a quantum computer using Shor's algorithm [Sho94].

2 Two-party cryptography

Modern cryptography is a mature field which addresses a wide range of applications. This thesis primarily focuses on *two-party cryptography*, which deals with situations where two mistrustful parties, namely Alice and Bob, want to perform a task together. Let us give some examples from everyday life.

(i) **Position-based cryptography.** Introduced by Chandran *et al.* [CGMO09], it uses the geographical location of a party as their only credential. For example, in a military context, one want to make sure that the orders from the headquarters are only accessible by someone inside the army base at a specific location, and not by the surrounding enemies.

(ii) **Bit commitment.** Alice wants to participate in a bidding, organized by Bob. She prepares her bid and puts all her effort to get the contract, but doesn't want to reveal anything about her bid amount, not even to Bob, until the bids are open. At this point, Bob asks Alice to reveal her bid. This type of primitive is called a *commitment* scheme [Blu82, BCC88]. Such a scheme is called secure if it satisfies two properties: it should be *hiding* meaning that Bob cannot learn any information about the bid before the opening phase and *binding* meaning that Alice cannot change the value of her bid after the commitment.

(iii) **Private information retrieval.** This corresponds to a situation where Alice wants to retrieve a specific message from a server, but doesn't want the server to learn which message she accessed. At the same time, Alice shouldn't be able to access more than one message, for instance if the server contains very sensitive information, like medical data. *Private information retrieval* is a primitive introduced by Chor *et al.* [CGKS95] that solves this problem.

Designing information-theoretically secure cryptographic schemes is a difficult task, and it is in fact not possible in general for two-party cryptography. A possible strategy to bypass impossibility results is to change the security model. For instance, *key exchange*, where two spatially separated parties want to share a secret by communicating through an insecure channel, is impossible if Alice and Bob are restricted to use only classical information, but becomes possible if they exchange quantum information. This is the famous protocol discovered by Charlie Bennett and Gilles Brassard [BB84]. In fact, their paper on *quantum key distribution* (QKD) gave birth to a new research direction, called *quantum cryptography*. Beside quantum mechanics, other physical theories like the *special theory of relativity*, can be exploited to perform tasks with information theoretic security. This is the case for instance for certain two-party cryptographic primitives like bit commitment, which cannot be obtained using only quantum mechanics. Such physical theories usually put an upper bound on the power and resources of the adversary. Another approach to enforce such bounds is to take into account the limitations of current day technology: for instance, one can argue that ideal quantum memories are not available now, and exploit this fact to define new security models such as the *bounded storage* and *noisy storage* models.

3 Cryptographic assumptions

We now discuss a number of possible cryptographic assumptions.

(i) **Assumption on limited shared resources:** for two-party cryptography, one can define a security guarantee under the assumption that the set of adversaries share a limited amount of resources. Usually, we put assumptions on the following resources:

- **Memory:**
  - **Bounded Storage Model:** here, one puts an assumption on the size of adversary's quantum (or classical) memory. In the quantum case, it was first introduced by Damgard *et al.* [DFSS05]. In this model, by bounding the memory size, we force the adversaries to convert some of their quantum information into classical one. This actually forces them to measure certain quantum states and this may irreversibly

destroy information. Under this assumption one can design information theoretically secure bit commitment and oblivious transfer protocols [DFSS05, WW08].

– **Noisy Storage Model:** here, we assume that the information (or quantum state) stored in a quantum memory and used by adversary is affected by noise. In such a model, basic cryptographic primitives like bit commitment or oblivious transfer can be constructed with information theoretic security [WST08, STW09, KWW12].

- **Entanglement:** limiting the amount of quantum correlations between the adversaries can be useful, for instance in the context of position-based cryptography [CGMO09]. Indeed, it is proven that if the adversaries share exponentially (in the length of input parameters) many entangled particles then any position verification scheme is insecure [BCF$^+$11]. However, there exist certain schemes for which no attack is known if the adversaries are restricted to share only a polynomial amount of entangled particles [BCF$^+$11], although we don't know any explicit constructions for such schemes.

(ii) **Non-Communication Assumption:** Cryptographic primitives, like bit-commitment or oblivious transfer do not exist with information theoretic security [BOGKW88, May97, LC97]. However, these no-go theorems don't apply any more if we go to the multi-party setting and put some assumption on the communication between the parties. In [BOGKW88, NP00], it was shown that if there are several spatially separated agents per party, then under the non-communication assumption between the agents, one can design perfectly secure bit-commitment schemes as well as oblivious transfer schemes. In Chapter 2, we will discuss this model in detail. Even though this model allows us to design information theoretically secure cryptographic primitives, it is very difficult to enforce this assumption in practice. In [Ken99], Kent uses the *special theory of relativity* to enforce non communicating parties, as we discuss later next.

(iii) **Relativistic Assumption:** According to the *special theory of relativity* and the *causality principle*, we can assume that no physical carrier of information can travel faster than the speed of light. Under this assumption, cryptographic primitives, like bit-commitment, can be constructed with information theoretical security [Ken99]. A main part of this thesis focuses on the security of cryptographic primitives in this model.

Part of this thesis is influenced by *quantum cryptography*, and we now give a brief introduction to that challenging and fascinating interdisciplinary field of research.

4 Quantum cryptography

The origin of *quantum cryptography* can be traced back to the 1960's when Stephen Wiesner designed a special type of unforgeable digital banknote, protected by the laws of quantum mechanics. The main disadvantage of his construction was that no one but the person who had created the bank note, could verify it. Around the same time, in another of his papers [Wie83], Wiesner used the concept of *quantum multiplexing channel* to allow one party to send two messages to another such that the receiving party could decide to read either one of the messages, but at the cost of destroying the other message irreversibly. Back in 60's, researchers already started to explore the use of quantum mechanics to design cryptographic primitives, but the term *Quantum Cryptography* was coined

by Bennett *et al.* in 1983 [BBBW83]. They came up with the idea of transmitting confidential information over an insecure quantum channel and gave birth to quantum key distribution [BB84]. Though the protocol for quantum key distribution was presented in [BB84], there was no rigorous security proof at that time. A rigorous security proof can be found in Renato Renner's thesis [Ren08].

The counterintuitive features of quantum mechanics put some constraints on information processing. For example, the *no cloning principle* [WZ82] states that it is impossible to design a universal copying machine to replicate an unknown quantum state. In quantum mechanics, to extract information from a quantum state, one needs to perform an irreversible operation on the state. This operation is called a *quantum measurement*. Some of the properties of quantum mechanics are discussed later in Chapter 2.

Quantum entanglement and non-locality are other fascinating features of quantum mechanics [EPR35]. They allow two spatially separated parties to share correlations which are stronger than classical ones.This can be witnessed by the violation of some inequality, called *Bell inequality*. In his seminal paper [Bel64], Bell proved a theorem, which says that no physical theory of local hidden variables (for example classical mechanics) can reproduce all of the results of quantum mechanics. This theorem clearly puts a separation line between quantum mechanics and classical mechanics. In computer science or cryptography, we often use non-local games as a mathematical abstraction of such Bell inequalities. These are games, played between a referee and two (or more) non-communicating parties, Alice & Bob. In the game, the referee asks some questions to Alice and Bob and they reply with some answers. On the basis of these questions and responses, the referee computes some predefined predicate to check whether the players win or lose at the end of the game. The aim of Alice and Bob is to win the game with high probability. One of the most commonly studied non-local games is the CHSH game, introduced by John Clauser, Michael Horne, Abner Shimony, and Richard Holt [CHSH69]. In this game, the referee sends random bits x, y to Alice and Bob respectively. Alice and Bob reply with bits a, b respectively to the referee. The players win if and only if $a + b = xy$. Quite surprisingly, if Alice and Bob share quantum entanglement, they can strictly outperform any classical strategy where they are only allowed to use shared randomness. For more details on non-local games, we refer to the survey by Carlos Palazuelos and Thomas Vidick [PV16]. Now, we discuss how entanglement can be exploited for cryptographic purposes.

Even if quantum key distribution is unconditionally secure, it doesn't mean that implementations necessarily are. Indeed, if the implementation deviates from the specifications of the protocol, for instance because the hardware isn't ideal, then this opens the door to possible side-channel attacks [GFK$^+$06, VMH01]. This type of attack can damage the trust we have in those systems, even if unconditional security is claimed. In order to address this issue, one can turn to *device-independent quantum cryptography*, whose goal is to design protocols which can be implemented with untrusted devices. In [MY98], Mayers and Yao initiated this line of work by "self-testing" quantum apparatus, where one can check the quantumness of a device just from the input-output statistics. The key idea behind checking the quantumness of two devices is to use a Bell inequality or a non-local game. If the devices achieve a sufficient violation of a Bell inequality, then we can infer some properties about them. Further extending the concept introduced in [MY98], Acín *et all* proposed a fully device independent QKD protocol [ABG$^+$07]. In device-independent quantum key distribution, usually, we make a no communication assumption between the adversary and the quantum devices. Under this assumption, Vazirani and Vidick in [VV14], gave the first general proof for a device-independent quantum key

distribution scheme. Current research in this area aims to propose more practical device-independent QKD schemes that retain their functionality at realistic levels of noise.

4.1 Quantum cryptography beyond QKD

After the successful design of information theoretically secure QKD, quantum cryptography expanded to other branches of cryptography. Here, we primarily discuss *bit commitment* and *position-based quantum cryptography*. Bit commitment is an important primitive used to design more sophisticated primitives. For example, it has been shown that one can construct a secure quantum oblivious transfer scheme by using a secure quantum bit commitment scheme as a building block [Yao95, DFL$^+$09, BBCS91, Unr10] whereas Kilian [Kil88] showed that, in classical cryptography, oblivious transfer can be used to implement secure two-party computations. Moreover, if there is a secure oblivious transfer protocol, then it is possible to design a secure bit commitment protocol from it. Therefore, this chain of arguments suggests that quantum bit commitment alone is sufficient for implementing secure two-party computations, thus solving a long-standing problem in cryptography. Knowing that a perfectly secure classical bit-commitment protocol is impossible to design [BOGKW88], there was a considerable effort in the community to design a perfectly secure quantum bit commitment [BB84, BC91, BCJL93]. It started with the seminal work by Bennett and Brassard [BB84], where they designed a bit-commitment protocol using a coin-tossing protocol. However, security wasn't guaranteed if one party deviates from the protocol. Later in [BC91], Brassard and Crépeau proposed another quantum bit commitment protocol, trying to overcome this issue. However, it remained vulnerable against an adversary who can perform *measurement* on multiple quantum particles. Later, a protocol of Brassard *et al.* [BCJL93] was thought to be secure, but this claim turned out to be wrong, due to a lack of a proper security definition.

Finally, in 1997, the work of Mayers [May97] and Lo and Chau [LC97] put an end to this line of research by showing that quantum bit commitment is impossible to achieve with perfect information theoretic security. Let us briefly explain the intuition behind the impossibility result in classical setting. In the protocol, during the *commit* phase Alice needs to hide her commitment d. Thus, she sends a function $E(d)$ to Bob and $E(d)$ should be independent of d to guarantee the hiding property. This independence implies that in the reveal phase Alice can choose to reveal either $d = 0$ or $d = 1$ and Bob has to accept both. Hence, Alice can cheat by changing her commitment. In the quantum setting, the same proof structure can be applied. Instead of a function $E(d)$, Alice prepares a joint quantum state and sends a part of the state to Bob to hide her commitment, while keeping the other part. In order to hide her commitment perfectly, the state held by Bob should be indistinguishable for $d = 0$ or $d = 1$. This condition is sufficient for Alice to cheat. During the reveal phase, Alice sends the other part of the quantum state to Bob. From the joint state Bob can distinguish whether $d = 0$ or $d = 1$. However, according to Uhlmann's theorem [Uhl76] Alice can locally perform some quantum evolution operation(unitary operation) on her part of the quantum state in order to make the joint state corresponding to either $d = 0$ or $d = 1$. This implies that Alice can change her commitment in the reveal phase by applying some unitary evolution.

As discussed earlier, a perfectly secure bit commitment scheme can be constructed from a perfectly secure oblivious transfer protocol, so the no-go result by Mayers and Lo, Chau [May97, LC97] also proves the impossibility of having a perfectly secure oblivious transfer protocol. In the classical

setting, for all the bit commitment schemes, it is always possible for either Alice or Bob to cheat with certainty. However, in the quantum setting it was not clear what type of security trade-offs are allowed. In [Kit03], Chailloux and Kerenidis proved that either Alice or Bob can cheat any bit commitment scheme with probability at least $\frac{1}{\sqrt{2}}$. In [CK11], Chailloux and Kerenidis improved that lower bound and proved that the optimal cheating probability for any bit commitment scheme is approximately 0.739. For more details on quantum cryptography beyond quantum key distribution, we refer to a recent survey by Broadbent and Schaffner [BS16].

It seems that there are certain cryptographic tasks which cannot be designed with information theoretic security, even using quantum mechanics. So the question is whether we can use other physical theories to go beyond those impossibility results. In the next section we are going to discuss relativistic quantum cryptography, which provides a positive answer to this question. This is the main subject of this thesis.

4.2 Relativistic quantum cryptography

The impossibility result on bit commitment, proposed by Mayers and Lo, Chau raises the question: under which physical assumption is it possible to design a perfectly secure bit commitment protocol. In [BOGKW88] Ben-Or *et al.* showed that by allowing each party to consist of two spatially separated agents, and by making a non-communication assumption between those agents, one can design an information theoretically secure bit commitment protocol. Under this type of non-communication assumption, it is also possible to design a secure oblivious transfer protocol [NP00]. However, pragmatically, the non-communication assumption is quite strong. Is there a way to enforce such an assumption? In [Ken99], Adrien Kent, inspired by the special theory of relativity, used the fact that information cannot travel faster than the speed of light to answer this question positively. Under this assumption, he proposed a bit commitment scheme in which during the commit phase, one of Alice's agent sends her commitment to Bob. The revealing task is done by the other agent of Alice. The only drawback of Kent's protocol is that this second agent should reveal before receiving any information from the first agent after the commit phase. This implies that if the two agents are separated by a distance D, then the reveal phase needs to take place within a time period equal to $\frac{D}{c}$, where c is the speed of light in vacuum. This protocol needs to enforce very strict timing constraints and is therefore impractical. However, this result was interesting and opened a new direction of research called *relativistic cryptography*. Later on, researchers have tried to design several other primitives based on these relativistic constraints. Mostly, these constraints are used for designing multi-party cryptographic primitives, such as bit commitment (see for instance the thesis of Kaniewski [Kan15]), oblivious transfer [PG16], multi-party computation [Col09], etc.

One problem with most of relativistic cryptographic protocols is the requirement of having multiple spatially separated agents: it is difficult to implement and makes the security analysis very complicated. A natural approach to proving the security of such protocols is to reduce attack strategies to strategies for winning non-local games. In this thesis, we use variants of the CHSH game in order to study the binding property of a relativistic bit commitment protocol.

Similarly to bit-commitment, *position-based cryptography* is another two-party primitive. The main idea behind position-based cryptography is to use the geographical location of an object as an identity. Publicly this concept was first introduced by Chandran *et al.* [CGMO09]. However, in

2002, under the name of quantum tagging Adrien Kent filed a patent on position-based cryptography [KMS11]. In Section 2 we gave an example of such a primitive. The security goals of cryptography, like *privacy*, *authenticity*, can also be defined in the realm of position-based cryptography. Among all those goals, position verification is the easiest one to achieve. Besides this, one can also achieve other security features using position verification schemes as a building block, which is why we mainly focus on the task of secure position verification in this thesis.

In the position verification task, a prover claims to be at a geographical position P and a set of remote verifiers collaborate with each other in order to verify the location of the prover. The question of secure positioning therefore involves designing a system which enables a prover to communicate back and forth with a group of verifiers and to give them an interactive proof of its geographic position. In the classical setting under the standard model, the task of secure position verification is impossible to achieve, even under computational assumptions [CGMO09]. However, to break any position verification protocol, a malicious prover needs to have more than one agent. Those multiple agents can collaborate together and fool the verifiers into believing that they are interacting with an honest prover at P. This negative result also rules out other interesting position-based cryptographic tasks. This no-go theorem in the classical setting leaves open the question of whether information theoretically secure position verification is possible or not in quantum setting. A considerable amount of effort was done in order to design such schemes [Mal10, KMS11, LL11]. Unfortunately, all of the proposals turned out to be insecure. In [BCF$^+$11], Buhrman *et al.* proposed a generic attack on any secure position verification scheme. Their attack was based on the technique called "instantaneous measurements of non-local variables", proposed by Vaidman [Vai03]. In the same paper Buhrman *et al.* also proved that if the adversaries don't have access to any quantum resource then secure position verification is possible. Their paper also leaves an interesting open question: is it possible to have a provably secure position verification scheme if the adversaries are allowed to share a limited amount of quantum resource? Indeed, the generic attack described in [BCF$^+$11] requires an amount of entanglement scaling doubly exponentially with the size of the input parameter. More recently, in [BK11, BFSS13], more efficient attacks were investigated, but the best generic attacks still require an exponential amount of entanglement. In chapter 3, we propose another type of attack, where the amount of required quantum resource not only depends the size of the input parameter but also on the circuit complexity of the quantum operation used in the protocol.

5 Outline of the thesis

Among several multi-party cryptographic primitives, this thesis focuses on position-based quantum cryptography and relativistic bit commitment protocols. While analysing the relativistic bit commitment protocols we also study the non-local games. This thesis therefore also contributes to better a understanding of non-local games.

Chapter 2 contains all the necessary background in quantum mechanics, non-local games, position-based cryptography and relativistic bit commitment.

In Chapter 3 we introduce the concept of position-based quantum cryptography in more detail and provide a small literature survey on this topic. We then present our attack based on the *Clifford hierarchy*. Finally, we provide a new practical position-based quantum cryptographic scheme and show the security of the protocol with respect to our proposed attack strategy as well as other existing attack strategies.

Chapter 4 focuses on non-local games. First, we give a brief introduction and a literature survey. Then we define and study different variants of CHSH-type non-local games, that will be relevant for the study of a relativistic bit commitment protocol.

Chapter 5 is divided into two parts. The first part studies the security of a classical multi-round relativistic bit commitment protocol introduced by Lunghi *et al.* [LKB$^+$15] against classical adversaries. The second part describes a robust version of that protocol for which we also establish security against classical adversaries.

In Chapter 6, we conclude the thesis by providing a brief summary and some interesting open problems both in the domain of position-based quantum cryptography and relativistic cryptography.

2 Preliminaries

In this chapter, we review relevant concepts from quantum information theory and cryptography that are used in this thesis. We first introduce the mathematical formalism of quantum mechanics: quantum states, time evolution, measurement. Then we discuss some interesting tools of quantum information theory, such as no-cloning theorem and quantum teleportation. We then move our discussion to cryptography, focusing on position-based cryptography and bit commitment. We conclude this chapter with a presentation of non-local games.

1 Preliminaries on quantum mechanics

Quantum mechanics is one of the most successful theories in physics, giving excellent predictions that have been experimentally confirmed with tremendous accuracy. In this section, we review the postulates of quantum mechanics. Please refer to Chapter 2 of [NC10] for further details.

Postulate 1: (Quantum State) A Hilbert space is associated to any isolated physical system and is called the *state space* of the system. The system is completely described by its state vector which is a unit vector in the system's state space.

Similarly to the concept of *bits* in classical information, the smallest possible information processing unit in quantum information is called *qubit*. It is an element of $\mathbb{C}^2$. It is written as,

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{2.1}$$

where $\alpha, \beta \in \mathbb{C}$ satisfy $|\alpha|^2 + |\beta|^2 = 1$ and $|0\rangle = \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right), |1\rangle = \left(\begin{smallmatrix}0\\1\end{smallmatrix}\right)$ are two basis vectors. In general any pure quantum state in a Q-dimensional Hilbert space $\mathcal{H}_Q \simeq \mathbb{C}^Q$ can be written as,

$$|\psi\rangle = \sum_{j=0}^{Q-1} \lambda_j\,|j\rangle\,, \tag{2.2}$$

where $\{|j\rangle\}_{j=0}^{Q-1}$ forms an orthonormal basis for $\mathcal{H}_Q$ and $\sum_j |\lambda_j|^2 = 1$.

Postulate 2: (Composite Quantum System) The state space of a composite physical system is the tensor product of the state spaces of the component physical systems.

For instance, the state space corresponding to a 2-qubit quantum state is $\mathbb{C}^2 \otimes \mathbb{C}^2$ and any such state $|\psi\rangle_{12}$ can be written as,

$$|\psi\rangle_{12} = \lambda_{0,0} |0\rangle |0\rangle + \lambda_{0,1} |0\rangle |1\rangle + \lambda_{1,0} |1\rangle |0\rangle + \lambda_{1,1} |1\rangle |1\rangle , \tag{2.3}$$

where $\lambda_{0,0}, \lambda_{0,1}, \lambda_{1,0}, \lambda_{1,1}$ are complex numbers satisfying $|\lambda_{0,0}|^2 + |\lambda_{0,1}|^2 + |\lambda_{1,0}|^2 + |\lambda_{1,1}|^2 = 1$, and where we write $|i\rangle|j\rangle$ instead of $|i\rangle \otimes |j\rangle$.

Postulate 3: (Unitary Evolution) The evolution of a *closed* quantum system is described by a unitary transformation. The state $|\psi_{t_1}\rangle$ at time t_1 is related to the state $|\psi_{t_2}\rangle$ at time t_2 through:

$$|\psi_{t_2}\rangle = U |\psi_{t_1}\rangle , \tag{2.4}$$

where U is an unitary operator.

Let us give some examples of the most commonly used unitary operators in quantum information.

(i) *Identity operator:* The single-qubit operator is simply the identity on $\mathbb{C}^2$ and its n-qubit generalisation is the identity $(\mathbb{C}^2)^{\otimes n}$.

(ii) *Pauli operators:* These single-qubit operators are defined as

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{2.5}$$

The group generated by the Pauli matrices with factors $\pm 1, \pm i$ is called the *Pauli group*. It is denoted by $\mathcal{P}_1$:

$$\mathcal{P}_1 = \{\pm I, \pm iI, \pm\sigma_x, \pm i\sigma_x \pm \sigma_y, \pm i\sigma_y, \pm\sigma_z, \pm i\sigma_z\}. \tag{2.6}$$

The n-qubit *Pauli group*, $\mathcal{P}_n$ is the group generated by the operators described above applied to any of n qubits in the tensor product Hilbert space $(\mathbb{C}^2)^{\otimes n}$.

(iii) *Hadamard operator:* This single-qubit operator is defined as follows,

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{2.7}$$

and its n-qubit generalization is $H^{\otimes n}$. Note that H satisfies $H^2 = I$.

(iv) *T-Gate:* This single-qubit operator is defined as follows,

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{pmatrix}. \tag{2.8}$$

(v) *Phase Gate:* This single-qubit operator is defined as follows,

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{2.9}$$

(vi) *CNOT Gate:* This is a two-qubit operator, defined as follows,

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \tag{2.10}$$

The CNOT gate is interesting because together with the family of single-qubit gates, it forms a universal set of gates, meaning that any unitary acting on n qubits can be decomposed as a product of such elementary gates. If one restricts the single-qubit gates to the Pauli operators, the T-gate, then combining them with the CNOT gate, one can approximate arbitrarily well any unitary acting on n qubits. This result is due to Solovay and Kitaev [NC10]. The approximation factor ε is related to the depth of the quantum circuit implementing the unitary according to the following theorem.

Theorem 2.1 (Solovay-Kitaev [NC10])**.** *If $\mathcal{G} \subseteq SU(Q)$ is a universal family of gates (where $SU(Q)$ is the special unitary group acting on $\mathbb{C}^Q$), if $\mathcal{G}$ is closed under inverse and generates a dense subset of $SU(Q)$, then for any $U \in SU(Q)$, $\varepsilon > 0$, there exist $U_{g_1}, U_{g_2}, \ldots, U_{g_l} \in \mathcal{G}$ such that $\|U - U_{g_1} U_{g_2} \ldots U_{g_l}\| \leqslant \varepsilon$ and $l = O\left(\log^c(1/\varepsilon)\right)$, where $c < 3$ is a positive constant.*

The fourth postulate gives a description of the measurement process.

Postulate 4: (Quantum Measurements) This process is described by a collection $\{M_m\}$ of *measurement operators*. These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability $p(m)$ that the result m occurs is given by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle, \tag{2.11}$$

and the state of the system after the measurement is

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{2.12}$$

The measurement operators satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I. \tag{2.13}$$

A measurement is called *projective* if the operators $\Pi_m = M_m^\dagger M_m$ are projectors, that is if $\Pi_m^2 = \Pi_m$. A property of such measurements is that performing the measurement again immediately after the first one yields the same result with probability 1.

Whenever one is not interested in the post-measurement state, the measurement process can be described more efficiently as a *Positive-Operator-Valued Measurement* (POVM), which is given by a set of nonnegative operators $\{E_m\}$ such that $\sum_m E_m = I$. As before, the index m is associated with the measurement outcome. If $|\psi\rangle$ is the quantum state being measured, then the probability of getting measurement outcome m is given by

$$p(m) = \langle\psi| E_m |\psi\rangle. \tag{2.14}$$

Mixed states

Whenever the complete information about a state is not available, for instance if a quantum system is in one of the states $\{|\psi_i\rangle\}_{1\leqslant i\leqslant k}$ with respective probability p_i, then one can represent the quantum system as a *mixed state*. Mathematically, it is described by a *density operator*, that is a positive semidefinite operator with unit trace, given by

$$\rho = \sum_i p_i \left|\psi_i\right\rangle \left\langle\psi_i\right| . \tag{2.15}$$

Note that a quantum state ρ is pure if it has rank 1, or equivalently if $\mathrm{Tr}[\rho^2] = 1$.

The postulates of Quantum Mechanics can be adapted to accommodate for mixed states. If the evolution of a closed quantum is described by a unitary evolution U between times t_1 and t_2, then the corresponding density operators ρ_{t_1} and ρ_{t_2} are related through:

$$\rho_{t_2} = U\rho_{t_1}U^\dagger, \tag{2.16}$$

where $U^\dagger$ is the Hermitian conjugate of U.

Measurements can also be described in this language. If we perform a measurement on a density operator ρ defined by measurement operators $\{M_m\}_m$, then the probability of obtaining outcome m is given by

$$p(m) = \mathrm{Tr}(M_m^\dagger M_m \rho) \tag{2.17}$$

and the post-measurement state is

$$\frac{M_m \rho M_m^\dagger}{\mathrm{Tr}(M_m \rho M_m^\dagger)}. \tag{2.18}$$

Density operators are also useful to describe subsystems of composite systems. This description is provided by the *reduced density operator*. Suppose we have a bipartite physical system in the state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, then the reduced density operator for system A is defined as

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}), \tag{2.19}$$

where Tr_B is the *partial trace* over system B. This is the linear map satisfying

$$\mathrm{Tr}_B(\left|a_1\right\rangle \left\langle a_2\right| \otimes \left|b_1\right\rangle \left\langle b_2\right|) = \left|a_1\right\rangle \left\langle a_2\right| \mathrm{Tr}(\left|b_1\right\rangle \left\langle b_2\right|), \tag{2.20}$$

where $\left|a_1\right\rangle, \left|a_2\right\rangle$ are any two elements of $\mathcal{H}_A$ and $\left|b_1\right\rangle, \left|b_2\right\rangle \in \mathcal{H}_B$. For a detailed explanation we refer to Chapter 2 of [NC10].

Entanglement

Entanglement is one of the defining features of quantum mechanics, capturing a form of strong correlations between quantum systems. A (pure) product state on $\mathcal{H}_A \otimes \mathcal{H}_B$ is a state of the form $|\phi\rangle \otimes |\psi\rangle$ with $|\phi\rangle \in \mathcal{H}_A$ and $|\psi\rangle \in \mathcal{H}_B$. We say that a density operator ρ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ is *separable*

if it can be written as a convex combination of *product states*, that is if there exist families of states $\{|\phi_i\rangle\}$ in $\mathcal{H}_A$ and $\{|\psi_i\rangle\}$ in $\mathcal{H}_B$, as well as a probability distribution $\{p_i\}$ such that

$$\rho = \sum_i p_i \left|\psi_i\right\rangle_A \left\langle\psi_i\right| \otimes \left|\phi_i\right\rangle_B \left\langle\phi_i\right| . \tag{2.21}$$

Operationally, mixed states are exactly those which can be prepared by means of *local operations* and *classical communication* (LOCC).

A state is called *entangled* if it is not separable. In particular, all the pure states which are not product states are entangled. This is for instance the case of the well-known EPR 2-qubit state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. This state is also known as the *maximally entangled state*. Since entanglement cannot be created from LOCC, it is a *resource* that can be exploited to perform for tasks which cannot be achieved with classical correlations. Even though entanglement cannot be used to carry information, manipulation of entangled states can help to increase the efficiency of many information processing tasks in the context of non-local games, communication complexity or quantum cryptography. For more details on quantum entanglement please refer to [HHHH09].

Fidelity

Closeness between quantum states can be measured with various distance metrics. In this thesis, we will only use the concept of *fidelity*.

Definition 2.1. *The* fidelity *between two density operators ρ and σ is defined to be*

$$F(\rho, \sigma) = \mathrm{Tr}\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}. \tag{2.22}$$

It satisfies $F \in [0, 1]$ and that $F(\rho, \rho) = 1$ for any state ρ. If the states are pure, then the fidelity reduces to

$$F(|\phi\rangle\langle\phi|, |\psi\rangle\langle\psi|) = |\langle\phi|\psi\rangle|.$$

Note that the fidelity is not a distance since it doesn't satisfy the triangle inequality. For more details on distance measures, we refer to Chapter 9 of the book [NC10].

2 Useful concepts of quantum information

This section focuses on important concepts of quantum information, which will be useful for quantum cryptography.

2.1 No-cloning principle

One of the most counterintuitive results in quantum information is *no-cloning principle*, discovered by Wootters and Zurek [WZ82]. This principle says that it is impossible to build a universal copying machine which takes an arbitrary quantum state $|\psi\rangle$ as input and outputs two identical copies of $|\psi\rangle$.

Theorem 2.2. *Assume there is a unitary operator U_{clone} that can prepare two copies of an arbitrary input state, i.e,*

$$U_{\text{clone}} |\phi\rangle \otimes |0\rangle = |\phi\rangle \otimes |\phi\rangle$$
$$U_{\text{clone}} |\psi\rangle \otimes |0\rangle = |\psi\rangle \otimes |\psi\rangle .$$

Then $\langle\psi|\phi\rangle$ is either 0 or 1.

Proof. Consider the inner product,

$$\begin{aligned}
\langle\phi|\psi\rangle &= (\langle\phi| \otimes \langle 0|)(|\psi\rangle \otimes |0\rangle) \\
&= (\langle\phi| \otimes \langle 0| U_{\text{clone}}^{\dagger})(U_{\text{clone}} |\psi\rangle \otimes |0\rangle) && \text{by unitarity of } U_{\text{clone}} \\
&= (\langle\phi| \otimes \langle\phi|)(|\psi\rangle \otimes |\psi\rangle) && \text{by definition of } U_{\text{clone}} \\
&= \langle\phi|\psi\rangle^2 .
\end{aligned}$$

This implies that $\langle\phi|\psi\rangle$ is either 0 or 1. □

The significance of Theorem 2.2 is that it is only possible to clone families of orthogonal states, which corresponds to copying classical information.

2.2 Quantum teleportation

Quantum teleportation is a physical process by which quantum information can be transferred from one location to another with the help of only entanglement, local operations and classical communication. This phenomenon was first discovered by Bennett *et al.* [BBC$^+$93]. In quantum teleportation, one party, say Alice, wants to transfer a quantum state $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ to another party, say Bob, without sending any physical quantum bit. Alice and Bob need to share an EPR pair, $|\Phi_+\rangle = \frac{1}{\sqrt{2}} |00\rangle_{AB} + \frac{1}{\sqrt{2}} |11\rangle_{AB}$, where Alice holds the first qubit and Bob the second one. The teleportation procedure is as follows:

- Alice performs the *Bell measurement* $\{|\Phi_+\rangle\langle\Phi_+|, |\Phi_-\rangle\langle\Phi_-|, |\Psi_+\rangle\langle\Psi_+|, |\Psi_-\rangle\langle\Psi_-|\}$ on her two qubits, $|\psi\rangle$ and her share of the EPR pair, where the Bell basis is given by

$$|\Phi_\pm\rangle = \frac{1}{\sqrt{2}} |00\rangle_{AB} \pm \frac{1}{\sqrt{2}} |11\rangle_{AB} , \quad |\Psi_\pm\rangle = \frac{1}{\sqrt{2}} |01\rangle_{AB} \pm \frac{1}{\sqrt{2}} |10\rangle_{AB} .$$

- She communicates the classical outcome of the measurement (two classical bits) to Bob, who performs the following correction to his share of the EPR pair: he applies σ_x for the measurement outcome $|\Psi_+\rangle$, σ_y for $|\Psi_-\rangle$, or σ_z for $|\Phi_-\rangle$.

Let us show that he then obtains the desired state $|\psi\rangle$. The initial state formed by $|\psi\rangle$ and the EPR pair reads:

$$\begin{aligned}|\psi\rangle_A \otimes |\Phi_+\rangle_{AB} &= \frac{\alpha}{\sqrt{2}}|000\rangle_{AB} + \frac{\alpha}{\sqrt{2}}|011\rangle_{AB} + \frac{\beta}{\sqrt{2}}|100\rangle_{AB} + \frac{\beta}{\sqrt{2}}|111\rangle_{AB} \\ &= |\Phi_+\rangle_A \otimes (\alpha|0\rangle + \beta|1\rangle) + |\Phi_-\rangle_A \otimes (\alpha|0\rangle - \beta|1\rangle) \\ &+ |\Psi_+\rangle_A \otimes (\alpha|1\rangle + \beta|0\rangle) + |\Psi_-\rangle_A \otimes (\alpha|1\rangle - \beta|0\rangle) \\ &= |\Phi_+\rangle_A \otimes |\psi\rangle + |\Phi_-\rangle_A \otimes \sigma_z|\psi\rangle + |\Psi_+\rangle_A \otimes \sigma_x|\psi\rangle + |\Psi_-\rangle_A \otimes i\sigma_y|\psi\rangle\,, \quad (2.23)\end{aligned}$$

It is clear that applying the specified correction yields the state $|\psi\rangle$ for Bob's system.

2.3 Port-based teleportation

One drawback of the standard teleportation scheme discussed above is that Bob needs to apply a nontrivial correction to his state in order to complete the process. For some applications, one would prefer procedures where Bob's correction is simpler, for instance, tracing out some quantum systems. This is the point of the *port-based teleportation* scheme introduced in [IH08]. In this procedure, Alice and Bob share many EPR pairs, which are called *ports*. To perform the teleportation, Alice performs a measurement on the state she wants to teleport and her shares of the EPR pairs. The measurement outcome corresponds to one of the ports. In order to complete the teleportation, she tells Bob her measurement result and Bob simply discards the qubits that do not correspond to the specified port. The two new features of this scheme compared to standard teleportation are that Bob's correction is much simpler, and that the teleportation is only approximate. The fidelity between the input and output state depends on the number of shared EPR pairs and tends to one when this number tends to infinity.

In Chapter 3 of this thesis, we will see how port-based teleportation can be used to attack some position-verification schemes. For completeness, let us describe the port-based teleportation procedure more precisely.

- Alice and Bob share a maximally entangled state over n qubits (corresponding to N EPR pairs): $\frac{1}{2^{n/2}}\sum_{x\in\{0,1\}^n}|x\rangle|x\rangle = |\Phi_+\rangle_{\mathcal{A}_1\mathcal{B}_1} \otimes \cdots \otimes |\Phi_+\rangle_{\mathcal{A}_N\mathcal{B}_N}$.
- In order to teleport the input state $|\psi\rangle$, Alice performs the so-called *pretty good measurement* on $|\psi\rangle$ and her N ports. This POVM $\{E_i\}_{1\leqslant i\leqslant N}$. The optimal measurement operator is called *pretty good measurement* [IH08]. It is defined as follows,

  $$E_i = E^{-1/2}\sigma^{(i)}E^{1/2}$$

  with $\sigma^{(i)} = I_{\text{input}} \otimes I_{\mathcal{A}_1\mathcal{B}_1} \otimes \cdots \otimes I_{\mathcal{A}_{i-1}\mathcal{B}_{i-1}} \otimes |\Phi_+\rangle\langle\Phi_+|_{\mathcal{A}_i\mathcal{B}_i} \otimes I_{\mathcal{A}_{i+1}\mathcal{B}_{i+1}} \otimes \cdots \otimes I_{\mathcal{A}_i\mathcal{B}_i}$ and $E = \sum_{i=1}^N \sigma^{(i)}$. This is clear that this forms a legitimate POVM since the operators are positive semidefinite and satisfy

  $$\sum_{i=1}^N E_i = E^{-1/2}\left(\sum_{i=1}^N \sigma^{(i)}\right)E^{1/2} = I.$$

- Alice sends her measurement outcome i to Bob who simply discards all his ports except for the i^{th} one.

The performance of the scheme depends on the dimension on the input state and the number of shared EPR pairs. The following lower bound was established in [IH09].

Lemma 2.3 ([IH09])**.** *The fidelity F between Alice's initial state and Bob's final state using port-based teleportation depends on both the number N of EPR pairs consumed in the scheme and the dimension d of Alice's state through*

$$F \geqslant 1 - \frac{d^2}{N}. \tag{2.24}$$

2.4 The Clifford hierarchy

In this thesis, we will consider position-verification schemes where the honest parties need to implement some given unitaries on n-qubit states. We will find attack strategies whose complexity will depend on the difficulty to implement the unitaries, in a fault-tolerant manner. This difficulty can be quantified thanks to a hierarchy of unitaries called the *Clifford hierarchy* which was introduced in [GC99]. More precisely, the first level $C_1(n)$ of the Clifford hierarchy corresponds to the Pauli group on n qubits: $C_1(n) = \mathcal{P}_n$. Then, the upper levels are defined recursively through

$$C_{k+1}(n) = \left\{ U \text{ such that } U\sigma U^\dagger \in C_k(n) \quad \forall \sigma \in \mathcal{P}_n \right\}.$$

In words, a unitary U belongs to level $k+1$ of the hierarchy if conjugating any Pauli matrix with U yields a matrix in the k^{th} level of the hierarchy. When n is clear from context, we simply write C_k instead of $C_k(n)$ for the k^{th} level of the Clifford hierarchy for n-qubit gates. It should be noted that the first two levels of the hierarchy are groups, namely the Pauli and the Clifford groups, whereas none of the higher levels are groups.

The gates from C_1 and C_2 can be "easily" implemented fault tolerantly [Got97]. However, it is well-known that they do not form a universal set for quantum computation. One therefore requires at least one gate from C_3 to obtain a universal set of gates. Not surprisingly, gates from C_3 or higher levels are usually much harder to implement fault-tolerantly.

3 Position-based quantum cryptography

We now turn to cryptography. This section and the next one explain the concept and models of PBQC and relativistic bit commitment. Recall that the goal of position-based quantum cryptography is to perform tasks using geographical locations as a credential. It was first introduced by Chandran *et al.* [CGMO09]. Position verification is a sub-domain of position-based cryptography, where a prover P tries to convince a set of verifiers $V_1, \ldots, V_k$, spread around several geographical locations, that P is at a location *Pos*. Note that similar tasks have been considered earlier in the literature under the name of "Distance-bounding", for instance in [BC93], and rely on the *No Superluminal Signalling(NSS)* principle that says that no information carrier can travel faster than the speed of light. Informally, the

idea to check the position of a prover is to send them challenges and measure when the response is received. For instance, if the response is received with time $2t$ after the challenge was sent, then the verifier knows that the prover was a most at a distance ct, where c is the speed of light in the vacuum. This thesis is mostly concerned with the position verification task in a single dimension, which will require two verifiers. In this thesis, we make the following simplifying assumptions:

(i) All the communication takes place at speed of light.

(ii) Computation time is negligible compared to communication time.

A typical verification task consists of three stages. In the *preparation phase*, the verifiers agree on a strategy, including shared randomness. The prover sends his location to the verifiers. In the *execution phase*, the verifiers send challenges to the prover who solves the challenge and sends back the answer to the verifiers. Finally, in the *verification phase*, the verifiers come together (or communicate on an authenticated channel) and check that the answer is correct and that it arrived in the required delay. They accept the location of the prover if it's the case and reject otherwise.

In the classical domain, all the protocols are of the following form (see Figure 2.1):

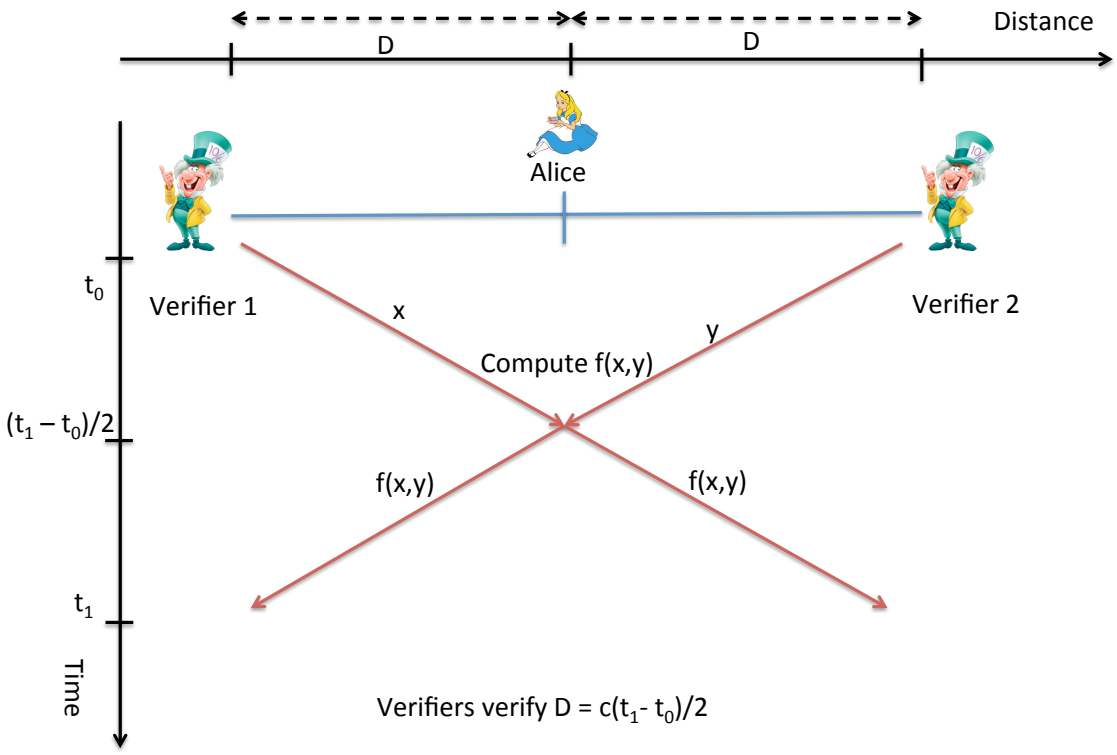

Figure 2.1: Pictorial view of the position verification task in the classical domain.

(i) *Preparation Phase:* The challenge takes the form of a public function $f : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. Verifier$_1$ and Verifier$_2$ choose respective inputs x and y from $\{0,1\}^n$. Let us denote by $2D$ the distance between the verifiers and assume that the prover sits at the middle of the two verifiers.

(ii) *Execution Phase:* At time t_0, Verifier$_1$ and Verifier$_2$ send x and y respectively to P, who receives both inputs at the same time. He computes $z = f(x,y)$ and sends z back to the verifiers. Let t_1 and t_2 be the times at which the verifiers receive the answer.

(iii) *Verification Phase:* The verifiers check whether $z = f(x,y)$ and whether $t_1 = t_2 = t_0 + 2\frac{D}{c}$. They accept if it is the case.

This protocol is secure as long as there is only one prover. However a coalition between two dishonest provers (say Cheater$_1$ and Cheater$_2$) can easily attack this protocol as follows,

(i) Cheater$_1$ is positioned at distance $\frac{D}{2}$ from Verifier$_1$ and Cheater$_2$ at distance $\frac{D}{2}$ from Verifier$_2$. They claim that their position is at distance D from both of the verifiers. In the execution phase, Cheater$_1$ receives x from Verifier$_1$ and Cheater$_2$ receives y from Verifier$_2$ at time $t_0 + \frac{D}{2c}$.

(ii) The cheater copy this information and forward the value of x and y to each other. At time $t_0 + \frac{3D}{2c}$ they both know x and y.

(iii) Both cheaters compute $f(x,y)$ and send this value to the verifiers, who both receive it at time $t_0 + \frac{2D}{c}$. The verifiers therefore incorrectly accept the claimed position.

We show this attack strategy in Figure 2.2. It seems that the attack strategy works simply because the cheaters can copy the information x and y. In particular, if one could come up with a protocol where such information cannot be copied, the attack would not work anymore. It is tempting to use the *no-cloning principle* to argue that a quantum version of this scheme should resist this kind of attack. Let us therefore define a quantum version of the position-verification protocol (see Figure 2.3):

(i) *Preparation Phase:* The challenge takes the form of a public set of measurement bases $\{M_x\}_{0 \leqslant x \leqslant 2^n}$ and a public set of quantum states $|\psi_x\rangle$, such that one can't recover x from the knowledge of either M_x nor $|\psi_x\rangle$. The measurement operators are chosen in such a manner so that measuring $|\psi_x\rangle$ with M_x basis returns x. The verifiers then agree on a secret value of x. As before, we assume that the claimed position is at distance D of both verifiers.

(ii) *Execution Phase:* Verifier$_1$ and Verifier$_2$ send respectively $|\psi_x\rangle$ and a classical description of M_x to the prover at time t_0. The prover measures $|\psi_x\rangle$ in the M_x basis and sends the measurement outcome z back to verifiers. The verifiers receive the answers at times t_1 and t_2.

(iii) *Verification Phase:* Both check whether z equals x or not, and check that $t_1 = t_2 = t_0 + \frac{2D}{c}$. If these conditions are satisfied then they accept the position of prover.

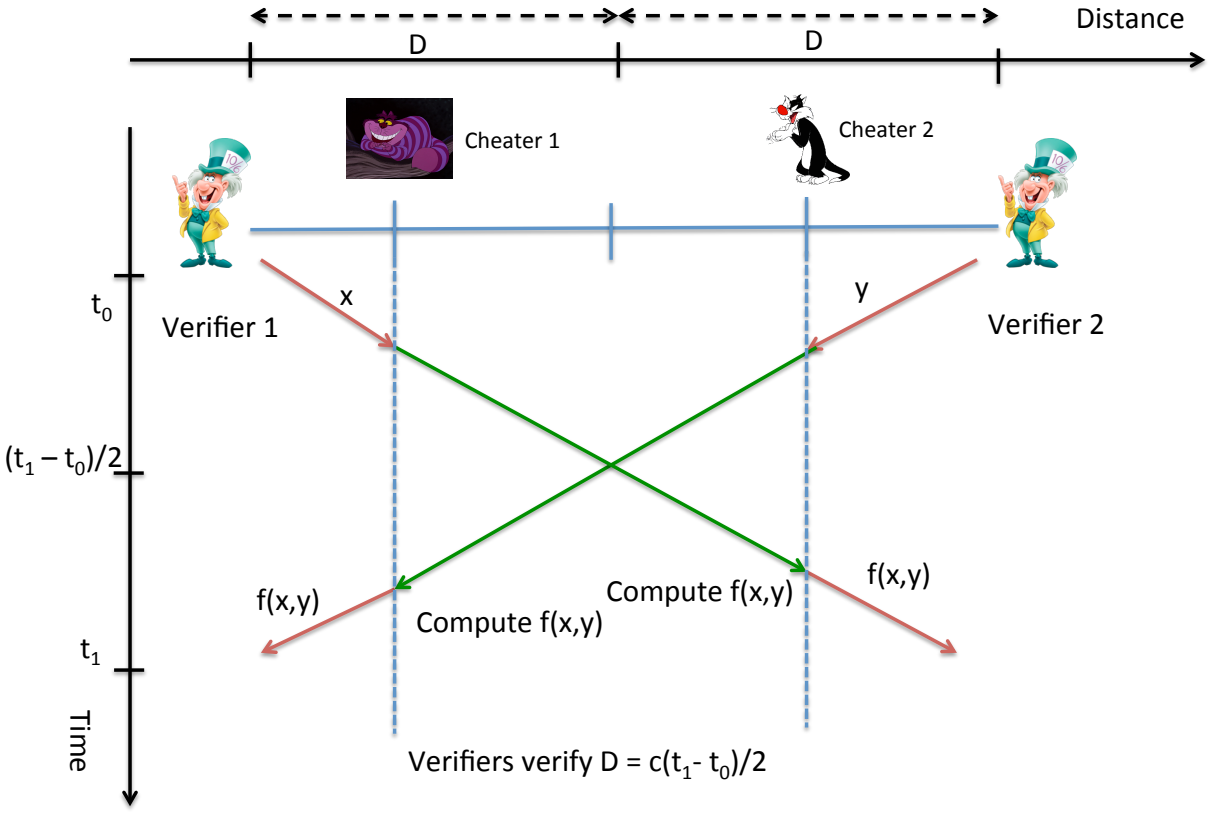

Figure 2.2: Attack strategy against the classical position verification scheme.

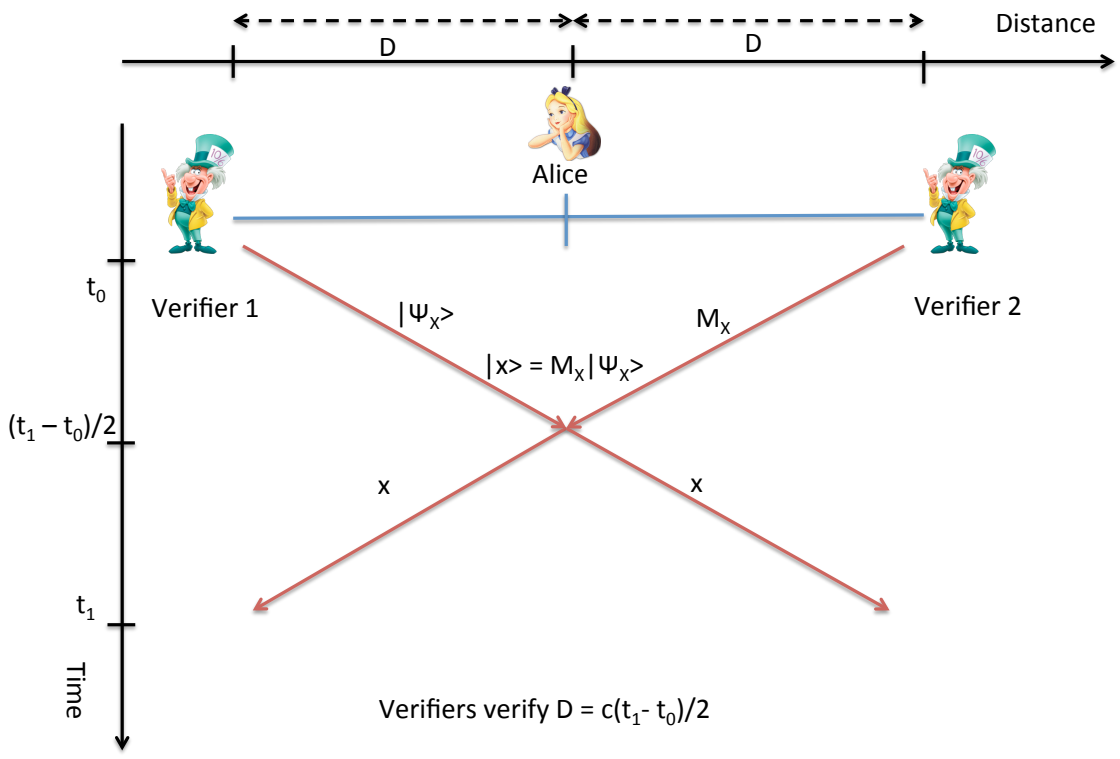

Figure 2.3: Pictorial view of the position verification task in the quantum domain.

Intuitively the attack strategy that was working against the classical scheme isn't available anymore. Indeed, Cheater$_1$ holds $|\psi_x\rangle$ but doesn't know how to measure it, and he cannot copy this state to send it to his accomplice. And indeed, Buhrman *et al.* proved that such a protocol is secure as long as the coalition of attackers doesn't share any quantum entanglement [BCF$^+$11]. However, perhaps surprisingly, if the cheaters share entanglement then they can break this scheme by performing a nonlocal measurement of the state $|\psi_x\rangle$ in the basis M_x, with only a single round of communication. In fact, with a sufficient amount of entanglement, there always exists a perfect cheating strategy against any quantum position-verification protocol, for instance using port-based teleportation [BCF$^+$11, BFSS13, BK11].

4 Bit commitment

A bit commitment is a cryptographic protocol between two players Alice (the committer), and Bob (the receiver) which do not trust each other. A bit commitment protocol has 2 main phases : a *commit phase* and a *open phase*. During the commit phase, Alice commits to a bit d. We say that the protocol is *hiding* if at the end of the commit phase, Bob has no information about d. During the open phase,

Alice reveals d to Bob. Bob wants to make sure that Alice didn't change her mind when revealing, this is the binding property.

A commitment scheme $\Pi = (COMM, OPEN)$ is the description of the protocol followed by the honest parties during both the commit and the open phases. All protocols that we will consider will be perfectly hiding and we will only be interested in the binding property. Therefore, we only consider the case of a cheating Alice, which will be described through her cheating strategy $Str^* = (Comm^*, Open^*)$ in both phases of the protocol. The binding property that we will use in this thesis is the standard sum-property, that was also used in previous work regarding relativistic bit commitment [CSST11, LKB$^+$15, FF16, CCL15].

Definition 2.2 (Sum-binding)**.** *We say that a bit commitment protocol Π is* ε-sum-binding *if*

$$\forall\, \mathrm{Comm}^*,\ \sum_{d=0}^{1} \max_{\mathrm{Open}^*} \left(\Pr[\textit{Alice successfully reveals } d \mid (\mathrm{Comm}^*, \mathrm{Open}^*)]\right) \leqslant 1 + \varepsilon.$$

Note that there are stronger notions of binding for quantum bit commitment [DFR$^+$07, Unr10]), which allow to compose these protocols in more general cryptosystems.

5 Non-local games

In [CHTW04], Cleve *et al.* first introduced the notion of non-local game to provide a mathematical framework for understanding quantum entanglement and non-locality. They have a wide range of applications: they can serve to quantify non-locality [BCP$^+$14], to study multi-prover interactive proof systems [CSST11, KRR14, CL17] and are also extremely useful in the context of quantum cryptography, for instance in device-independent cryptography [HRW10, VV14] or device-independent random amplification and expansion [Col06], etc. In this thesis, we are interested in such games because they play an important role in the context of relativistic cryptography. Indeed, many attack strategies can be reduced to such nom-local games and establishing upper bounds on the winning probability of such games allows us to prove the security of some relativistic cryptographic protocols [LKB$^+$15, CCL15, FF16, CCL16, CL17].

Formally, a two-player single-round non-local game $G = (\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{B}, \pi, \mathcal{V})$ is specified by four finite sets $\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{B}$, a joint probability distribution $\pi : \mathbf{X} \times \mathbf{Y} \to [0, 1]$ and a map (also called *predicate*) $\mathcal{V} : \mathbf{X} \times \mathbf{Y} \times \mathbf{A} \times \mathbf{B} \to \{0, 1\}$. In this thesis, the players of a two-player games are called Alice (or Adeline) and Bob (or Bastian). The game goes as follows:

(i) The *referee* picks $(x, y) \in \mathbf{X} \times \mathbf{Y}$ following the joint probability distribution π and sends x, y to *Alice* and *Bob* respectively.

(ii) Upon receiving x and y, Alice and Bob sends back $a \in \mathbf{A}$ and $b \in \mathbf{B}$ respectively to the referee.

(iii) Finally the *referee* checks whether the players win, that is whether $\mathcal{V}(x, y, a, b) = 1$.

One important quantity associated to a non-local game is its *value*, that is the maximum winning probability. In fact, one can define the classical value $\omega(G)$ and the quantum value $\omega^*(G)$ of the

game, depending on whether Alice and Bob apply a classical or a quantum strategy: in the former case, the players are allowed to exploit shared randomness, while in the latter, they are allowed to perform measurements on a shared quantum state.

5.1 Classical strategies

The most general classical strategy the players can follow is a randomised one. The players can co-operate each other with shared randomness as well as private randomness. However the winning probability with this type of randomised strategy can be written as a convex combination of winning probabilities with deterministic strategies. It is therefore sufficient to consider the deterministic strategy which corresponds to the maximum winning probability [CHTW04].

A deterministic classical strategy can be expressed as deterministic functions of the questions, asked by referee. The players use functions $f : \mathbf{X} \to \mathbf{A}$ for Alice and $g : \mathbf{Y} \to \mathbf{B}$ for Bob, in order to compute their answers. Their winning probability for the non-local game $G = (\mathbf{X}, \mathbf{Y}, \mathbf{A}, \mathbf{B}, \pi, \mathcal{V})$ is given by

$$\Pr_{x,y\sim\pi}[\mathcal{V}(f(x), g(y), x, y) = 1] = \mathbb{E}_{x,y\sim\pi}[\mathcal{V}(f(x), g(y), x, y)], \tag{2.25}$$

where $x, y \sim \pi$ means that (x, y) is drawn from the distribution π. The classical value of the game, denoted as $\omega(G)$ is then defined as

$$\omega(G) = \max_{f,g} \mathbb{E}_{x,y\sim\pi}[\mathcal{V}(f(x), g(y), x, y)]. \tag{2.26}$$

5.2 Quantum strategies

In contrast to classical strategies, in the quantum setting, the players are allowed to share an entangled state. Let $|\psi\rangle$ be the bipartite quantum state shared by Alice and Bob and let $\{\mathcal{M}^x\}_{x\in\mathbf{X}}$, $\{\mathcal{N}^y\}_{y\in\mathbf{Y}}$ denote the sets of measurements used by the players. Upon receiving x, Alice performs the local measurement $\mathcal{M}^x = \{M_a^x\}_{a\in\mathbf{A}}$ on her part of the shared entangled state $|\psi\rangle$ and uses the outcome a as her answer. Similarly upon receiving input y, Bob performs the local measurement $\mathcal{N}^y = \{N_b^y\}_{b\in\mathbf{B}}$ on his part of $|\psi\rangle$ and sends back the outcome b to the referee. The probability of observing a, b as output is given by

$$\langle\psi| M_a^x \otimes N_b^y |\psi\rangle .$$

The average winning probability is therefore given by

$$\Pr_{x,y,a,b}[\mathcal{V}(a, b, x, y) = 1] = \mathbb{E}_{x,y\sim\pi}\left[\sum_{a\in\mathbf{A}}\sum_{b\in\mathbf{B}} \langle\psi| M_a^x \otimes N_b^y |\psi\rangle \mathcal{V}(a, b, x, y)\right]. \tag{2.27}$$

The quantum value of the game, denoted by $\omega^*(G)$, is defined as the supremum over all possible sets of measurement operators $\{M_a^x\}_{x\in\mathbf{X},a\in\mathbf{A}}, \{N_b^y\}_{y\in\mathbf{Y},b\in\mathbf{B}}$.

$$\omega^*(G) = \sup_{|\Psi\rangle,\{\mathcal{M}^x\},\{\mathcal{N}^y\}} \mathbb{E}_{x,y\sim\pi}\left[\sum_{a\in\mathbf{A}}\sum_{b\in\mathbf{B}} \langle\psi| M_a^x \otimes N_b^y |\psi\rangle \mathcal{V}(a, b, x, y)\right]. \tag{2.28}$$

Note that we have a supremum here instead of a maximum because the set of states and measurements one optimizes over is infinite.

5.3 The CHSH game

The most well-known non-local game is the CHSH game, named after its inventors Clauser, Horne, Shimony and Holt [CHSH69]. It is the two-player game with $\mathbf{X} = \mathbf{Y} = \mathbf{A} = \mathbf{B} = \{0, 1\}$, with π equal to the uniform distribution over $\{0, 1\} \times \{0, 1\}$, that is, $\Pr[x = 0] = \Pr[x = 1] = \Pr[y = 0] = \Pr[y = 1] = \frac{1}{2}$. The predicates $\mathcal{V}$ evaluates to 1 if and only if $a \oplus b = xy$: the players win the game if the XOR of their output is equal to the product of the inputs.

Let us first consider the classical value of the game and denote by a_x and b_y the answers Alice and Bob give for inputs x and y. In order to win the game, these should satisfy the following system of equations:

$$\begin{aligned} a_0 \oplus b_0 &= 0 \\ a_0 \oplus b_1 &= 0 \\ a_1 \oplus b_0 &= 0 \\ a_1 \oplus b_1 &= 1. \end{aligned}$$

It is clear that this system of equations is overdetermined and that only three of the equations can be satisfied simultaneously. Therefore, the classical value of this game cannot be greater than $\frac{3}{4}$. This value is achieved with the trivial strategy where Alice and Bob always output 0. This proves that $\omega(CHSH) = \frac{3}{4}$.

Let us now consider quantum strategies. Cirel'son proved that $\omega^*(CHSH) = \cos^2(\pi/8) \approx 0.85$, which strictly beats the classical value [Cir80]. Let us describe a strategy that achieves this winning probability. For a given angle $\theta \in [0, 2\pi)$, we define

$$\begin{aligned} |\phi_0(\theta)\rangle &= \cos(\theta)\,|0\rangle + \sin(\theta)\,|1\rangle \\ |\phi_1(\theta)\rangle &= -\sin(\theta)\,|0\rangle + \cos(\theta)\,|1\rangle\,. \end{aligned}$$

Then Alice and Bob perform the following measurements on a shared EPR pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

- If Alice receives $x = 0$ then she measures her part of the EPR pair with

  $$\mathcal{M}^0 = \{|\phi_0(0)\rangle\langle\phi_0(0)|\,, |\phi_1(0)\rangle\langle\phi_1(0)|\}$$

  . Otherwise, she measures her state with

  $$\mathcal{M}^1 = \{|\phi_0(\pi/4)\rangle\langle\phi_0(\pi/4)|\,, |\phi_1(\pi/4)\rangle\langle\phi_1(\pi/4)|\}.$$

- Similarly, for $y = 0$, Bob measures his part of the EPR pair with

  $$\mathcal{N}^0 = \{|\phi_0(\pi/8)\rangle\langle\phi_0(\pi/8|\,, |\phi_1(\pi/8)\rangle\langle\phi_1(\pi/8)|\}.$$

  Otherwise he measures it with

  $$\mathcal{N}1 = \{|\phi_0(-\pi/8)\rangle\langle\phi_0(-\pi/8)|\,, |\phi_1(-\pi/8\rangle\langle\phi_1(-\pi/8)|\}.$$

By substituting the value of M_a^x and N_b^y in equation (2.25), one can check that the winning probability is indeed $\cos^2(\pi/8)$.

3 Position-based quantum cryptography

1 Introduction

Position-based cryptography studies how to design cryptographic primitives using someone's location at a given time as a credential. There are several primitives in position-based cryptography such as position-based authentication or position-based encryption. This chapter studies the task of position verification. The goal of position verification is to check that a certain party, called the prover, holds a given position in space-time. Such a protocol typically goes as follows: a set of verifiers coordinate and send some challenges to the prover, and it is expected that only someone sitting in the supposed position of the prover can successfully pass the challenge. In this chapter, we focus on designing and analyzing position verification schemes in the quantum domain.

Position verification protocols have been studied in the standard classical model and it was proven that no such protocol can have information theoretic security, or even computational security[CGMO09]. More precisely, it is always possible for a *coalition* of adversaries to convince the verifiers, even if none of the adversaries sits in the spatio-temporal region where the prover is supposed to be. However, note that the same paper gives secure constructions of this task in the Bounded-Retrieval Model. Another possible way-out of this no-go theorem would be to consider the quantum setting. Indeed, several classical tasks which are known to be impossible in the classical domain can be achieved in the quantum domain: this is the case for instance of secret key expansion [SBPC$^+$09], randomness amplification [CR12] or randomness expansion [VV12].

Position-based cryptography in the quantum setting was first investigated under the name of *quantum tagging* by Kent around 2002, but only appeared in the literature much later in [KMS11]. In the same paper Kent *et al.* proposed attacks against other possible constructions for other quantum position verification schemes. Let us present an example of position verification scheme in the quantum setting in 1 dimension. We have 2 verifiers: one verifier, say V_0, sends a qubit $|\phi\rangle = U|x\rangle$ with $x \in \{0, 1\}$, where U is some unitary, and the second verifier, say V_1, sends a classical description of the unitary U. The task for the prover (say P), who has claimed his position is exactly between V_0 and V_1, is then to measure the qubit in the basis $\{U|0\rangle, U|1\rangle\}$ and to return the classical value of x to both verifiers. The verifiers will be convinced if the prover can perform this task fast enough. There are many variations of this protocol, and the intuition for security of such protocols is that only

someone sitting in a claimed position can obtain both U and $|\phi\rangle$, perform the required measurement, and return the correct value x on time. In [LL11], Lau and Lo extended the attack from [KMS11] to show that the above intuition is incorrect if the unitary U is a *Clifford* gate. In that case, a couple of cheaters, Alice lying between V_0 and P, and Bob lying between V_1 and P, can always fool the verifiers provided that they share a small number of EPR pairs. This result was later generalised by Buhrman *et al.* in [BCF$^+$11]. They showed that for any general position verification scheme such an attack always exists provided that the coalition of cheaters share sufficiently many EPR pairs. This implies that no position-based quantum cryptographic protocol can display information-theoretic security.

Two general families of attacks against such position-verification protocols have been considered in the literature so far. Both of them are based on quantum teleportation. The first one is inspired by Vaidman's protocol for instantaneous nonlocal computation [Vai03]. In this type of attack strategy cheaters teleport the n qubit quantum state, sent by the verifier, back and forth with the hope that in one of the rounds after teleportation, the resulting state doesn't need any correction. At each round this happens with probability $\frac{1}{4^n}$. This probability goes to one after 4^n rounds. If the position-based protocol involves n qubits, the resource (number of EPR pairs) required for this type of attacks to succeed typically scales double-exponentially with n [BCF$^+$11]. Another class of attacks uses *port-based* teleportation [IH08] and requires only an exponential number of EPR pairs to succeed [BK11]. If one could prove that such an attack was indeed optimal, one would obtain a secure position-based protocol for all practical purposes.

A different class of position verification protocols based on the nonlocal computation of Boolean functions was introduced by Buhrman *et al.* in [BFSS13]. In the same paper they suggested a new type of attacks based on the *Garden-hose complexity* of Boolean functions. In particular they showed that finding an explicit Boolean function with polynomial circuit complexity (so that the honest prover can efficiently compute it) but exponential attack complexity in the garden-hose model is at least as difficult as separating the complexity classes P and L, corresponding respectively to decision problems decidable in polynomial time and those decidable logarithmic space. This result was recently extended by Klauck and Podder who showed that explicit Boolean functions on k variables with Garden-hose complexity $\Omega(k^{2+\varepsilon})$ is hard to obtain [KP14]. These results give us little hope of finding an explicit position-verification scheme, which is both practical and secure.

Establishing lower bounds on the amount of entanglement shared by a coalition of provers in order to successfully attack the protocol is a non trivial task. Current lower bounds are linear in the security parameter of the protocol [BK11], [TFKW13]. Recently, a tight (linear) lower bound was proved for the BB84-based protocol where the challenge unitary U is either an identity or a Hadamard gate. The lower bound works for a model where the cheaters share an initial entangled state, but they are not allowed to exchange physical qubits during the protocol [RG15]. It was also shown by Unruh that the security of some position-verification protocols could be established in the quantum random oracle model, that is if one has access to one-way functions [Unr14].

Recently, Qi and Siopsis initiated the study of imperfections in quantum position verification schemes. In particular, they are interested in exploring the effect of losses in the quantum channel between the verifiers and the prover [QS15]. Indeed, in order to achieve practical distances between the verifiers and the prover it is necessary for the protocol to be reasonable loss-tolerant.

In this chapter, we investigate the family of protocols described above, where the challenge unitary

U is chosen from a family of n-qubit gates. We present some new attacks based on the Clifford hierarchy against such protocols that might become particularly efficient when the position-verification protocol is practical for the honest prover. We then introduce a new practical position-verification scheme involving only single-qubit operations, for which we show that the best known attacks require an exponential amount of entanglement. However, if we allow some losses in our protocol then in [Spe16] Florian Speelman proposed an attack based on the Clifford hierarchy and garden-hose model, which take a polynomial amount of resources to break the security.

Before explaining our contribution in Section 2 we will explain the general framework of position-based quantum cryptography protocols. The attack strategy based on the Clifford hierarchy is described in Section 3. Finally, in Section 4 we will describe the *Interleaved Product* protocol.

This chapter is based on the following paper,

- **Practical position-based quantum cryptography**,
  K. Chakraborty, and A. Leverrier,
  Physical Review A, **92.5**, 052304 (2015).

2 A general family of position-verification protocols

For simplicity, we mainly focus on one-dimensional protocols where two verifiers V_0 and V_1 aim at verifying the position of a prover P located between them. We note that complications occur when dealing with more realistic 2 or 3-dimensional protocols (see for instance [Unr14]), but explicitly avoid these questions here. Moreover, without loss of generality, we can always assume that the position P of the prover is exactly at equal distance to V_0 and V_1 and that it takes one unit of time for light to travel from V_0 (or V_1) to P.

Roughly speaking, a general position-verification protocol consists of three distinct phases:

- *The preparation phase*, where V_0 and V_1 prepare a challenge for the prover. The challenge typically involves a quantum state (for instance an n-qubit state, or n single-qubit states in the protocols considered in the present chapter) as well as some classical information. The challenge is always given to the prover in a distributed fashion, one part coming from V_0, the other part coming from V_1.

- *The execution phase*, during which V_0 and V_1 send their respective share of the challenge towards the prover P, who solves the challenge she is given, and returns her answer to the verifiers.

- *The verification phase*, during which the verifiers check that (i) the answer is correct, and that (ii) they received it not more than two time units after the beginning of the protocol. This assumes the idealized scenario where all communications are performed at the speed of light, and local computation take negligible time. Even in that idealized scenario, it makes sense to allow the honest prover to err a small fraction of the time. For this reason, the provers accept the answer if it meets some tolerance threshold η. In fact, one should distinguish between two sources of imperfections, losses and noises, and the tolerance threshold should therefore specify

the amount of losses (i.e. no answer from the prover) and noise (i.e. incorrect answer) that can be tolerated.

In this chapter, we first focus on an important family of position verification protocols where V_0 sends an n-qubit state and V_1 sends the classical description of a measurement basis, and the prover is required to measure the state in the correct measurement basis and to communicate the outcome to both verifiers. These protocols have been widely discussed in the literature for instance in [KMS11] or [LL11]. In Section 4, we introduce the Interleaved Product protocol where the description of measurement basis is transmitted to the prover as a product of a large number of single-qubit unitaries $\prod_u u_i v_i$, where the unitaries $\{u_i\}$ and $\{v_i\}$ are respectively described to the prover by V_0 and V_1. This scheme appears to be reasonably new, although similar ideas, with more verifiers, were already considered in [LL11]. We note that the *interleaved group product* (i.e. $\prod u_i v_i$ where the $\{u_i\}$ and $\{v_i\}$) are described by different verifiers) has been considered in the communication complexity literature, for instance in a recent paper by Gowers and Viola [GV15].

Before defining these protocols more formally, let us comment on some assumptions we make here. In this chapter, our main goal is to present some natural position verification protocols and to study general classes of attacks that can be carried out by coalitions of cheaters. While we try to be as general as possible, we think it is sensible to make some specific choices in order to simplify the analysis. For instance, we restrict our protocols to using qubit states, and more importantly, we consider one-dimensional protocols with only two verifiers. Most of our analysis would carry through to arbitrary qudit protocols involving many verifiers. We also decided to leave aside all the problems related to timing in order to focus on the genuinely quantum part of the procedure. This means that we consider all communication (classical or quantum) is performed at the speed of light, and that all computation is instantaneous. These are obviously unrealistic assumptions, but dealing with more realistic ones can be done independently as the analysis we provide here (see for instance the work of Kent [Ken12a]). The main source of imperfection in a position verification protocol is the quantum channel between the verifiers and the prover, which can never be assumed to be perfect. In general, the channel is both lossy and noisy, which is why even an ideal prover cannot possibly pass the test perfectly. On the other hand, it makes sense to assume that the classical channels are essentially perfect (lossless and noiseless).

2.1 Formal description of the position-verification protocols

Following the literature, we find it useful to describe the protocol in terms of distributed collaborative games, where two players, named Alice and Bob, independently receive some query from a referee, are allowed a single round of (bipartite) communication and need to output some answer. In the honest prover case, Alice and Bob hold the same spatial position and the prover has access to both their inputs. In the cheating coalition case, Alice and Bob sit respectively between P and V_0 or between P and V_1 and are only allowed one simultaneous round of communication. The main result of [BCF$^+$11] is that if Alice and Bob can win the game with arbitrarily many rounds of communication, then they can also win it with a single simultaneous round, provided that they are sufficiently entangled.

The main family of protocols we consider corresponding to games denoted by $G(n, \mathcal{U}, \eta)$ where n refers to the number of qubits involved in the protocol, $\mathcal{U}$ is a set of n-qubit unitaries, and η is the tolerance threshold. We also write $G(n, k, \eta)$ when the set $\mathcal{U}$ is a subset of C_k, the k^{th} level of the

Clifford hierarchy (see the appendix for a formal definition of the Clifford Hierarchy). The protocol $G(n, \mathcal{U}, \eta)$ consists of the following phases:

Preparation Phase:

(i) The verifier V_0 chooses an n-qubit unitary operator $U \in_R \mathcal{U}$ and an n-bit string $x = (x_1, \ldots, x_n) \in_R \{0,1\}^n$. V_0 prepares $|\psi\rangle = U|x\rangle$, where $|x\rangle = \bigotimes_{i=1}^n |x_i\rangle$ is a computational basis state.

(ii) V_0 sends x and U to V_1 through some secure authenticated classical channel.

Execution Phase:

(i) V_0 sends the n qubit quantum state $|\psi\rangle$ to prover P at time $\tau = 0$. V_1 sends the unitary U to P at time $\tau = 0$.

(ii) The prover P receives both $|\psi\rangle$ and U at time $\tau = 1$.

(iii) After receiving $|\psi\rangle$ and U, the honest prover P computes $U^\dagger|\psi\rangle$ and measures it in computational basis, obtaining some outcome string y. P then sends back y to both V_0 and V_1.

Verification Phase:

(i) The prover P wins the game if V_0 and V_1 receive the same string y at time $\tau = 2$, and if the Hamming distance between x and y is less than ηn: $d_H(x, y) \leqslant \eta n$.

In the literature, this family is often considered in the single qubit case, for instance with $\mathcal{U} = \{I, H\}$ where H is the Hadamard gate and I is the identity operator [CGMO09, BCF$^+$11, RG15]. Then it makes sense to repeat the protocol n times in order to build some statistics.

In our case, we aim at giving a more general picture of the possible attacks working against this scheme and consider n-qubit gates. For such protocols, we show that there exists a trade-off between the complexity of the protocol for the honest prover and the resources needed to break the protocol for a coalition of cheaters.

2.2 Attack strategies against position-verification protocols

As was proved in [BCF$^+$11], there always exists a working attack strategy against any position verification protocol that allows a coalition of adversaries to perfectly impersonate the honest prover. In the case of the one-dimensional protocols considered in this chapter, such a coalition consists without loss of generality of two players, Alice (A) and Bob (B), with Alice lying on the line between V_0 and P, and Bob lying between V_1 and P.

The attack strategies we consider here have the following structure:

(i) Alice and Bob initially share a (possibly entangled) initial bipartite state ρ_{AB} of dimension to be specified later. Typically, ρ_{AB} consists of many EPR pairs.

(ii) Alice intercepts the communication from V_0, namely a quantum register ρ_C (where C stands for challenge), as well as some classical information.

(iii) Bob intercepts the classical communication from V_1.

(iv) Depending on the classical information they received, Alice and Bob perform respectively a quantum measurement on their respective registers, AC and B.

(v) Alice and Bob exchange all the classical information as well as the outcomes of the measurement with each other.

(vi) Finally, upon receiving this information, they prepare and send their response to the verifiers.

The main question of interest is to decide how the dimension of ρ_{AB}, and more particularly the entanglement of this state, scales with the size of the input parameters of the position verification protocol.

This scenario allows us to see the cheating procedure as a distributed task, or game, where Alice and Bob are asked questions (possibly consisting of a quantum state) and are required to output some specific answer. They win the game if they fool the verifiers. In the game they are allowed to have a single round of simultaneous communication.

We can interpret the family $G(n,\mathcal{U},\eta)$ in these terms:

Definition 3.1. *The distributed game $G(n,\mathcal{U},\eta)$ is defined as follows:*

- ***Input:*** *$|\psi\rangle = U|x\rangle$ for Alice, $U \in \mathcal{U}$ for Bob*
- ***Output:*** *$a \in \{0,1\}^n$ for Alice, $b \in \{0,1\}^n$ for Bob*
- ***Winning condition:*** *$a = b$ and $d_H(a,x) \leqslant \eta n$*

We now list a few questions of interest. In the perfect setting ($\eta = 0$), how many EPR pairs do Alice and Bob need to share to carry out a successful attack with reasonable probability? One of the main open questions of the field is to find an explicit protocol that requires an exponential number of EPR pairs to break.

Second, if $\eta > 0$, this opens the door to new attacks, even for non entangled cheaters. A possible strategy consists in Alice measuring the state in a random basis and forwarding her measurement outcome to Bob. Ideally, it would be interesting to understand how the amount of entanglement required for cheating behaves as a function of η.

We should also comment on the definition of a successful attack. If the goal is to design a secure protocol, then Alice and Bob should not be able to cheat, even with a very small probability. Indeed, even if the cheating strategy only succeeds with probability 10^{-2} or 10^{-3}, it is difficult to claim that the protocol is secure. Ideally, we want this cheating probability to be exponentially small in n. In this chapter, however, for simplicity we focus on attacks that work with high probability (close to 1).

3 Attacks for $\eta = 0$ based on the Clifford hierarchy

In this section, we first study attack techniques based on the Clifford hierarchy that can be applied by cheaters against the family of protocols $G(n, \mathcal{U}, 0)$, where the value of the tolerance threshold η is set to 0. The definition of the Clifford hierarchy is given in Section 2 of Chapter 2. Let us simply recall here that the first two levels $C_1(n)$ and $C_2(n)$ of the hierarchy correspond respectively to the Pauli and the Clifford groups.

In particular, we give explicit attacks that may be efficient in the following practically relevant cases: (1) if $\mathcal{U} \subseteq C_k(n)$, that is if the unitaries all belong to some low level k of the Clifford hierarchy, (2) if the unitaries in $\mathcal{U}$ can all be implemented with a quantum circuit with a fixed layout.

We note that these two cases correspond to protocols that appear to be practical for a honest prover. Indeed, gates in a low level of the Clifford Hierarchy are much easier to implement fault tolerantly than arbitrary gates. Moreover, if the quantum states are photonic states, and the honest prover uses integrated photonics to implement the unitaries in $\mathcal{U}$, a fairly reasonable choice in practice, then it makes sense to fix some layout, that is an optical circuit consisting of single or 2-qubit gates for instance, and to obtain the family $\mathcal{U}$ by changing the value of the single and 2-qubit gates.

3.1 A general attack for $\mathcal{U} = C_k$

Let us first define the *Clifford complexity* of a family $\mathcal{U}$ of unitaries.

Definition 3.2. *Let $\mathcal{U}$ be a set of n-qubit unitaries. We define the* Clifford complexity *of the set $\mathcal{U}$, denoted by $\mathrm{CC}[\mathcal{U}]$, to be the minimum number of EPR pairs that Alice and Bob must share to perfectly win the game $G(n, \mathcal{U}, 0)$.*

It is easy to see that if the unitary U is a Pauli matrix, then Alice and Bob can win the game $G(n, k = 1, 0)$ without sharing any entanglement because $|\psi\rangle$ is also a basis state $|y\rangle$. The two strings x and y coincide on the qubits for which U is the identity or a Z Pauli matrix, and differ for the other qubits. Therefore, Alice simply needs to measure $|\psi\rangle$ in the computational basis and to forward her results to Bob, who can recover the correct string x using his knowledge of U. This shows that

$$\mathrm{CC}[C_1(n)] = 0.$$

If the unitary U belongs to the Clifford group $C_2(n)$, then Alice and Bob can again win the game perfectly if they share n EPR pairs. The idea is for Alice to teleport the state $|\psi\rangle$ to Bob using the n EPR pairs. Bob obtains the state $\sigma|\psi\rangle$ where $\sigma \in C_1(n)$ is a Pauli correction. Applying the unitary $U^\dagger$ to his state, Bob obtains

$$U^\dagger \sigma |\psi\rangle = U^\dagger \sigma U |x\rangle,$$

where $U^\dagger \sigma U \in C_1(n)$. This means, Bob simply needs to measure this state in the computational basis, and forward his result to Alice. Once they know both the value of σ and the result of the measurement, both Alice and Bob are able to recover the correct value of the string x and they win the game. This proves that

$$\mathrm{CC}[C_2(n)] \leqslant n.$$

If the unitary U to be implemented belongs to the k^{th} level of the Clifford hierarchy, then Alice and Bob can apply an iterative procedure which is described in Algorithm 1. This algorithm is similar to the cheating strategy of [BCF+11]. The main difference lies in the termination condition: here, the algorithm terminates after a deterministic number of rounds that depends on the considered level of the Clifford Hierarchy.

Input: $|\psi\rangle = U|x\rangle$ received by Alice, $U = U_0 \in C_k$ received by Bob
Output: $x \in \{0,1\}^n$

1 Alice teleports the state $|\psi\rangle$ to B using n EPR pairs and obtains a string describing $\sigma_{A_1} \in \mathcal{P}_n$. Bob obtains the state $\sigma_{A_1}|\psi\rangle = \sigma_{A_1} U|x\rangle$.

2 Bob applies $U^\dagger$ to his state and teleports the outcome $U^\dagger \sigma_{A_1} U|x\rangle$ to Alice, obtaining some classical description of $\sigma_{B_1} \in \mathcal{P}_n$. Alice obtains the state $U_1|x\rangle$ where $U_1 = \sigma_{B_1} U^\dagger \sigma_{A_1} U \in C_{k-1}$.

for $j = 1$ *to* $k-3$ **do**

3 Alice knows the value of $\sigma_{A_1}, \ldots, \sigma_{A_j}$ (among the 4^{jn} possibilities). Alice and Bob share $4^n \times (n4^{(j-1)n})$ EPR pairs devoted to Round j, corresponding to 4^n sets of $n \times 4^{(j-1)n}$ EPR pairs, one set for each possible value of σ_{A_j}. Alice teleports back each of the $4^{(j-1)n}$ n-qubit states (of the form $U_j|x\rangle$ for some unitary $U_j \in C_{k-j}(n)$) she received from Bob using the "teleportation channel" indexed by σ_{A_j}. In that teleportation channel, Bob obtains the state $\sigma_{A_{j+1}} U_j|x\rangle$, applies $U_j^\dagger$ to that state, before teleporting it back to Alice in the corresponding teleportation channel. Alice receives $U_{j+1}|x\rangle$ with $U_{j+1} = \sigma_{B_{j+1}} U_j^\dagger A_{j+1} U_j \in C_{k-(j+1)}$.

end

4 Alice uses a final round of teleportation for the $4^{(k-2)n}$ n-qubit states, and obtains a classical description of $\sigma_{A_{k-1}}$.

5 Alice sends the classical value of $\sigma_{A_1}, \ldots, \sigma_{A_{k-1}}$ to Bob.

6 Bob applies $U_{k-1}^\dagger$ to each n-qubit state, measures in the computational basis, and forwards the classical output, as well as the value of $\sigma_{B_1}, \ldots, \sigma_{A_{k-2}}$ to Alice.

7 Both Alice and Bob compute the value of x.

Algorithm 1: Cheating strategy for $G(n, C_k(n), 1)$ based on the Clifford hierarchy

Lemma 3.1. *If Alice and Bob apply Algorithm 1, then they win the game with probability one.*

Proof. To prove the correctness of the algorithm, we need to show that $U_j \in C_{k-j}$ and that Bob can perform $U_j^\dagger$ since he knows the value of U_j. The first point is shown by recurrence: $U_0 = U \in C_k$ and if $U_j \in C_{k-j}$, then $U_{j+1} = \sigma_{B_{j+1}} U_j^\dagger A_{j+1} U_j \in C_{k-j-1}$. Moreover, the value of U_j is a function of U_{j-1}, σ_{A_j} and σ_{B_j}. For the quantum channel labeled by σ_{A_j}, Bob is therefore able to apply $U_j^\dagger$. □

The existence of the attack strategy described in Algorithm 1 allows us to obtain the following

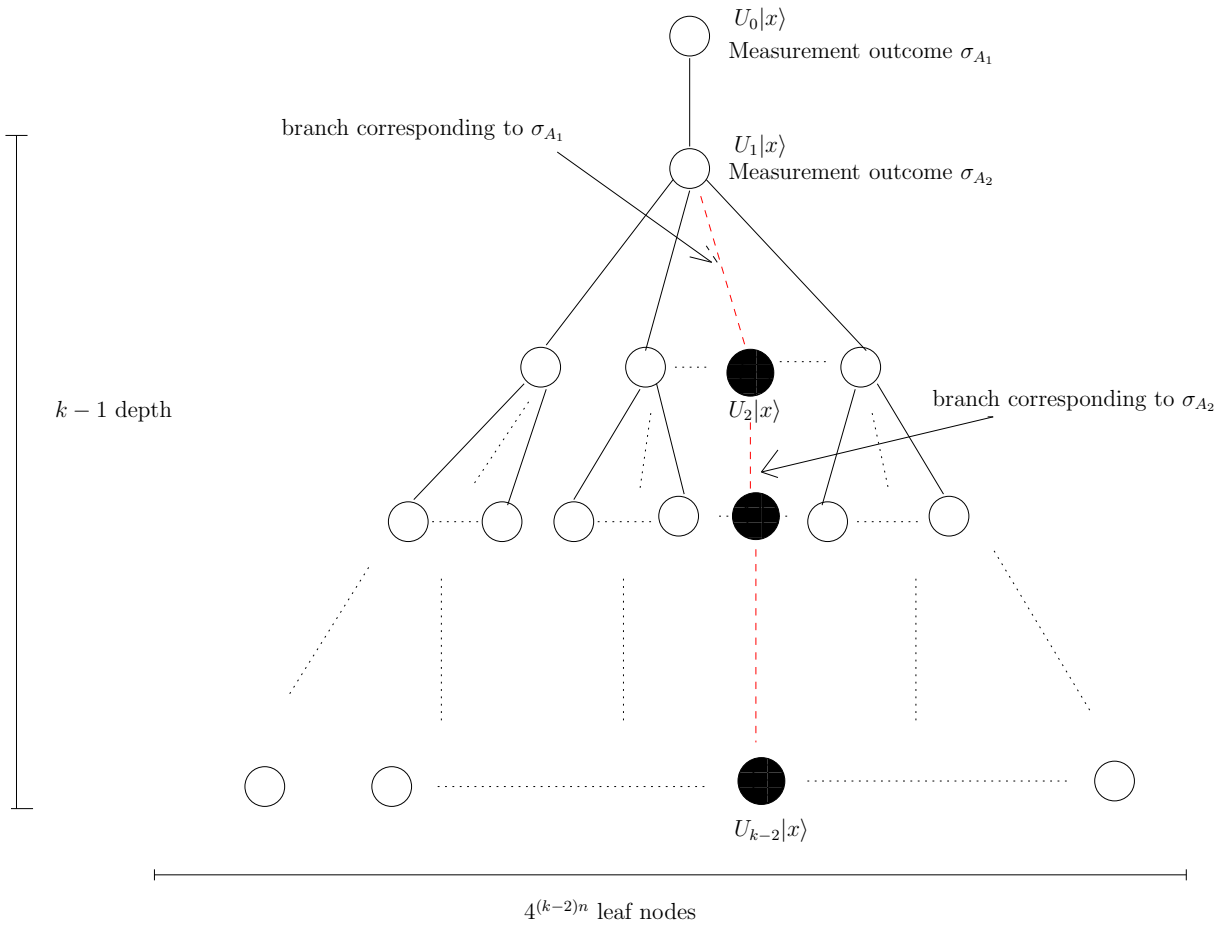

Figure 3.1: Pictorial view of Step 3 of Algorithm 1: Each level of the tree corresponds to a round trip between Alice and Bob. Each of the nodes correspond to a quantum state. In particular, the root node is the initial quantum state $U_0|x\rangle$ received by Alice, and the path in red dash (determined by the successive outputs of the Bell measurements) goes along the various states held by Alice at different steps of the protocol, namely $U_1|x\rangle, \ldots, U_{k-2}|x\rangle$.

upper bound for the Clifford complexity of the set $C_k(n)$.

Theorem 3.2.

$$\mathrm{CC}[C_k(n)] \leqslant 4n\, 4^{n(k-2)}. \tag{3.1}$$

Proof. The loop at Step 3 in Algorithm 1 can be viewed as a branching tree with depth $k-2$ (see Fig. 5.1). This tree is regular with each internal node having 4^n children (corresponding to the 4^n possible values for Alice's Bell measurement result). Each layer of the tree corresponds to a round trip between Alice and Bob, that is $2n$ EPR pairs. Computing the complexity of the attack therefore amounts at counting the number of branches in the tree. For a tree of depth $k-2$, the number of branches is $\sum_{j=0}^{k-3} 4^{jn}$. Moreover, the last step of the protocol consists in a quantum teleportation

of $n \times 4^{n(k-2)}$ qubits from Alice to Bob. In total, the number of EPR pairs used in the protocols is therefore

$$2n \sum_{j=0}^{k-2} 4^{jn} + n4^{n(k-2)} \leqslant 4n4^{n(k-2)}.$$

□

In the following, we denote by $\mathrm{Tree}[C_k(n)]$ the number of EPR pairs required to perform the attack described by Algorithm 1 on the set of unitaries $C_k(n)$. Theorem 3.2 simply says that

$$\mathrm{CC}[C_k(n)] \leqslant \mathrm{Tree}[C_k(n)] \leqslant 4n\, 4^{n(k-2)}. \tag{3.2}$$

3.2 Attacks when $\mathcal{U}$ correspond to quantum circuits with a fixed layout

The attack corresponding to Algorithm 1 is general and works for any n-qubit gate in some given level of the Clifford hierarchy. In the context of position verification protocols, however, the interesting set of gates $\mathcal{U}$ from which the unitary to be implemented is chosen, is often more restricted. Indeed, if the protocol is to be practical, then a honest prover should be able to implement the unitaries reasonably efficiently. For this reason, it is interesting to consider unitaries described by quantum circuits.

In a practical scenario, where the quantum states given to Alice are photonic qubits, it makes sense to consider photonic implementations for the quantum circuit, and therefore to consider unitaries with a fixed layout for the quantum circuit, and adjustable single and two-qubit gates. This is typically the case for experimental implementations based on integrated photonics [OFV09].

For this reason, the set $\mathcal{U}$ of unitaries considered could be described by a fixed layout, and a specific unitary $U \in \mathcal{U}$ is then described by giving the value of each single or two-qubit gate in the layout. For a quantum circuit based on linear optics, the layout $\mathcal{L}$ corresponds to the position of the phase-shifters and beamsplitters, and the unitary is given by the specific values of the phase-shifts and transmission of the beamsplitters.

We are interested in the complexity of attacks for such schemes as a function of the depth and width of such quantum circuits.

Definition 3.3. *Let $\mathcal{L}$ be the layout for an n-qubit quantum circuit, consisting of adjustable elementary gates. The set $\mathcal{U}_\mathcal{L}$ of n-qubit unitaries corresponds to the set of unitaries which can be implemented with a quantum circuit with layout $\mathcal{L}$.*

Let us prove elementary results about the composition of circuit layouts.

Lemma 3.3 (Parallel circuits)**.** *Let $\mathcal{L}_1, \mathcal{L}_2$ be two layouts for quantum circuits. Then*

$$\mathrm{CC}[\mathcal{U}_{\mathcal{L}_1} || \mathcal{U}_{\mathcal{L}_2}] \leqslant \mathrm{CC}[\mathcal{U}_{\mathcal{L}_1}] + \mathrm{CC}[\mathcal{U}_{\mathcal{L}_2}], \tag{3.3}$$

where $\mathcal{L}_1 || \mathcal{L}_2$ is the layout corresponding to putting $\mathcal{L}_1$ and $\mathcal{L}_2$ in parallel.

We note that the quantum unitary corresponding to two circuits in parallel is simply the tensor product of the unitaries: $U_{\mathcal{L}_1||\mathcal{L}_2} = U_{\mathcal{L}_1} \otimes U_{\mathcal{L}_2}$ and therefore

$$\mathcal{U}_{\mathcal{L}_1||\mathcal{L}_2} \subset \mathcal{U}_{\mathcal{L}_1} \otimes \mathcal{U}_{\mathcal{L}_2}.$$

Proof. Consider any gate $U_1 \otimes U_2 \in \mathcal{U}_{\mathcal{L}_1||\mathcal{L}_2}$. Since both Alice and Bob know the decomposition $U_1 \otimes U_2$, they can implement the optimal attack for U_1 and for U_2 independently, since these unitaries act on distinct sets of qubits. The complexity of the overall attack is simply the sum of the complexities of implementing U_1 and U_2, which is upper bounded by $\mathrm{CC}[\mathcal{U}_{\mathcal{L}_1}] + \mathrm{CC}[\mathcal{U}_{\mathcal{L}_2}]$. □

Lemma 3.4 (Concatenated circuits)**.** *Let $\mathcal{L}_1, \mathcal{L}_2$ be two layouts for quantum circuits. Then*

$$\mathrm{CC}[\mathcal{U}_{\mathcal{L}_1\mathcal{L}_2}] \leqslant \mathrm{Tree}[\mathcal{U}_{\mathcal{L}_1}]\mathrm{Tree}[\mathcal{U}_{\mathcal{L}_2}], \tag{3.4}$$

where $\mathcal{L}_1\mathcal{L}_2$ is the layout corresponding to concatenating the layouts $\mathcal{L}_1$ and $\mathcal{L}_2$.

Proof. The strategy consists in first applying the strategy corresponding to Algorithm 1 for unitary $U_1 \in \mathcal{U}_{\mathcal{L}_1}$. Then, at the last round, instead of measuring the state, Bob continues the teleportation protocol in order to implement $U_2 \in \mathcal{U}_{\mathcal{L}_2}$. There are at most $\mathrm{Tree}[\mathcal{U}_{\mathcal{L}_1}]$ nodes in the tree corresponding to the implementation of U_1, and it is sufficient to apply the protocol to each of the leaves in order to implement to concatenation of U_1 and U_2. Therefore, $\mathrm{Tree}[\mathcal{U}_{\mathcal{L}_1}]\mathrm{Tree}[\mathcal{U}_{\mathcal{L}_2}]$ EPR pairs are sufficient to implement the total unitary. □

From Lemmas 3.3 and 3.4, it is possible to compute an upper bound for the Clifford complexity of any layout, as a function of its depth and size.

Theorem 3.5. *Let $\mathcal{L}$ be the layout of an n-qubit quantum circuit of depth d where each layer consists of gates in C_{k_i}. Then*

$$\mathrm{CC}[\mathcal{U}_{\mathcal{L}}] \leqslant 4^{n\sum_{i=1}^{d}(k_i-2)} \times (4n)^d. \tag{3.5}$$

Proof. The layout $\mathcal{L}$ can be decomposed into d layers: $\mathcal{L} = \mathcal{L}_1\mathcal{L}_2\cdots\mathcal{L}_d$. By applying Lemma 3.4 recursively, one obtains that

$$\mathrm{CC}[\mathcal{U}_{\mathcal{L}}] \leqslant \prod_{i=1}^{d} \mathrm{Tree}[\mathcal{U}_{\mathcal{L}_i}].$$

Combining this with the result of Theorem 3.2, one finally obtains

$$\mathrm{CC}[\mathcal{U}_{\mathcal{L}}] \leqslant \prod_{i=1}^{d} 4n4^{n(k_i-2)},$$

which establishes the result. □

We note that this result can be slightly improved by using Lemma 3.3 together with Theorem 3.2 for the last layer. Indeed, if the last layer only consists of 1 or 2-qubit gates, then it can be implemented with at most $n \times (4n) \times 4^{2(k-2)}$ EPR pairs since the layer can be seen as at most n parallel circuits acting on at most 2 qubits each.

We conclude this section with an important remark, which was already made in [QS15]. If the value of η is too large, then there always exists a winning strategy for non-entangled cheaters. For the protocols considered above, $\eta = 1/2$ is always achievable by a simple random guessing strategy: Alice and Bob simply agree on a random string and return it to the verifiers. For specific protocols where the family $\mathcal{U}$ displays some structure, better attacks are available. For instance, in the case of the BB84 scheme, measuring in the Breidbart basis allows the cheaters to win if $\eta \geqslant 1 - \cos^2(\pi/8) \approx 0.15$.

4 The Interleaved Product protocol

In this section, we introduce a new scheme for position verification based on the interleaved group product. This scheme depends on two main parameters: the number n of single-qubit states used and a parameter t quantifying the size of the product. More formally, the *Interleaved Product* protocol denoted by $G_{\mathrm{IP}}(n, t, \eta_{\mathrm{err}}, \eta_{\mathrm{loss}})$, goes as follows:

Preparation Phase:

(i) V_0 chooses a random bit string $x \in_R \{0,1\}^n$ and and a single-qubit unitary U chosen from the Haar measure on unitary group $U(2)$. V_0 also chooses $2t-1$ additional independent unitaries $u_1, \ldots, u_t, v_1, \ldots, v_{t-1}$ from the Haar measure on $U(2)$ and computes $v_t = u_t^\dagger v_{t-1}^\dagger \ldots v_1^\dagger u_1^\dagger U$, thus ensuring that $U = \prod_{i=1}^t u_i v_i$. Verifier V_0 then informs V_1 of these choices thanks to a secure classical channel.

(ii) V_0 prepares the n-qubit state $|\psi\rangle = U^{\otimes n}|x\rangle$, applying the same unitary U to all the qubits of $|x\rangle$.

Execution Phase:

(i) At time $\tau = 0$, V_0 sends the state $|\psi\rangle$ as well as the classical description of $(u_1, \ldots, u_t)$ to the prover, and V_1 sends the classical description of $(v_1, \ldots, v_t)$ to P.

(ii) At time $\tau = 1$, the prover receives $|\psi\rangle$, computes $U = \prod_{i=1}^t u_i v_i$, applies $(U^\dagger)^{\otimes n}$ to $|\psi\rangle$ and measures the resulting state in the computational basis, obtaining some outcome $y \in \{\emptyset, 0, 1\}^n$, which is sent to both V_0 and V_1. Here the symbol $\emptyset$ refers to an empty measurement result.

Verification Phase:

(i) The prover P wins the game if V_0 and V_1 both receive an identical string y at time $\tau = 2$, if the number of errors is less than $\eta_{\mathrm{err}} n$ and the number of empty results $\emptyset$ is less than $\eta_{\mathrm{loss}} n$.

Interestingly for this protocol, the verifiers only need to prepare arbitrary single-qubit states and the honest prover is simply required to measure a qubit in a given basis, which is quite practical. We note that a similar family of protocols was considered in [LL11], but with more verifiers, which made the protocol less practical. Here we make the choice that the same unitary U is applied to all the qubits. A variant of the protocol would be to send n successive challenges to the prover, with n different choices for the unitary.

The main feature of this protocol is that the value of the unitary U that defines the measurement basis is described by a product $U = \prod_{i=1}^t u_i v_i$ which is communicated to the prover in a distributed fashion. Intuitively, if a coalition of cheaters tries to break the protocol, it seems that they need to follow a back-and-forth strategy to take care of each of the unitaries, one at the time. As we see in the next section, this leads to attacks with a complexity exponential in the parameter t. On the other hand,

the honest prover simply needs to compute the $2t$-fold product of 2×2 matrices, which takes time linear in t.

In fact, for a practical implementation, each of the $2t$ unitaries should be described with a given (finite) level of accuracy, meaning that describing a unitary is done with a constant number of bits. We ignore this subtlety in the present chapter.

5 Attack strategies for the Interleaved-Product protocol

By construction, the Interleaved-Product protocol is immune to the attacks based on the Clifford hierarchy: this is simply because all the gates are chosen from the Haar measure and therefore do not belong to any low level of the Clifford hierarchy. Moreover, the product structure enforces a large depth (of order $2t$ which can be taken as arbitrarily large in practice) for the quantum circuit. Note that in the proposal of [LL11], neither of these conditions was enforced because t corresponded to the number of verifiers (which should remain quite small for practical protocols) and all the gates belong to some low level of the Clifford hierarchy.

There exist, however, some attacks working in the regime $\eta_{\text{err}} > 0$, which we investigate now. Recall that we consider here the lossless scenario where the prover is required to give a bit value 0 or 1 for each qubit. The first strategy uses port-based teleportation over $2t$ rounds. The second strategy we consider relies on the Solovay-Kitaev theorem for approximating arbitrary gates with gates in a low level of the Clifford hierarchy, for which the attack of Algorithm 1 can be applied. Both attacks lead to the same complexity and require $2^{O(t \log(t/\eta_{\text{err}}))}$ EPR pairs. Both strategies work in the lossless case $\eta_{\text{loss}} = 0$.

we end this section with a discussion of possible attack strategies for non-entangled cheaters, which works if $\eta_{\text{err}} + \eta_{\text{loss}}/4 \geqslant 1/4$.

5.1 Attack based on port-based teleportation

We explain the concept of port-based teleportation in Section 2 of Chapter 2. Here we use this concept to attack the position verification scheme, proposed in the last section. The attack proceeds as follows:

- Alice applies the unitary $u_1^\dagger$ to each of her n qubits and uses m_1 EPR pairs to teleport each qubit to Bob. This consumes a total of $M_1 = m_1 n$ EPR pairs.
- Bob applies the unitary $v_1^\dagger$ to all of his qubits, and uses m_2 EPR pairs to teleport each one back to Alice. This consumes a total of $M_2 = m_2 M_1$ EPR pairs.
- This process is repeated for $2t$ rounds, after which the unitary $U^\dagger$ has been applied to all the qubits. At each step, Alice or Bob uses m_i EPR pairs to perform the port-based teleportation of a single qubit.
- At the last step, Bob measures each qubit in the computational basis, and both he and Alice exchange their measurement results.

There are two quantities of interest to analyze the attacks: the total number of EPR pairs used by Alice and Bob, and the fidelity of the final state. Recall indeed that port-based teleportation is not perfect, and that the teleported state is only an approximation of the input state.

The number M of EPR pairs is given by:

$$M = M_1 + M_2 + \cdots + M_{2t-1} \tag{3.6}$$

$$= n\left[m_1 + m_1 m_2 + \cdots + \prod_{i=1}^{2t-1} m_i\right]. \tag{3.7}$$

The fidelity F between the qubit after the $2t-1$ rounds of teleportation and the initial qubit is:

$$F \geqslant \prod_{i=1}^{2t-1}\left(1 - \frac{4}{m_i}\right). \tag{3.8}$$

Choosing the slightly suboptimal strategy where all the m_i are taken to be equal to a constant m gives: $M = nm\frac{m^{2t-1}-1}{m-1} \approx nm^{2t-1}$ and $F = (1-4/m)^{2t-1}$, that is:

$$M \approx n\left(\frac{8t}{\eta_{\text{err}}}\right)^{2t-1}, \tag{3.9}$$

where $\eta_{\text{err}} = 1 - F$ is assumed to be small. This establishes the following result.

Theorem 3.6. *Port-based teleportation provides an attack strategy against $G_{\text{IP}}(n, t, \eta_{\text{err}}, \eta_{\text{loss}} = 0)$ that requires $n\exp(O(t\log(t/\eta_{\text{err}})))$ EPR pairs.*

5.2 Attack based on the Solovay-Kitaev approximation

We now consider a different attack strategy based on the Solovay-Kitaev approximation, which guarantees that any single-qubit unitary can be approximated with accuracy ε by a sequence of unitaries taken from some fixed universal set of gates. We mention about Solovay-Kitaev approximation in Section 1 of Chapter 2. For the ease of the readers here we restate the statement of the theorem again.

Theorem 3.7 (Solovay-Kitaev [NC10])**.** *If $\mathcal{G} \subseteq SU(d)$ is a universal family of gates (where $SU(d)$ is the group of unitary operators in a d-dimensional Hilbert space), $\mathcal{G}$ is closed under inverse and $\mathcal{G}$ generates a dense subset of $SU(d)$, then for any $U \in SU(d)$, $\varepsilon > 0$, there exist $g_1, g_2, \ldots, g_l \in \mathcal{G}$ such that $\|U - U_{g_1}U_{g_2}\ldots U_{g_l}\| \leqslant \varepsilon$ and $l = O(\log^c\left(\frac{1}{\varepsilon}\right))$, where $c < 3$ is a positive constant.*

Let us fix $\mathcal{G} = \{H, T\}$ where H is the Hadamard operator and T is the $\frac{\pi}{8}$ qubit gate, and note that this set lies in the third level C_3 of the Clifford hierarchy. The Solovay-Kitaev theorem guarantees that for each unitary U_i used in the game $G_{\text{IP}}(n, t, \eta_{\text{err}}, \eta_{\text{loss}})$, there exists another unitary U_i', obtained as a product of exactly l gates from $\{H, T, \mathbb{1}_2\}$ (where the identity is chosen so that the size l can be chosen to be independent the unitary U_i). By decomposing their respective gates u_i and v_i into products of gates in C_3, Alice and Bob are able to implement the attack strategy of Algorithm 1.

Theorem 3.8. *There exists an attack strategy for $G_{\text{IP}}(n, t, \eta_{\text{err}}, \eta_{\text{loss}} = 0)$ requiring $2^{8t\log^c(2t/\eta_{\text{err}})}n$ EPR pairs, where $c < 3$.*

Proof. According to Solovay-Kitaev theorem, one can approximate each unitary U_i used in the protocol by another unitary U_i' such that $\|U_i - U_i'\| \leqslant \frac{\eta_{\text{err}}}{2t}$, using a sequence of $l = O(\log^c(2t/\eta_{\text{err}}))$ gates. Overall, the approximation quality is given by

$$\left\| \prod_{i=1}^{t} U_i V_i - \prod_{i=1}^{t} U_i' V_i' \right\| \leqslant \eta_{\text{err}}.$$

The circuit to implement the gate $\prod_{i=1}^{t} U_i' V_i'$ has depth $2tl$ and uses only gates from C_2 or C_3. According to Theorem 3.5, the number M of EPR pairs needed to perform the attack is

$$M = 2^{8tl} = 2^{8t \log^c(2t/\eta_{\text{err}})}. \tag{3.10}$$

Performing this attack for each of the n qubits proves the theorem.

□

This attack can in fact be improved by noting that the gates in $\mathcal{G} = \{H, T\}$ are semi-Clifford (see the appendix for a definition). Recall that for a semi-Clifford unitary U, there are 2^n operators $\sigma \in \mathcal{P}_n$ such that $U\sigma U^\dagger \in \mathcal{P}_n$. This implies that for such gates, the tree described in Algorithm 1 can be taken to have degree $4^n - 2^n$. For $n = 1$, as is the case here, this means that the complexity of approximating $\prod_{i=1}^{t} U_i V_i$ can be reduced to 2^{4lt} instead of 2^{8lt}, leading to an overall quadratic improvement in the complexity of the attack.

5.3 Attacks for a non-entangled coalition of cheaters

A possible cheating strategy for non-entangled cheaters was considered in [QS15] and goes as follows: Alice measures each qubit $|\psi_i\rangle$ of the incoming state in a random basis, obtains some measurement result corresponding to a qubit state $|\tilde{\psi}_i\rangle$ and communicates the classical description of $\tilde{\psi}_i$ to Bob. When Alice and Bob learn the value of the unitary $U = \prod_{i=1}^{t} u_i v_i$, they can simply consider the state $U^\dagger|\tilde{\psi}_i\rangle$ and output 0 or 1, depending on whether $U^\dagger|\tilde{\psi}_i\rangle$ is closer to $|0\rangle$ or to $|1\rangle$. This strategy gives them the correct bit with probability $3/4$. Overall, this strategy leads to an expected fraction of correct bits equal to $3/4$, which means that the protocol $G_{\text{IP}}(n, t, 1/4, 0)$ is not secure against non entangled cheaters.

If $\eta_{\text{loss}} > 0$, that is if losses are tolerated, then Alice and Bob can apply the same technique and return a value only if $\max\{|\langle 0|U^\dagger|\tilde{\psi}_i\rangle|^2, |\langle 0|U^\dagger|\tilde{\psi}_i\rangle|^2\}$ is large enough. A similar analysis as in [QS15] shows that if Alice and Bob only return a value for a fraction $1 - \eta_{\text{loss}}$ of the qubits, then their error rate is $(1 - \eta_{\text{loss}})/4$. This shows that non entangled cheaters have a winning strategy as soon as $\eta_{\text{err}} + \eta_{\text{loss}}/4 \geqslant 1/4$.

6 Loss-tolerant protocols

In general, the strategies consisting in measuring the state in a random basis allow the cheaters to win a constant fraction of the n "rounds" of a game. This is problematic because it seems that a honest prover cannot do much better as soon as the quantum channel from the verifiers is imperfect, either

lossy or noisy. As a consequence, it would appear that position verification is not robust against losses or noise (see [QS15] for possible trade-offs between loss and noise). Fortunately, this conclusion is a little bit too pessimistic.

For instance, the Interleaved Product protocol can be straightforwardly modified to be made loss-tolerant, provided that the prover has access to a good quantum memory. The crucial point to note here is that this protocol appears to remain secure even if the quantum state is distributed in advance compared to the classical information required to decide in which basis to measure the state or to which verifier it should be forwarded. From this observation, we propose the following modification of the Interleaved Product protocol:

In addition to the verifiers, there is a central "bank" of quantum states available to the prover. This bank (whose role can be played by the verifiers) distributes quantum states, along with some identification number, to interested parties. The value of the states is not revealed to the client but the verifiers have access to a complete listing of pairs: (state ID, state value). When a prover wants to authenticate her position thanks to a position verification protocol, she should therefore obtain a quantum state from the bank, put it in a quantum memory, and then inform the verifiers of the state ID. Then, the verifiers can apply the usual protocol, with the exception that the state $|\psi\rangle$ does not need to be distributed since the game is played with the state the prover obtained from the bank.

It seems to us that this modified protocol remains as secure as the original Interleaved Product protocol. More precisely, we could not think of any attack working against the modified version that would not also work against the original version.

The advantage of this modified version is that the quantum channel between the verifiers and the prover is replaced by the quantum memory of the prover. This could become quite advantageous in a scenario where the physical distance between the verifiers and the prover is large, meaning that fiber optics communication would lead to high losses, provided that the prover has access to a good quantum memory. While the current state-of-the-art on quantum memories (see for instance [SAA$^+$10] for a recent review) is certainly not sufficient to implement this modified version of the protocol, there are no reason to doubt that high fidelity quantum memories with long coherence time will not become available in the future.

7 Discussion & conclusion

In this chapter we studied a general family of attack strategies against position-based quantum cryptography. In particular, we established a connection between several well studied quantum information processing tasks and position-based quantum cryptography. It was previously known that there exists some efficient attack when the verifiers choose the challenge unitary from the Clifford group. Here, we showed that this remains true if the unitaries lie in a low level of the Clifford hierarchy. This result connects the notions relevant in fault-tolerant quantum computing with the attack complexity of position-based quantum cryptography.

Then, we introduced a practical position-verification scheme, the Interleaved Product protocol, which appears to be immune to these attacks and displays the further advantage of being loss-tolerant in a scenario where the quantum state is distributed independently from the classical challenge.

4 Some generalizations of the CHSH game

1 Introduction

In this chapter, we are interested in a variant of the CHSH game introduced by Buhrman and Massar [BM05]. This game, denoted CHSH_Q, is a natural generalisation of CHSH when inputs and outputs belong to the field $\mathbb{F}_Q$, where Q a prime power. More precisely, two non-communicating parties, Alice and Bob, receive inputs x and y chosen uniformly at random from $\mathbb{F}_Q$, and output two elements a, b from $\mathbb{F}_Q$. They win the game whenever the condition $a+b = xy$ is satisfied. In [BM05] Buhrman and Massar considered the CHSH_3 game, and using the non-signalling principle together with a Fourier analysis over finite fields, they established the following upper bound on its quantum value.

$$\omega^*(\mathrm{CHSH}_3) \leqslant \frac{2}{3\sqrt{3}} + \frac{1}{3}. \tag{4.1}$$

Recently, Bavarian and Shor [BS15] studied the case of arbitrary $Q = P^k$, where P is a prime number. They obtained the following upper and lower bounds on the classical value of the game:

$$\omega(\mathrm{CHSH}_Q) = O\left(Q^{-1/2-\varepsilon_0}\right) \quad \text{when } k \text{ is odd}, \tag{4.2}$$

$$= \Omega(Q^{-1/2}) \quad \text{when } k \text{ is even}, \tag{4.3}$$

where $\varepsilon_0 > 0$ is a universal constant. They also proved the following upper bound for the quantum value:

$$\omega^*(\mathrm{CHSH}_Q) \leqslant \frac{Q-1}{Q\sqrt{Q}} + \frac{1}{Q}. \tag{4.4}$$

In this thesis, we are mostly interested in variants of these CHSH_Q games that are relevant in the context of relativistic bit commitment (see Chapter 5). We define families of games where the input distribution for Alice is no longer uniform over $\mathbb{F}_Q$, but is such that the most likely input has probability at most p for some parameter $p \in [1/Q, 1]$. We denote such a family by $\mathrm{CHSH}_Q(p)$.

For these games, Bob's input distribution is still uniform over $\mathbb{F}_Q$. In particular, $\mathrm{CHSH}_Q(1/Q)$ is restricted to the single game CHSH_Q.

In [SCK14], Sikora *et al.* studied an asymmetric variation of the CHSH_Q game, where Alice receives a random bit $x \in \{0, 1\}$ as input and Bob receives a random element y from $\mathbb{F}_Q$, where $Q = 2^k$, for some positive integer k. They win the game iff $a + b = xy$, where $a, b \in \mathbb{F}_Q$. Clearly, this game belongs to the family $\mathrm{CHSH}_Q(\frac{1}{2})$. They establish an upper bound for the quantum value of their specific game G:

$$\omega^*(G) \leqslant \frac{1}{2} + \frac{1}{\sqrt{2Q}}.$$

Let us now formally define the family $\mathrm{CHSH}_Q(p)$.

Definition 4.1. *For Q a prime or power of prime, and $p \in [\frac{1}{Q}, 1]$, we say that a bipartite non-local game G belongs to the $\mathrm{CHSH}_Q(p)$ family if :*

- *Alice ($\mathcal{A}$) receives $x \in \mathbb{F}_Q$ with probability p_x, satisfying $\max_x p_x \leqslant p$ and Bob ($\mathcal{B}$) receives y uniformly at random from $\mathbb{F}_Q$.*
- *Alice outputs $a \in \mathbb{F}_Q$ and Bob outputs $b \in F_Q$.*
- *They win the game iff a and b satisfy the following equation:*

$$a + b = xy, \tag{4.5}$$

where addition and multiplication are defined over the finite field $\mathbb{F}_Q$.

In Section 2, we prove an upper bound on the classical value of arbitrary games in the $\mathrm{CHSH}_Q(p)$ family. Then in Section 3, we consider yet another variant of the CHSH game where Bob's input is drawn from a subset of $\mathbb{F}_Q$.

2 Upper bound on the classical value of games in $\mathrm{CHSH}_Q(p)$

Our general approach to establish upper bounds on the values of games in $\mathrm{CHSH}_Q(p)$ is to show that if Alice and Bob can win with high probability then it gives Alice a way to obtain some information about Bob's input, something that is prohibited by the non-signalling principle. When Alice and Bob are restricted to classical strategies, we prove the following:

Theorem 4.1. *For any game $G \in \mathrm{CHSH}_Q(p)$, we have*

$$\omega(G) \leqslant p + \sqrt{\frac{1}{Q}}. \tag{4.6}$$

Proof. Fix a game $G \in \mathrm{CHSH}_Q(p)$. Without loss of generality, we can assume that Alice's and Bob's strategies are deterministic since any randomised strategy can be modelled as a convex combination

of deterministic strategies. It is therefore sufficient to model Alice and Bob's strategies as functions $f, g : \mathbb{F}_Q \to \mathbb{F}_Q$, namely: $a = f(x)$ and $b = g(y)$. Let us define the binary variable r_x^y equal to 1 if $f(x) + g(y) = xy$ and 0 otherwise. The classical value of the game can be written as:

$$\omega(G) = \max_{f,g} \frac{1}{Q} \sum_{x,y} p_x r_x^y. \tag{4.7}$$

Our proof is by contradiction: if $\omega(G)$ is too large, then Alice could use her strategy to obtain some information about y, which is prohibited by non-signalling.

Alice's strategy to learn Bob's input:

The idea behind Alice's strategy is to play the game twice: if she wins both, then she can infer Bob's input. More precisely,

(i) Alice picks a random pair of distinct inputs (x, x') with probability $p_x p_{x'}/D$ where $D = \sum_{x \neq x'} p_x p_{x'}$.

(ii) Alice outputs $a = f(x), a' = f(x')$ and Bob outputs b.

(iii) Alice's guess for Bob's input is $\hat{y} = (f(x) - f(x'))(x - x')^{-1}$.

Analysis of Alice's guessing strategy:

It is easy to see that if Alice and Bob can win the game with probability 1, then her guess for Bob's input is always correct, which would violate the non-signalling constraint. We now analyze the case where the value of the game is bounded away from 1. Let S_y be the probability of correctly guessing the value y. Non-signalling imposes that the expectation of S_y is equal to $1/Q$, $\mathbb{E}_y[S_y] = 1/Q$, since the value y is uniformly distributed in $\mathbb{F}_Q$.

Similarly as in the discussion above, we note that if the game G is won for both inputs (x, y) and (x', y), then Alice's strategy outputs the correct value for y. Indeed, winning the game implies that $f(x) - f(x') = (x - x')y$ and therefore $\hat{y} = y$. We obtain the following lower bound on S_y:

$$S_y \geqslant \frac{1}{D} \sum_{x \neq x'} p_x r_x^y p_{x'} r_{x'}^y \tag{4.8}$$

$$\geqslant \sum_{x \neq x'} p_x r_x^y p_{x'} r_{x'}^y. \tag{4.9}$$

Consider the quantity $\omega^y(G) = \sum_x p_x r_x^y$. Note that the classical value of the game corresponds to the expectation of $\omega^y(G)$: $\omega(G) = \mathbb{E}_y[\omega^y(G)]$. Furthermore, $\omega^y(G)$ satisfies:

$$\begin{aligned}
(\omega^y(G))^2 &= \sum_x p_x^2 (r_x^y)^2 + \sum_{x \neq x'} p_x r_x^y p_{x'} r_{x'}^y \\
&\leqslant \sum_x p_x^2 (r_x^y)^2 + S_y \\
&= \sum_x (p_x)^2 r_x^y + S_y \leqslant p\omega^y(G) + S_y,
\end{aligned}$$

where we used that $(p_x)^2 \leqslant (\max_x\{p_x\})\, p_x \leqslant p p_x$. This yields

$$\begin{aligned}\omega^y(G) &\leqslant \frac{1}{2}\left(p + \sqrt{p^2 + 4S_y}\right)\\ &\leqslant p + \sqrt{S_y},\end{aligned}$$

where the last inequality results from the concavity of the square-root function.

Derivation of the Upper Bound:

Finally, since $\omega(G) = \mathbb{E}_y[\omega^y(G)]$ by definition, we obtain:

$$\begin{aligned}\omega(G) &\leqslant p + \mathbb{E}_y[\sqrt{S_y}]\\ &\leqslant p + \sqrt{\mathbb{E}_y[S_y]}\\ &\leqslant p + \sqrt{1/Q},\end{aligned}$$

which concludes the proof. □

3 A generalization of $\mathrm{CHSH}_Q(p)$ games with restricted inputs.

Here, we consider a slight variant of the $\mathrm{CHSH}_Q(p)$ games where the only difference is now that Bob's inputs are drawn uniformly from a subset S of $\mathbb{F}_Q$. We denote this class of games by $\mathrm{CHSH}_Q^S(p)$. In particular, one has $\mathrm{CHSH}_Q(p) = \mathrm{CHSH}_Q^{\mathbb{F}_Q}(p)$. These games will be relevant for analysing the binding property of some *loss-tolerant* relativistic bit commitment protocols in Chapter 5. Although the analysis is very similar to that of the previous section, we include it here for completeness.

Lemma 4.2. *For any game $G \in \mathrm{CHSH}_Q^S(p)$, we have*

$$\omega(G) \leqslant p + \sqrt{\frac{1}{|S|}}. \tag{4.10}$$

The proof follows the same strategy as for Theorem 4.1.

Proof. Fix a game $G \in \mathrm{CHSH}_Q^S(p)$. Without loss of generality, Alice and Bob's strategies can be modeled by functions f and g, namely: $a = f(x)$ and $b = g(y)$. Define the variable r_x^y equal to 1 if $f(x) + g(y) = xy$ and 0 otherwise.

Alice's guessing strategy is the same as before:

(i) Alice picks a random pair of distinct inputs (x, x') each with probability $p_x p_{x'}/D$ where $D = \sum_{x \neq x'} p_x p_{x'}$.

(ii) Alice outputs $a = f(x), a' = f(x')$ and Bob outputs b.

(iii) Alice's guess for y is $\hat{y} = (f(x) - f(x'))(x - x')^{-1}$.

Let S_y be the probability of correctly guessing the value y with this strategy. The difference with the previous proof is now that non-signalling imposes that $\mathbb{E}_y[S_y] = 1/|S|$, instead of $1/Q$. As before, we have that

$$\omega^y(G) \leqslant p + \sqrt{S_y}.$$

Taking the expectation and using the concavity of the square-root function, we finally get

$$\omega(G) \leqslant p + \mathbb{E}_y[\sqrt{S_y}] \leqslant p + \sqrt{\mathbb{E}_y[S_y]} \leqslant p + \sqrt{1/|S|}.$$

□

5 Relativistic bit commitment

1 Introduction

In this chapter, we consider relativistic bit commitment protocols and we exploit the results of Chapter 4 to study their security against classical adversaries.

Bit commitment is a cryptographic primitive between two players, Alice (the committer), and Bob (the receiver) who do not trust each other. A bit commitment protocol has two main phases: a *commit phase* and an *open* (or *reveal*) *phase*. Alice commits to a bit d during the commit phase. We say that the protocol is *hiding* if before the open phase, Bob has no information about d. During the open phase, Alice reveals d to Bob, who wants to make sure that Alice didn't change her mind about the value of d. This is termed as the *binding* property.

It is well-known that bit commitment is impossible in the standard model [BOGKW88], even when allowing for quantum protocols [May97, LC97]. In that case, it was shown that a protocol cannot be both hiding and binding. On the other hand, bit commitment becomes possible in the splitting agent model, where the two players Alice and Bob have a coalition of agents at their disposal: $\mathcal{A}_1, \ldots, \mathcal{A}_m$ for Alice, $\mathcal{B}_1, \ldots, \mathcal{B}_m$ for Bob. The basic idea is to dispatch these agents in m distant locations and restrict the information exchange between different locations. This model has been extensively considered in the classical domain since the no communication assumption allows to implement many interesting cryptographic primitives: bit commitment [BOGKW88], oblivious transfer [NP00] or protocols for private information retrieval [GIKM98, KdW04, Gas04].

From a practical point of view, however, the *no communication* assumption is a bit difficult to justify. A convincing way to enforce it is to rely on the *No Superluminal Signaling* (NSS) principle which states that no carrier of information can travel faster than the speed of light. In particular, an event in spacetime cannot be influenced by events which do not lie in its past causal cone.

The idea of using the NSS principle for cryptographic protocols originated in a pioneering work by Kent in 1999 [Ken99] as a way to physically enforce the non communication constraint between the different agents of one party. The original goal of Kent was to bypass the model on which the no-go theorems for quantum bit-commitment [May97, LC97] were proven. Interestingly, this original protocol was classical and allowed for several rounds which increased the lifespan of the

protocol. However, the protocol required to exchange messages whose length scaled exponentially in the number of rounds (*et al.* the commitment time) and a feasible implementation was not possible for a large number of rounds. A subsequent work [Ken05] improved this scaling, but to our knowledge, no precise time/security tradeoff is available for this protocol.

More recently, quantum relativistic bit commitment protocols were developed where the parties exchange quantum systems, with the hope that combining the NSS principle with quantum theory will lead to more secure (but less practical) protocols [Ken11, Ken12b, KTHW13]. In particular, the protocol [Ken12b] was implemented in Ref. [LKB$^+$13].

The original idea of [BOGKW88] was recently revisited by Crépeau *et al.* [CSST11] (see also [Sim07]). Based on this work, Lunghi *et al.* devised a multi-round bit commitment protocol involving only four agents, two for Alice and two for Bob [LKB$^+$15]. They managed to prove that this protocol, which we call the "$\mathbb{F}_Q$ protocol" from now on, remains secure for several rounds, against classical attacks. Unfortunately, this proof was rather inefficient since the complexity of the protocol (the size of the messages the agents need to exchange at each round) scaled exponentially with the number of rounds. This make the protocol impractical for realistic applications. For instance, with the optimal configuration on Earth (meaning that each party has agents occupying antipodal locations on Earth), the commitment time is limited to less than a second.

In Section 2, we provide a new security analysis of the $\mathbb{F}_Q$-protocol, establishing that it remains secure even after a very large number of rounds, provided that the dishonest player is classical. This much better scaling shows that the protocol is actually quite practical, and a convincing experiment recently demonstrated the possibility of sustaining a commitment for 24 hours [VMH$^+$16], consisting of 5×10^9 rounds.

Although quite impressive, it should be noted that this implementation crucially used a one meter dedicated optical link between $\mathcal{A}_1$ and $\mathcal{B}_1$ (as well as between $\mathcal{A}_2$ and $\mathcal{B}_2$). In order to implement the protocol in a more realistic fashion, Alice and Bob's agents would need to communicate over a real telecom network, which is prone to rare failures, for instance delays in packet deliveries that would invalidate the no communication assumption and would cause the protocol to abort.

A caveat is that the commitment time is intrinsically limited by the spatial configuration of the players, and increasing this time requires the agents to exchange messages during the whole duration of the protocol. While such a solution remains computationally attractive, its practicality is severely limited in realistic settings since all communication must remain perfectly synchronized at all times.

In Section 3, we introduce a robust protocol for relativistic bit commitment that tolerates failures of the classical communication network. This is done by adding a third agent to both parties. Our scheme provides a quadratic improvement in terms of expected sustain time compared to the original protocol, while retaining the same level of security. An important drawback of the $\mathbb{F}_Q$ protocol is that it is not at all robust against losses, or delays. Indeed, for the bit commitment to succeed, it is crucial that the various agents communicate with perfect synchronization for all k rounds of the protocol: if one agent fails to answer one challenge in time, then the whole protocol aborts. While this could be fine for small values of k, say $k \leqslant 10$, this is obviously disastrous for much larger values, for instance k ranging in the millions or billions as in [VMH$^+$16]. For this reason, it is important to see whether some variant of the $\mathbb{F}_Q$ protocol can be made tolerant against (a limited) amount of losses.

This chapter is based on the following two publications,

- **Arbitrarily Long Relativistic Bit Commitment**
  K. Chakraborty, A. Chailloux and A. Leverrier,
  Physical Review Letters, **115**, 250501 (2015).

- **Robust relativistic bit commitment**,
  K. Chakraborty, A. Chailloux, and A. Leverrier,
  Physical Review A, **94.6**, 062314 (2016).

2 Multi-round relativistic bit commitment

In this part of the chapter, we investigate the multi-round $\mathbb{F}_Q$ protocol, proposed by Lunghi *et al.* [LKB$^+$15]. Here we mostly analyse the binding property of the protocol. For completeness, in Section 2.1 of this chapter we give the description of the protocol. Section 2.2 discusses about the notations we use to prove the security in the next chapter. Finally, in Section 2.3 we prove its security against classical adversaries. We prove that the attackers winning probability scales linearly with the number of rounds.

2.1 Description of the commitment schemes

In this section, we describe successively the single-round protocol (with commitment time bounded by $\tau = D/c$ where D is the distance between the distant locations and c is the speed of light), the $\mathbb{F}_Q$ multi-round protocol.

For simplicity of analysis, in this chapter we consider that all computations are performed instantaneously and that information travels at the speed of light. One could relax these assumptions by replacing τ by a smaller constant, but this would not change the various scalings of parameters and we therefore ignore this issue here.

The single-round protocol

Here we describe the single-round relativistic bit commitment protocol which was introduced by Crépeau *et al.* [CSST11] (see also [Sim07]). Both players, Alice and Bob, have agents $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{B}_1, \mathcal{B}_2$ present at two spatial locations, L_1 and L_2, separated by a distance D. We consider the case where Alice makes the commitment. The protocol (followed by honest players) consists of four phases: preparation, commit, sustain and reveal. The sustain phase in the single-round protocol is trivial and simply consists in waiting for a time less than τ, which is the time needed for light to travel between the two locations.

Overall the bit commitment protocol goes as follows.

(i) *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share a random number $a \in \mathbb{F}_Q$ (resp. $b \in \mathbb{F}_Q$). Here, for simplicity we assume that Q is of the form 2^m, for some integer $m \geqslant 1$.

(ii) *Commit phase*: $\mathcal{B}_1$ sends b to $\mathcal{A}_1$, who returns $y = a + d * b$ where $d \in \mathbb{F}_2$ is the committed bit. Here and everywhere in this paper, all operations like $+$ and $*$ are understood as addition and

multiplications in $\mathbb{F}_Q$.

(iii) *Sustain phase*: $\mathcal{A}_1$ and $\mathcal{A}_2$ wait for some time less than τ.

(iv) *Reveal phase*: $\mathcal{A}_2$ reveals the values of d and a to $\mathcal{B}_2$ who checks that $y = a + d * b$.

The $\mathbb{F}_Q$-protocol (multi-round)

The single-round protocol above was recently extended to a multi-round commitment scheme [LKB$^+$15]. The main idea to increase the commitment time is to delay the reveal phase and have $\mathcal{A}_2$ commit to the *string* a instead of revealing it. In fact, the new sustain phase will now consist of many rounds where the active agents (*i.e.* the agent of Alice who commits in that given round and the corresponding agent for Bob) alternate between locations L_1 and L_2. Overall the k-round bit commitment protocol goes as follows (for k even):

(i) *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share k random numbers $a_1, \ldots, a_k$ (resp. $b_1, \ldots, b_k$) $\in \mathbb{F}_Q$.

(ii) *Commit phase* (round 1): $\mathcal{B}_1$ sends b_1 to $\mathcal{A}_1$, who returns $y_1 = a_1 + d * b_1$ where $d \in \mathbb{F}_2$ is the committed bit.

(iii) *Sustain phase*: At round $j \leqslant k$, active Bob sends $b_j \in \mathbb{F}_Q$ to active Alice, who returns $y_j = a_j + b_j * a_{j-1}$.

(iv) *Reveal phase*: $\mathcal{A}_1$ reveals d and a_k to $\mathcal{B}_1$. $\mathcal{B}_1$ computes recursively $\alpha_0 = d$ and $\alpha_{i+1} = y_{i+1} - b_{i+1} * \alpha_i$ and checks that $\alpha_k = a_k$. If this is the case, Alice has successfully revealed the bit d.

The main idea of the multi-round protocol is to delay the reveal phase in order to increase the commitment time. This delay is obtained by making the passive Alice commit to the value of the string she was supposed to reveal in the previous round. Since each round increases the total commitment time by a quantity equal to τ (modulo the time needed for the various algebraic manipulations in $\mathbb{F}_Q$ that we ignore), one sees that the required number of rounds scales linearly with the commitment time one wishes to achieve.

We require that round j finishes before any information about b_{j-1} reaches the other Alice. This implies that for any j, Alice's active agent has no information about b_{j-1}. In particular, this means that y_j is independent of b_{j-1}. This will be crucial in order to show security of the protocol.

2.2 Notations and definitions

In this section, we define the notations which we are going to use for analysing the security of multi-round $\mathbb{F}_Q$-protocol.

In order to prove the binding property of the protocol we consider the case of a cheating Alice. At round j, active Alice receives a string $b_j \in \mathbb{F}_Q$ and sends back a message y_j. We denote the cheating Alice's strategy as a deterministic function $y_\cdot : \mathbb{F}_2 \times \mathbb{F}_Q \times \ldots \times \mathbb{F}_Q \to \mathbb{F}_Q$. In the protocol from

the relativistic constraints, we know that this message y_j is totally independent of b_{j-1}. Therefore we can consider y_j as a function of $d, b_1, \ldots, b_{j-2}, b_j$. We also recursively define the functions $\alpha_j = y_j - (b_j * \alpha_{j-1})$, with $\alpha_0 = d$. This implies $\alpha_j : \mathbb{F}_2 \times \mathbb{F}_Q \times \ldots \times \mathbb{F}_Q \to \mathbb{F}_Q$ is a function of $d, b_1, \ldots, b_{j-2}, b_j$. These are functions of $d, b_1, \ldots, b_j$.

Here we also define another object called *independence parameter*, which we use in the next section to quantify how independent one function is from one of its input variable. Formally we define the independence parameter of function f for a variable y as follows :

Definition 5.1 (Independence parameter of a variable on a function)**.** *Let $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$ be a function. The* Independence Parameter *of f for variable $y \in \mathcal{Y}$, denoted by $INDP(f||y)$, is defined by*

$$INDP(f||y) := \max_{g:\mathcal{X}\to\mathcal{Z}} \left[\Pr_{x,y}\left[f(x,y) = g(x)\right]\right], \tag{5.1}$$

where we use the uniform measure on $\mathcal{X} \times \mathcal{Y}$.

By definition, the case $INDP(f||y) = 1$ corresponds to a function f independent of y. If $INDP(f||y) < 1$, then the function f depends on y.

2.3 Security of multi-round $\mathbb{F}_Q$ protocol

In this section, we give proofs of the hiding and binding properties of multi-round $\mathbb{F}_Q$ protocol. The two protocols described above all share the property that they are perfectly hiding. Indeed, the role of the variables a's shared by Alice's agents is to hide the value of d. If all the a's are chosen uniformly at random from $\mathbb{F}_Q$ which is the case if Alice follows honestly the protocol, then they provide a one-time pad of the secret and Bob's agents cannot obtain any information about the value of d before the reveal phase.

For this reason, our goal is to study whether these protocols are binding. In particular, this means that we will only be interested in the case where Bob is honest and follows the protocol, and Alice's agents might deviate from the protocol in order to reveal a bit that is not necessarily the one they had in mind during the commit phase. In this paper, we assume that Alice is classical, *i.e.*, that her agents only share classical variables and not an entangled quantum state for instance. The question of proving security against a quantum adversary is left for future research.

Against classical adversary for k-round $\mathbb{F}_Q$-protocol we have the following theorem,

Theorem 5.1. *The k-round $\mathbb{F}_Q$ protocol is ε-binding against classical adversary, with $\varepsilon \leqslant 2k\sqrt{\frac{1}{Q}}$ where k is the number of rounds used in the protocol.*

Sketch

Let us give a brief overview of the proof. Our goal is to prove that the value of ε, in the definition of *sum-binding* (defined in Section 4 of Chapter 2), is upper bounded by a quantity which is negligible

in $\lceil \log q \rceil$. To prove the upper bound, first we establish a connection between the ε in the definition of *sum-binding* property and *independence parameter*, $INDP(\alpha_k||b_k)$. The connection is of the following form,

$$1 + \varepsilon = 2INDP(\alpha_k||b_k). \tag{5.2}$$

At round $j \leqslant k$, we give a recursive upper bound on the quantity $INDP(\alpha_j||b_j)$ in terms of $INDP(\alpha_{j-1}||b_{j-1})$. Explicitly, the upper bound is of the following form,

$$INDP(\alpha_j||b_j) \leqslant INDP(\alpha_{j-1}||b_{j-1}) + \sqrt{\frac{1}{Q}}. \tag{5.3}$$

We derive the above upper bound by relating $INDP(\alpha_j||b_j)$ with the classical value of a non-local game called $\mathrm{CHSH}_Q(p)$. For the base case of this recursion, the value of $INDP(\alpha_0||b_0)$ is related to the classical value of the game $\mathrm{CHSH}_Q(\frac{1}{2})$. By solving the recursive inequality we get the following upper bound on $INDP(\alpha_k||b_k)$.

$$INDP(\alpha_k||b_k) \leqslant \frac{1}{2} + k\sqrt{\frac{1}{Q}}. \tag{5.4}$$

Hence, from Equation 5.2 we get desired upper bound on the value of ε.

Proof of Theorem 5.1

Proof. Let us fix a cheating strategy for Alice, which consists of the messages y_j that the agents will send depending on the current history and the bit d she wants to reveal to. During the reveal phase, Alice successfully reveals d if $\mathcal{A}_1$ sends the correct α_k to Bob. For a fixed cheating strategy, α_k is a function of $d, b_1, \ldots, b_k$. However, during the reveal phase, $\mathcal{A}_1$ has no information about b_k. Therefore, $\mathcal{A}_1$ will not be able to reveal α_k if it has too much dependence in b_k on average on d . We show that this is indeed the case. Note that if Alice's performs a probabilistic cheating strategy, her success probability will be the average of the success probabilities for each possible strategy she performs. It is therefore sufficient to bound Alice's cheating probability over all deterministic strategies. Let us then consider the best deterministic cheating strategy for Alice $Str^* = (Comm^*, Open^*)$: it is fully determined by the functions y_j, as well as a function $g(d, b_1, \ldots, b_{k-1})$ that $\mathcal{A}_1$ uses to guess α_k during the reveal phase. Alice successfully reveals d iff $[g(d, b_1, \ldots, b_{k-1}) = \alpha_k(d, b_1, \ldots, b_k)]$. Therefore, we have

$$\begin{aligned}
1 + \varepsilon &= \Pr[\text{Alice successfully reveals } d = 0|Str^*] + \Pr[\text{Alice successfully reveals } d = 1|Str*] \\
&= \Pr_{b_1,\ldots,b_k}[g(0, b_1, \ldots, b_{k-1}) = \alpha_k(0, b_1, \ldots, b_k)] + \\
&\Pr_{b_1,\ldots,b_k}[g(1, b_1, \ldots, b_{k-1}) = \alpha_k(1, b_1, \ldots, b_k)] \\
&= 2 \Pr_{d,b_1,\ldots,b_k}[g(d, b_1, \ldots, b_{k-1}) = \alpha_k(d, b_1, \ldots, b_k)].
\end{aligned} \tag{5.5}$$

Intuitively, Alice will be able to win if the function α_k is independent of b_k, on average on d and the other b_i. We will prove that α_k has some large dependence on b_k, which will limit Alice's cheating possibilities. We will actually show by induction that for each j, the function a_j has some large dependency on b_j.

The definition of the independence parameter immediately yields $1 + \varepsilon = 2INDP(\alpha_k||b_k)$, and our goal is therefore to obtain a tight upper bound for $INDP(\alpha_k||b_k)$.

We prove the following :

Proposition 5.1. $\forall j,\ INDP(\alpha_j||b_j) \leqslant \frac{1}{2} + j\sqrt{\frac{1}{Q}}$.

Proof. We prove the proposition by induction on j.

Let us first consider the base case:

$$INDP(\alpha_1||b_1) = \max_{g:\mathbb{F}_Q \to \mathbb{F}_Q} \Pr_{d,b_1}[\alpha_1(d, b_1) = g(d)] \tag{5.6}$$

where b_1 is uniformly distributed in $\mathbb{F}_Q$ and d is equal to either 0 or 1, each with probability $1/2$. Let g the function that maximizes the above expression, which gives $INDP(\alpha_1||b_1) = \Pr_{d,b_1}[\alpha_1(d, b_1) = g(d)]$. We write $\alpha_1(d, b_1) = y_1(b_1) + (b_1 d)$ for some function y_1. We now use the functions g and y_1 to construct a strategy for a game $G \in \mathrm{CHSH}_Q(1/2)$. The game $\mathrm{CHSH}_Q(\frac{1}{2})$ is defined as follows:

- Adeline receives a random element $x \in \mathbb{F}_Q$. Bastian receives an element $y \in \mathbb{F}_Q$ which is equal to 0 with probability $1/2$ and 1 with probability $1/2$.
- Their goal is to respectively output a and b in $\mathbb{F}_Q$ such that $a + b = xy$.

The above game is in $\mathrm{CHSH}_Q(1/2)$. Intuitively, we mapped $\mathcal{A}_1$ to Adeline and $\mathcal{A}_2$ to Bastian, where the input x corresponds to b_1 and the input y corresponds to d.

We consider the following strategy for this game: Adeline outputs $a = y_1(x)$ and Bastian outputs $b = -g(y)$. They win the game iff $y_1(x) - g(y) = xy$. Therefore, we have

$$\begin{aligned}\omega(G) &\geqslant \Pr_{x,y}[y_1(x) - g(y) = xy] = \Pr_{x,y}[\alpha_1(y, x) + xy - g(y) = xy] \\ &= \Pr_{x,y}[\alpha_1(y, x) = g(y)] = INDP(\alpha_1||b_1).\end{aligned}$$

Combining this lower bound on the value $\omega(G)$ of the game with Theorem 4.1 applied to $G \in \mathrm{CHSH}_Q(1/2)$ gives $INDP(\alpha_1||b_1) \leqslant \omega(G) \leqslant \frac{1}{2} + \sqrt{\frac{1}{Q}}$, which establishes the base case.

We now move to the induction step and assume that $INDP(\alpha_j||b_j) \leqslant \frac{1}{2} + j\sqrt{\frac{1}{Q}}$. Let us fix $h := (d, b_1, \ldots, b_{j-1})$ the history before time j. Let us define the independence parameter conditioned on the history h:

$$INDP(\alpha_{j+1}||b_{j+1})^h = \max_{g_{j+1}:\mathbb{F}_Q \to \mathbb{F}_Q} \Pr_{b_j, b_{j+1}}[\alpha_{j+1}(h, b_j, b_{j+1}) = g_{j+1}(b_j)].$$

Averaging over h gives back the independence parameter:

$$INDP(\alpha_{j+1}||b_{j+1}) = \mathbb{E}_h[INDP(\alpha_{j+1}||b_{j+1})^h].$$

we write $\alpha_{j+1}(h, b_j, b_{j+1}) = y^h_{j+1}(b_{j+1}) + (b_{j+1} * \alpha_j(h, b_j))$. Notice that the dependence in b_j of the function $\alpha_{j+1}(h, b_j, b_{j+1})$ lies only in the function $\alpha_j(h, b_j)$. Therefore, we can write

$$INDP(\alpha_{j+1}||b_{j+1})^h = \max_{g_{j+1}:\mathbb{F}_Q\to\mathbb{F}_Q} \Pr_{b_j,b_{j+1}}[\alpha_{j+1}(h, b_j, b_{j+1}) = g_{j+1}(\alpha_j(h, b_j))].$$

Let g^h_{j+1} be the function that maximizes the expression:

$$INDP(\alpha_{j+1}||b_{j+1})^h = \Pr_{b_j,b_{j+1}}[\alpha_{j+1}(h, b_j, b_{j+1}) = g^h_{j+1}(\alpha_j(h, b_j))].$$

We now use the functions y^h_{j+1} and g^h_{j+1} to construct a strategy for a game $G^h_{j+1} \in \mathrm{CHSH}_Q(INDP(\alpha_j||b_j)^h)$. We consider the following game between two players Adeline and Bastian :

- Adeline receives a random element $x \in \mathbb{F}_Q$. Bastian receives an element $y \in \mathbb{F}_Q$ such that $\Pr[y = c] = \Pr_{b_j}[\alpha_j(h, b_j) = c]$.
- Their goal is to respectively output a and b in $\mathbb{F}_Q$ such that $a + b = xy$

Intuitively, we mapped the active Alice (during round $j + 1$) to Adeline and the passive Alice to Bastian, where the input x corresponds to b_{j+1} and the input y corresponds to a_j. Recall that the active Alice has no information about b_j during step $j + 1$. Therefore, she can determine α_j with probability at most: $INDP(\alpha_j||b_j)^h := \max_c \Pr_{b_j}[\alpha_j(h, b_j) = c]$. This shows that the above game G^h_{j+1} is in $\mathrm{CHSH}_Q(INDP(\alpha_j||b_j)^h)$.

We consider the following strategy for this game: Adeline outputs $a = y^h_{j+1}(x)$ and Bastian outputs $b = -g^h_{j+1}(y)$. They win the game iff $y^h_{j+1}(x) - g^h_{j+1}(y) = xy$, which implies that

$$\begin{aligned}
\omega(G^h_{j+1}) &\geqslant \Pr_{x,y}[y^h_{j+1}(x) - g^h_{j+1}(y) = xy] \\
&= \Pr_{x,b_j}[y^h_{j+1}(x) - g^h_{j+1}(\alpha_j(h, b_j)) = x\alpha_j(h, b_j)] \\
&\qquad \text{where the distribution over both } x \text{ and } b_j \text{ is uniform} \\
&= \Pr_{x,b_j}[\alpha_{j+1}(h, b_j, x) + (\alpha_j(h, b_j)x) - g^h_{j+1}(\alpha_j(b_j)) = (x\alpha_j(h, b_j))] \\
&= \Pr_{x,b_j}[\alpha_{j+1}(h, b_j, x) = g^h_{j+1}(\alpha_j(h, b_j))] \\
&= INDP(\alpha_{j+1}||b_{j+1})^h.
\end{aligned}$$

Moreover, Theorem 4.1 shows that $\omega(G^h_{j+1}) \leqslant INDP(\alpha_j||b_j)^h + \sqrt{\frac{1}{Q}}$ since the game G belongs to $\mathrm{CHSH}_Q(INDP(\alpha_j||b_j)^h)$. Combining both inequalities gives:

$$INDP(\alpha_{j+1}||b_{j+1})^h \leqslant INDP(\alpha_j||b_j)^h + \sqrt{\frac{1}{Q}}. \tag{5.7}$$

In order to conclude, notice that $INDP(\alpha_j||b_j) = \mathbb{E}_h[INDP(\alpha_j||b_j)^h]$ and $INDP(\alpha_{j+1}||b_{j+1}) = \mathbb{E}_h[INDP(\alpha_{j+1}||b_{j+1})^h]$. Taking the expectation of Equation (5.7) over the history h finally gives:

$$\begin{aligned} INDP(\alpha_{j+1}||b_{j+1}) = \mathbb{E}_h[INDP(\alpha_{j+1}||b_{j+1})^h] &\leqslant \mathbb{E}_h\left[INDP(\alpha_j||b_j)^h + \sqrt{\frac{1}{Q}}\right] \\ &= INDP(\alpha_j||b_j) + \sqrt{\frac{1}{Q}} \\ &\leqslant \frac{1}{2} + (j+1)\sqrt{\frac{1}{Q}}. \end{aligned}$$

□

Proposition 5.1 implies that $INDP(\alpha_k||b_k) \leqslant \frac{1}{2} + k\sqrt{\frac{1}{Q}}$, and Equation (5.5) allows us to conclude that the protocol is ε-binding with $\varepsilon \leqslant 2k\sqrt{\frac{1}{Q}}$. □

3 The loss-tolerant Tree protocol

In this section, we show how to make the original multi-round $\mathbb{F}_Q$ protocol loss tolerant. Here we modify the $\mathbb{F}_Q$ protocol so that both parties have now three agents at their disposal instead of two. We present the protocol in Section 3.1. We prove its security against classical adversaries in Section 3.2 where we show that the security scales similarly as for the $\mathbb{F}_Q$ protocol. Finally, in Section 3.4, we show that the communication cost of the protocol is comparable to that of the $\mathbb{F}_Q$ protocol but that its expected commitment time is quadratically improved.

3.1 Description of the protocol

In order to formulate a loss-tolerant variant of the $\mathbb{F}_Q$-protocol, we require that each party has 3 agents located at three locations L_1, L_2, L_3 which are at least at a distance D from each other. As in the $\mathbb{F}_Q$ multi-round protocol, timing constraints are represented by rounds. In the original protocol, at each round, a pair of agents $(\mathcal{A}_i, \mathcal{B}_i)$ performs a communication round, consisting of a challenge b_i from Bob's agent to Alice's agent and an answer y_i from Alice's agent to Bob's.

Our k-round Tree protocol is represented by the complete binary tree of depth k with $2^{k+1} - 1$ nodes (recalling that the tree with a single node has depth 0 by convention). The depth of a node v is equal to the length $|v|$ of the string v. A node of the tree is a string v of $j \leqslant k$ letters in the alphabet $\{\ell, r\}$, corresponding to left or right child. Let us denote by V the set of all nodes of the tree, so that $|V| = 2^{k+1} - 1$ and by V^* the set of all internal nodes of the tree, that is nodes that are not leaves. Let us further denote $n_k = |V^*| = 2^k - 1$ the cardinality of V^*. The root of the tree is the empty string $\varnothing$. A given node v of depth $j < k$ has two children, a left child $v\ell$ and a right child vr. A node v of depth $j \geqslant 1$ has a unique parent $v(\text{parent})$ and a unique brother $v(\text{brother})$: indeed, if v is of the form wt with $t \in \{\ell, r\}$, then $v(\text{parent}) = w$ and $v(\text{brother}) = w\bar{t}$ where $\bar{t}$ is the element of $\{\ell, r\}$ distinct from t.

To describe the Tree protocol, we need a 3-coloring c of this complete binary tree of depth k. The coloring c is a function

$$c : \left\{ \begin{array}{ccc} V & \to & \{1,2,3\} \\ v & \mapsto & c(v) \end{array} \right.$$

where V is the set of all $2^{k+1}-1$ nodes in the tree, with the coloring property that for all v of depth $j < k$, it holds that

$$\{c(v), c(v\ell), c(vr)\} = \{1,2,3\}.$$

The above constraints on the colors means that for any node v, the colors $c(v), c(v\ell)$ and $c(vr)$ are all different. In particular, two brothers have different color (see Fig. 5.1). This coloring will be used to assign a location L_1, L_2 or L_3 to each node of the tree. In other words, each node of the tree corresponds to a communication round taking place at the location $L_{c(v)}$ corresponding to the color $c(v)$ of the node v.

More precisely, each node v of depth j of the tree corresponds to a communication round with a challenge b_v and an answer y_v between agents $\mathcal{A}_{c(v)}$ and $\mathcal{B}_{c(v)}$ at round $j+1$. For a fixed depth, several nodes can have the same color col, the corresponding agents $\mathcal{A}_{col}$ and $\mathcal{B}_{col}$ will then perform all those communication rounds at this time $j+1$. The leaves of the protocol correspond to the revealing phase.

The new notion that appears in the context of loss-tolerant protocols is that of a *dead or alive* node: we will say that a node v fails (or is dead, or non responsive) if the corresponding agent $\mathcal{A}_{c(v)}$ fails to answer the challenge sent to her by $\mathcal{B}_{c(v)}$ within time τ at round $j = |v| - 1$. Alternatively, an agent is *alive* (or responsive) if she succeeds in replying in time to the challenge. In order to account for this extra piece of information, we will denote by $\perp$ Alice's answer in case her agent is non responsive for a given node. Said otherwise, while Bob challenges will still be elements of $\mathbb{F}_Q$, the answers of Alice's agents are elements of $\mathbb{F}_Q \cup \{\perp\}$.

This failure can result from a global failure of the network for one agent i for some rounds, in which case for all nodes v of the corresponding depth with $c(v) = i$, we will have $b_v = \perp$. It may also happen that agent $\mathcal{A}_i$ may answer some queries in time but not some others, which will result in the corresponding nodes being alive or dead. Of course, a cheating Alice will try to exploit such failures to increase to probability to successfully reveal the bit d of her choice.

Overall the k-round Tree bit commitment protocol goes as follows (for $k \geqslant 2$):

(i) *Preparation phase*: Agents $\mathcal{A}_i$ and $\mathcal{B}_i$ are located at L_i for $i \in \{1,2,3\}$. Moreover, $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ (resp. $\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3$) share $n_k = 2^k - 1$ random numbers $(a_v)_{v \in V^*} \in \mathbb{F}_Q^{n_k}$ (resp. $(b_v)_{v \in V^*} \in \mathbb{F}_Q^{n_k}$). This means that the agents share random numbers for all the internal nodes of the tree (not for the leaves). Alice's agents also share $d \in \{0,1\}$ which is the committed bit.

(ii) *Commit phase* (round 1): $\mathcal{B}_{c(\varnothing)}$ sends $b_\varnothing$ to $\mathcal{A}_{c(\varnothing)}$, who returns $y_\varnothing = a_\varnothing + d * b_\varnothing$. If Bob's agent $\mathcal{B}_{c(\varnothing)}$ does not receive Alice's response before time τ, then the protocol aborts.

(iii) *Sustain phase* (rounds 2 to k): at round $j+1 \leqslant k$, for each node vt of depth $j+1$ (*i.e.* $|v| = j$ and $t \in \{\ell, r\}$), agent $\mathcal{B}_{c(vt)}$ sends $b_{vt} \in \mathbb{F}_Q$ to $\mathcal{A}_{c(vt)}$ who returns $y_{vt} = a_{vt} + b_{vt} * a_v$. If $\mathcal{B}_{c(vt)}$ does not receive Alice's response within time τ, the corresponding value of y_{vt} is set to

the value corresponding to a dead node, that is $y_{vt} = \perp$. When this is the case, the branch is considered to be dead, and Bob's agents stop sending challenges for that particular branch as soon as they know it is dead.

(iv) *Reveal phase*: For each node $v = wt$ of depth k (*i.e.* with $|w| = k - 1$ and $t \in \{\ell, r\}$), Agent $\mathcal{A}_{c(v)}$ reveals d and a_w to $\mathcal{B}_{c(v)}$. Bob's agents check (i) that for each depth $j < k$, the leftmost alive node of the tree has at least one child alive and if it's the case, then (ii) that for the leftmost alive path $(v_0 = \varnothing, v_1, \ldots, v_k = v)$ in the tree, Bob's agents compute recursively the values $\alpha_\varnothing = y_\varnothing - b_\varnothing * d$, $\alpha_{v_i} = y_{v_i} - b_{v_i} * \alpha_{v_{i-1}}$ and check that $\alpha_{v_k} = a_{v_k}$. If both conditions are satisfied, then Alice has successfully revealed the bit d.

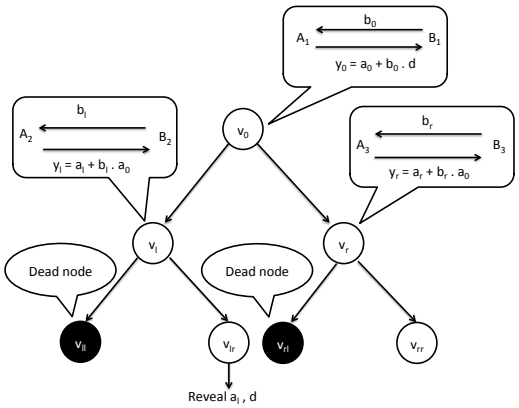

Figure 5.1: Pictorial view for an internal node of the Tree protocol. Here the coloring is such that $c(v) = 1, c(v\ell) = 2, c(vr) = 3$.

Remark: Since only the values of the leftmost alive branch matter for the verification step, it is useless in practice to keep other branches alive. A simple modification of the above protocol consists for Bob's agents to keep track of the leftmost alive branch and stop sending challenges for all other branches. We will analyze this in further detail in Section 3.4 where we investigate the communication cost of the Tree protocol.

3.2 Security of the Tree protocol

In this section, we prove that the multi-round Tree protocol is hiding and binding against classical adversaries. The $\mathbb{F}_Q$-protocol, it is perfectly hiding. If Alice is honest, as all the a's are chosen uniformly at random from $\mathbb{F}_Q$, so they provide a one-time pad of the secret and Bob's agents cannot obtain any information about the value of d before the reveal phase. As the protocol is hiding, we focus on the binding property with honest Bob. Similarly as before we assume that Alice is classical, *i.e.*, that her agents only share classical variables and not an entangled quantum state for instance.

Since, Bob is assumed to be honest in the analysis, it means that his agents are correctly located at stations L_1, L_2 and L_3. In particular, there is no need for them to check where Alice's agents are located: it is sufficient to know that they responded in time to guarantee that for each round, each

of them has to answer their own challenge without having access to the challenges sent to the other agents at the same round.

In all that follows, we consider without loss of generality a deterministic strategy for Alice for the k-round Tree protocol, in which any alive node has at least a live child. Indeed, any probabilisitic cheating strategy can be expressed as a convex sum of deterministic ones, and the optimal strategy is the best one among these deterministic strategies. Moreover, it is useful to understand what an optimal strategy for Alice looks like. Since only the leftmost alive branch matters in the reveal phase, at each round, Alice should make sure that the leftmost alive node has a live child, but she has some freedom to decide which one. It is easy to see that the best strategy is to always keep the right child responsive and to decide whether the keep the left one alive or not based on the value of the challenge it receives. In other words, at each round, the left child of the leftmost alive child will decide either to answer its challenge (in which case, it will be the leftmost alive node at the next round), or to refuse to answer the challenge (in which case, its brother will become the leftmost alive node at the next round).

Sketch

Our goal is to prove the security against a cheating Alice, on average over all of Bob's random strings b, which are drawn from the uniform distribution since Bob is honest. Depending on Alice's strategy and on those strings, the players will follow different leftmost paths in the tree. The idea of the proof will be to use a recursive argument, similarly as in Section 2.3. Informally, the proof will proceed as follows:

For each node v, we will keep track of a quantity $IP(v)$ (the Independence Parameter) that will quantify how independent y_v is from $b_{v(\text{parent})}$. For a fixed node v of depth $j \leqslant k-2$, we will relate $IP(v)$ with $IP(v\ell)$ and $IP(vr)$. Then, if we define IP_j to be the average independence parameter for nodes of depth j, we will use the previous relation to show that $IP_{j+1} \leqslant IP_j + \frac{5}{4}\varepsilon$ where $\varepsilon = O(1/\sqrt{Q})$ is a security parameter. Finally, a bound on IP_0 can be readily derived from known bounds on the classical value of CHSH-like games.

Finally, in order to conclude, we will show that IP_{k-1} corresponds exactly to Alice's cheating probability. Putting this together with the fact that $IP_0 \leqslant \frac{1}{2} + \varepsilon$, we will obtain the desired result.

In the above sketch, we omitted many discussions about the dependencies of the above quantities. In this section, we make the above argument formal, but defer several proofs to the next sections. We will organize this section as follows.

In Subsection 3.3 below, we formally define several notions of history and of independence parameters that will be useful for our proofs. In Subsection 3.3, we relate the independence parameter IP_{k-1} at the last round to the binding property of the protocol. Finally, in Section 3.3, we prove our recursive argument, and therefore prove the security of our protocol.

3.3 Notations & definitions

For any $j \leqslant k$, let $V_{\leqslant j}$ be the set of nodes of depth at most j and $V_{=j}$ the set of nodes of depth j.

Definition 5.2. *For any integer $j \in [k]$, for any set $S \subseteq V_{\leqslant j}$, let H_j^S be the* set of possible histories *of S, i.e. the set of possible commitment values $d \in \{0,1\}$ and strings $b_v \in \mathbb{F}_Q$ for every $v \in S$.*

Since each b_v is an element of $\mathbb{F}_Q$ for $v \in S$, we will identify an element of H_j^S as an element of $\{0,1\} \times \mathbb{F}_Q^{|S|}$.

Let us note that in practice, Bob's agents stop sending challenges to nodes they know to be in a "dead" branch, which means that the corresponding b_v's do not formally belong to $\mathbb{F}_Q$. For the security analysis, hoIver, this is irrelevant since these nodes have no impact on the revealing phase of the bit commitment, which means that we can assume that these b_v's are elements of $\mathbb{F}_Q$, so that the set of histories introduced above is well defined.

We also define $H_j := H_j^{V_{\leqslant j}}$ and $H_j^{-S} := H_j^{(V_{\leqslant j} - S)}$, which correspond respectively to the full history of nodes of depth at most j, and to the full history of such nodes, except for those in the set S. Moreover, we define $H_j^{S-Comm} := H_j^S \backslash \{0,1\}$ as the set H_j^S where we remove the set of the committed bit. This is convenient when we need to talk about the history of the variables b_v's only. In particular, we have $H_j = H_j^S \times H_j^{-S-Comm}$. The set of all possible histories of the tree is $H_{k-1} := H_{k-1}^{V^*}$, since the leaf nodes only consist of Alice revealing (Bob's agents do not send any challenge for those nodes).

Since we assume without loss of generality that Alice follows a deterministic strategy, a history $h \in H_{k-1}$ induces Alice's answers $\{y_v\}_{v \in V^*}$ and therefore, if we run Alice's strategy on some history h, the state of all nodes, alive or dead, is fixed. Similarly, if we consider $h \in H_j$, this induces Alice's answers $\{y_v\}_{v \in V_{\leqslant j}}$ and therefore, all nodes of depth at most j are known to be either alive or dead.

Definition 5.3. *Let $v \in V_{\leqslant j}$ and $h \in H_j$ be a node and a history. We say that h is* consistent with v *if when running Alice's strategy on h, the node v is the leftmost alive one at depth* $\mathrm{depth}(v)$*. We denote by $H_j(v) \subseteq H_j$ the set of histories consistent with v.*

Notice that we have

$$\bigcup_{v \in V_{=j}} H_j(v) = H_j \quad \text{and} \quad \forall v, v' \neq v \in V_{=j},$$
$$H_j(v) \cap H_j(v') = \varnothing,$$

which simply states that each history up to depth j is consistent with exactly one node of $V_{=j}$.

Definition 5.4. *For $v \in V_{\leqslant j}$, $S \subseteq V_{\leqslant j}$ and $h_1 \in H_j^S$, we say that h_1 is* consistent with v *if there exists $h_2 \in H_j^{-S-Comm}$ such that $(h_1, h_2) \in H_j(v)$. We denote by $H_j^S(v) \subseteq H_j^S$ the set of $h_1 \in S$ consistent with v.*

By construction of the protocol, if Alice successfully reveals a value at the end, it means that for all rounds, the leftmost alive node has an alive child. In particular, this implies that the prefix of the leftmost alive branch doesn't change during the execution of the protocol: if v be the leftmost alive node at depth $\mathrm{depth}(v)$ for a given $H_{depth(v)}^S(v)$, then it remains the leftmost alive node at depth $\mathrm{depth}(v)$ for any future history $H_j^S(v)$ with $j > \mathrm{depth}(v)$. We therefore have that for any non root node $v \in V_{\leqslant j}$ and set $S \subseteq V_{\leqslant j}$, $H_j^S(v) \subseteq H_j^S(w)$ where w is the parent of v.

Definition 5.5. *For a fixed vertex $v \in V_{\leqslant j}$, a set $S \subseteq (V_{\leqslant j} - \{v\})$ and a history $h \in H_j^S(v)$, let $B_j^h(v) := \{b_v \in F_Q : (h, b_v) \in H_j^{S \cup \{v\}}(v)\}$ be the set of values for b_v for which node v answers*

in time. Equivalently, $\mathbb{F}_Q - B_j^h(v)$ is the set of questions for which node v will be non responsive, according to Alice's strategy and the history h.

Note that if $v = wl$ is the left child of the leftmost alive node at depth $\mathrm{depth}(v) - 1$, then $B_j^h(v)$ is the set of values in $\mathbb{F}_Q$ for which v chooses to respond in time for Alice's strategy. On the other hand, if $b_v \notin B_j^h(v)$, then the node chooses to be non responsive, and the leftmost alive node at that round becomes the right brother of v. Notice that $B_j^h(v)$ is independent of b_w.

Definition 5.6. *For $j \leqslant k$, we define the random variable Z_j which takes value $v \in V_{=j}$ with probability $\frac{H_j(v)}{H_j}$. This random variable corresponds to the node that is the leftmost alive node at depth j.*

For each node v, let us recall that $\mathcal{A}_{c(v)}$ (resp. $\mathcal{B}_{c(v)}$) refers to Alice's (resp. Bob's) agent at that node.

Definition 5.7. *For any node $v \in V_{=j}$, let $Acc(v) \subseteq V_{\leqslant j}$ be the set of nodes containing history information accessible to $\mathcal{A}_{c(v)}$, including the value of the commitment.*

Crucially, the relativistic constraints impose that $v(parent), v(brother) \notin Acc(v)$.

Let us consider a vertex v_j of depth j and a history h consistent with v_j. The leftmost alive path up to depth j has the form $(v_0 = \varnothing, v_1, \ldots, v_j)$. Recall that the variables α_{v_i} are recursively defined for $i \leqslant j$ by

$$\alpha_{v_i} := \begin{cases} y_{v_0} - b_{v_0} * d & \text{if} \quad i = 0, \\ y_{v_i} - b_{v_i} * \alpha_{v_i(parent)} & \text{otherwise.} \end{cases} \tag{5.8}$$

Recall also that α_{v_j} and y_{v_j} are functions of the history H_j since Alice's strategy is deterministic.

Similarly as in [CCL15], we introduce a quantity IP which is the independence parameter between a variable and a function (or a family of functions). Intuitively, this quantity is large if the function is independent of the variable and close to 0 otherwise. In particular, it quantifies how well the function can be approximated by another function that does not depend on the given variable. This is relevant here since in a cheating strategy, Alice's agent tries to answer to Bob's challenge without knowing the value of the challenge sent to her parent, and she wins if she manages to give an answer that depends on that specific challenge.

Definition 5.8. *For any integer $j \leqslant k - 1$, any family of functions $\{g_v : H_j^{Acc(v)}(v) \to \mathbb{F}_Q\}_{v \in V_{=j}}$, we define*

$$IP_j(\{g_v\}_{v \in V_{=j}}) := \\ \mathbb{E}_{v \leftarrow Z_j} \mathbb{E}_{h \leftarrow H_j^{-\{v\}}(v)} \mathbb{E}_{b_v \leftarrow B_j^h(v)} [g_v(d,h) == \alpha_v(d,h,b_v)],$$

where $g_v(d,h) == \alpha_v(d,h,b_v)$ represents the variable that equals 1 if the equality $[g_v(d,h) = \alpha_v(d,h,b_v)]$ holds and 0 otherwise. Moreover, the notation $\mathbb{E}_{v \leftarrow Z_j}$ corresponds to the expectation over the possible values v of the random variable Z_j, and similarly for the other expectations.

Intuitively, this quantity is simply the expectation that Alice's agent (at round $j+1$) gives an answer consistent with the value (α_v) expected by Bob's agent, for the leftmost alive node, when averaging over all possible histories: the restriction on Alice's strategy is that her agent at round $j+1$ does not know the value of b_v at round j. Note here that in the above definition, the function g takes as inputs elements more history elements than those in $H_j^{Acc(v)}(v)$. The function g will simply disregard those inputs. We added them for notational simplicity but we will use later the fact that the outcome $g_v(d,h)$ actually depends only on the history elements of $H_j^{Acc(v)}(v)$.

We are finally in position to define the IP parameter at depth j.

Definition 5.9. *For $j \leqslant k-1$, the IP parameter at depth j is*

$$IP_j := \max_{\{g_v\}_{v\in V_{=j}}} IP_j(\{g_v\}_{v\in V_{=j}}). \tag{5.9}$$

In the next subsection, we provide some motivation for this definition by showing that IP_{k-1} corresponds to Alice's cheating probability. This can be understood intuitively because IP_{k-1} quantifies how well the agents of Alice at the k^{th} round (*i.e.* those you reveal the bit value) can give an answer consistent with Alice's agent's answer at the previous round.

Final condition

Proposition 5.2. *The IP parameter satisfies the following bound:*

$$1+\varepsilon_k \leqslant 2IP_{k-1}$$

where ε_k is the binding security parameter of the k-round protocol.

Proof. Let P_A^* be Alice's cheating probability. Let $P_{A|v}^*$ be Alice's cheating probability when the leftmost alive node at depth $k-1$ is v. We have by definition $P_A^* = \mathbb{E}_{v\leftarrow Z_{k-1}}[P_{A|v}^*]$. Let $\text{leaf}(v)$ be the associated leaf that will be used for the reveal phase: $\text{leaf}(v) = v\ell$ if $v\ell$ is alive, otherwise $\text{leaf}(v) = vr$. Let $(a_{\text{leaf}(v)}, d)$ be Alice's output for that leaf. Recall that Bob then checks whether $\alpha_v = a_{\text{leaf}(v)}$ where α_v is computed recursively as in Equation (5.8). Bob's checking procedure implies that

$$\begin{aligned}
P_{A|v}^* &= \mathbb{E}_{h\leftarrow H_j^{-\{v\}}(v)} \mathbb{E}_{b_v\leftarrow B_j^h(v)}[a_{\text{leaf}(v)}(h) == \alpha_v(h,b_v)] \\
&\leqslant \mathbb{E}_{h\leftarrow H_j^{-\{v\}}(v)}\Big[\\
&\quad \max_{g_v : H_j^{Acc(v)}(v)\to\mathbb{F}_Q} \{\mathbb{E}_{b_v\leftarrow B_j^h(v)}[g_v(h) == \alpha_v(h,b_v)]\}\Big] \\
&=: IP_{k-1}(v)
\end{aligned}$$

where we averaged over all histories giving v as the leftmost node of depth $k-1$. From there, we have

$$P_A^* = \mathbb{E}_{v\leftarrow Z_{k-1}}[P_{A|v}^*] \leqslant \mathbb{E}_{v\leftarrow Z_{k-1}}[IP_{k-1}(v)] = IP_{k-1}$$

By definition of the binding property, it holds that $P_A^* = \frac{1}{2}(1+\varepsilon_k)$, which yields the desired result. □

Proposition 5.2 shows that it is sufficient to prove a good upper bound on IP_{k-1} in order to show that the bit-commitment protocol is binding.

Bounding the value of IP_{k-1}

Our goal is now to bound the value of IP_{k-1}. For this, we will use a recursive argument to bound IP_j for all $j \leqslant k-1$. Before that, we start by finding an expression for IP_j that is suitable for a recursive analysis. Consider a node v of depth $j \leqslant k-2$. For a fixed history $h_0 \in H_{j+1}^{-\{v,v\ell,vr\}}(v)$, two nodes v and vt (with $t \in \{\ell, r\}$), we define the quantity $IP_{vt}^{h_0}$:

$$\begin{aligned} IP_{vt}^{h_0} := \max_{g:\mathbb{F}_Q \to \mathbb{F}_Q} & \mathbb{E}_{b_v \leftarrow B_j^{h_0}(v)} \\ & \mathbb{E}_{b_{vt} \leftarrow B_{j+1}^{h_0,b_v}(vt)} [g(b_v) == \alpha_{vt}(h_0, b_v, b_{vt})], \end{aligned} \tag{5.10}$$

where vt is a child of node v. We show the following:

Proposition 5.3. *For all $j \leqslant k-2$, it holds that:*

$$IP_{j+1} = \mathbb{E}_{v \leftarrow Z_j} \mathbb{E}_{h_0 \leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)} \mathbb{E}_{t \leftarrow T(v|h_0)} [IP_{vt}^{h_0}],$$

where $T(v|h_0)$ is the function that outputs $t \in \{\ell, r\}$ if the leftmost alive child of v is vt.

Proof. Fix an integer j, a node $v \in V_{=j}$ and a history $h_1 \in H_{j+1}^{-\{v\ell,vr\}}(v)$. Let us define $T(v|h_1)$, the random variable equal to 'ℓ' with probability $\frac{|B_{j+1}^{h_1}(v\ell)|}{Q}$ and 'r' with probability $1 - \frac{|B_{j+1}^{h_1}(v\ell)|}{Q}$. If h_1 is consistent with v, then vt with $t = T(v|h_1)$ is the leftmost alive node at depth $j+1$. Let us also define

$$C_t^{h_1}(v\ell) = \begin{cases} B_{j+1}^{h_1}(v\ell) & \text{if } t = \ell \\ \mathbb{F}_Q - B_{j+1}^{h_1}(v\ell) & \text{if } t = r \end{cases}$$

to be the set of possible values of $b_{v\ell}$ conditioned on the node $v\ell$ being responsive (C_ℓ) or not (C_r).

By averaging over histories h_1 consistent with the node v, we define the random variable $T(v)$ equal to 'ℓ' with probability $\frac{|H_{j+1}(v\ell)|}{|H_{j+1}(v)|}$ and to 'r' with probability $\frac{|H_{j+1}(vr)|}{|H_{j+1}(v)|} = 1 - \frac{|H_{j+1}(v\ell)|}{|H_{j+1}(v)|}$:

$$T(v) := \mathbb{E}_{h_1 \leftarrow H_{j+1}^{-\{v\ell,vr\}}(v)} [T(v|h_1)]. \tag{5.11}$$

Lemma 5.2.

$$\begin{aligned} & IP_{j+1}(\{g_{v'}\}_{v' \in V_{=j+1}}) \\ & = \mathbb{E}_{v \leftarrow Z_j} \mathbb{E}_{h_1 \leftarrow H_{j+1}^{-\{v\ell,vr\}}(v)} \mathbb{E}_{t \leftarrow T(v|h_1)} \\ & \mathbb{E}_{b_{v\ell} \leftarrow C_t^{h_1}(v\ell)} \mathbb{E}_{b_{vr} \leftarrow \mathbb{F}_Q} [g_{vt}(d, h_1) == \alpha_{vt}(d, h_1, b_{vt})] \end{aligned}$$

Proof. According to the definition of IP_{j+1} we have,

$$\begin{aligned} & IP_{j+1}(\{g_{v'}\}_{v' \in V_{=j+1}}) \\ & = \mathbb{E}_{v' \leftarrow Z_{j+1}} \mathbb{E}_{h \leftarrow H_{j+1}^{-\{v'\}}(v')} \mathbb{E}_{b_{v'} \leftarrow B_{j+1}^{h}(v')} \\ & [g_{v'}(d, h) == \alpha_{v'}(d, h, b_{v'})] \\ & = \mathbb{E}_{v \leftarrow Z_j} \mathbb{E}_{t \leftarrow T(v)} \mathbb{E}_{h \leftarrow H_{j+1}^{-\{vt\}}(vt)} \\ & \mathbb{E}_{b_{vt} \leftarrow B_{j+1}^{h}(vt)} [g_{vt}(d, h) == \alpha_{vt}(d, h, b_{vt})] \end{aligned}$$

The statement of the lemma follows from the fact that a_{vt} does not depend on $b_{v\bar{t}}$. □

Lemma 5.3.

$$IP_{j+1} = \mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\in H_{j+1}^{-\{v,v\ell,vr\}}(v)}\mathbb{E}_{t\leftarrow T(v|h_0)} \max_{g_{vt}}\mathbb{E}_{b_v\in B_j^{h_0}(v)}\mathbb{E}_{b_{vt}\in B_{j+1}^{(h_0,b_v)}(vt)} [g_{vt}(d,h_0,b_v) == \alpha_{vt}(d,h_0,b_v,b_{vt})].$$

Proof. From Lemma 5.2, we have

$$\begin{aligned} &IP_{j+1}(\{g_{v'}\}) = \\ &\mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_1\leftarrow H_{j+1}^{-\{v\ell,vr\}}(v)}\mathbb{E}_{t\leftarrow T(v|h_1)}\mathbb{E}_{b_{v\ell}\leftarrow C_t^{h_1}(v\ell)}\mathbb{E}_{b_{vr}\leftarrow F_Q} \\ &[g_{vt}(d,h_1,b_{v\bar{t}}) == \alpha_{vt}(d,h_1,b_{vt})] \end{aligned} \tag{5.12}$$

From the definition of IP_j we have,

$$IP_{j+1} = \max_{g_{vt}\in V_{=j+1}} IP_{j+1}(\{g_{v'}\}) \tag{5.13}$$

Since $a_{vt}(d,h_1,b_{vt})$ doesn't depend on $b_{v\bar{t}}$, the value of IP_{j+1} remains unchanged if g_{vt} depends only on h_1. This implies that we can write IP_{j+1} as follows,

$$\begin{aligned} IP_{j+1} &= \max_{g_{vt}}\mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_1\leftarrow H_{j+1}^{-\{v\ell,vr\}}(v)}\mathbb{E}_{t\leftarrow T(v|h_1)} \\ &\quad \mathbb{E}_{b_{vt}\leftarrow B_{j+1}^{h_1}(vt)}[g_{vt}(d,h_1) == \alpha_{vt}(d,h_1,b_{vt})] \\ &= \max_{g_{vt}}\mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{(h_0,b_v)\leftarrow (H_{j+1}^{-\{v,v\ell,vr\}}(v)\times B_j^{h_0})} \\ &\quad \mathbb{E}_{t\leftarrow T(v|h_0,b_v)}\mathbb{E}_{b_{vt}\leftarrow B_{j+1}^{h_0,b_v}(vt)} \\ &\quad [g_{vt}(d,h_1) == \alpha_{vt}(d,h_1,b_{vt})] \end{aligned}$$

where $h_1 = (h_0, b_v)$

$$\begin{aligned} IP_{j+1} &= \max_{g_{vt}}\mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)}\mathbb{E}_{b_v\in B_j^{h_0}} \\ &\quad \mathbb{E}_{t\leftarrow T(v|h_0,b_v)}\mathbb{E}_{b_{vt}\leftarrow B_{j+1}^{h_0,b_v}(vt)} \\ &\quad [g_{vt}(d,h_1) == \alpha_{vt}(d,h_1,b_{vt})] \\ &= \max_{g_{vt}}\mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)}\mathbb{E}_{b_v\in B_j^{h_0}} \\ &\quad \mathbb{E}_{t\leftarrow T(v|h_0)}\mathbb{E}_{b_{vt}\leftarrow B_{j+1}^{h_0,b_v}(vt)} \\ &\quad [g_{vt}(d,h_0,b_v) == \alpha_{vt}(d,h_0,b_v,b_{vt})] \end{aligned}$$

Notice that once we fix a leftmost alive node, the decision to go left or right is independent of b_v. Therefore, we have $T(v|h_0) = T(v|h_0,b_v)$, for any $b_v \in B_j^{h_0}(v)$.

$$IP_{j+1} = \mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)}\mathbb{E}_{t\leftarrow T(v|h_0)}\max_{g_{vt}}\mathbb{E}_{b_v\in B_j^{h_0}} \mathbb{E}_{b_{vt}\leftarrow B_{j+1}^{h_0,b_v}(vt)}[g_{vt}(d,h_0,b_v) == \alpha_{vt}(d,h_0,b_v,b_{vt})].$$

□

For a fixed history $h_0 \in H_{j+1}^{-\{v,v\ell,vr\}}(v)$ and d, we define the quantity $IP_{vt}^{h_0}$ in following manner,

$$\begin{aligned} IP_{vt}^{h_0} := \max_{g^{h_0}} \mathbb{E}_{b_v \leftarrow B_j^{h_0}(v)} \mathbb{E}_{b_{vt} \leftarrow B_{j+1}^{h_0,b_v}(vt)} \\ [g(d, h_0, b_v) == \alpha_{vt}(d, h_0, b_v, b_{vt})]. \end{aligned} \tag{5.14}$$

Substituting the expression of $IP_{vt}^{h_0,d}$ in the expression of IP_{j+1} we get,

$$IP_{j+1} = \mathbb{E}_{v \leftarrow Z_j} \mathbb{E}_{h_0 \in H_{j+1}^{-\{v,v\ell,vr\}}(v)} \mathbb{E}_{t \leftarrow T(v|h_0)} [IP_{vt}^{h_0}]. \tag{5.15}$$

□

We can now proceed to bounding IP_j. We first consider the base case where $j = 0$.

Lemma 5.4.

$$IP_0 \leqslant \frac{1}{2} + \sqrt{\frac{2}{Q}}.$$

Proof. According to the definition of IP_j we have,

$$IP_j = \max_{\{g_v\}_{v \in V_{=j}}} IP_j(\{g_v\}_{v \in V_{=j}}), \tag{5.16}$$

where,

$$\begin{aligned} IP_j(\{g_v\}_{v \in V_{=j}}) = \mathbb{E}_{v \leftarrow Z_j} \mathbb{E}_{h \leftarrow H_j^{-\{v\}}(v)} \mathbb{E}_{b_v \leftarrow B_j^h(v)} \\ [g_v(d, h) == \alpha_j(d, h, b_v)]. \end{aligned} \tag{5.17}$$

For $j = 0$, *i.e.*, at the root of the tree, we have $V_{=j} = \{v_0\}$, where $v_0 = \varnothing$, $H_0^{-\{v_0\}}(v_0)$ contains only the commitment d and $B_j^h(v) = \mathbb{F}_Q$. So, we have $IP_0 = \max_{g_{v_0}} \mathbb{E}_{d \leftarrow \{0,1\}} \mathbb{E}_{b_{v_0} \leftarrow \mathbb{F}_Q} [g_{v_0}(d) == \alpha_{v_0}(d, b_{v_0})]$. Here we give the upper bound on IP_0 by reducing it to an instance G of the following nonlocal games between two players Adeline and Bastian, where

- Adeline receives a random element $b_{v_0} \in \mathbb{F}_Q$. Bastian receives a random element $d \in \{0, 1\}$.
- Their goal is to respectively output A and B in $\mathbb{F}_Q$ such that $A + B = b_{v_0} * d$.

Without any loss of generality we can consider Adeline and Bastian's strategy to be deterministic, namely Adeline's strategy is a deterministic function $y_{v_0}(b_{v_0})$ and Bastian's strategy is a deterministic function $-g_{v_0}(d)$. This strategy gives a lower bound on the value $\omega(G)$ of the game:

$$\begin{aligned} \omega(G) &\geqslant \max_{g_{v_0}} \Pr_{b_{v_0},d} [y_{v_0}(b_{v_0}) - g_{v_0}(d) = b_{v_0} * d] \\ &= \max_{g_{v_0}} \Pr_{b_{v_0},d} [\alpha_{v_0}(d, b_{v_0}) + d * b_{v_0}) - g_{v_0}(d) = (b_{v_0} * d)] \\ &\text{(substituting } y_{v_0} = \alpha_{v_0} + b_{v_0} * d) \\ &= \max_{g_{v_0}} \Pr_{b_{v_0},d} [g_{v_0}(d) == \alpha_{v_0}(d, b_{v_0})] \\ &= IP_0. \end{aligned}$$

We can conclude using the result of Lemma 4.2 proven in the next section to the case where $p = 1/2$ and $S = \{0, 1\}$: we obtain

$$IP_0 \leqslant \frac{1}{2} + \sqrt{\frac{2}{Q}}. \tag{5.18}$$

□

Lemma 5.5. *For every node $v \in V_{=j}$, $t \in \{\ell, r\}$ and history $h_0 \in H_{j+1}^{-\{v,v\ell,vr\}}(v)$ it holds that:*

$$IP_{vt}^{h_0} \leqslant IP_v^{h_0} + \sqrt{\frac{2}{|B_{j+1}^{h_0}(vt)|}}.$$

where we slightly abuse notation by defining $IP_v^{h_0} := \max_g \mathbb{E}_{b_v \leftarrow B_j^{h_0}}[g = \alpha_v(h_0, b_v)]$.

The reason we say we slightly abuse notation is the discrepancy on what is fixed between this definition and the one in Equation 5.10. Notice that we have

$$IP_j = \mathbb{E}_{v \leftarrow Z_j} \mathbb{E}_{h_0 \leftarrow H_{j+1}^{-\{v,v\ell,vr\}}}[IP_v^{h_0}].$$

Proof. We prove here Lemma 5.5. As in [CCL15], we use the Alice's cheating strategy to come up with a strategy for a variant of the CHSH game with inputs and outputs in $\mathbb{F}_Q$ instead of $\mathbb{F}_2$. Then upper bounds on the classical value of this CHSH variant allow us to bound the value of IP.

The class of $\mathrm{CHSH}_Q(p)$ games was introduced in [CCL15] in order to analyze the security of the $\mathbb{F}_Q$ protocols. These are simply two-party nonlocal games between Adeline and Bastian who respectively receive inputs $x, y \in \mathbb{F}_Q$ and output $a, b \in F_Q$. Here x is drawn from the uniform distribution while y is drawn according to a probability distribution $\{p_y\}_{y \in \mathbb{F}_Q}$ such that $\max_y p_y \leqslant p$. Adeline and Bastian win the game if $a + b = x * y$ in $\mathbb{F}_Q$. Let us define a slight variant of these games where the only difference is now that Adeline's inputs are drawn uniformly from a subset S of $\mathbb{F}_Q$. We denote this class of games by $\mathrm{CHSH}_Q^S(p)$.

We start with Equation 5.10:

$$\begin{aligned} IP_{vt}^{h_0} = \max_{g:\mathbb{F}_Q \to \mathbb{F}_Q} & \mathbb{E}_{b_v \leftarrow B_j^{h_0}(v)} \mathbb{E}_{b_{vt} \leftarrow B_{j+1}^{h_0, b_v}(vt)} \\ & [g(b_v) == \alpha_{vt}(h_0, b_v, b_{vt})]. \end{aligned}$$

We write $\alpha_{vt}(h, b_v, b_{vt}) = y_{vt}(h, b_{vt}) + b_{vt} * \alpha_v(h, b_v)$. From there, we can see that the dependence in b_v of the function $\alpha_{vt}(h, b_v, b_{vt})$ lies only in the function $\alpha_v(h, b_v)$. Therefore, we can write

$$\begin{aligned} IP_{vt}^{h_0} = \max_{g:\mathbb{F}_Q \to \mathbb{F}_Q} & \mathbb{E}_{b_v \leftarrow B_j^{h_0}(v)} \mathbb{E}_{b_{vt} \leftarrow B_{j+1}^{h_0, b_v}(vt)} \\ & [g(\alpha_v(h_0, b_v)) == \alpha_{vt}(h_0, b_v, b_{vt})]. \end{aligned} \tag{5.19}$$

Let $\mathcal{G}^{h_0}$ be the function g that maximizes the above expression. In order to end the proof, we perform the following steps: (1) we define an entangled game that will be an instance of some CHSH_Q^S game

for some S, (2) we construct a cheating strategy for this game using the functions y_{vt} and G^{h^0} and finally (3) we use the known bounds on CHSH_Q^S to derive a bound on $IP_{vt}^{h_0}$.

We consider the following game between two players Adeline and Bastian:

- Adeline receives a random element $X \in B_{j+1}^{h_0}(vt)$. Bastian receives an element $Y \in \mathbb{F}_Q$ such that $\Pr[Y = c] = \Pr_{b_v}[\alpha_v(h, b_v) = c]$.
- Their goal is to respectively output A and B in $\mathbb{F}_q$ such that $A + B = X * Y$

Recall that $IP_v^{h_0} = \max_c \Pr_{b_v \leftarrow B_j^{h_0}(v)}[\alpha_v(h, b_v) = c]$. Since Adeline has no information about b_v, her probability of guessing Y is upper bounded by $IP_v^{h_0}$. This means that the two player game we study is an instance of $\mathrm{CHSH}_Q^{B_{j+1}^{h_0}(vt)}(IP_v^{h_0})$. We know from Lemma 4.2 (proven in chapter 3) the following upper bound on the classical value of such a game:

$$\omega\Big(\mathrm{CHSH}_Q^{B_{j+1}^{h_0}(vt)}(IP_v^{h_0})\Big) \leqslant IP_v^{h_0} + \sqrt{\frac{2}{|B_{j+1}^{h_0,b_v}(vt)|}}.$$

We now use Alice's cheating strategy to derive a strategy for the above game. Adeline outputs $A = y_{vt}(h_0, X)$ and Bastian outputs $B = -\mathcal{G}^{h_0}(Y)$. We can lower bound the value of the game as follows:

$$\begin{aligned}
&\omega(\mathrm{CHSH}_Q^{B_{j+1}^{h_0}(vt)}(IP_v^{h_0})) \\
&\geqslant \Pr_{X,Y}[A + B = X * Y] \\
&\geqslant \Pr_{X,Y}[y_{vt}(h_0, X) - \mathcal{G}^{h_0}(Y) = X * Y] \\
&= \Pr_{X,b_v}[y_{vt}(h_0, X) - \mathcal{G}^{h_0}(\alpha_v(h_0, b_v)) = X * \alpha_v(h_0, b_v)] \\
&= \Pr_{X,b_v}[\alpha_{vt}(h, b_v, X) + (\alpha_v(h_0, b_v) * X) \\
&- \mathcal{G}^{h_0}(\alpha_v(h_0, b_v)) = (X * \alpha_v(h_0, b_v))] \\
&= \Pr_{X,b_j}[\alpha_{vt}(h, b_v, X) = \mathcal{G}^{h_0}(\alpha_v(h_0, b_v))] \\
&= IP_{vt}^{h_0}.
\end{aligned}$$

Combining the upper and the lower bound on $\omega(\mathrm{CHSH}_Q^{B_{j+1}^{h_0}(vt)}(IP_v^{h_0}))$, we conclude that

$$IP_{vt}^{h_0} \leqslant IP_v^{h_0} + \sqrt{\frac{2}{|B_{j+1}^{h_0}(vt)|}}.$$

□

We are now ready to prove the recurrence relation.

Proposition 5.4. *For $j \leqslant k-2$, it holds that:*

$$IP_{j+1} \leqslant IP_j + \frac{5}{4}\sqrt{\frac{2}{Q}}.$$

Proof. For $v \in Z_j, h_0 \in H_{j+1}^{-\{v,v\ell,vr\}}$, the probability that Alice is responsive at node $v\ell$, or equivalently, that $v\ell$ is the leftmost alive node at round $j+1$, is $\Pr[T(v|h_0) = \ell] = \frac{|B_{j+1}^{h_0}(v\ell)|}{Q} =: P_{h_0}$. Proposition 5.3 gives:

$$\begin{aligned} IP_{j+1} &= \mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)}\mathbb{E}_{t\leftarrow T(v|h_0)}[IP_{vt}^{h_0}] \\ &= \mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)}[P_{h_0}IP_{v\ell}^{h_0} + (1-P_{h_0})IP_{vr}^{h_0}] \end{aligned}$$

We use Lemma 5.5 in order to bound $IP_{vl}^{h_0}$ and $IP_{vr}^{h_0}$. We have by definition $|B_{j+1}^{h_0}(vl)| = P_{h_0}Q$ and $|B_{j+1}^{h_0}(vr)| = Q$. From there, we have

$$\begin{aligned} &IP_{j+1} \\ &= \mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)} \\ &\left[P_{h_0}\left(IP_v^{h_0} + \sqrt{\frac{2}{P_{h_0}Q}}\right) + (1-P_{h_0})\left(IP_v^{h_0} + \sqrt{\frac{2}{Q}}\right)\right] \qquad (5.20) \\ &= \mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)} \\ &\left[IP_v^{h_0} + (1+\sqrt{P_{h_0}} - P_{h_0})\sqrt{\frac{2}{Q}}\right] \\ &\leqslant \mathbb{E}_{v\leftarrow Z_j}\mathbb{E}_{h_0\leftarrow H_{j+1}^{-\{v,v\ell,vr\}}(v)}\left[IP_v^{h_0} + \frac{5}{4}\sqrt{\frac{2}{Q}}\right] \qquad (5.21) \\ &= IP_j + \frac{5}{4}\sqrt{\frac{2}{Q}} \end{aligned}$$

where we used the bound $(1+\sqrt{P}-P) \leqslant \frac{5}{4}$ for $P \geqslant 0$ in Equation (5.21). □

Combining Propositions 5.2, 5.4 and Lemma 5.4 gives our main result.

Corollary 5.1. *The k-round Tree protocol is ε_k-sum-binding with*

$$\varepsilon_k \leqslant \frac{5k}{\sqrt{2Q}}.$$

This scaling is very close to the one of the $\mathbb{F}_Q$ protocol for which the binding parameter is upper bounded by $2\sqrt{2}k/\sqrt{Q}$ according to Ref. [CCL15].

3.4 Loss tolerance and communication cost of the Tree protocol

Lifetime of the Tree protocol

The main point of considering the Tree protocol instead of the simpler $\mathbb{F}_Q$-protocol is that it displays some loss tolerance. In this section, we consider a very simple model of loss and evaluate the performance of the Tree protocol compared to the $\mathbb{F}_Q$-protocol.

For this, we assume that in the honest case, each station (corresponding to a couple $\mathcal{A}_i, \mathcal{B}_i$) dies with some probability p at each round of the protocol. This process is taken to be independent and identical. Moreover, we consider the scenario where a dead station remain dead for a time $m\tau$, where m is some small integer such that $m \ll k$ and $mp \ll 1$. This loss model could of course be refined, for instance by adding correlations between the various probabilities of dying for modelling a global network failure for example, or by taking the dead time to be a random variable as well, but our simplified model allows for a more straightforward comparison of the different protocols and arguably already captures the behavior of realistic failures due to loss in bit commitment protocols.

Observation 1. *In the honest scenario where all players follow the protocol but losses are allowed, the Tree protocol protocol aborts if and only if two stations are dead at the same time (except at the first round).*

Proposition 5.5. *Provided that $mp \ll 1$ and $m \ll k$, the probabilities that the k-round $\mathbb{F}_Q$ and Tree protocols don't abort are given by*

$$P_{\text{ok}}(\mathbb{F}_Q) = (1-p)^k \tag{5.22}$$

$$P_{\text{ok}}(\text{Tree}) = (1-q)^k \tag{5.23}$$

with $q = 3(mp)^2 + (mp)^3$.

Proof. Let us first consider the $\mathbb{F}_Q$ protocol: it aborts as soon as one station dies. At each round, a honest Alice responds in time with probability $1-p$. Since these events are assumed to be independent, the probability that Alice responds in time for the full protocol, that is, all k rounds, is $P_{\text{ok}}(\mathbb{F}_Q) = (1-p)^k$.

In the Tree protocol, each station is non-responsive at a given round $i \geqslant m$ with probability mp if we assume that $mp \ll 1$: this is the probability that the station died during any of the m previous rounds. The probability that at least two stations are alive at a given round is equal to the probability that at most one of the three stations is non-responsive, that is $(mp)^3 + 3(mp)^2 = q$. It follows that the probability that the Tree protocol does not abort is $(1-q)^k$, in the regime where m is negligible compared to the number of rounds. □

Let us define the lifetime $t_{\Pi}(p)$ of a protocol Π as the number of rounds required to achieve $P_{\text{ok}}(\Pi) \approx 1/e$ if each station dies independently with probability p. Then, Proposition 5.5 states that

$$t_{\mathbb{F}_Q}(p) = \frac{1}{mp} \quad \text{and} \quad t_{\text{Tree}}(p) = \frac{1}{q} \approx \frac{1}{3m^2p^2} \tag{5.24}$$

provided that $mp \ll 1$. In particular, adding a third player to the standard $\mathbb{F}_Q$-protocol provides a quadratic improvement in the expected lifetime of the commitment time.

Communication cost of the protocol

Trimming the tree. One drawback of the tree protocol is that size of the tree grows exponentially with number of rounds, causing a huge overhead in both computation and communication cost. If up to the $j-1$-th round all nodes of the tree are alive then the j-th round would consist in executing 2^j rounds of the $\mathbb{F}_Q$ protocol in parallel, which is clearly unpractical for large values of j. To keep this complexity under control, one can note that only the leftmost alive path matters for the protocol: none of the other branches will ever be considered in the reveal phase, and it is therefore useless to maintain them during the whole protocol. For this reason, it is natural to modify the tree protocol as follows: after each round, each one of Bob's agents sends a classical message to his two colleagues in order to inform them on which branches Ire alive or dead. If the maximum distance between two agents of Bob is $D_{\max}$, then they all learn which branches Ire alive up to round j after a time $D_{\max}/c$. In other words, it takes them the equivalent of $N := D_{\max}/(c\tau)$ rounds to learn this information, and therefore to learn which was the leftmost alive path until round j. Once they share this information, they can stop applying the $\mathbb{F}_Q$ protocol on other branches of the tree.

The modification suggested above implies that at each instant, the actual size of the maintained tree is $O(2^N)$, which remains practical provided that the distance between Bob's agents is not considerably larger than $c\tau$. One should also emphasize that this trimming of the tree has no consequence on the security of the protocol, since it simply consists in aborting classical communication that will not intervene at all in the protocol.

Let us now evaluate the communication cost of the various protocols, that is the number of bits that are exchanged among various agents during the whole protocol. Note first that by construction, all the challenges and responses are elements of $\mathbb{F}_Q$, meaning that each round (corresponding to each alive node in the Tree protocol) has an individual cost of $2\log_2 Q$ bits.

Proposition 5.6. *The communication cost $C_{\mathbb{F}_Q}$ and C_{Tree} of the k-round $\mathbb{F}_Q$ and Tree protocols are given by:*

$$C_{\mathbb{F}_Q} = 2k\log_2 Q \tag{5.25}$$

$$C_{\mathrm{Tree}} \approx k2^{N+2}\log_2 Q, \tag{5.26}$$

where N is the number of rounds necessary for all agents to realize that a given branch is dead. Recall that taking $\log_2 Q = O(\log(k/\varepsilon))$ is sufficient to guarantee that the protocol is ε-binding.

In practice, the value of N will be a small constant, which shows that the communication cost of the Tree protocol compares favorably with that of the original k-round $\mathbb{F}_Q$ protocol.

Proof. Obtaining the communication cost of the $\mathbb{F}_Q$ protocol is straightforward: there are k rounds that each cost $2\log_2 Q$ bits.

For the Tree protocol, we consider the "worst case scenario" where Alice's agents always respond in time. This means that all branches are alive unless Bob's agents decide not to send them challenges anymore. Since only the leftmost alive branch matters in the reveal phase, and since the prefix of the leftmost alive node never changes during the protocol, it is easy to see that Bob's agents do not need to continue sending challenges to branches that they know not to be the leftmost alive branch.

In general, it may take N additional rounds before all agents learn the status of all the history up to a given round. This means that in the worst case, Bob's agents should send challenges to all the descendants of the current leftmost alive node for N rounds. The number of such nodes is upper bounded by 2^{N+1}. Since there are k rounds in total, the communication cost of the Tree protocol Tree can be upper bounded by $2^{N+1}k \times 2\log_2 Q$ bits. □

3.5 Generalization to n agents per party

It is straightforward to generalize the Tree protocol to the case where each party is represented by n agents. In that case, the binary tree should be replaced by a complete n-ary tree, together with an n-coloring of that tree. For the protocol to abort, it requires that $n-1$ stations die simultaneously. It is straightforward to see that the probability that the protocol succeeds becomes $(1-q(n))^k$ with

$$q(n) = n(mp)^{n-1} + (mp)^n. \tag{5.27}$$

Provided that $nmp \ll 1$, the lifetime of the generalized Tree protocol $\mathrm{Tree}(n)$ with n agents per player becomes:

$$t_{\mathrm{Tree}(n)}(p,m) \approx \frac{1}{n(mp)^{n-1}}. \tag{5.28}$$

It is less straightforward to generalize the security proof to the case of n agents. HoIver, it is natural to conjecture that an analysis similar to that of Proposition 5.4 for the Tree protocol with 3 locations will work.

Conjecture 5.6. *The k-round Tree protocol with $n \geqslant 3$ agents per party is $\varepsilon_{k,n}$-binding with*

$$\varepsilon_{k,n} = 2kx_n\sqrt{\frac{2}{Q}} \tag{5.29}$$

with

$$x_2 = 1, \quad x_n = x_{n-1} + \frac{1}{4x_{n-1}}. \tag{5.30}$$

In particular, asymptotically, it holds that $x_n \sim \sqrt{n/2}$.

4 Conclusion and open problems

In this chapter, we explained two of our contributions on relativistic bit commitment. In Section 2, we gave a doubly exponential improvement on the binding property of the $\mathbb{F}_Q$-protocol compared to previous works. If the distance between $\mathcal{A}_1/\mathcal{B}_1$ and $\mathcal{A}_2/\mathcal{B}_2$ is D, then the commitment can be sustained for a time

$$T = (D/c)\,\varepsilon\sqrt{Q/4},$$

where c is the speed of light. In particular, provided that $Q \gg 1/\varepsilon^2$, the commitment time can be made arbitrary long. For instance in [VMH$^+$16], Verbanis *et al.* exploited our bound and took the

security parameter $\varepsilon = 7.8 \times 10^{-10}$ and $Q = 2^{128}$, allowing them to sustain a commitment for 24 hours for a distance $D = 7$ km.

It is also possible to reduce the distance between $\mathcal{A}_1/\mathcal{B}_1$ and $\mathcal{A}_2/\mathcal{B}_2$, at the condition that both the computation time and the communication time between $\mathcal{A}_i$ and $\mathcal{B}_i$ remain negligible compared to D/c. This is necessary to enforce the non-signalling condition of the CHSH_Q game. For instance, if the computation time is on the order of the microsecond, then the distance D should be at least 300 meters.

In Section 3, we introduced a new relativistic bit commitment protocol that addresses one of the main weaknesses of the $\mathbb{F}_Q$ protocol, namely its fragility against network failures. Indeed, the $\mathbb{F}_Q$ protocol aborts as soon as one agent fails to respond to a single challenge in time. We fix this issue by modifying the $\mathbb{F}_Q$ protocol, so that each party is now represented by three agents in three distinct locations. The communication cost of this variant is relatively modest, but the gain in terms of tolerance to loss is very good: one expects a quadratic gain for the number of rounds that the protocol can sustain, making it very promising for implementations in real telecom networks (instead of dedicated networks), which is crucial for a possible future deployment of this technology.

Let us conclude by mentioning a few open questions.

(i) Certainly the most pressing one concerns the security of the $\mathbb{F}_Q$ protocol and tree protocol against quantum adversaries. A first step in that direction would be to obtain tight upper bounds on the quantum value ω^* of games in $\mathrm{CHSH}_Q(p)$. For the tree protocol the difficulty arises also from the composition of the rounds because the history is not described by classical random variables anymore, but rather by quantum states.

(ii) Another outstanding problem is whether the bit-commitment protocol of [LKB$^+$15] can be used to obtain a protocol for Oblivious Transfer [Kil88]. In particular, this would have the way for arbitrary two-party cryptography with security based on the non-signalling principle.

(iii) For the Tree protocol, the complete binary tree structure does not seem to be optimal and simpler schemes with reduced communication complexity would be interesting.

(iv) Finally, another disadvantage of $\mathbb{F}_Q$ protocol is that throughout the protocol, Bob needs to store the information about all of the ys. At the end, to check the consistency of Alice's commitment Bob needs to perform computation over all of the y's. If the number of rounds k is very large then it would be a resource consuming task. For example, in the experiment by Verbanis *et al.* in [VMH$^+$16], the value of k is of order 10^9 and it took 72 hours for Bob to verify the consistency of Alice's answers. This is definitely a big problem. It would be particularly interesting to design a new variant of $\mathbb{F}_Q$ protocol where agents of Bob don't need to store and compute over all of the y's.

6 Conclusion

In this thesis, we have studied how to exploit relativistic constraints such as the non-superluminal signalling principle to design secure cryptographic primitives such as position-verification and bit commitment.

In Chapter 3, we have designed a new attack strategy against quantum position-verification schemes. This attack is interesting because it is the most efficient when the protocol is easy to implement for the honest parties. Then we devised a new scheme which is practical for the honest parties but immune against the type of attacks we designed. Unfortunately, an "efficient" attack (requiring only a polynomial amount of entanglement) was recently proposed against our scheme by Florian Speelman [Spe16]. The main open question of the field therefore remains to understand whether there exist position-verification protocols that are both practical and require an exponential amount of entanglement to break. Given the difficulty of establishing any nontrivial lower bound on the amount of entanglement required to break a position-verification scheme, it is probably fair to say that this question is completely out of reach with current techniques.

In Chapter 4, we have considered generalisations of the CHSH game to finite fields of size larger than two, with arbitrary probability distributions for the questions. Such games are relevant in the study of some relativistic bit commitment protocols. We have established some upper bound on the classical value of such games. An interesting problem is of course to obtain similar upper bounds on the quantum value of such games, with the hope that they could be useful to prove the security of bit commitment protocols against quantum adversaries. Such a bound was recently obtained in [CL17] in the case where the probability distribution is uniform over the inputs. Another interesting open question would be to understand whether all these bounds are tight by providing explicit strategies for the game.

In Chapter 5, we have considered two relativistic bit commitment protocols: the multi-round $\mathbb{F}_Q$ protocol initially proposed by [LKB$^+$15] for which we improved the security analysis against classical adversaries, as well as a new protocol that is tolerant to losses and can therefore be implemented in realistic network conditions. For both of these protocols, we have exploited the results from Chapter 4 to bound their binding parameter. Crucially, our security analysis cannot be generalised against quantum adversaries. In order to analyse this situation, one would need upper bounds on the quantum value of a modified version of the games considered in Chapter 4. Indeed, here the issue is that during

the protocol, the adversaries share a quantum state. When performing the reduction for the security analysis to the non-local game, it yields a game where Alice and Bob are allowed to share a quantum state which *depends* on the questions they receive. Modelling this in a meaningful and useful way has turned out to be very challenging. In particular, the results from [CL17] cannot be used to analyse the multi-round bit commitment protocol beyond 2 rounds, which is clearly insufficient for any practical application. Another interesting open problem would be to make the multi-round $\mathbb{F}_Q$ protocol more practical. In this protocol, in order to verify Alice's commitment, the agents of Bob needs to keep the informations about all y_i's until the end of the last round. Moreover, Bob cannot start the verifying process until the end of the protocol. For long sustain time, this would require lots of memory and time.

Bibliography

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, 98(23):230501, 2007.

[Adl83] Leonard M Adleman. On breaking the iterated Merkle-Hellman public-key cryptosystem. In *Advances in Cryptology*, pages 303–308. Springer, 1983.

[BB84] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. in Proceedings Of IEEE International Conference on Computer Systems and Signal Processing, Bangalore, Kartarna, (Institute of Electrical and Electronics Engineers, New York, 1984.

[BBBW83] Charles H Bennett, Gilles Brassard, Seth Breidbart, and Stephen Wiesner. Quantum cryptography, or unforgeable subway tokens. In *Advances in Cryptology-CRYPTO 1983*, pages 267–275. Springer, 1983.

[BBC+93] Charles H Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Physical Review Letters*, 70(13):1895, 1993.

[BBCS91] Charles H Bennett, Gilles Brassard, Claude Crépeau, and Marie-Hélene Skubiszewska. Practical quantum oblivious transfer. In *Annual International Cryptology Conference*, pages 351–366. Springer, 1991.

[BC91] Gilles Brassard and Claude Crépeau. Quantum bit commitment and coin tossing protocols. *Advances in Cryptology-CRYPT0 1990*, pages 49–61, 1991.

[BC93] Stefan Brands and David Chaum. Distance-bounding protocols. In *Workshop on the Theory and Application of of Cryptographic Techniques*, pages 344–359. Springer, 1993.

[BCC88] Gilles Brassard, David Chaum, and Claude Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156–189, 1988.

[BCF+11] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. In *Advances in Cryptology–CRYPTO 2011*, pages 429–446. Springer, 2011.

[BCJL93] Gilles Brassard, Claude Crépeau, Richard Jozsa, and Denis Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Foundations of Computer Science, 1993. Proceedings., 34th Annual Symposium on*, pages 362–371. IEEE, 1993.

[BCP+14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86:419–478, Apr 2014.

[Bel64] John S Bell. On the Einstein Podolsky Rosen paradox, 1964.

[BFSS13] Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, pages 145–158. ACM, 2013.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[Blu82] Manuel Blum. Coin flipping by telephone: A protocol for solving impossible problems. *Advances in Cryptology-CRYPTO-1981*, 1982.

[BM05] Harry Buhrman and Serge Massar. Causality and Tsirelson's bounds. *Physical Review A*, 72(5):052103, 2005.

[BOGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 113–131. ACM, 1988.

[BS15] Mohammad Bavarian and Peter W. Shor. Information Causality, Szemerédi-Trotter and Algebraic Variants of CHSH. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science, ITCS 2015, Rehovot, Israel, January 11-13, 2015*, pages 123–132, 2015.

[BS16] Anne Broadbent and Christian Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1):351–382, 2016.

[CCL15] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Arbitrarily long relativistic bit commitment. *Physical Review Letters*, 115:250501, Dec 2015.

[CCL16] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Robust relativistic bit commitment. *Physical Review A*, 94(6):062314, 2016.

[CGKS95] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *Foundations of Computer Science, 1995. Proceedings., 36th Annual Symposium on*, pages 41–50. IEEE, 1995.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Advances in Cryptology-CRYPTO 2009*, pages 391–407. Springer, 2009.

[CHSH69] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, 23(15):880, 1969.

[CHTW04] Richard Cleve, Peter Hoyer, Benjamin Toner, and John Watrous. Consequences and limits of nonlocal strategies. In *Computational Complexity, 2004. Proceedings. 19th IEEE Annual Conference on*, pages 236–249. IEEE, 2004.

[Cir80] Boris S Cirel'son. Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, 4(2):93–100, 1980.

[CK11] A. Chailloux and I. Kerenidis. Optimal bounds for quantum bit commitment. In *Proceedings of the 52nd Annual IEEE Symposium on Foundations of Computer Science*, pages 354–362, October 2011.

[CL17] André Chailloux and Anthony Leverrier. Relativistic (or 2-prover 1-round) Zero-Knowledge protocol for NP secure against quantum adversaries. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 369–396. Springer, 2017.

[Col06] Roger Colbeck. *Quantum and Relativistic Protocols for Secure Multi-Party Computation*. PhD thesis, University of Cambridge, Cambridge, U.K., 2006.

[Col09] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. *arXiv preprint arXiv:0911.3814*, 2009.

[CR12] Roger Colbeck and Renato Renner. Free randomness can be amplified. *Nature Physics*, 8(6):450–453, 2012.

[CSST11] Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two provers in isolation. In *Advances in Cryptology–ASIACRYPT 2011*, pages 407–430. Springer, 2011.

[DFL+09] Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, and Christian Schaffner. Improving the security of quantum protocols via commit-and-open. In *Advances in Cryptology-CRYPTO 2009*, pages 408–427. Springer, 2009.

[DFR+07] Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Proceedings of the 27th annual international cryptology conference on Advances in cryptology*, CRYPTO'07, pages 360–378, Berlin, Heidelberg, 2007. Springer-Verlag.

[DFSS05] I. B. Damgard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.*, pages 24–27, Oct 2005.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, May 1935.

[FF16] Serge Fehr and Max Fillinger. On the composition of two-prover commitments, and applications to multi-round relativistic commitments. In *Advances in Cryptology–EUROCRYPT 2016*, pages 477–496. Springer, 2016.

[Gas04] William Gasarch. A survey on private information retrieval. In *Bulletin of the EATCS*. Citeseer, 2004.

[GC99] Daniel Gottesman and Isaac L Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[GFK+06] Nicolas Gisin, Sylvain Fasel, Barbara Kraus, Hugo Zbinden, and Grégoire Ribordy. Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2):022320, 2006.

[GIKM98] Yael Gertner, Yuval Ishai, Eyal Kushilevitz, and Tal Malkin. Protecting data privacy in private information retrieval schemes. In *Proceedings of the Thirtieth Annual ACM Symposium on Theory of Computing*, STOC '98, pages 151–160, New York, NY, USA, 1998. ACM.

[Got97] Daniel Gottesman. Stabilizer codes and quantum error correction. *PhD Thesis, California Institute of Technology, arXiv:quant-ph/9705052*, 1997.

[GV15] WT Gowers and Emanuele Viola. The communication complexity of interleaved group products. *ECCC preprint TR15-044*, 2015.

[HHHH09] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865, 2009.

[HRW10] Esther Hänggi, Renato Renner, and Stefan Wolf. Efficient device-independent quantum key distribution. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 216–234. Springer, 2010.

[IH08] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Physical Review Letters*, 101(24):240501, 2008.

[IH09] Satoshi Ishizaka and Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Physical Review A*, 79(4):042306, 2009.

[Kah96] David Kahn. *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*. Scribner, rev sub edition, December 1996.

[Kan15] Jędrzej Kaniewski. Relativistic quantum cryptography. *arXiv preprint arXiv:1512.00602*, 2015.

[KdW04] Iordanis Kerenidis and Ronald de Wolf. Quantum symmetrically-private information retrieval. *Information Processing Letters*, 90(3):109–114, May 2004.

[Ken99] Adrian Kent. Unconditionally secure bit commitment. *Physical Review Letters*, 83:1447–1450, Aug 1999.

[Ken05] Adrian Kent. Secure classical bit commitment using fixed capacity communication channels. *Journal of Cryptology*, 18(4):313–335, 2005.

[Ken11] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011.

[Ken12a] Adrian Kent. Quantum tasks in Minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012.

[Ken12b] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Physical Review Letters*, 109:130501, Sep 2012.

[Kil88] Joe Kilian. Founding crytpography on oblivious transfer. In *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 20–31, New York, NY, USA, 1988. ACM Press.

[Kit03] Alexei Kitaev. Quantum coin-flipping. *Talk at QIP*, 2003.

[KMS11] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1):012326, 2011.

[KP14] Hartmut Klauck and Supartha Podder. New bounds for the garden-hose model. In *34th International Conference on Foundation of Software Technology and Theoretical Computer Science, FSTTCS 2014, December 15-17, 2014, New Delhi, India*, pages 481–492, 2014.

[KRR14] Yael Tauman Kalai, Ran Raz, and Ron D Rothblum. How to delegate computations: the power of no-signaling proofs. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 485–494. ACM, 2014.

[KTHW13] Jed Kaniewski, Marco Tomamichel, Esther Hanggi, and Stephanie Wehner. Secure bit commitment from relativistic constraints. *IEEE Transactions on Information Theory*, 59(7):4687–4699, 2013.

[KWW12] Robert Konig, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.

[LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410–3413, Apr 1997.

[LKB+13] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Physical Review Letters*, 111:180504, Nov 2013.

[LKB+15] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden. Practical relativistic bit commitment. *Physical Review Letters*, 115:030502, Jul 2015.

[LL11] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical Review A*, 83(1):012322, 2011.

[Mal10] Robert A Malaney. Quantum location verification in noisy channels. In *Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE*, pages 1–6. IEEE, 2010.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78(17):3414–3417, Apr 1997.

[MH06] R. Merkle and M. Hellman. Hiding information and signatures in trapdoor knapsacks. *IEEE Transaction on Information Theory*, 24(5):525–530, September 2006.

[MY98] Dominic Mayers and Andrew Yao. Quantum cryptography with imperfect apparatus. In *Foundations of Computer Science, 1998. Proceedings. 39th Annual Symposium on*, pages 503–509. IEEE, 1998.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[NP00] Moni Naor and Benny Pinkas. Distributed oblivious transfer. In *Advances in Cryptology–ASIACRYPT 2000*, pages 205–219. Springer-Verlag, 2000.

[OFV09] Jeremy L O'Brien, Akira Furusawa, and Jelena Vučković. Photonic quantum technologies. *Nature Photonics*, 3(12):687–695, 2009.

[PG16] Damián Pitalúa-García. Spacetime-constrained oblivious transfer. *Physical Review A*, 93(6):062346, 2016.

[PV16] Carlos Palazuelos and Thomas Vidick. Survey on nonlocal games and operator space theory. *Journal of Mathematical Physics*, 57(1):015220, 2016.

[QS15] Bing Qi and George Siopsis. Loss-tolerant position-based quantum cryptography. *Physical Review A*, 91(4):042337, 2015.

[Ren08] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[RG15] Jérémy Ribeiro and Frédéric Grosshans. A tight lower bound for the bb84-states quantum-position-verification protocol. *arXiv preprint arXiv:1504.07171*, 2015.

[RSA78] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

[SAA+10] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, and R. J. Young. Quantum memories. *The European Physical Journal D*, 58(1):1–22, 2010.

[SBPC+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301, 2009.

[SCK14] Jamie Sikora, André Chailloux, and Iordanis Kerenidis. Strong connections between quantum encodings, nonlocality, and quantum cryptography. *Physical Review A*, 89(2):022334, 2014.

[Sha49] Claude E Shannon. Communication theory of secrecy systems. *Bell Labs Technical Journal*, 28(4):656–715, 1949.

[Sha82] A. Shamir. A polynomial time algorithm for breaking the basic Merkle-Hellman cryptosystem. In *23rd Annual Symposium on Foundations of Computer Science (sfcs 1982)*, pages 145–152, Nov 1982.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[Sim07] Jean-Raymond Simard. Classical and quantum strategies for bit commitment schemes in the two-prover model. Master's thesis, McGill University, 2007.

[Spe16] Florian Speelman. Instantaneous non-local computation of low t-depth quantum circuits. In *11th Conference on the Theory of Quantum Computation, Communication and Cryptography, TQC 2016, September 27-29, 2016, Berlin, Germany*, pages 9:1–9:24, 2016.

[STW09] Christian Schaffner, Barbara M. Terhal, and Stephanie Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Informatino & Computation*, 9(11&12):963–996, 2009.

[TFKW13] Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner. One-sided device-independent QKD and position-based cryptography from monogamy games. In *Advances in Cryptology–EUROCRYPT 2013*, pages 609–625. Springer, 2013.

[Uhl76] Armin Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

[Unr10] Dominique Unruh. Universally composable quantum multi-party computation. In *Advances in Cryptology–EUROCRYPT 2010*, volume 6110, pages 486–505. Springer, 2010.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology–CRYPTO 2014*, pages 1–18. Springer Berlin Heidelberg, 2014.

[Vai03] Lev Vaidman. Instantaneous measurement of nonlocal variables. *Physical Review Letters*, 90:010402, Jan 2003.

[VMH01] Artem Vakhitov, Vadim Makarov, and Dag R Hjelme. Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography. *Journal of Modern Optics*, 48(13):2023–2038, 2001.

[VMH+16] Ephanielle Verbanis, Anthony Martin, Raphaël Houlmann, Gianluca Boso, Félix Bussières, and Hugo Zbinden. 24-hour relativistic bit commitment. *Physical Review Letters*, 117(14):140506, 2016.

[VV12] Umesh Vazirani and Thomas Vidick. Certifiable quantum dice: or, true random number generation secure against quantum adversaries. In *Proceedings of the 44th symposium on Theory of Computing*, pages 61–76. ACM, 2012.

[VV14] Umesh Vazirani and Thomas Vidick. Fully device-independent quantum key distribution. *Physical Review Letters*, 113(14):140501, 2014.

[Wie83] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[WST08] Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.

[WW08] Stephanie Wehner and Jürg Wullschleger. Composable security in the bounded-quantum-storage model. *Automata, Languages and Programming*, pages 604–615, 2008.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 10 1982.

[Yao95] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, pages 67–75. ACM, 1995.