Relativistic quantum cryptography

JĘDRZEJ KANIEWSKI
(MMath, University of Cambridge)

A thesis submitted in fulfilment of the requirements
for the degree of Doctor of Philosophy

in the

Centre for Quantum Technologies
National University of Singapore

2015

Declaration

I hereby declare that this thesis is my original work and has been written by me in its entirety. I have duly acknowledged all the sources of information which have been used in the thesis.

This thesis has also not been submitted for any degree in any university previously.

Jędrzej Kaniewski

9 September 2015

Acknowledgements

I would like to thank my supervisor, Stephanie Wehner, for the opportunity to conduct a PhD in quantum information. I am grateful for her time, effort and resources invested in my education. Working with her and being part of her active and diverse research group made the last four years a great learning experience.

The fact that I was even able to apply for PhD positions is largely thanks to my brilliant and inspiring undergraduate supervisor, mentor and friend, Dr Peter Wothers MBE. I am particularly grateful for his supportive attitude when I decided to dedicate myself to quantum information. I am grateful to St. Catharine's College for a wonderful university experience and several long-lasting friendships.

I would like to thank my collaborators, Félix Bussières, Patrick J. Coles, Serge Fehr, Nicolas Gisin, Esther Hänggi, Raphael Houlmann, Adrian Kent, Troy Lee, Tommaso Lunghi, Atul Mantri, Nathan McMahon, Gerard Milburn, Corsin Pfister, Robin Schmucker, Marco Tomamichel, Ronald de Wolf and Hugo Zbinden, who made research enjoyable and from whom I have learnt a lot.

I am also indebted to Corsin Pfister and Le Phuc Thinh, who have read a preliminary version of this thesis, and Tommaso Lunghi and Laura Mančinska, who have given comments on parts of it.

Special thanks go to Evon Tan for being the omnipresent good spirit of CQT. Her incredible problem-solving skills allowed me to focus on research and contributed greatly to the scientific output of this thesis.

I would like to thank Valerio Scarani for being approachable and always happy to talk about various aspects of quantum information and the scientific world in general.

I am grateful to my examiners: Anne Broadbent, Marcin Pawłowski and Miklos Santha for the careful reading of this thesis and providing stimulating feedback. I would like to thank Alexandre Roulet, Jamie Sikora, Marco Tomamichel and Marek Wajs for useful comments on the defence presentation.

Dziękuję Markowi Wajsowi za nieocenioną pomoc przy drukowaniu i składaniu doktoratu.

Arturowi Ekertowi chciałbym podziękować za czas, wsparcie i konkretne wskazówki w chwilach zwątpienia.

Choć to już parę lat chciałbym również gorąco podziękować Krzysztofowi Kuśmierczykowi, Annie Mazurkiewicz i Bognie Lubańskiej za czas i wysiłek włożony w moją edukację oraz za bycie źródłem motywacji i inspiracji. Wszystko to, co udało mi się osiągnąć, jest oparte na solidnych licealnych fundementach i bez ich wkładu nie byłoby możliwe. Chcę także podziękować Poniatówce za niezapomniane trzy lata i wiele przyjaźni, które trwają do dzisiaj.

Jackowi Jemielitemu chciałbym podziękować za pierwsze spotkanie z nauką z prawdziwego zdarzenia, niespotykaną wytrwałość i cierpliwość a przede wszystkim za unikalne na skalę światową poczucie humoru, którego często mi brakuje.

Doktorat dedykuję w całości Mamie, Tacie, Siostrze i Bratu, bez wsparcia których to przełomowe dzieło nigdy by nie powstało.

Abstract

Special relativity states that information cannot travel faster than the speed of light, which means that communication between agents occupying distinct locations incurs some minimal delay. Alternatively, we can see it as temporary communication constraints between distinct agents and such constraints turn out to be useful for cryptographic purposes. In relativistic cryptography we consider protocols in which interactions occur at distinct locations at well-defined times and we investigate why such a setting allows to implement primitives which would not be possible otherwise.

Relativistic cryptography is closely related to non-communicating models, which have been extensively studied in theoretical computer science. Therefore, we start by discussing non-communicating models and its applications in the context of interactive proofs and cryptography. We find which non-communicating models might be useful for the purpose of bit commitment, propose suitable bit commitment protocols and investigate their limitations. We explain how some non-communicating models can be justified by special relativity and study what consequences such a translation brings about. In particular, we present a framework for analysing security of multiround relativistic protocols. We show that while the analysis of classical protocols against classical adversaries is tractable, the case of quantum protocols or quantum adversaries in a classical protocol constitutes a significantly harder task.

The second part of the thesis is dedicated to analysing specific protocols. We start by considering a recently proposed two-round quantum bit commitment protocol. We start by proving security under the assumption that idealised devices (single-photon source, perfect detectors) are available. Then, we propose a fault-tolerant variant of the protocol which can be implemented using realistic devices (weak-coherent source, noisy and inefficient detectors) and present a security analysis which takes into account losses, errors, multiphoton pulses, etc. We also report on an experimental implementation performed in collaboration with an experimental group at the University of Geneva.

In the last part we focus on classical schemes. We start by analysing a known two-round classical protocol and we show that successful cheating is equivalent to winning a certain non-local game. This is interesting as it demonstrates that even if the protocol is entirely classical, it might be advantageous for the adversary to

use quantum systems. We also propose a new, multiround classical bit commitment protocol and prove its security against classical adversaries. The advantage of the multiround protocol is that it allows us to increase the commitment time without changing the locations of the agents. This demonstrates that in the classical world an arbitrary long commitment can be achieved even if the agents are restricted to occupy a finite region of space. Moreover, the protocol is easy to implement and we discuss an experiment performed in collaboration with the Geneva group.

We conclude with a brief summary of the current state of knowledge on relativistic cryptography and some interesting open questions that might lead to a better understanding of the exact power of relativistic models.

List of publications

This thesis is based on three publications.
Chapters 3 and 4 are based on

- **Secure bit commitment from relativistic constraints** [arXiv:1206.1740]
  J. Kaniewski, M. Tomamichel, E. Hänggi and S. Wehner
  IEEE Transactions on Information Theory **59**, 7 (2013).
  (presented at *QCrypt '12*)

Chapter 5 is based on

- **Experimental bit commitment based on quantum communication and special relativity** [arXiv:1306.4801]
  T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner and H. Zbinden
  Physical Review Letters **111**, 180504 (2013).
  (presented at *QCrypt '13*)

Chapter 6 is based on

- **Practical relativistic bit commitment** [arXiv:1411.4917]
  T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner and H. Zbinden
  Physical Review Letters **115**, 030502 (2015).
  (presented at *QCrypt '14*)

During his graduate studies the author has also contributed to the following publications.

1. **Query complexity in expectation** [arXiv:1411.7280]
   J. Kaniewski, T. Lee and R. de Wolf
   Automata, Languages, and Programming: Proceedings of ICALP '15,
   Lecture Notes in Computer Science **9134** (2015).

2. **Equivalence of wave-particle duality to entropic uncertainty** [arXiv:1403.4687]
   P. J. Coles, J. Kaniewski and S. Wehner

Nature Communications **5**, 5814 (2014).
(presented at *AQIS '14*)

3. **Entropic uncertainty from effective anticommutators** [arXiv:1402.5722]
   J. Kaniewski, M. Tomamichel and S. Wehner
   Physical Review A **90**, 012332 (2014).
   (presented at *AQIS '14* and *QCrypt '14*)

4. **A monogamy-of-entanglement game with applications to device-independent quantum cryptography** [arXiv:1210.4359]
   M. Tomamichel, S. Fehr, J. Kaniewski and S. Wehner
   New Journal of Physics **15**, 103002 (2013).
   (presented at *Eurocrypt '13* and *QCrypt '13*)

Contents

Notation and list of symbols

Symbol	Meaning
$[n]$	set of integers from 1 to n
$\lvert\cdot\rvert$	cardinality of a set or modulus of a number
$\mathcal{H}$	a Hilbert space
$\dim \mathcal{H}$	dimension of $\mathcal{H}$
$\mathcal{H}^*$	dual space of $\mathcal{H}$
$\mathcal{L}(\mathcal{H})$	linear operators acting on $\mathcal{H}$
$\mathcal{H}(\mathcal{H})$	Hermitian operators acting on $\mathcal{H}$
$\mathbb{1}$	identity matrix
L^*	complex conjugate of L
L^{T}	transpose of L (with respect to the standard basis)
$L^\dagger$	Hermitian conjugate of L
$\lvert\phi\rangle, \lvert\psi\rangle$	pure quantum states
ρ, σ	mixed quantum states
$\lvert\Psi_d\rangle$	maximally entangled state of dimension d
H	Hadamard matrix
$\lVert\cdot\rVert_p$	Schatten p-norm
$\lVert\cdot\rVert$	Schatten ∞-norm
tr	trace
tr_A	partial trace over A
Φ	quantum channel
id	identity channel
$\mathrm{w_H}(\cdot)$	Hamming weight
$\mathrm{d_H}(\cdot)$	Hamming distance
$\oplus$	exclusive-OR (`XOR`)
$*$	finite-field multiplication
$\Pr[\cdot]$	probability
$\langle\cdot,\cdot\rangle$	inner product
$\mathcal{X}, \mathcal{Y}$	finite alphabets
$\mathbb{F}_q$	finite field of order q
$\mathcal{P}_k$	k^{th} player (in a multiplayer game)

Chapter 1

Introduction

Quantum cryptography lies at the intersection of physics and computer science. It brings together different communities and makes for a lively and exciting environment. It demonstrates that the fundamental principles of quantum physics can be cast and studied using the operational approach of cryptography. Besides, thanks to recent technological advances, practical applications are just round the corner.

Due to the interdisciplinary nature of quantum cryptography the relevant background knowledge spans multiple fields, which makes it particularly difficult to provide an introduction which would be both complete and concise. We have, therefore, chosen to focus on the topics which are directly related to quantum cryptography and skip over the less relevant areas.

This chapter starts with a short introduction to *cryptography*, which is the study of exchanging and processing information in a secure fashion. We focus on *two-party* (or *mistrustful*) cryptography, whose goal is to protect the *privacy* of an honest party interacting with potentially dishonest partners. Then, we introduce *quantum information theory*, which studies how quantum systems can be used to store and process information. We discuss the main features that distinguish it from the classical information theory and briefly describe the early history of the field. The next part of this chapter brings the two topics together under the name of *quantum cryptography*. We give a brief account of its early days, again, with a particular focus on two-party cryptography. We finish by giving a brief outline of this thesis.

1.1 Cryptography

Cryptography has been around ever since rulers of ancient tribes realised the need to send secret (or private) messages. Ideally, such messages should reveal no information if intercepted by an unauthorised party. The solution to this problem is known as a *cipher*, which is simply a procedure for converting a secret message

(called the *plaintext*) into another message (called the *ciphertext*), which should be intelligible to a friend (who knows the particular cipher we are using) but should give no information to an enemy. The first confirmed accounts of simple ciphers come from ancient Greece and Rome, for example Julius Caesar used a simple shift cipher (now also known as a Caesar cipher) to ensure privacy of his correspondence. Until modern times designing practical (i.e. easy to implement and difficult to break) ciphers was essentially the only branch of cryptography. One such cipher known as the *one-time pad* was invented by Gilbert S. Vernam and Joseph O. Mauborgne in 1917.[1] While the one-time pad guarantees (provably) secure communication it requires the two parties to share a random string of bits, known as a *key*, which is as long as the message they want to send. This quickly becomes impractical if the parties want to exchange large amounts of data.

A report presented by Claude Shannon in 1945 marks the birth of modern cryptography [Sha49].[2] Shannon proposed a formal definition of a (perfectly) secure cipher and proved that one-time pad satisfies such a stringent requirement. Moreover, he proved that any cipher that guarantees perfect security requires the key to be as long as the message (which essentially means that the one-time pad cannot be improved). But the contributions of this work go well beyond encryption and the analysis of one-time pad, as it was the first time that cryptography was phrased in the rigorous language of mathematics. This put cryptography on equal footing with other established sciences and set the stage for information theory (discovered by Shannon a couple of years later).

Nowadays cryptography is a mature field within which hundreds of *cryptographic tasks* (or *primitives*) have been defined and studied (and encryption, while obviously very important, is just one of them). Except for purely practical reasons for studying these tasks there is also a deeper motivation. Certain questions in cryptography (e.g. finding sufficient assumptions to perform a given task or proving impossibility results) give us valuable and operational insight into the underlying information theory. While classical information theory is relatively well understood, its quantum counterpart is not. That is why studying quantum cryptography is an important pursuit and contributes towards our understanding of the quantum world we (probably) live in.

In this thesis we only consider a branch of cryptography known as *two-party* or *mistrustful* cryptography, in which two parties, usually referred to as Alice and Bob, want to perform a certain task together but since they do not fully trust

[1] Note, however, that ideas that the one-time pad hinges on appeared as early as 1882 in a book by Frank Miller. For details consult an interesting survey on the state of cryptography at the turn of the century by Bellovin [Bel11].

[2] This work, presented in 1945 as a classified report at Bell Telephone Labs, was declassified and published in 1949.

each other they want to minimise the amount of information revealed during the protocol. A simple example of such a scenario is the *millionaires' problem* introduced by Andrew Yao [Yao82], in which two millionaires want to find out who is richer without revealing their actual wealth. This is certainly an interesting problem and, in fact, one that we often face in our everyday lives. Below we present and motivate some other natural two-party tasks.

- **Example 1:** Alice uses an online movie service called Bob, which charges separately for every downloaded movie. Alice has paid for one movie and wants to download it but being paranoid about privacy she is reluctant to reveal her choice to Bob. On the other hand, Bob wants to make sure that Alice only downloads one movie (and not more) so he is not keen on giving her access to the entire database. This problem, called *oblivious transfer*[3], turns out to be a convenient building block for two-party cryptography. In fact, it can be used to construct any other two-party primitive [Kil88].

- **Example 2:** Alice has supernatural powers that allow her to predict the future, for example the results of tomorrow's draw of the national lottery. She wants to impress Bob (she likes to be admired) but she does not want him to get rich (she knows that money does not bring happiness). Hence, the goal is to *commit* to a message without actually *revealing* it until some later time. Such primitives are known as *commitment schemes* [Blu81, BCC88][4] and the simplest one, in which the committed message is just one bit, is called *bit commitment* and constitutes one of the main topics of this thesis.

- **Example 3:** Alice is a quantum hacker and throughout the years she has exposed dozens of improperly formulated security proofs and misguided calculations. Having realised the damage done to the quantum community she has contacted a law enforcement agency represented by Bob to negotiate turning herself in. Alice and Bob want to schedule a secret meeting but for obvious security reasons they want to make sure that the location is chosen in a truly random fashion. In other words, Alice and Bob want to agree on a random choice, which neither of them can bias (or predict it in advance). This primitive known as *coin tossing* (or *coin flipping*) was introduced by Blum [Blu81].

[3] Oblivious transfer comes in multiple flavours and the one described above is called 1-out-of-N oblivious transfer, where $N \geq 2$ is the total number of movies offered by Bob. Since we are only interested in fundamental possibility or impossibility results, studying the case of $N = 2$ is sufficient (it is known how to interconvert these primitives including even more exotic variants like Rabin oblivious transfer [Cré88]).

[4] Blum [Blu81] only implicitly mentions commitment schemes while Brassard, Chaum and Crépeau [BCC88] define them explicitly. See an encyclopedia entry on commitment schemes for more details [Cré11].

All these tasks produce conflicting interests between Alice and Bob. It is clear that security for either party can be ensured at the cost of leaving the other party completely unprotected. In case of oblivious transfer, for example, Alice could give up her privacy and simply announce which movie she wants to watch. Alternatively, Bob could provide Alice with the entire database, hoping that she will not abuse his trust.

The goal of two-party cryptography is to first come up with the right mathematical definition of these primitives and then find in what circumstances and under what assumptions they can (or cannot) be implemented. It is also interesting to study *reductions* between different primitives, i.e. how to use one primitive to implement another one, which leads to a resource theory for cryptography. For example, oblivious transfer can be used to implement commitment schemes because choosing a particular message can be interpreted as committing to its label. Commitment schemes, on the other hand, can be used to generate trusted randomness. For example, in order to generate one trusted bit we use a commitment scheme with two possible values (such a primitive is known as *bit commitment*). Alice commits to a bit a, then Bob announces bit b and finally Alice reveals a and the outcome of the coin toss is declared to be $a \oplus b$. As long as at least one of the parties is honest the resulting bit is uniform. The use of a commitment scheme ensures that b does not depend on a (which would allow Bob to cheat).

The holy grail of the field is the so-called *information-theoretic security*[5]. There, the basic assumption is that the dishonest party is restricted by the underlying information theory, which is arguably the weakest assumption that one needs to perform security analysis. The term information-theoretic security goes back to Shannon (e.g. see his definition of secure encryption [Sha49]).

Unfortunately, it turns out that two-party primitives cannot be implemented with information-theoretic security (for both parties) unless we make some further assumptions.[6] Below we give a brief overview of various (reasonable) assumptions that make information-theoretically secure two-party cryptography possible.

- **Trusted third-party :** The trivial solution is to introduce a trusted third-party, which implements the primitive for Alice and Bob. In the paranoid

[5]Some authors prefer to use the term *unconditional security* instead. The name is motivated by the fact that the security proof assumes *nothing* about the adversary. However, this has been criticised as every security model contains assumptions and no security statement can be proven without referring to them.

[6]While the impossibility is usually intuitive showing it formally requires some effort. As an example we present an informal argument why oblivious transfer is not possible with information-theoretic security. Consider the situation at the end of the protocol. If Bob is not able to deduce which movie Alice chose to download, it must be the case that the knowledge contained in the interaction is sufficient to reconstruct at least two different movies and nothing can stop Alice from doing that.

world, in which Alice and Bob trust nobody but themselves, this is not a satisfactory solution. Moreover, it makes all tasks trivially possible.

- **Pre-shared resources :** Another solution that allows for two-party cryptography is to equip Alice and Bob with some shared correlations. This could be either shared randomness [Riv99] or access to a source of inherent and unpredictable noise that allows to generate such correlations during the protocol [Cré97, WNI03].[7]

- **Technological limitations :** The standard real-world solution to the commitment task is for Alice to lock her message in a safe box, which she then hands over to Bob while keeping the key. Whenever Alice wants to reveal the message, she gives the key to Bob, who opens the safe box and reads the message. This is secure as long as Alice has no way of remotely modifying the message and Bob has no tools to open the safe box, i.e. we must assume that they are subject to certain technological limitations. One can also assume that their "digital technology" is limited, e.g. by restricting their computational power or storage capabilities, which again makes secure two-party cryptography possible. The former leads to the rich and practically important field of computational security[8], while the latter leads to the bounded storage model [Mau91].

- **Communication constraints :** It is well-known that interrogating suspects one by one leads to better results than dealing with the whole group at the same time. In the cryptographic language this corresponds to forcing one (or more) parties to delegate agents, who perform certain parts of the protocol without communicating. Such setting was originally introduced in complexity theory under the name of *multiprover models*[9] to evade certain impossibility results [BGKW88]. These models are interesting from the cryptographic point of view but we must be explicit how they are adjusted to fit the framework of standard

[7] Even for tasks whose only purpose is to generate trusted randomness like coin tossing this is still a non-trivial scenario because the correlations initially shared between Alice and Bob might be different from the ones we want to generate.

[8] Computational security relies on the assumption that the adversary cannot solve a certain mathematical problem and let us mention two problematic aspects of this assumption. First of all, our belief that some mathematical problems are difficult is based mainly on the fact that many bright people have tried to solve them and failed (or maybe the successful ones prefer to keep a low profile). An efficient algorithm for solving such problems might be announced tomorrow and render all the currently used cryptographic protocols insecure. Secondly, most such schemes are vulnerable to *retroactive* attacks. If a message sent today is required to remain secret for the next twenty years, the mathematical problem must resist new algorithms and improved computing power that might be developed in these twenty years. This is why we would like to ultimately drop such assumptions and find more solid foundations for our cryptographic systems.

[9] To avoid confusion we talk about *multiprover* models in the context of complexity theory but use the term *multiagent* in case of cryptographic protocols.

two-party cryptography (in which there are only two parties interacting and not more). On the bright side some types of non-communicating models can (with subtle adjustments) be implemented by requiring multiple agents to interact simultaneously at multiple locations (under the assumption that the speed of light is finite). The first explicit examples of such relativistic protocols came from Adrian Kent [Ken99, Ken05]. This field, now known as *relativistic cryptography*, constitutes the main topic of this thesis.

1.2 Quantum information theory

As mentioned before the report written by Shannon in 1945 marks the beginning of modern cryptography [Sha49]. Thinking about encryption and the one-time pad led him to questions about the nature of information. Shannon's next paper investigating fundamental limits of compression and transmission [Sha48] is considered the beginning of *(classical) information theory*, which became an active field of research with a wide range of practical implications. While the basic framework of quantum mechanics already existed at the time (introduced in the 1920s and 30s by Bohr, Born, de Broglie, Dirac, Einstein, Heisenberg, Planck, Schrödinger and others), rigorous connections between the two were not established until much later.

In 1935 Einstein, Podolsky and Rosen wrote a paper in which they argue that quantum mechanics cannot be considered a complete theory [EPR35]. They postulate that for every measurement whose outcome is certain there exists an "element of reality" and deduce that due to the uncertainty principle incompatible observables cannot have simultaneous elements of reality. On the other hand, they note that in case of *entangled*[10] particles the elements of reality of one system depend on the measurements performed on the other. Since they perceive the elements of reality as something objective, independent of any measurement process, they conclude that the quantum-mechanical description must be incomplete. This idea was further developed by John Bell [Bel64] who realised that the assumptions of Einstein, Podolsky and Rosen boil down to the existence of *local hidden variables*, which completely determine the outcome of all possible measurements. Bell showed that any theory satisfying these requirements (like the classical theory) is subject to certain restrictions (now known as *Bell inequalities*) and demonstrated that quantum mechanics violates such restrictions. The first explicit Bell inequality proposed by Clauser, Horne, Shimony and Holt [CHSH69] is a clear-cut evidence that the set of quantum correlations is strictly bigger than its classical counterpart. Realising

[10] The term *Verschränkung* used "to describe the correlations between two particles that interact and then separate, as in the Einstein-Podolsky-Rosen experiment" first appeared in a letter written by Schrödinger who also proposed the English translation: *entanglement*.

that quantum mechanics gives rise to an information theory which is qualitatively different that the classical version, opened a new, fruitful research direction. Questions concerning storing or transmitting information using quantum systems have the appealing feature of being operational and fundamental at the same time. In the 1970s Holevo proved how many classical bits can be reliably stored in a quantum system [Hol73] and Helstrom showed how to optimally distinguish two quantum states [Hel76].

In 1980 Boris Tsirelson published a breakthrough paper, which exactly characterises the set of correlations achievable using quantum systems (in a restricted class of scenarios) [Tsi80]. Another important result concerning quantum correlations comes from Reinhard Werner, who showed that entanglement, while necessary, is not a sufficient condition for observing stronger-than-classical correlations [Wer89]. In 1982 Wootters and Żurek proved the celebrated *no-cloning* theorem, which states that given a single copy of an unknown quantum state, there does not exist a physical procedure that produces two (perfect) copies [WŻ82]. While the result itself is rather simple (including the proof), it has far-reaching consequences and shows that one should be rather careful when applying the classical intuition to quantum systems. Around the same time the first ideas to use quantum systems to perform computation came about. Richard Feynman proposed the concept of *quantum simulation*, i.e. using one quantum system to simulate another [Fey82] while David Deutsch initiated the study of *quantum computation* by introducing the concept of a quantum Turing machine and presenting a simple problem which can be solved more efficiently using quantum systems [Deu85]. While the problem introduced by Deutsch is of little practical use, it is important as the first demonstration that quantum computing is strictly more powerful than its classical counterpart.

In 1994 Peter Shor published a paper that changed the status of quantum computation from an exercise in linear algebra to a field of potentially enormous practical impact [Sho94]. Shor proposed an algorithm that can efficiently factor large numbers and solve the discrete logarithm problem, which, as a consequence, allows to break all commonly used public cryptography systems. In 1996 Lov Grover published an algorithm that gives a quadratic speed-up while searching an unstructured database [Gro96].[11] These two results sparked enormous interest as they showed that quantum computation might be important from the practical point of view. Since then the task of finding new quantum algorithms and building an actual quantum computer has been a full-time job of hundreds of computer scientists, physicists and engineers.

[11] Note that the speed-up of Grover's algorithm is provable, i.e. it is quadratically faster than *any* classical algorithm. Shor's algorithm, on the other hand, is exponentially faster than *the best known* classical algorithm.

It seems fair to say that it is the breakthroughs in quantum computation that gave the whole field a significant push and encouraged many brilliant researchers to work on quantum information. Since then the field has developed rapidly and this includes aspects closely related to quantum computation like quantum error-correction or quantum computer architecture but also areas which are not directly relevant like quantum correlations, quantum foundations, quantum Shannon theory or quantum cryptography. For more information we refer to a brief survey on early quantum information written by Bennett and Shor in 1998 [BS98] or to a book by Nielsen and Chuang [NC00], which became the primary textbook in the field (in particular for quantum computation). For a detailed introduction to the information-theoretic aspects (the quantum Shannon theory) see Chapter 1 of Mark M. Wilde's book [Wil13].

1.3 Quantum cryptography

In the late 1960s Stephen Wiesner wrote a paper on how to use quantum particles of spin-$\frac{1}{2}$ to produce money that is "physically impossible to counterfeit". The paper got rejected from a journal and ended up in Wiesner's drawer (the paper was eventually published in ACM SIGACT News [Wie83] about fifteen years later). These ideas were further pursued by Bennett, Brassard, Breidbart and Wiesner [BBBW83] and led to a groundbreaking paper proposing the first quantum key distribution protocol, which allows two distant parties to communicate securely through an insecure quantum channel [BB84]. In 1991 Artur Ekert proposed a quantum key distribution protocol that relied on entanglement and Bell's theorem [Eke91]. Another protocol (which relies on entanglement but not Bell's theorem) was presented in Ref. [BBM92] and soon the first experimental demonstration of quantum key distribution was reported together with concrete solutions for the classical post-processing phase and explicit security estimates [BBB$^+$92]. Since then an enormous amount of progress has been made in both theoretical and practical aspects of quantum key distribution and it is well beyond the scope of this introduction to discuss it. A recent article by Ekert and Renner is an excellent account of the current state of quantum key distribution [ER14].

Before we go into the details let us state very clearly that throughout this thesis we work under the (implicit) assumption that Alice and Bob trust their own devices. In other words, if the protocol requires Alice to generate a certain quantum state, she is capable of constructing a device that does just that and she may rest assured that the source does not accumulate information about the previous uses or leak secret data through extra degrees of freedom. While this assumption seems natural and easy to ensure in the classical world, it becomes more of a challenge in the

quantum world simply because our understanding and expertise in quantum technologies are limited. These considerations gave rise to the field of *device-independent* cryptography which aims to design protocols which remain secure even if executed using faulty or malicious devices. The fact that such strong security guarantees are even possible is clearly remarkable and this topic has received a lot of interest in the last couple of years. Due to a large volume of works on this topic we do not attempt to list the relevant references and point the interested reader at comprehensible and accessible lectures notes by Valerio Scarani [Sca12] as well as Sections IV.C and IV.D of a recent review on Bell nonlocality [BCP+14].

While quantum key distribution was and still remains the predominant area of research in quantum cryptography, other applications have been present from the very beginning as exemplified by Wiesner's unforgeable quantum money. The original paper of Bennett and Brassard contains a bit-commitment-based coin tossing protocol [BB84]. As pointed out by the authors the protocol is insecure if one of the parties leaves the quantum states untouched (instead of performing the prescribed measurements) but they consider it a "merely theoretical threat" due to the technological difficulty of implementing such a strategy. In 1991 Brassard and Crépeau proposed a different quantum bit commitment protocol [BC91], which does not suffer from the previous problem but is vulnerable against an adversary who can perform *coherent measurements*, i.e. joint measurements on multiple quantum particles, which, again, is considered difficult. By combining the two quantum bit commitment protocols they obtain a coin tossing protocol which can only be broken by an adversary who can *both* keep entanglement *and* perform coherent measurements. In the meantime a quantum protocol for oblivious transfer was proposed whose security, again, relies on the adversary being technologically limited [BBCS92]. In 1993 Brassard, Crépeau, Jozsa and Langlois [BCJL93] proposed a new bit commitment protocol which comes with a complete security proof that does not rely on any technological assumptions. In other words, the protocol is claimed to be secure against all attacks compatible with quantum physics. In 1992 Bennett et al. suggested how bit commitment and quantum communication can be used to construct oblivious transfer [BBCS92]. This construction was formalised and proven secure by Yao [Yao95], who refers to it as the "canonical construction", which gave the optimistic impression that quantum mechanics allows for secure two-party cryptography without any extra assumptions.[12] Unfortunately, it was later discovered that the protocol proposed in Ref. [BCJL93] is insecure, which soon led to a complete impossibility result [May97, LC97]. For a detailed account of quantum cryptography until that point please consult Refs. [BC96, Cré96, BCMS97].

[12] This construction shows that in the quantum world bit commitment and oblivious transfer are equivalent, which is believed not to be true classically.

The initial results of Mayers, Lo and Chau began a sequence of negative results. Impossibility of bit commitment immediately rules out oblivious transfer and, in fact, the same techniques can be used to rule out any one-sided two-party computation (i.e. a primitive in which inputs from two parties produce output which is only given to one of them) [Lo97]. The more complicated case of two-sided computation was first considered by Colbeck (for a restricted class of functions) [Col07] while the general impossibility result was proven by Buhrman, Christandl and Schaffner [BCS12]. In case of string commitment (i.e. when we simultaneously commit to multiple bits) it is clear that the perfect primitive cannot be implemented but the situation becomes slightly more involved when it comes to imperfect primitives as the results depend on the exact security criteria used [BCH+06, BCH+08]. For more recent impossibility proofs of bit commitment see Refs. [DKSW07, WTHR11, CDP+13].

While perfect quantum bit commitment is not possible, it is interesting to know what security trade-offs are permitted by quantum mechanics. In the classical case the trade-offs are trivial: in any classical protocol at least one of the parties can cheat with certainty. Preliminary results on the quantum security trade-offs were proven by Spekkens and Rudolph [SR01], while the optimal trade-off curve was found by Chailloux and Kerenidis [CK11]. Interestingly enough, the achievability is argued through a construction that uses a complicated and rather poorly understood weak coin flipping protocol by Mochon [Moc07].

Another direction (similar to what was done previously in the classical world) is to identify the minimal assumptions that would make two-party cryptography possible in the quantum world.

One solution available in the classical world is to give Alice and Bob access to some trusted randomness. The quantum generalisation of this assumption would be to give Alice and Bob access to quantum systems or some other source of stronger-than-classical correlations [BCU+06, WWW11]. Such correlations indeed allow us to implement secure bit commitment. The advantage of this assumption over the classical counterpart is that in the classical case we had to trust whoever distributed the randomness (in the original paper referred to as the *trusted initialiser* [Riv99]). On the other hand, stronger-than-classical correlations guarantee security regardless of where they came from.

A natural quantum extension of the bounded storage model proposed by Maurer [Mau91] is the quantum bounded storage model [DFSS05, DFR+07, Sch10] and its generalisation to the case of noisy quantum storage [WST08, KWW12, BFW14]. While storing classical information seems easy and cheap (which makes the assumption of the adversary's bounded storage not particularly convincing), reliable storage of quantum information continues to pose a significant challenge and, hence, makes

for a reasonable assumption. Another technological limitation that leads to secure bit commitment is the restriction on the class of quantum measurements that the dishonest party can perform [Sal98].

The proposal to combine quantum mechanics with relativistic[13] communication constraints (attributed to Louis Salvail) was already mentioned in 1996 [BC96, Cré96]. The early papers of Kent [Ken99, Ken05] consider security against quantum adversaries but the actual protocols are completely classical. To the best of our knowledge, the first quantum relativistic protocol was proposed by Colbeck and Kent for a certain variant of coin tossing [CK06]. This marks the beginning of *quantum relativistic cryptography*.

1.4 Outline

The main theme of this thesis is relativistic quantum cryptography with a particular focus on commitment schemes. Chapter 2 contains the necessary background in quantum information theory and cryptography.

In Chapter 3 we introduce non-communicating models as they originally appeared in the context of interactive proofs. We show why they are useful in cryptography and determine the exact communication constraints that might allow for secure commitment schemes. For each of these models we present a provably secure bit commitment protocol.

Chapter 4 introduces the framework for relativistic protocols. We start with a couple of simple examples and then present a procedure which maps a relativistic protocol onto a model with partial communication constraints. We show that at least in some scenarios the analysis of such models is tractable.

In Chapter 5 we focus on a particular quantum bit commitment protocol. We analyse its security by mapping it onto a simple quantum guessing game. Moreover, we adapt the original protocol to make it robust against experimental errors and we extend the security analysis appropriately. We briefly report on an implementation of the protocol done in collaboration with an experimental group at the University of Geneva.

In Chapter 6 we propose a new, classical multiround bit commitment protocol and analyse its security against classical adversaries. The multiround protocol allows to achieve arbitrarily long commitments (at the cost of growing resources) with explicit and easily-computable security guarantees. Again, we briefly discuss an experiment performed in collaboration with the Geneva group.

Chapter 7 summarises the content of this thesis and outlines a couple of interesting direction for future research in quantum relativistic cryptography.

[13] Throughout this thesis the term relativity always refers to special relativity.

Chapter 2

Preliminaries

In this chapter we establish the notation, nomenclature and some basic concepts used throughout this thesis.

2.1 Notation and miscellaneous lemmas

2.1.1 Strings of bits

Given two bits $a, b \in \{0,1\}$ we use "$\oplus$" to denote their exclusive-OR (`XOR`)

$$a \oplus b := a + b \mod 2.$$

For an n-bit string $x \in \{0,1\}^n$, let x_k be the k^{th} bit of x and the `XOR` of two strings (of equal length) is defined bitwise. The fractional Hamming weight of x is the fraction of ones in the string

$$\mathrm{w_H}(x) = \frac{1}{n}\big|\{k \in [n] : x_k = 1\}\big|,$$

where $|\cdot|$ denotes the cardinality of the set. The fractional Hamming distance between x and y is the fraction of positions at which the two strings differ

$$\mathrm{d_H}(x,y) = \frac{1}{n}\big|\{k \in [n] : x_k \neq y_k\}\big|.$$

Note that the Hamming weight can be interpreted as the distance from the string of all zeroes 0^n: $\mathrm{w_H}(x) = \mathrm{d_H}(x, 0^n)$. For $S \subseteq [n]$, we use x_S to denote the substring of x specified by the indices in S. If $d \in \{0,1\}$ is a bit, we define

$$d \cdot x = \begin{cases} 0^n & \text{if } \ d = 0, \\ x & \text{if } \ d = 1. \end{cases}$$

2.1.2 Cauchy-Schwarz inequality for probabilities

When dealing with probabilities we use uppercase letters to denote random variables and lowercase letters to denote values they might take, e.g. $\Pr[X = x]$. For $j, k \in \mathcal{S}$ we use $\sum_{j \neq k}$ as a shorthand notation for $\sum_{j \in \mathcal{S}} \sum_{k \in \mathcal{S} \setminus \{j\}}$.

LEMMA 2.1. *Let X be a uniform random variable over $[n]$, i.e. $\Pr[X = x] = \frac{1}{n}$ for all $x \in [n]$, and let $\{E_j\}_{j=1}^m$ be a family of events defined on $[n]$. Let p be the average probability (of these events)*

$$p := \frac{1}{m} \sum_{j=1}^{m} \Pr[E_j]$$

and c be the cumulative size of the pairwise intersections

$$c := \sum_{j \neq k} \Pr[E_j \wedge E_k].$$

Then the following inequality holds

$$p \leq \frac{1 + \sqrt{1 + 4c}}{2m}.$$

Proof. Each event can be represented by a vector in $\mathbb{R}^n$ whose entries are labelled by integers from $[n]$. If a particular outcome belongs to the event, we set the corresponding component to $1/\sqrt{n}$ and if it does not we set it to 0

$$[s_j]_x = \begin{cases} \frac{1}{\sqrt{n}} & \text{if } x \in E_j, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, let n be the normalised, uniform vector: $[n]_x = 1/\sqrt{n}$ for all $x \in [n]$. It is straightforward to check that with these definitions we have

$$\Pr[E_j] = \langle s_j, n \rangle = \langle s_j, s_j \rangle \quad \text{and} \quad \Pr[E_j \wedge E_k] = \langle s_j, s_k \rangle,$$

where $\langle \cdot, \cdot \rangle$ denotes the standard inner product on $\mathbb{R}^n$ and since the vectors are non-negative we have $\langle s_j, s_k \rangle \geq 0$. Since the inner product is linear we have

$$p = \frac{1}{m} \sum_{j=1}^{m} \Pr[E_j] = \frac{1}{m} \sum_{j} \langle s_j, n \rangle = \frac{1}{m} \langle \sum_{j} s_j, n \rangle,$$

which can be upper bounded using the Cauchy-Schwarz inequality. Since $\langle n, n \rangle = 1$

we have

$$\langle \sum_j s_j, n\rangle^2 \leq \sum_{jk} \langle s_j, s_k\rangle = \sum_j \langle s_j, s_j\rangle + \sum_{j\neq k} \langle s_j, s_k\rangle = mp + c,$$

which gives the following quadratic constraint

$$p^2 \leq \frac{p}{m} + \frac{c}{m^2}.$$

Solving for p gives the desired bound.

2.1.3 Chernoff bound for the binomial distribution

LEMMA 2.2 ([Che52]). *Let $X_1, X_2, \ldots, X_n$ be independent random variables taking on values 0 or 1. Let $X = \sum_{i=1}^n X_i$ and μ be the expectation value of X. Then for any $\delta > 0$ the following inequality holds*

$$\Pr[X < (1-\delta)\mu] < \left(\frac{e^{-\delta}}{(1-\delta)^{1-\delta}}\right)^{\mu} \leq \exp\left(-\frac{\mu\delta^2}{2}\right).$$

Alternatively, setting $s = (1-\delta)\mu$ gives

$$\Pr[X < s] < \exp\left(-\frac{1}{2}\left(\sqrt{\mu} - \frac{s}{\sqrt{\mu}}\right)^2\right).$$

2.2 Quantum mechanics

Quantum mechanics despite its mysterious nature admits a relatively simple mathematical description. While it is an interesting question to ask *why* quantum mechanics is as it is, instead of being more (or less) powerful (and indeed such questions constitute the main topic of quantum foundations), we take a more hands-on approach. Namely, we accept the standard textbook formulation of quantum mechanics as it is and investigate its consequences. Section 2.2.1 defines the basic notions of linear algebra (and, hence, can be skipped by most readers), which will be necessary to describe the quantum formalism in Section 2.2.2.

2.2.1 Linear algebra

The following section contains the bare minimum of linear algebra necessary to understand this thesis and serves primarily the purpose of establishing consistent notation and nomenclature. For a complete and detailed introduction to linear algebra we refer to the excellent textbooks by Rajendra Bhatia [Bha97, Bha09].

In this thesis we restrict our attention to finite-dimensional systems. Let $\mathcal{H}$ be a Hilbert space of finite dimension $d = \dim \mathcal{H} < \infty$ over complex numbers. Let $\mathcal{H}^*$ denote the dual space of $\mathcal{H}$, i.e. the space of linear functionals on $\mathcal{H}$. We employ the *bra-ket* notation proposed by Paul Dirac [Dir39], in which elements of $\mathcal{H}$ are written as *kets* $|\psi\rangle \in \mathcal{H}$ and each ket has an associated *bra*, denoted by $\langle\psi| \in \mathcal{H}^*$, such that applying the linear functional $\langle\psi|$ to an arbitrary vector $|\phi\rangle$, written as a *bra-ket* $\langle\psi|\phi\rangle$, corresponds exactly to evaluating the inner product between $|\phi\rangle$ and $|\psi\rangle$. A set of d vectors $\{|e_j\rangle\}_{j=1}^d$ constitutes an orthonormal basis if the vectors are orthogonal and normalised, i.e. $\langle e_j|e_k\rangle = \delta_{jk}$, where δ_{jk} is the Kronecker delta.

Let $\mathcal{L}(\mathcal{H})$ be the set of linear operators acting on $\mathcal{H}$. The *identity operator*, denoted by $\mathbb{1}$, is the unique operator that satisfies

$$\mathbb{1}|\psi\rangle = |\psi\rangle$$

for all $|\psi\rangle \in \mathcal{H}$. Writing a linear operator $L \in \mathcal{L}(\mathcal{H})$ in a particular basis $\{|e_j\rangle\}_{j=1}^d$ leads to a $d \times d$ (complex) matrix whose entries equal

$$L_{jk} = \langle e_j|L|e_k\rangle,$$

where the expression $\langle e_j|L|e_k\rangle$ should be understood as $\langle e_j|\big(L|e_k\rangle\big)$. Note that while the operator and its matrix representation are not the same object (the former is basis-independent, while the latter corresponds to a particular basis) for the purpose of this thesis this distinction may be ignored and we will use the two terms interchangeably. The *trace* of a square matrix L is the sum of its diagonal entries

$$\operatorname{tr} L = \sum_j L_{jj} = \sum_j \langle e_j|L|e_j\rangle.$$

The *Hermitian conjugate* of an operator L, denoted by $L^\dagger$, is defined to satisfy

$$[L^\dagger]_{jk} = [L_{kj}]^*,$$

where * denotes the complex conjugate. An operator satisfying $L^\dagger = L$ is called *Hermitian* (or *self-adjoint*) and we denote the set of Hermitian operators acting on $\mathcal{H}$ by $\mathcal{H}(\mathcal{H})$. Operators satisfying $LL^\dagger = L^\dagger L = \mathbb{1}$ are called unitary operators or unitaries.

It is easy to verify that for a Hermitian operator $H = H^\dagger$ we have $\langle\psi|H|\psi\rangle \in \mathbb{R}$ for all vectors $|\psi\rangle \in \mathcal{H}$. A Hermitian operator is called *positive semidefinite* if

$$\langle\psi|H|\psi\rangle \geq 0$$

for all vectors $|\psi\rangle \in \mathcal{H}$, which is often written as $H \geq 0$.

Every linear operator $L \in \mathcal{L}(\mathcal{H})$ admits a *singular value decomposition*, i.e. it can be written in the form $L = USV$, where U and V are unitary operators and S is a diagonal matrix of real, non-negative entries known as the *singular values* of L. Let $s = (s_1, s_2, \ldots, s_d)$ be the vector of singular values. For $p \in [1, \infty)$ the Schatten p-norm of L, denoted by $\|L\|_p$, is defined as the vector p-norm of s

$$\|L\|_p := \Big(\sum_{j=1}^{d} s_j^p\Big)^{1/p}.$$

For the purpose of this thesis we will only need the limit $p \to \infty$ so let us define

$$\|L\| := \lim_{p\to\infty} \|L\|_p = \max_j s_j.$$

2.2.2 Quantum formalism

A pure state of a quantum system is described by a normalised vector, i.e. $|\psi\rangle \in \mathcal{H}$ such that $\langle\psi|\psi\rangle = 1$. We adopt the convention that every d-dimensional Hilbert space $\mathcal{H}$ is equipped with an orthonormal basis $\{|k\rangle\}_{k=0}^{d-1}$, which we call the *computational* (or *standard*) basis. Writing $|\psi\rangle$ in this basis

$$|\psi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle$$

allows us to interpret it as a d-dimensional complex unit vector. The global phase of a state is inconsequential, i.e. quantum mechanics tells us that vectors $|\psi\rangle$ and $e^{i\alpha}|\psi\rangle$ (for $\alpha \in \mathbb{R}$) correspond to the same physical state. The smallest non-trivial quantum system corresponds to $d = 2$ and is called a *qubit* (a term coined by Schumacher and Wootters [Sch95]). The Hadamard operator is defined as

$$H = \frac{1}{\sqrt{2}} \sum_{j,k\in\{0,1\}} (-1)^{jk} |j\rangle\langle k|$$

or

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

It is easy to verify that H is simultaneously Hermitian ($H = H^\dagger$) and unitary ($HH^\dagger = H^\dagger H = H^2 = \mathbb{1}$). Define $|+\rangle := H|0\rangle$, $|-\rangle := H|1\rangle$ and let us call $\{|+\rangle, |-\rangle\}$ the *Hadamard* (or *diagonal*) basis. The computational and Hadamard bases are widely used in cryptography because they are an example of *mutually*

unbiased bases (for $d = 2$), i.e. they satisfy

$$|\langle 0|+\rangle| = |\langle 0|-\rangle| = |\langle 1|+\rangle| = |\langle 1|-\rangle| = \frac{1}{\sqrt{2}}\left(= \frac{1}{\sqrt{d}}\right),$$

which captures the notion of being maximally incompatible.

A mixed quantum state on $\mathcal{H}$ is a Hermitian operator, which is positive semidefinite and of unit trace. We define the set of (mixed) quantum states on $\mathcal{H}$

$$\mathcal{S}(\mathcal{H}) := \{\rho \in \mathcal{H}(\mathcal{H}) : \rho \geq 0 \quad \text{and} \quad \operatorname{tr}\rho = 1\}.$$

The operator ρ describing a mixed state is called the *density matrix*. Mixed states are a generalisation of pure states: an arbitrary pure state $|\psi\rangle$ can be represented as a density matrix $\rho = |\psi\rangle\langle\psi|$. Mixed states arise naturally when dealing with composite systems.

Suppose we have two systems (or registers) A and B described by Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, respectively, and we want to describe the global state of the system. What are the allowed states on A and B taken together? In case of pure states, quantum mechanics tells us to take the tensor product of the two Hilbert spaces, i.e. $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$. Therefore, an arbitrary pure bipartite state can be written as

$$|\psi\rangle_{AB} = \sum_{jk} c_{jk}|j\rangle_A|k\rangle_B,$$

where $|j\rangle_A|k\rangle_B$ should be understood as $|j\rangle_A \otimes |k\rangle_B$ (the tensor product symbol is commonly omitted to avoid notational clutter). Given a bipartite system one might wonder what can be said about the *marginal states* on A and B (similar to the concept of the marginals of a probability distribution). In particular, one would expect that if we restrict ourselves to measurements on A alone then it should be possible to "truncate" $|\psi\rangle_{AB}$ to A by disregarding any information about B. This intuition leads the concept of *reduced states*. Let us first write the density matrix corresponding to $|\psi\rangle_{AB}$

$$\rho_{AB} = |\psi\rangle\langle\psi|_{AB} = \sum_{jj'kk'} c_{jk}c^*_{j'k'}|j\rangle\langle j'|_A \otimes |k\rangle\langle k'|_B.$$

Given an operator acting on multiple registers we define the operation of *partial trace* which "traces out" a particular register, e.g.

$$\operatorname{tr}_B\left(|j\rangle\langle j'|_A \otimes |k\rangle\langle k'|_B\right) = |j\rangle\langle j'|_A \cdot \operatorname{tr}_B\left(|k\rangle\langle k'|_B\right) = |j\rangle\langle j'|_A \cdot \delta_{kk'}.$$

Note that the standard trace operation corresponds to tracing all the registers. It is easy to verify that partial traces commute so we can without ambiguity write

$\mathrm{tr}_{AB}(\cdot) = \mathrm{tr}_A \mathrm{tr}_B(\cdot) = \mathrm{tr}_B \mathrm{tr}_A(\cdot)$. Tracing out the B register from the density matrix ρ_{AB} gives

$$\rho_A = \mathrm{tr}_B \rho_{AB} = \sum_{jj'k} c_{jk} c^*_{j'k} |j\rangle\langle j'|_A,$$

which is easily verified to be a valid quantum state $\rho_A \in \mathcal{S}(\mathcal{H}_A)$ and which we call *the reduced state on* A. It is easy to verify that the knowledge of ρ_A suffices to make all possible predictions about operations or measurements that act solely upon subsystem A. In cryptography reduced states are important because they allow us to quantify the amount of knowledge that a particular subsystem provides to its holder.

Once we know how to describe the state of a quantum system we would like to know how we can interact with it. To extract any information from a quantum state one needs to *measure* it. Note that this is one of the aspects in which quantum theory differs significantly from its classical counterpart. In the classical world the object and its (complete) description are *operationally equivalent*: given the description one can construct the object and given the object one can determine (to an arbitrary precision) its description. In the quantum world a single copy of an object gives us significantly less information than its complete description as demonstrated by the no-cloning theorem [WŻ82]. In contrast to the classical world, every quantum system can be measured in multiple ways, which means that the measurement process must be described explicitly. A measurement[1] on a d-dimensional quantum state which yields outcomes from a finite alphabet $\mathcal{X}$ is a collection of positive semidefinite operators $\{F_x\}_{x\in\mathcal{X}}$[2] that add up to ($d$-dimensional) identity

$$F_x \geq 0 \quad \text{and} \quad \sum_{x\in\mathcal{X}} F_x = \mathbb{1}. \tag{2.1}$$

Quantum mechanics is a probabilistic theory, i.e. it only allows us to calculate *probabilities* of observing different outcomes. According to *Born's rule* [Bor26] measuring the state $\rho \in \mathcal{S}(\mathcal{H})$ yields outcome x with probability

$$p(x) = \mathrm{tr}(F_x \rho).$$

It is easy to see that the condition (2.1) is imposed to ensure that the resulting probability distribution is non-negative and normalised *for every state*. Note that such an information-theoretic formulation of the measurement process does not necessarily coincide with the notion of measuring a physical quantity, e.g. the outcome might

[1] We implicitly assume that we are only interested in the classical outcome of the measurement and ignore the post-measurement state.

[2] To avoid confusion whenever describing the set of measurement operators we explicitly state the index that must be summed over to obtain identity.

not be a number so one cannot talk about the expectation value or the standard deviation of the measurement.

The process of measuring a quantum state can be seen as a map that takes a quantum state and outputs a probability distribution. This naturally generalises to maps in which the output remains quantum and such maps are known as *quantum channels*. The identity channel (i.e. the unique channel that leaves every state unaffected) is denoted by id[3]. Generally, a map $\Phi : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is a quantum channel iff:

1. Φ is linear, i.e. for any $\alpha, \beta \in \mathbb{C}$ and $X, Y \in \mathcal{L}(\mathcal{H}_A)$

$$\Phi(\alpha X + \beta Y) = \alpha\Phi(X) + \beta\Phi(Y).$$

2. Φ is completely positive, i.e. for any $X_{AR} \in \mathcal{H}(\mathcal{H}_A \otimes \mathcal{H}_R)$, where $\mathcal{H}_R$ is an auxiliary Hilbert space of arbitrary dimension,

$$X \geq 0 \implies (\Phi_A \otimes \mathrm{id}_R)(X_{AR}) \geq 0.$$

3. Φ is trace-preserving, i.e. for any $X \in \mathcal{L}(\mathcal{H}_A)$

$$\mathrm{tr}\,\Phi(X) = \mathrm{tr}\,X.$$

These properties can be rigorously derived from the assumption that a channel is a result of a unitary evolution acting on a larger Hilbert space. On a more pragmatic level, these rules ensure that the channel is a linear map that takes quantum states on A into valid quantum states on B. When dealing with multipartite states it might be useful to explicitly write out the input and output registers, e.g. $\Phi_{A\to B}$.

2.2.3 Remote state preparation

A state of the form

$$\rho_{XB} = \sum_x p_x |x\rangle\langle x|_X \otimes \rho_B^x \tag{2.2}$$

is called *classical-quantum* (cq) since the first register represents a classical random variable X while the second is a general quantum system. Such states describe how a quantum system can be correlated with some classical data. One way of obtaining such a state is to sample the classical random variable X and prepare subsystem B in a particular state conditional on the outcome. Here, we show how to use

[3]Note that it is common in quantum information to use the same symbol for the identity channel and the identity operator since it is usually clear from the context which one is meant. To avoid confusion we prefer to use different symbols.

entanglement to *remotely* prepare a certain class of such states, a phenomenon also known as *steering*.

Define the maximally entangled state of dimension d as

$$|\Psi_d\rangle_{AB} := \frac{1}{\sqrt{d}} \sum_{j=1}^{d} |j\rangle_A |j\rangle_B.$$

It is easy to verify that in this case both marginals are *maximally mixed*, i.e. proportional to the identity matrix

$$\mathrm{tr}_A \, |\Psi_d\rangle\langle\Psi_d|_{AB} = \mathrm{tr}_B \, |\Psi_d\rangle\langle\Psi_d|_{AB} = \frac{\mathbb{1}}{d}.$$

Moreover, for an arbitrary linear operator $L = \sum_{jk} L_{jk} |j\rangle\langle k|$, we have

$$\mathrm{tr}_A \left[(L \otimes \mathbb{1}) |\Psi_d\rangle\langle\Psi_d| \right] = L^{\mathrm{T}},$$

where L^{T} denotes the transpose with respect to the computational basis

$$L^{\mathrm{T}} = \sum_{jk} L_{jk} |k\rangle\langle j|.^{4}$$

If we replace L with a measurement operator this implies that observing a particular outcome on A results in a particular subnormalised quantum state on B. Hence, we have *remotely prepared* a state on B by performing a measurement on A. It is easy to see that any cq-state of the form (2.2) which satisfies

$$\sum_x p_x \rho^x = \frac{\mathbb{1}}{d}, \tag{2.3}$$

can be obtained by performing the right measurement on one half of the d-dimensional maximally entangled state. More specifically, the appropriate measurement $\{F_x\}_x$ is described by measurement operators $F_x = d p_x (\rho^x)^{\mathrm{T}}$. The restriction (2.3) expresses the rule that the reduced state on B must remain unchanged, i.e. it must remain maximally mixed. This phenomenon turns out to be important in quantum cryptography.

An essential feature of quantum information is the ability to encode information in two (or more) incompatible bases. The most common example was originally introduced by Wiesner [Wie83] but goes under the name of *BB84 states* (after Bennett and Brassard who popularised the term [BB84]). In this case Alice uses either computational or Hadamard basis to encode a logical bit $x \in \{0, 1\}$ in a qubit

[4] The transpose operation is basis-dependent just like the definition of the maximally entangled state.

which she later sends to Bob. If the logical bit is uniform the two encodings lead to

$$\rho_{XB} = \frac{1}{2}\sum_x |x\rangle\langle x|_X \otimes |x\rangle\langle x|_B.$$

and

$$\rho_{XB} = \frac{1}{2}\sum_x |x\rangle\langle x|_X \otimes H|x\rangle\langle x|_B H,$$

respectively. It is easy to verify that both of these satisfy relation (2.3) with $d = 2$. This leads to an important observation (in this particular cryptographic context due to Bennett, Brassard and Mermin [BBM92]) that such states can be prepared by first generating the maximally entangled state of two qubits $|\Psi_2\rangle$ and then measuring subsystem A in the right basis. In fact, Alice simply makes a measurement in either computational or Hadamard basis.

Since measurements on Alice's side commute with any operations on Bob's side, they can be delayed until some later point in the protocol, which means that now Alice and Bob share entanglement during the protocol. In other words, we have turned a prepare-and-measure scheme (Alice prepares a state and sends it to Bob, who performs a measurement), in which there is no entanglement between Alice and Bob, into an equivalent (from the security point of view) entanglement-based scheme (Alice and Bob simultaneously perform measurements on a shared entangled state). Often the entanglement-based schemes are easier to analyse, which we we will take advantage of to prove security of a quantum relativistic bit commitment protocol in Chapter 5.

2.3 Multiplayer games

For the purpose of this thesis, a game is an interaction between a *referee* and one or more *players*. The referee asks each player a question and the player must give an answer. In most cases the players are not allowed to communicate during the game. A *strategy* is a procedure that the players follow to generate their answers. At the end of the game, the referee decides whether the game is won or lost.

2.3.1 Classical and quantum strategies

For concreteness, we consider a game of m *non-communicating* players. Each player receives an *input* from $\mathcal{X}$ and is required to *output* a symbol from $\mathcal{Y}$ ($\mathcal{X}$ and $\mathcal{Y}$ are arbitrary finite alphabets). A game is defined by the input distribution

$$p : \underbrace{\mathcal{X} \times \mathcal{X} \times \ldots \times \mathcal{X}}_{m \text{ times}} \mapsto [0, 1]$$

and a *predicate function*

$$V : \underbrace{(\mathcal{X} \times \mathcal{Y}) \times \ldots \times (\mathcal{X} \times \mathcal{Y})}_{m \text{ times}} \mapsto \{0, 1\}$$

which specifies whether the players *win* or *lose* for a particular combination of inputs and outputs.[5]

Every strategy available to classical players can be written as a convex combination of deterministic strategies. Hence, the maximum winning probability, denoted by ω and referred to as *the classical value* of the game, can be achieved by a deterministic strategy. A deterministic strategy is a collection of m functions $(f_j)_{j=1}^m$, $f_j : \mathcal{X} \mapsto \mathcal{Y}$, which determine each player's response. Therefore,

$$\omega := \max_{f_1, f_2, \ldots, f_m} \sum_{x_1 \in \mathcal{X}} \ldots \sum_{x_m \in \mathcal{X}} p(x_1, \ldots, x_m) V\big(x_1, f_1(x_1), \ldots, x_m, f_m(x_m)\big),$$

where the maximum is taken over all combinations of functions.

Quantum players, in turn, are allowed to share a quantum state and perform measurements that depend on the inputs. For simplicity in the quantum setting we only describe two-player games ($m = 2$) but these concepts extend in a straightforward way to an arbitrary number of players (see for example Ref. [Vid13]). A quantum strategy consists of a bipartite pure quantum state (of finite dimension) $|\psi\rangle_{AB}$[6] and measurements that each player will perform for every possible input $x \in \mathcal{X}$, denoted by $\{F_y^x\}_{y \in \mathcal{Y}}, \{G_y^x\}_{y \in \mathcal{Y}}$. The maximum winning probability achievable by quantum players denoted by ω^* is called *the quantum value*

$$\omega^* := \sup \sum_{y_1, y_2 \in \mathcal{Y}} \sum_{x_1, x_2 \in \mathcal{X}} p(x_1, x_2) V\big(x_1, y_2, x_2, y_2\big) \langle \psi | F_{y_1}^{x_1} \otimes G_{y_2}^{x_2} | \psi \rangle,$$

where the optimisation is taken over all quantum strategies.

Calculating the classical value of a game can be done by iterating over all possible strategies. While this is clearly not efficient (the number of strategies to check is exponential in the number of inputs), at least in principle it can be done.[7] On the other hand, computing the quantum value is a more difficult problem and no generic procedure is known.[8] The problem stems from the fact that we do not

[5] Clearly, this generalises in a straightforward manner to the case where the range of V is $\mathbb{R}$. Then V assigns a particular *score* to every combination of inputs and outputs. However, in this thesis we only consider games in which the players either win or lose.

[6] It is sufficient to consider pure states since a mixed state can be written as a convex combination of pure states.

[7] In fact, finding the classical value of a general game is NP-hard, i.e. we believe it cannot be done efficiently.

[8] The quantum value of an `XOR` game can be calculated using semidefinite programming techniques [Weh06]. For general games there exist hierarchies by Navascués, Pironio, Acín [NPA07]

have a convenient description of the quantum set of correlations (i.e. there is no efficient procedure to decide whether a given point belongs to the set or not). To establish an upper bound on the quantum value of a game it is common to consider a larger set of correlations known as the *no-signalling* correlations, which does admit a simple description. Intuitively, this is the largest set of correlations that does not allow to send messages between different parties and the simplest example is the so-called Popescu-Rohrlich box [PR94]. Because the no-signalling set is a polytope (i.e. the convex hull of a finite set of extreme points) we know how to optimise over it (at least in principle, efficiency considerations apply as before). For a detailed characterisation of different sets of correlations refer to a recent review paper on Bell nonlocality [BCP+14].

2.3.2 Finite fields

A field is a set with two operations: addition and multiplication, which satisfy the usual properties as listed below.

- The field is closed under multiplication and addition.
- Both operations are associative.
- Both operations are commutative.
- There exist additive and multiplicative identity elements.
- There exist additive and multiplicative inverses (except for the additive identity which does not have a multiplicative inverse).
- Multiplication is distributive over addition.

It is easy to see that real or complex numbers form with the standard addition and multiplication are fields. We call a field *finite* (the name *Galois field* is also used after Évariste Galois) if the set of elements is finite. The order of a finite field is the number of elements in the set and a finite field of order q exists iff q is a prime power, i.e. $q = p^k$ for some prime p and integer k. Since all finite fields of a given order are isomorphic (i.e. they are identical up to relabelling of the elements), we speak of *the* finite field of order q denoted by $\mathbb{F}_q$. For a thorough introduction to finite fields please consult an excellent book by Mullen and Mummert [MM07].

Finite fields appear often in coding theory and cryptography since they are finite sets closed under (appropriately defined) addition, multiplication and their inverses.

and Doherty, Liang, Toner, Wehner [DLTW08], which give increasingly tighter approximations on the correct value. While these hierarchies ultimately converge to the correct value, the rate of convergence is not well-understood. Moreover, calculating the higher level approximations becomes a difficult task from the computational point of view.

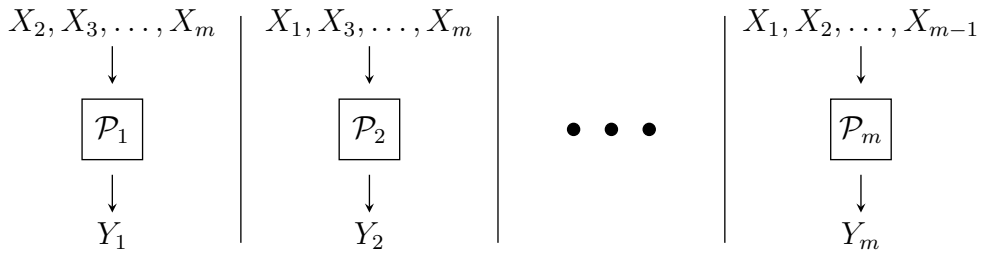

Fig. 2.1: The "Number on the Forehead" model. Vertical lines remind us that the players are not allowed to communicate.

Moreover, all these operations can be implemented efficiently on a computer. Fields corresponding to $p = 2$ are a common choice since their elements have a natural representation as strings of bits. The protocol proposed in Chapter 6 uses finite-field arithmetic and its security hinges on the difficulty of a certain family of multiplayer games. In this section we prove upper bounds on the classical value of such games and discuss the connection to a natural algebraic problem concerning multivariate polynomials over finite fields.

2.3.3 Definition of the game

Buhrman and Massar [BM05] proposed a generalisation of the CHSH game [CHSH69], which was further studied by Bavarian and Shor [BS15]. A natural multiplayer generalisation of this game arises in the security analysis of the multiround bit commitment protocol in Chapter 6. Since the analysis does not require familiarity with the actual actual bit commitment protocol and might be of independent interest, we have decided to make it a stand-alone component of the Preliminaries (rather than incorporating it in Chapter 6).

Consider a game with m players, denoted by $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_m$, and let $X_1, X_2, \ldots, X_m$ be random variables drawn independently, uniformly at random from $\mathbb{F}_q$

$$p(x_1, x_2, \ldots, x_m) = (q^{-1})^m = q^{-m}.$$

We use $[n]$ to denote the set of integers between 1 and n, $[n] := \{1, 2, \ldots, n\}$. In the "Number on the Forehead" model [CFL83] $\mathcal{P}_k$ receives *all the random variables except for the* k^{th} *one*, which we denote by $X_{[m]\setminus\{k\}}$, and is required to output an element of $\mathbb{F}_q$, which we denote by Y_k (see Fig. 2.1). The game is won if the *sum of the outputs equals the product of the inputs* (all the operations are performed in the finite field), i.e. the predicate function is

$$V(x_1, y_2, \ldots, x_m, y_m) = \begin{cases} 1 & \text{if } \prod_{k=1}^m x_k = \sum_{k=1}^m y_k, \\ 0 & \text{otherwise.} \end{cases}$$

If the player $\mathcal{P}_k$ employs a deterministic strategy described by $f_k : \mathbb{F}_q^{(m-1)} \mapsto \mathbb{F}_q$, i.e. he outputs $Y_k = f_k(X_{[m]\setminus\{k\}})$, then the winning probability equals

$$\omega_m(f_1, f_2, \ldots, f_m) := \Pr\Big[\prod_{k=1}^{m} X_k = \sum_{k=1}^{m} f_k(X_{[m]\setminus\{k\}})\Big].$$

As described in Section 2.3 the classical value of the game equals

$$\omega_m := \max_{f_1, f_2, \ldots, f_m} \omega_m(f_1, f_2, \ldots, f_m), \tag{2.4}$$

where the maximisation is taken over all combinations of functions from $\mathbb{F}_q^{(m-1)}$ to $\mathbb{F}_q$.[9] Our goal is to find an upper bound on ω_m as a function of q and m.

2.3.4 Relation to multivariate polynomials over finite fields

As the probability distribution of inputs is uniform the winning probability of a particular deterministic strategy (defined by a collection of functions $f_1, f_2, \ldots, f_m$) is proportional to the number of inputs $(x_1, x_2, \ldots, x_m)$ on which the following equality holds

$$\prod_{k=1}^{m} x_k = \sum_{k=1}^{m} f_k(x_{[m]\setminus\{k\}}). \tag{2.5}$$

Alternatively, we can count the zeroes of the following function

$$P(x_1, x_2, \ldots, x_m) = \prod_{k=1}^{m} x_k - \sum_{k=1}^{m} f_k(x_{[m]\setminus\{k\}}).$$

By the Lagrange interpolation method every function from $\mathbb{F}_q^n$ to $\mathbb{F}_q$ (for arbitrary $n \in \mathbb{N}$) can be written as a polynomial. Therefore, the question concerns the number of zeroes of the polynomial P. Different strategies employed by the players give rise to different polynomials and we need to characterise what polynomials are "reachable" in this scenario. The output of $\mathcal{P}_k$ is an arbitrary polynomial of $x_{[m]\setminus\{k\}}$, hence, it only contains terms that depend on *at most* $m-1$ *variables*. This means that the part of P that depends on *all* m *variables* comes solely from the first term and equals $\prod_{k=1}^{m} x_k$. Therefore, finding the classical value of the game is equivalent to finding the polynomial with the largest number of zeroes, whose only term that depends on all m variables equals $\prod_{k=1}^{m} x_k$. This shows that the optimal strategy for our game is closely related to purely algebraic properties of polynomials over finite fields.

[9] Clearly, this is a function of both q and m but we have decided not to mention the dependence on q explicitly (to avoid overcrowding the symbol with sub- or superscripts). This is justified because in our application q is a parameter that has to be chosen before the protocol begins, whereas m can be decided upon at some later point.

2.3.5 A recursive upper bound on the classical value

Here, we find explicit upper bounds on ω_m through an induction argument. First, note that for $m = 1$ there is only one term on the right-hand side of Eq. (2.5) and since this term takes no arguments it is actually a constant. Since X_1 is uniform we have

$$\omega_1 := \max_{c\in\mathbb{F}_q} \Pr[X_1 = c] = \frac{1}{q}.$$

Now, we derive an upper bound on ω_m in terms of ω_{m-1}. For a fixed strategy $(f_1, f_2, \ldots, f_m)$ the winning probability can be written as

$$\begin{aligned}\omega_m(f_1, f_2, \ldots, f_m) &= \Pr\left[X_1X_2\ldots X_m = \sum_{k=1}^{m} f_k(X_{[m]\setminus\{k\}})\right] \\ &= \sum_{y\in\mathbb{F}_q} \Pr[X_m = y] \cdot \Pr\left[X_1X_2\ldots X_m = \sum_{k=1}^{m} f_k(X_{[m]\setminus\{k\}})\Big|X_m = y\right] \\ &= q^{-1}\sum_{y} \Pr\left[X_1X_2\ldots X_m = \sum_{k=1}^{m} f_k(X_{[m]\setminus\{k\}})\Big|X_m = y\right].\end{aligned}$$

Conditioning on a particular value of X_m leads to events that only depend on $X_1, X_2, \ldots, X_{m-1}$. In particular, setting $X_m = y$ defines the event F_y

$$F_y \iff X_1X_2\ldots X_{m-1}y = \sum_{k=1}^{m-1} f_k(X_{[m-1]\setminus\{k\}}, y) + f_m(X_{[m-1]}),$$

which satisfies

$$\Pr[F_y] = \Pr\left[X_1X_2\ldots X_m = \sum_{k=1}^{m} f_k(X_{[m]\setminus\{k\}})|X_m = y\right]. \tag{2.6}$$

We can use Lemma 2.1 to find a bound on $\omega_m(f_1, f_2, \ldots, f_m) = q^{-1}\sum_y \Pr[F_y]$ as long as we are given bounds on $\Pr[F_y \wedge F_z]$ for $y \neq z$.

PROPOSITION 2.1. *For $y \neq z$ we have $\Pr[F_y \wedge F_z] \leq \omega_{m-1}$.*

Proof. Eq. (2.6) defines F_y through a certain equation in the finite field. If the equations corresponding to F_y and F_z are satisfied simultaneously then any linear combination of these equations is also satisfied. More specifically, we define a new event

$$G_{yz} \iff X_1X_2\ldots X_{m-1}(y - z) = \sum_{k=1}^{m-1} f_k(X_{[m-1]\setminus\{k\}}, y) - f_k(X_{[m-1]\setminus\{k\}}, z) \tag{2.7}$$

and since $F_y \wedge F_z \implies G_{yz}$ we are guaranteed that $\Pr[F_y \wedge F_z] \leq \Pr[G_{yz}]$. To find an upper bound on $\Pr[G_{yz}]$ we give the players more power by allowing a more general

expression on the right-hand side. In Eq. (2.7) the k^{th} term is a particular function of $X_{[m-1]\setminus\{k\}}, y$ and z, so let us replace it by an arbitrary function of these variables

$$f_k(X_{[m-1]\setminus\{k\}}, y) - f_k(X_{[m-1]\setminus\{k\}}, z) \quad \rightarrow \quad g_k(X_{[m-1]\setminus\{k\}}, y, z).$$

Under this relaxation, we arrive at the following equality

$$X_1 X_2 \dots X_{m-1}(y - z) = \sum_{k=1}^{m-1} g_k(X_{[m-1]\setminus\{k\}}, y, z).$$

Clearly, $(y - z)$ is a constant, non-zero multiplicative factor known to each player. Dividing the equation through by $(y-z)$ leads to the same game as considered before but one player has been eliminated (there are only $m - 1$ players now). Therefore,

$$\Pr[F_y \wedge F_z] \leq \Pr[G_{yz}] \leq \omega_{m-1}.$$

□

This allows us to prove the main technical result.

PROPOSITION 2.2. *The classical value of the game defined in Section 2.3.3 satisfies the following recursive relation*

$$\omega_m \leq \frac{1 + \sqrt{1 + 4q(q-1)\omega_{m-1}}}{2q}. \tag{2.8}$$

Proof. The statement follows directly from combining Lemma 2.1 with Proposition 2.1. □

Since we know that $\omega_1 = q^{-1}$, we can obtain a bound on ω_m by recursive evaluation of Eq. (2.8). More precisely, we get $\omega_m \leq c_m$ for

$$c_m = \begin{cases} q^{-1} & \text{for} \quad m = 1, \\ \frac{1+\sqrt{1+4q(q-1)c_{m-1}}}{2q} & \text{for} \quad m \geq 2. \end{cases}$$

Note that this bound is always non trivial, i.e. $c_m < 1$ for all values of q and m. To obtain a slightly weaker but simpler form presented in Eq. (6.9) in Chapter 6 we note that $1 - 4qc_{m-1} \leq 0$ and set $q = 2^n$.

2.4 Cryptographic protocols and implementations

Cryptography is a field is driven by applications, i.e. the starting point is a particular task that two (or more) parties want to perform. Formulating a task in a rigorous,

mathematical language gives rise to a *cryptographic primitive*. In case of two-party cryptography two aspects must be specified.

- **Correctness:** The expected behaviour when executed by honest parties.
- **Security:** A list of behaviours that are forbidden *regardless* of the strategies that the dishonest parties might employ.

Defining correctness is straightforward because what we want to achieve is clear from the beginning. Finding the right definition of security, on the other hand, might be a challenging task. Converting our intuition about what the primitive should not allow for into a mathematical statement is not always straightforward and often multiple security definitions are simultaneously in use depending on the exact context. Sometimes security is perfect (cf. the hiding property of bit commitment in Definition 2.2), but more often it is quantified by a (small) number usually denoted by ε (cf. the binding property in Definition 2.3), which can be (usually) understood as an upper bound on the probability that a cheating attempt is successful.

It is worth emphasising that no meaningful statements can be made if *all involved parties* decide to cheat simply because if they collectively deviate in the "right" way they can produce any imaginable output. If all the dishonest parties form a coalition whose only goal is to enforce a certain output, nothing can stop them from achieving it. In particular, in the two-party case Alice and Bob could, instead of executing the protocol, decide to play a game of chess and then the output of the interaction would be a complete account of a chess game. Clearly, no cryptographic statements can be made about a chess game. Therefore, we only consider scenarios in which at least one party is honest and that is why in the two-party setting we prefer to talk about *security for honest Alice (Bob)* instead of *security against dishonest Bob (Alice)*.

Once the primitive has been defined we propose a protocol (i.e. a sequence of interactions between the players) that implements it. Verifying the correctness of a cryptographic protocol is simple since the honest parties behave in a well-defined manner. Showing security, on the other hand, is more complicated because we need to characterise all possible ways in which the dishonest parties might deviate from the protocol and argue that none of them violates the security requirements of the primitive. In a protocol that does not achieve perfect security, the final outcome of a security proof is an upper bound on how well the dishonest party can cheat. Since the level of security that we are happy to accept depends on the precise circumstances, protocols usually come in families parametrised by an integer $n \in \mathbb{N}$ and the security guarantee is a function of n ideally satisfying $\varepsilon(n) \to 0$ as $n \to \infty$. Increasing the value of n leads to protocols that use more resources (e.g. computation, communication or randomness) but achieve better security. Ideally, we would

like $\varepsilon(n)$ to decay exponentially but inverse polynomial decay might also be acceptable. Security analysis of such a family of protocols aims to find the tightest bound, i.e. lowest $\varepsilon(n)$, as a function of n.

Having performed the theoretical analysis of a protocol, the last step is to actually implement it. In case of mature technologies (e.g. modern digital devices) *fault-tolerance* (capability of terminating correctly even in the presence of errors) is ensured at the hardware level so there is no need to introduce any extra measures in the actual protocol. The multiround classical relativistic bit commitment protocol discussed in Chapter 6 is a prime example: the simplest theoretical protocol is already suitable for implementation and no modifications are necessary. On the other hand, in case of less developed fields like quantum technologies the situation is a bit more complicated. Since we have not yet found a way to (generically) eliminate all the errors, we must consider how they will affect our protocol. What happens when honest parties follow the protocol but their communication or storage suffers from noise? Depending on how severe the errors are, the protocol either terminates with the wrong output or it aborts. To prevent such an undesirable outcome the protocol must be modified to become fault-tolerant. The exact modifications that need to be made depend on what type of noise we want to protect ourselves against. More specifically, we need to have a model of noise that is simple enough to analyse but remains a reasonably faithful description of the experimental setup. As a consequence, turning a theoretical protocol into an experimental proposal is not so straightforward and usually requires multiple rounds of communication between the theoretician and the experimentalist. The new fault-tolerant protocol admits a couple of parameters, which determine its error tolerance, and these should be chosen to ensure that the protocol terminates successfully (with high probability) when performed by the honest parties. In this case asymptotic analysis is sufficient, since it is the actual experiment that demonstrates correctness (while calculations simply give us an indication whether the experiment is worth setting up).

Having modified our protocol we need to reassess its security and it is clear that introducing fault-tolerant features makes a protocol more vulnerable to cheating. Moreover, since the security analysis is supposed to please the most paranoid cryptographers, we must make minimal assumptions about the adversary. In particular, we do not want to impose on him any technological restrictions. Our devices are imperfect due to our lack of skills and knowledge but we do not want to assume that about the adversary. The standard approach to quantum cryptography is to assume that the devices used by the honest party are trusted (i.e. their precise description including potential imperfections is known) but the devices used by the adversary might be arbitrary (i.e. they are only limited by the laws of physics).[10]

[10] As mentioned before the trust assumption can in fact be dropped. See Section 1.3 for references.

Clearly, requiring that our protocol is correct for honest parties with imperfect devices and remains secure against an all-powerful adversary puts us in a difficult situation. As mentioned before, the fault-tolerant protocol takes a couple of parameters which we can try adjusting but we might nevertheless reach the conclusion that guaranteeing correctness and security simultaneously is not possible. This means that the quality of the devices available to the honest parties is not sufficient to allow for a secure execution of the protocol.

We can turn this statement around and ask about the minimal requirements on the honest devices. How much noise can we tolerate before the protocol becomes insecure? Note that now this is a property of the protocol alone and we should aim to design protocols with the highest possible noise tolerance. In case of quantum technologies a successful implementation of a cryptographic protocol often requires a collective effort of the experimentalist (who attempts to reduce the experimental noise to the absolute minimum) and the theoretician (who improves the theoretical security analysis). An example of such an analysis for a quantum bit commitment protocol is presented in Chapter 5.

2.5 Bit commitment

Recall Example 2 from Section 1.1, in which Alice wants to commit to a certain message without actually revealing it. Commitment schemes have multiple applications, for example they allow us to prove that we know something or that we are able to predict some future event without revealing any information in advance. They are also a useful tool to force different parties to act simultaneously, even if the communication model is inherently sequential. Consider two bidders who want to take part in an auction but there is no trusted auctioneer at hand. In the usual, sequential communication model one of them has to announce his bid first, which gives an unfair advantage to the other bidder. This can be rectified if the first bidder commits to his bid (instead of announcing it) and opens it only after the second bidder has announced his price. Hence, given access to a commitment functionality, one can perform a fair auction without a trusted third party. Moreover, commitment schemes are often used in reductions to construct other cryptographic primitives. For the purpose of this section we restrict ourselves to schemes in which the committed message is just one bit.

As explained in Section 2.4 the protocol should be correct (it should succeed if executed by honest parties) and secure (the honest party should be protected even if the other party deviates arbitrarily from the protocol).[11] To make precise math-

[11] One can also design *cheat-sensitive* protocols [ATVY00, HK04], in which one party constantly monitors the other party's action and might abort the protocol in the middle if they believe that

ematical statements, we need a formal description of the protocol in the quantum language.

2.5.1 Formal definition

The primitive of bit commitment is usually split into two phases: the commit phase and the open phase. In the commit phase Alice interacts with Bob and at the end of the commit phase she should be committed, i.e. she should no longer have the freedom to choose (or change) her commitment. Nevertheless, Bob should remain ignorant about Alice's commitment. In the open phase Alice sends to Bob the bit she has committed to, along with a proof of her commitment, which he examines to decide whether to accept the opening or not.

While this description is sufficient for most purposes, it has some undesirable features. First of all, since it does not explicitly *mention* the period in between the two phases, it might create the impression that there *is* no interval in between, i.e. it might lead to the false conclusion that the *end of the commit phase* and the *beginning of the open phase* correspond to the same point of time. This is clearly misleading as the whole point of a commitment scheme is to obtain a finite interval *between* the two, i.e. a period in which Alice is committed to a message which Bob remains ignorant about. The distinction is usually not made explicit because in most protocols nothing happens in between the two phases (Alice and Bob just savour the moment of being securely committed), which means that the two points are *operationally* equivalent (e.g. any information that Bob might extract about Alice's commitment just before the open phase he might also extract immediately after the commit phase). This is not true for protocols in which communication continues in between the two phases and there the distinction is important. Therefore, we explicitly introduce the *sustain* phase, i.e. the period during which the commitment is valid. For reasons which will become clear soon, we call the beginning of the sustain phase the *commitment point* and the end the *opening point*. We also split up what is usually called the open phase into two separate parts: in the *open* phase Alice unveils d to Bob and sends him a proof of her commitment (which we assume to be a single message[12]), while in the *verify* phase Bob decides whether to accept

the other party is cheating, but we do not consider them here. Similarly, cheat-sensitive coin flipping protocols have been proposed [SR02].

[12]The assumption that the open phase consists of a single message from Alice to Bob might seem restrictive but it does not rule out any interesting protocols. Any interaction between Alice and Bob in the open phase can be simulated locally by Bob given that Alice provides him with all the relevant information. Since there is no need to protect Alice's privacy any more, the security of the protocol is not affected. In fact, we could consider an extreme case in which Alice does not even extract a proof and instead passes all the (possibly quantum) information in her possession to Bob. Again, this would not affect security but might unnecessarily increase the size of the message. Note that while this simulation argument does not change the situation of honest Alice, it might

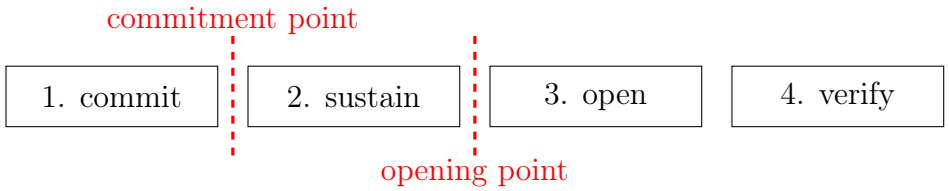

Fig. 2.2: The phase structure of a generic bit commitment protocol.

the opening or not. The phase structure is shown in Fig. 2.2.

We use A and B to denote the subsystems of Alice and Bob, respectively. We use P to denote the proof, which is generated (in the open phase) by Alice and sent to Bob. We implicitly assume that P contains the information about the value d that Alice is trying to unveil. Since the commit and sustain phases are interactive they do not admit a compact description in the quantum formalism. The open phase can be described as a quantum channel $\Phi^{\text{open}}_{A\to P}$, which acts on Alice's subsystem (A) to produce a proof (P). Bob's decision whether to accept or reject the commitment in the verify phase can be described by a binary measurement $\mathcal{M} = \{M_{\text{accept}}, M_{\text{reject}}\}$ performed jointly on subsystems B and P.

The honest scenario is relatively straightforward to analyse. The protocol specifies uniquely (for each value of Alice's commitment d) the state shared between Alice and Bob at every stage of the protocol and finding it explicitly is a matter of simple calculation.

DEFINITION 2.1. *Let ρ^d_{AB} be the state shared between Alice and Bob at the opening point, $\Phi^{\text{open}}_{A\to P}$ be the opening map and $\mathcal{M} = \{M_{\text{accept}}, M_{\text{reject}}\}$ be the final measurement. A bit commitment protocol is $(1-\delta)$-**correct** if for $d \in \{0,1\}$ we have*

$$\begin{aligned} &\operatorname{tr}(M_{\text{accept}}\rho^d_{BP}) \geq 1-\delta, \\ &\text{where} \quad \rho^d_{BP} = \Phi^{\text{open}}_{A\to P}(\rho^d_{AB}). \end{aligned}$$

In the dishonest scenario the situation becomes a bit more complicated because the state shared between Alice and Bob is no longer uniquely specified. For example, if Alice is dishonest then the state of her subsystem might be completely arbitrary. For the purpose of defining security it is convenient to talk about the *set* of states that dishonest Alice (or Bob) can *enforce* during the protocol and we will use σ_{AB} to denote such states (to distinguish them from the honest states denoted by ρ_{AB}).[13] These sets are then used to quantify security.

As discussed before, coming up with the right security definition is not trivial because it requires us to turn the intuitive notion of security into a mathematical

change (to worse) the situation of dishonest Alice but this shall not concern us.

[13]Note that for a generic, multiround protocol characterising such sets might be a difficult task. Nevertheless, these sets are always well-defined and allow us to define security in a convenient way.

statement. It is useful to realise that the dishonest scenario is operationally equivalent to a game between the honest party (acting as a referee since their behaviour is determined by the protocol) and the dishonest party (a player who is allowed to adopt an arbitrary strategy). Thus, defining security is equivalent to specifying the exact rules of such a "cheating game".

To look at a concrete example let us start with the case of honest Alice and dishonest Bob. Bob's goal is to find out the value of Alice's commitment before the open phase begins, i.e. at the opening point, and to achieve this he might deviate arbitrarily from the protocol. This admits a natural formulation as a game in which Alice (the referee) chooses $d \in \{0, 1\}$ uniformly at random and follows the honest protocol until the opening point. Then, Bob is challenged to guess d at the opening point and the probability of guessing d correctly is a natural measure of his cheating abilities. To phrase this in terms of quantum states, let σ_{AB}^d be the state at the opening point and note that a particular strategy of dishonest Bob enforces two distinct states $(\sigma_{AB}^0, \sigma_{AB}^1)$.

DEFINITION 2.2. *A bit commitment protocol is* ***hiding*** *if all pairs of states* $(\sigma_{AB}^0, \sigma_{AB}^1)$ *that Bob can enforce at the opening point satisfy*

$$\sigma_B^0 = \sigma_B^1, \tag{2.9}$$

where $\sigma_B^d = \mathrm{tr}_A\, \sigma_{AB}^d$.

This definition implies that whatever strategy Bob employs, he obtains no information about Alice's commitment.[14] Note that this property is sometimes referred to as being *perfectly hiding*, in contrast to schemes that only guarantee Alice partial security. Since all protocols considered in this thesis are perfectly hiding, we always use hiding to mean perfect security.

The case of dishonest Alice and honest Bob is a bit more complex. In order to claim that Alice's commitment begins *at* the commitment point, we must show that at that point she no longer has the freedom to unveil both values, *regardless* of the strategy adopted prior to that. In other words, the dishonest behaviour of Alice can be seen as two distinct strategies (corresponding to $d = 0$ and $d = 1$) which are identical until the commitment point and let us call such strategies *compatible*. Intuitively, this means that she can delay the choice which strategy to follow until the commitment point.

[14] Note that this implies that the equality (2.9) holds not just *at* at the opening point but at all times *until* that point. If at any point the two reduced states were not equal Bob could simply store his system until the opening time (possibly sending Alice some freshly prepared states if necessary).

DEFINITION 2.3. *Let $(\sigma^0_{AB}, \sigma^1_{AB})$ be a pair of states that Alice can enforce at the opening point using compatible strategies and let $(\Phi^{\text{cheat},0}_{A\to P}, \Phi^{\text{cheat},1}_{A\to P})$ be opening maps. Define p_d to be the probability that Alice's attempt to unveil d is accepted by Bob*

$$p_d = \operatorname{tr}\left(M_{\text{accept}}\left[\Phi^{\text{cheat},d}_{A\to P}(\sigma^d_{AB})\right]\right).$$

A bit commitment protocol is called ***ε-binding*** *if for all states $(\sigma^0_{AB}, \sigma^1_{AB})$ and for all opening maps $(\Phi^{\text{cheat},0}_{A\to P}, \Phi^{\text{cheat},1}_{A\to P})$ we have*

$$p_0 + p_1 \leq 1 + \varepsilon.$$

Note that finding the optimal opening map for a particular intermediate state σ^d_{AB} is a semidefinite program so it can be solved efficiently. Therefore, the cheating strategy is essentially specified by a pair of compatible strategies.

It is clear that the restriction that the two strategies are compatible is crucial. Clearly, Alice can enforce the honest pair of states $(\rho^0_{AB}, \rho^1_{AB})$, which leads to $p_0 = p_1 = 1$ (as long as the protocol is correct), but this cannot be achieved using compatible strategies (if it was possible, the protocol would be completely insecure).

Note that this formulation is equivalent to a game in which Alice employs some generic strategy until the commitment point and is *immediately after* challenged to open either $d = 0$ or $d = 1$ chosen uniformly at random.[15] A strategy that wins such a game with probability p_{win} is equivalent to a cheating strategy which achieves $p_0 + p_1 = 2p_{\text{win}}$. Thinking of the cheating scenario as a game often allows a more intuitive understanding of what the dishonest party is trying to achieve.

Note that it might seem natural to demand that there is *only one* value that Alice might successfully open. However, this requirement is too strong because we cannot prevent Alice from committing to a random bit which leads to $p_0 = p_1 = \frac{1}{2}$. This idea can be developed further to produce a reachable notion of security [DFSS05, WST08], which has the advantage of being *composable*, i.e. security is guaranteed even if the primitive is used as a subroutine in a longer procedure [Can01]. However, it is known that this stronger notion of security cannot be reached in the relativistic setting (see Appendix A for details). Therefore, in this thesis we only consider the weaker, non-composable Definition 2.3.

2.5.2 The Mayers-Lo-Chau impossibility result

As explained in Section 1.3, in the early 1990s a significant effort went into investigating whether various two-party tasks can be solved using quantum protocols.

[15] Note that this challenge must come from an external source like the referee. It is not convincing for Alice to unveil a bit chosen by herself.

Unfortunately, most of such tasks were ultimately shown to be impossible even in the quantum world. In this section we sketch out the impossibility proof for quantum bit commitment discovered independently by Mayers [May97] and Lo and Chau [LC97].

Before going into the details of the quantum no-go argument let us sketch out the classical one. Consider a protocol which is correct and hiding and suppose Alice follows the honest strategy for $d = 0$ until the commitment point. Since the protocol is correct Alice can proceed with the honest strategy and successfully unveil $d = 0$. What if she wants to cheat and unveil $d = 1$ instead? The protocol is hiding, which means that Bob does not know the value of her commitment. This implies that there *exists* a particular strategy for Alice after the commitment point that will make him accept $d = 1$ (otherwise he could eliminate this possibility). The existence of such a strategy implies that Alice can unveil either value (with certainty), i.e. achieve $p_0 + p_1 = 2$. This argument can be extended to show that in every classical protocol (which is correct) at least one of the parties can cheat with certainty. Such arguments are formalised using the notion of a transcript, which is simply the complete list of messages exchanged by Alice and Bob. It is clear that in the classical world each party can produce a transcript by copying all the messages to a private, auxiliary register. In the quantum world one cannot simply copy messages so it is not meaningful to talk about the transcript of a quantum protocol. That is why this simple classical argument does not apply to quantum protocols.

The quantum impossibility argument hinges on the fact that, without loss of generality, we can assume that Alice and Bob keep the entire quantum state pure until the commitment point. Since Alice and Bob share no correlations (these would count as a resource) and private randomness can be purified locally, we can assume that Alice and Bob start in a pure, product state. Then, all the measurements can be performed coherently (also known as *keeping the measurements quantum*, see Section 1.3 of Ref. [Col06] for an explanation). This requires us to replace all the classical channels in the protocol by quantum channels. Since this might open up new, inherently quantum cheating strategies we must instruct each party to measure (coherently) each incoming message. This gives rise to a new (but equivalent from the security point of view) protocol, in which all the interactions happen at the quantum level and at the commitment point Alice and Bob share a pure state, which we denote by $|\psi^d\rangle_{AB}$.[16] According to Definition 2.2 the protocol is hiding if $\rho_B^0 = \rho_B^1$. Unfortunately, due to Uhlmann's theorem [Uhl76] this implies that there

[16] This is one way of dealing with classical communication known as the *indirect approach*. For more details on the indirect approach and also the alternative *direct approach* see Ref. [BCMS97].

exists a unitary U_A acting on subsystem A alone such that

$$(U_A \otimes \mathbb{1}_B)|\psi^0\rangle_{AB} = |\psi^1\rangle_{AB}.$$

In other words, Alice can switch between the two honest states by acting on her system alone, which allows her to unveil either bit (with certainty) and, therefore, renders the protocol completely insecure. Formally the impossibility can be stated in the following manner.

THEOREM 2.1. *Any protocol which is perfectly correct and hiding allows Alice to cheat perfectly. In other words, there exists a cheating strategy for Alice which achieves* $p_0 = p_1 = 1$.

This simple argument applies only to the exact case where $\rho_B^0 = \rho_B^1$ but it is easy to show that if ρ_B^0 is close to ρ_B^1 (i.e. Bob finds it difficult to distinguish them) then Alice can cheat with high probability and trade-offs based on this idea were derived by Spekkens and Rudolph [SR01]. Optimal bounds on quantum bit commitment have been found by Chailloux and Kerenidis [CK11].

While quantum mechanics does not allow for perfect bit commitment, it still beats classical protocols. As mentioned before every classical protocol is completely insecure against one of the parties. Quantum protocols, on the other hand, allow us to achieve some intermediate points, in which security is in some sense "distributed" between Alice and Bob. □

Chapter 3

Non-communicating models

This chapter (excluding Section 3.1) is based on

- **Secure bit commitment from relativistic constraints** [arXiv:1206.1740]
  J. Kaniewski, M. Tomamichel, E. Hänggi and S. Wehner
  IEEE Transactions on Information Theory **59**, 7 (2013).
  (presented at *QCrypt '12*)

It is well-known that interrogating suspects is more fruitful if they cannot communicate during the process, simply because coming up with two reasonable stories is more difficult than with one.[1] This intuition was first made rigorous in the context of complexity theory but similar features can be seen in cryptography, in which non-communicating models allow us to implement primitives which would be otherwise forbidden. Care has to be taken, however, since the primitive implemented in the non-communicating model is usually subtly different (weaker) than the original one and, hence, might not be suitable for all applications.

Non-communicating models can be formalised using the concept of *agents*. For example, if in the standard protocol Alice interacts with Bob, in the multiagent variant she might be required to interact with two distinct agents of Bob. In this case we think of Bob as being the main party, who decides on the strategy and briefs all his agents beforehand but steps back as soon as the protocol begins. During the protocol the agents follow the instructions but are not allowed to communicate with each other (or the main party). In this chapter we adopt the convention that if Alice (Bob) only needs to delegate one agent we do not make an explicit distinction between the main party and the agent. If more agents are involved we make a distinction by calling the agents Alice_1 and Alice_2 (Bob_1 and Bob_2).

While it is entirely possible to discuss multiagent commitment schemes without any reference to complexity theory, we feel it is beneficial to explain where

[1] This only holds if the interrogation is an interactive and unpredictable process. If the suspects can predict all the possible questions in advance, nothing prohibits them from producing consistent answers.

the idea of employing multiple agents originally came from. We explain how such models arose in the context of *interactive proofs* [Bab85, GMR85, BGKW88] and we discuss connections between *zero-knowledge proofs* and cryptography [GMW86, BGKW88, Gol08]. We also consider a multiagent variant of oblivious transfer and present a (trivial) protocol that implements it. This serves as a useful example to demonstrate that the functionality implemented in the multiagent scenario might differ significantly from the original primitive.

When it comes to analysing multiagent commitment schemes one of the major conceptual challenges is to establish a framework which encompasses all interesting schemes without being overly complicated. While for a particular scheme it is fairly straightforward to come up with an ad hoc treatment and security definition (which is often left implicit), a general framework is necessary for comparing various schemes. We propose such a framework based largely on results published in Ref. [KTHW13].

Outline: We start by explaining the concept of an interactive proof system and why employing multiple agents makes the model significantly more powerful. Then we discuss how such models can be used in the context of cryptography using *distributed oblivious transfer* [NP00] as an example. The last section of the chapter is dedicated to multiagent commitment schemes. We explain what kind of arrangements of agents are useful for the purpose of commitment schemes and propose how to quantify security in these new, multiagent models.

3.1 Interactive proof systems

The purpose of this section is to give a brief, non-technical introduction to the field of interactive proof systems. We are particularly interested in multiprover models[2], zero-knowledge proofs and their relation to cryptography. The notes of Oded Goldreich [Gol08] provide a thorough and accessible introduction to interactive proof systems. Readers interested in the early history of interactive proofs are referred to a wonderfully entertaining essay by László Babai [Bab90].

Let us start with a motivating story. Suppose that Bob wants to be convinced that a certain statement is true. His own computational powers are limited (so he cannot simply verify the statement on his own) but he has access to an all-powerful computer called Alice. Unfortunately, Alice is a malicious machine and she will always assert that the statement is true (even if it is actually false). To make things worse she will even provide an incorrect proof, hoping that Bob will fall for it. Bob wants to interact with Alice in such a way that if she is honest and the proof is correct

[2] In the context of complexity theory, it is always the prover (one of the involved parties) who is required to delegate multiple agents.

he accepts it, but if she misbehaves and outputs an incorrect proof her misconduct should be noticed. On a more fundamental level, we are asking whether it is possible to verify computations that are, by assumption, beyond our own capabilities.

Since we always assume that Alice knows the statement that Bob wants to be convinced of, she might simply produce a proof and send it to Bob. This coincides with the way we usually think of proofs as static, non-interactive objects, e.g. something that can be published in a book. This is a valid solution but we know from everyday experience that the process of learning and understanding is often facilitated by the possibility of asking questions and receiving answers. The same phenomenon occurs in case of proofs and gives rise to the concept of an *interactive proof*, which cannot be published in a book but can be explained in class. It turns out that allowing Alice and Bob to interact might significantly simplify certain proofs. Moreover, as counter-intuitive as it sounds it allows Alice to prove a statement without revealing anything about the actual proof. In complexity theory the setting described above is known as an *interactive proof system*, with Alice being the *prover* and Bob the *verifier*, and was introduced independently by Babai [Bab85] and Goldwasser, Micali and Rackoff [GMR85].

To demonstrate the advantage of interactive proofs we need some concrete statements, which we will then construct (interactive) proofs for. It turns out that graph theory is a good source of intuitive and interesting examples. Given two graphs G_0 and G_1 we say that they are *isomorphic* if we can map G_0 onto G_1 by simply relabelling the vertices. The problem of deciding whether two graphs are isomorphic is known as the *graph isomorphism problem* and we do not know how to solve it efficiently.[3]

This is exactly the setting we want to look at: Bob has two graphs G_0 and G_1 and he wants to know whether they are isomorphic. Since he is unable to solve this problem on his own, he asks Alice for help. If the graphs are isomorphic Alice simply sends Bob a valid relabelling (of vertices) and he verifies that it indeed maps G_0 onto G_1. This is an efficient, non-interactive proof. The problem becomes a bit more complex if the graphs are *not* isomorphic. Alice could, of course, write down all possible relabellings and show that none of them achieves the goal but this does not really save Bob any computational effort. Verifying such a brute-force "proof" is not any easier than producing it. As of today, we do not know how to (generically) construct a non-interactive, efficient proof that two graphs are not isomorphic.

On the other hand, a beautifully simple solution exists if Alice and Bob are

[3]In fact, it is one of the few interesting problems that seem to sit in the middle between the "easy problems" (i.e. the ones that can be solved efficiently) and the really hard ones (i.e. the ones that we do not think can be solved efficiently, like the travelling salesman problem). Interested readers are encouraged to read a survey by Scott Aaronson on the distinction between the easy and the hard problems and how they relate to physical reality [Aar05].

allowed to interact [GMW86]. Bob picks a random bit $b \in \{0, 1\}$, applies a random relabelling to G_b and sends it to Alice, whose task is to guess b. If the graphs are not isomorphic then Alice can always correctly identify the original graph (she is all-powerful so she can simply try all possible relabellings) and successfully answer Bob's challenge. On the other hand, if the graphs are isomorphic then by applying a random relabelling Bob made the message that Alice receives independent of b.[4] Hence, her probability of guessing b correctly is exactly $\frac{1}{2}$. If we repeat this game multiple times the probability of correctly answering all the challenges decays exponentially. If Alice can reliably tell the two graphs apart, then Bob should be convinced that the two graphs are not isomorphic (except for exponentially small probability).

The connection between interactive proofs and cryptography appears when we impose an additional requirement that the proof should carry no information beyond *the validity of the statement*. This concept introduced by Goldwasser, Micali and Wigderson goes under the name of a *zero-knowledge proof* [GMW86]. Note that this formulation sounds suspiciously similar to our initial motivation for commitment schemes in Section 1.1, in which Alice wants to prove to Bob that she knows something without revealing any additional information.

Let us go back to the problem of proving that two graphs are isomorphic. The obvious solution presented before is to provide a valid relabelling explicitly. Unfortunately, this reveals much more information than necessary: we want to prove the *existence* of a relabelling rather to exhibit a particular one. Can we prove that two graphs are isomorphic in a zero-knowledge manner? Clearly, this cannot be done using a static proof but adding interactions helps as demonstrated below.[5]

Again, we assume that Alice knows both graphs G_0 and G_1. She applies a random relabelling to G_0 and sends it to Bob as H. Bob chooses a random bit b and challenges Alice to reveal the relabelling that maps H onto G_b. Clearly, if G_0 and G_1 are isomorphic Alice can always produce a valid answer. However, if they are not, she can find a valid answer to at most one of the two challenges (regardless of how she chose H). Again, by repeating this test a number of times Bob can be convinced that the two graphs are indeed isomorphic. Why is this proof zero-knowledge? This is clear if Bob acts honestly (i.e. he chooses the bit b at random), because then at the end of the protocol we can see H as a random relabelling of G_b. This is something that Bob could have generated himself, hence, he has obtained no extra knowledge. The situation becomes more complex if we consider malicious Bob who might choose b based on the graph H he receives. A rigorous proof that this protocol remains

[4] More precisely, the probability distributions over graphs sent to Alice are identical for $b = 0$ and $b = 1$.

[5] Requiring a static proof to be zero-knowledge reduces it to a trivial assertion "this statement is true", which the verifier will not find too convincing.

zero-knowledge in this adversarial scenario is significantly more involved [GMW86].

Once we know how to prove that two graphs are isomorphic in a zero-knowledge manner it is natural to ask what other statements can be proven in such a way. If we are happy to accept an extra computational assumption then it turns out that any statement that can be proven using a static proof can also be proven in a zero-knowledge fashion [GMW86]. Ben-Or, Goldwasser, Kilian and Wigderson realised that the computational assumption can be dropped by introducing an extra prover (who is not allowed to communicate with the first one during the protocol) and, in fact, their solution is quite simple [BGKW88]. Before the protocol begins the provers generate a long, random string. During the protocol all the work is done by Prover_1, while Prover_2 simply outputs segments of the shared randomness (randomly chosen by the verifier). Essentially, the goal is to convince the verifier that Prover_1 is using genuine, pre-existing randomness rather than generating (faking?) it on the spot. As a crucial step in the proof they propose a bit commitment scheme in the two-prover model and prove its security. They also present a construction for a particular flavour of distributed oblivious transfer.

The observation that computational security in Ref. [GMW86] is used to provide commitment-like functionality is made explicit in Construction 2.4 from Goldreich's lecture notes [Gol08], in which a generic zero-knowledge proof is constructed under the assumption that commitment functionality is available for free. This shows that the primitive of bit commitment establishes a connection between zero-knowledge proofs and multiprover models.

Multiprover models were introduced to remove computational assumptions in the context of zero-knowledge proofs but have since become an independent object of study in complexity theory. In fact, they have been shown to be significantly more powerful than the single-prover class [FRS94, BFL91]. The quantum versions of these complexity classes have been proposed by allowing the provers to share entanglement either with [KM02] or without [CHTW04] quantum communication (with the verifier). The two classes have recently been shown to be equal [RUV13].

3.2 Applications in cryptography

We have seen that introducing multiple provers is useful in the context of interactive proofs and now we would like to see what can be gained in cryptography. Here, we consider a simple example and our main goal is to convince the reader that such models are not subject to the usual impossibility arguments and explain why that is the case.

Let us go back to the primitive of oblivious transfer explained by the example of an online movie service in Section 1.1. Alice has paid for one movie and wants

to download it without revealing her choice to the company (Bob). In spirit of the previous section we consider a multiagent model in which Bob is required to delegate two agents, who interact with Alice but cannot communicate with each other. In the original primitive Bob should never find out which movie Alice chose to download. However, in the multiprover setting an interesting question arises: what happens to the agents after the protocol ends? Since it is hard to envision keeping them isolated until the end of time, we may first lean towards a model in which they are allowed to communicate after the protocol is finished. However, as pointed out in Appendix A.2 of Ref. [BGKW88] in that case secure oblivious transfer is not possible. Temporary communication constraints are not sufficient as the standard no-go argument applies whenever the agents meet: if their combined knowledge does not allow them to deduce which message was retrieved, both messages must have leaked out to Alice.[6]

This encourages us to investigate the other extreme case in which the provers are not allowed to ever communicate again.[7] Such a primitive is known as *distributed oblivious transfer* [NP00] (or *symmetrically-private information retrieval* if we focus on the limit of a large number of messages [GIKM00, Mal00, Gas04, KdW04]) and it admits the following simple solution based on secret sharing[8]. For simplicity let us consider the case of Bob having only two messages $m_0, m_1 \in \{0,1\}^n$.

Protocol 1: `Distributed oblivious transfer`

1. (prepare) Bob generates an n-bit string $r \in \{0,1\}^n$ uniformly at random and sends $(u_0, u_1) = (m_0 \oplus r, m_1 \oplus r)$ to Bob_1 and $(v_0, v_1) = (r, m_0 \oplus m_1 \oplus r)$ to Bob_2.

2. (execute) Alice chooses a random bit $c \in \{0,1\}$ and requests u_c from Bob_1.

[6] It is possible to retain some security if we assume that the amount of communication between the provers is bounded [BGKW88].

[7] Note, however, a certain conceptual weakness of this model. The only manner in which Alice can ensure that the two agents never communicate again is to keep at least one of them isolated forever. But in that case it should not matter if that particular agent finds out which movie she wants to watch, hence, no cryptography is necessary. Note that keeping an agent isolated forever sounds morally wrong if we think of him as a human being but becomes more socially acceptable if we replace him by a disposable electronic device. Unfortunately, while in case of a human agent the assumption that he will only allow Alice to retrieve one movie is natural (an agent is capable of protecting the integrity of his laboratory), in case of an inanimate device this becomes essentially a technological assumption. Such devices have been proposed under the name of *one-time memories* [GKR08].

[8] We only use the simplest type of secret sharing in which an unknown string x is split up into two shares: $s_1 = x \oplus r$ and $s_2 = r$, where r is a string chosen uniformly at random. The two shares together allow us to reconstruct the string but it is easy to verify that having just one share conveys no information about x.

To retrieve m_d she requests $v_{d\oplus c}$ from Bob_2 and computes the message as $m_d = u_c \oplus v_{d\oplus c}$.

This protocol is secure because both Bob_1 and Bob_2 see Alice asking for a random message so neither of them obtains any knowledge about her choice. Moreover, it is easy to verify that no information is leaked about the message that Alice did not choose. Hence, this constitutes a secure multiagent implementation of oblivious transfer. However, as discussed in Section 4.1 we do not know how to usefully implement this protocol in a relativistic setting.

Why does such a protocol evade the standard no-go result[9]? It is important to realise that the no-go implicitly assumes that the whole world is split between Alice and Bob and there are no third parties: Alice can only be sure about the systems in her possession and everything else is fully controlled by Bob (this is equivalent to the assumption that the state shared between Alice and Bob is pure). In the multiagent model this must be modified as the state is now shared between Alice, Bob_1 and Bob_2. Since Bob_1 and Bob_2 cannot communicate (their knowledge cannot be combined), the usual impossibility argument does not apply.

3.3 Commitment schemes

The original zero-knowledge interactive proof proposed by Ben-Or et al. relies on a multiagent bit commitment scheme [BGKW88]. The proposed scheme is correct, hiding and ε-binding for $\varepsilon = \frac{1}{2}$. On the other hand, in Section 2.5.2 we have argued that in the standard two-party model such schemes cannot exist.

Again, we must realise that the standard notion of a commitment scheme implicitly assumes that the protocol is executed by two parties only (no additional agents) and the impossibility result only holds for that case. Multiagent schemes require new security definitions and in general the usual limitations (proven in the standard two-party model) will not apply. While it is usually clear how security definitions should be extended to multiagent protocols, it is important to do it explicitly, as it helps to understand the exact nature of the primitives under consideration.

Requiring a party to delegate agents who are not allowed to communicate (which we also refer to as *splitting*) restricts the range of actions available to that party. Clearly, this might only be useful for security purposes if communication constraints

[9]The intuition behind the standard no-go argument in the classical case is as follows. If at the end of the protocol Bob cannot tell which message Alice has decided to retrieve it must mean that through the interaction he has leaked both of them. In a world split only between Alice and Bob whatever Bob leaks becomes immediately available to Alice, which implies that she must have learnt both messages.

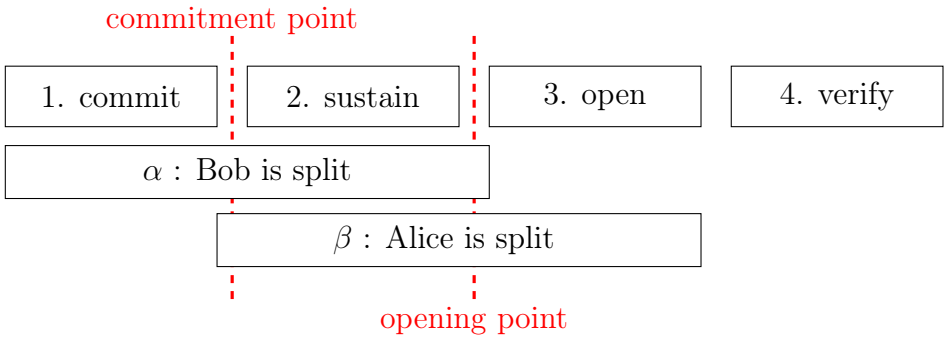

Fig. 3.1: The two types of minimal splits that are potentially useful for the purpose of commitment schemes.

apply during the relevant party's "turn to cheat". According to the phase structure discussed in Section 2.5, this leads to either splitting Bob *until the opening point* (which we call α-split) or splitting Alice *from the commitment point* (β-split).[10] The two different splits are shown in Fig. 3.1. Since we are interested in the fundamental possibilities and limitations, we will discuss protocols for both splits (and we will find that the resulting bit commitment primitives exhibit subtle differences).

Before proposing particular protocols, let us first adapt the security definitions to such multiagent scenarios. Since security requirements state what the dishonest party should not be able to achieve, it is clear that we need a new definition of the hiding property in the α-split and a new definition of the binding property in the β-split.

A commitment scheme is hiding if at the opening point Bob remains ignorant about Alice's commitment. In the α-split model at the opening point there are two agents Bob_1 and Bob_2, who are not allowed to communicate. Similarly to the case of distributed oblivious transfer if we require that even their *combined* knowledge does not allow them to learn the commitment, then the standard no-go applies (i.e. Alice can cheat with certainty). However, we can instead require that *neither* Bob_1 *nor* Bob_2 can guess the commitment, which leads to a natural condition closely resembling Definition 2.2.

DEFINITION 3.1. *A multiagent bit commitment protocol is* ***hiding*** *if all pairs of states* $(\sigma^0_{AB_1B_2}, \sigma^1_{AB_1B_2})$ *that* Bob_1 *and* Bob_2 *can enforce at the opening point satisfy*

$$\sigma^0_{B_1} = \sigma^1_{B_1} \quad \text{and} \quad \sigma^0_{B_2} = \sigma^1_{B_2},$$

where $\sigma^d_{B_c} = \text{tr}_{AB_{1-c}}\, \sigma^d_{AB_1B_2}$.

This definition means that neither of the agents has learnt anything about Alice's

[10] Note that these are the *minimal* splits, i.e. they are necessary to evade the impossibility result. Later we will consider models which impose more than the minimal splits.

commitment but it says nothing about their combined knowledge. This naturally leads to the following protocol based on secret sharing. For bit commitment protocols we adopt the convention that a (b) denotes to the private randomness of Alice (Bob) while x (y) are the messages sent during the protocol by Alice (Bob). Note that the labels x and y are used regardless of whether the parties are honest or not.

Protocol 2: `Bit commitment from secret sharing`

1. (commit) Alice generates a random bit $a \in \{0, 1\}$, sends $x_1 = d \oplus a$ to Bob_1 and $x_2 = a$ to Bob_2.
2. (open and verify) Bob_1 and Bob_2 get together and compute the commitment as $d = x_1 \oplus x_2$.

This protocol is so simple that neither party can even attempt to cheat! In the commit phase whatever combination of messages Alice decides to produce, it will correspond to an honest commitment, which she has no influence over once the messages are received by Bob_1 and Bob_2 (i.e. this is exactly the commitment point of the protocol). On the other hand, if Alice is honest then both Bob_1 and Bob_2 receive a uniform bit (regardless of the value of d) so the protocol is hiding according to Definition 3.1.

A potential drawback of this protocol is that in certain scenarios, we might want to give Alice the right to *refuse* opening a commitment. Clearly, in this protocol this could only be done if Bob_1 and Bob_2 were never allowed to communicate again, which is a problematic assumption (cf. footnote 7 in Section 3.2).

It turns out that this feature (of allowing Alice to keep the commitment value hidden forever) is much easier to achieve in the β-split model. As explained in Section 2.5.1 security for honest Bob can be quantified through a game in which Alice performs some generic strategy until the commitment point and is then challenged (by an external referee) to open either $d = 0$ or $d = 1$ with equal probabilities. The commitment is considered secure if she is not able to win this game with probability significantly exceeding $\frac{1}{2}$ (an honest commitment achieves at least $\frac{1}{2}$ as long as the scheme is correct). In case of Alice_1 and Alice_2 performing the open phase in a non-communicating fashion, we need to specify who actually receives the challenge. Is it both Alice_1 and Alice_2 or just, say, Alice_1? The former scenario might arise if Alice_1 and Alice_2 despite not being able to communicate with each other might still receive messages from an external source (it might be easier to isolate the agents

from each other than from the external world). For example, what they attempt to unveil might depend on the latest stock market news. It turns out that this distinction is important and gives rise to two different models, which we call *global* and *local command*, respectively. This choice does not affect Alice_1: in both cases her cheating behaviour is determined by two compatible strategies[11], just like in the standard single-agent model. However, the allowed behaviour of Alice_2 is affected. In the global command model she chooses two compatible strategies but in the local command she may only choose one (since she never actually finds out what they are trying to unveil).

DEFINITION 3.2. *Let $(\sigma^0_{AB}, \sigma^1_{AB})$ be a pair of states that Alice_1 and Alice_2 can enforce at the opening point given that Alice_1 employs two compatible strategies and Alice_2 employs*

- ***local command:*** *only one strategy (regardless of the value of d).*
- ***global command:*** *two compatible strategies.*

Let $(\Phi^{\text{cheat},0}_{A\to P}, \Phi^{\text{cheat},1}_{A\to P})$ be opening maps of the form

- ***local command:*** $\Phi^{\text{cheat},d}_{A\to P} = \Phi^{\text{cheat},d}_{A_1\to P_1} \otimes \Phi^{\text{cheat}}_{A_2\to P_2}$.
- ***global command:*** $\Phi^{\text{cheat},d}_{A\to P} = \Phi^{\text{cheat},d}_{A_1\to P_1} \otimes \Phi^{\text{cheat},d}_{A_2\to P_2}$.

Define p_d to be the probability that Alice's attempt to unveil d is accepted by Bob

$$p_d = \operatorname{tr}\left(M_{\text{accept}}\left[\Phi^{\text{cheat},d}_{A\to P}(\sigma^d_{AB})\right]\right).$$

*A multiagent bit commitment protocol is called ε-**binding** in the **local/global command** model if for all states $(\sigma^0_{AB}, \sigma^1_{AB})$ and for all opening maps $(\Phi^{\text{cheat},0}_{A\to P}, \Phi^{\text{cheat},1}_{A\to P})$ allowed by the model we have*

$$p_0 + p_1 \leq 1 + \varepsilon.$$

To see that the distinction between the two models is important, note that the local command model allows for the following trivial bit commitment protocol.

Protocol 3: `Bit commitment in the local command model`

1. (commit) Alice sends d to Alice_1 and Alice_2.

[11] See Section 2.5.1 for an explanation what it means for two strategies to be compatible.

2. (open) Alice_1 sends $x_1 = d$ and Alice_2 sends $x_2 = d$ to Bob.

3. (verify) Bob verifies that $x_1 = x_2$.

In the local command model dishonest Alice_1 receives the challenge and knows what they are trying to unveil but Alice_2 does not. Since the value they are challenged to unveil is chosen uniformly at random, she cannot guess it too well. In fact, the best she can do is to always output the same value, which essentially corresponds to an honest commitment. Here, security is a direct consequence of the fact that Alice_2 does not know what she is supposed to be unveiling. It is clear that in this protocol Alice is committed as soon as communication between Alice_1 and Alice_2 is forbidden. Protocol 3 is secure in the local command model but it is easy to see that it is completely insecure in the more stringent global command model. Does there exist a protocol that remains secure in the global command model?

It turns out that no classical protocol in the β-split model can meet this requirement and the argument is similar to the standard no-go for bit commitment. Let us assume that the protocol is correct and hiding, i.e. it allows Alice_1 and Alice_2 to make an honest commitment, which until the opening point leaks no information to Bob and the opening is always accepted. Suppose Alice_1 and Alice_2 honestly commit to $d = 0$. Clearly, unveiling $d = 0$ in the open phase is easy but since Bob cannot rule out Alice's commitment to $d = 1$, there must also exist a sequence of messages from Alice_1 and Alice_2 which will make him accept $d = 1$. Since now both of them know what they are trying to unveil, this strategy can be implemented and the protocol is completely insecure.

The intuitive argument presented above makes a subtle assumption that all information that Alice and Bob exchange in the commit phase is available to *both* Alice_1 and Alice_2 in the open phase. There are two ways of invalidating this assumption.

1. Make the information that Bob shares with Alice in the commit phase quantum. Then, by the no-cloning theorem [WŻ82] it will not (in general) be possible for both Alice_1 and Alice_2 to have an exact copy.

2. Strengthen the communication constraint, i.e. require that only Alice_1 takes part in the commit phase while Alice_2 is already isolated.

The first solution was explored under the name of *quantum relativistic bit commitment* by Kent [Ken11, Ken12b] and a rigorous security analysis of the latter protocol (including experimental imperfections like noise and losses) can be found in Chapter 5 of this thesis. Moreover, two new protocols based on different features of quantum theory were recently proposed [AK15a, AK15b]. The second solution

corresponds to the original proposal of Ben-Or et al. [BGKW88], further developed in Refs. [Sim07, CSST11]. Since the protocol is simple and intuitive we present it here but we defer rigorous security analysis until Chapter 6.

The bit commitment scheme proposed in Ref. [BGKW88] is sufficient from the complexity point of view but it is not the most convenient formulation for cryptographic purposes. As described in Section 2.4 in cryptography it is convenient to have a family of protocols with a parameter $n \in \mathbb{N}$ which can be chosen to guarantee the desired level of security. Such a protocol was presented under the name `simplified-BGKW` (`sBGKW`) in Refs. [Sim07, CSST11]. In this case Alice_1 and Alice_2 are not allowed to communicate throughout the entire protocol. Let a and b be n-bit strings chosen uniformly at random by Alice and Bob, respectively.

Protocol 4: `Simplified-BGKW`

1. (commit) Bob sends $y_1 = b$ to Alice_1 and she replies with $x_1 = d \cdot y_1 \oplus a$.
2. (open) Alice_2 reveals $x_2 = a$ to Bob.
3. (verify) Bob verifies that $x_1 \oplus x_2 = d \cdot b$.

(The bit-by-string multiplication was defined in Section 2.1.1.) In a protocol which requires Alice_1 and Alice_2 to be already isolated in the commit phase, it becomes important whether the value of the commitment must be known to both or just one of them. In this particular case Alice_1 can single-handedly decide on the value of the commitment.[12] Correctness of the protocol is easy to verify while the hiding property is a simple consequence of the fact that the message that Alice_1 sends to Bob in the commit phase is "one-time padded" with a uniformly random string. On the other hand, we intuitively see that the binding property is a direct consequence of the communication constraint between Alice_1 and Alice_2 (cheating would be easy if Alice_2 knew b). Moreover, note that in this protocol Alice_2 can simply refuse to take part in the open phase and then the commitment made by Alice_1 (if she indeed followed the protocol in the commit phase) will remain secret forever. In this aspect, this protocol differs significantly from Protocol 2. This difference will have quite interesting consequences when we consider relativistic variants of these protocols in Section 4.1.

[12] It is interesting to note that Alice_2 (the only agent of Alice who takes part in the open phase) does not need to know the value she is unveiling.

Chapter 4

Relativistic protocols

This chapter is based on

- **Secure bit commitment from relativistic constraints** [arXiv:1206.1740]
  J. Kaniewski, M. Tomamichel, E. Hänggi and S. Wehner
  IEEE Transactions on Information Theory **59**, 7 (2013).
  (presented at *QCrypt '12*)

In Chapter 3 we saw that communication constraints are useful in a variety of situations. In particular, they enable us to implement cryptographic primitives which are not possible otherwise. Non-communicating models are widely studied in computer science but unless one can justify such communication constraints, they should be treated on equal footing with other technological limitations and we already know that assumptions concerning computational power or storage capabilities make two-party cryptography possible.

How could Alice possibly ensure that Bob_1 and Bob_2 cannot communicate? Well, in principle she could lock each of them up in separate rooms. First of all, Bob_1 and Bob_2 might not be happy with such a solution but even if they are, how does she ensure that the rooms are perfectly shielded from the outside world? Does this not lead to yet another technological assumption?

One way out of the vicious circle of technological assumptions is relativity. Imposing an upper bound on the speed at which information spreads implies that communication between any two distinct locations incurs some minimal delay (proportional to the distance between them). This gives rise to temporary communication constraints, which rely solely on the correctness of the theory of relativity. It is worth pointing out that this is the *only* feature of relativity used in relativistic cryptography.

It is important to stress the difference between non-communicating and relativistic protocols. In a non-communicating protocol (like the ones discussed in Chapter 3) we first explicitly specify communication constraints and then the interactions

between the agents. On the other hand, in a relativistic protocol one cannot simply impose such arbitrary communication constraints. Instead, they must *arise* from the arrangement of agents in space and appropriately chosen timing of the protocol. Therefore, the description of the protocol must specify where and when each interaction takes place and then the resulting communication constraints may be used to prove security. Note that not every combination of communication constraints might be achieved in this model, e.g. if Alice simultaneously communicates with Bob_1 and Bob_2, they must be able to communicate too.

To the best of our knowledge, the idea of combining relativity and quantum mechanics for cryptographic purposes first appeared in writing in a summary article by Gilles Brassard and Claude Crépeau [BC96, Cré96], who attributed it to Louis Salvail. The foundations were laid by Adrian Kent (first relativistic commitment schemes [Ken99, Ken05]) and Roger Colbeck (proposals for various flavours of cointossing and impossibility results for secure two-party computation [Col06, CK06, Col07]). More recently, significant interest was sparked by position-verification schemes [KMS11, BCF+11, TFKW13, Unr14, RG15]. A relativistic quantum key distribution scheme has also been proposed [RKKM14].

The defining feature of relativistic cryptography is the requirement that different phases of the protocol take place at distinct locations. With the appropriate choice of timing this imposes communication constraints, which are no longer due to technological limitations but result directly from the physical theory (security of such schemes is often advertised to be "guaranteed by the laws of physics"). Unfortunately, this desirable feature comes at a price. Communication constraints guaranteed by relativity are *temporary*, which means that we must leave the neat and tidy world of non-communicating models, in which we are free to impose arbitrary communication constraints, and enter the complex world of relativistic models, in which communication is only *delayed* rather than *forbidden*.[1] The analysis of such scenarios becomes significantly more involved if the agents are required to handle quantum information (or when dishonest parties use quantum devices to cheat in a classical protocol). In fact, this has led to interesting and fundamental questions about how to *define* the location of a quantum system. Consider the process of teleportation [BBC+93], in which a quantum state ρ located initially at one place is reconstructed at another place by using entanglement (pre-shared between the two locations) and sending classical data. Interestingly enough, during this procedure there is a period of time when the state seemingly "ceases to exist", in the sense that there is *no loca-*

[1] It is useful to contrast this aspect of relativistic models with the non-communicating case. In the non-communicating world we can choose whether or not the agents are allowed to communicate once the protocol is finished and both options are equally valid. In the relativistic setting there is only one natural solution, which lies somewhere in between the two extremes: the agents can communicate but their communication is not instantaneous.

tion at which any information about ρ can be *immediately* extracted. Where is the state then? This counter-intuitive phenomenon is captured operationally through the task of *summoning* recently investigated by Kent [Ken13, Ken12a], Hayden and May [HM12].

Outline: In this chapter we first show how some of the protocols discussed in Chapter 3 can be implemented in the relativistic setting and what limitations such a "translation" brings about. We then present an explicit procedure for mapping a relativistic protocol onto a communication-constrained model. We show that in the fully classical setting communication-constrained models can be further mapped onto non-communicating models and we discuss why such a simplifying reduction cannot be done when quantum information is involved. Finally, we discuss the power and limitations of relativistic cryptography.

4.1 Non-communicating schemes in the relativistic setting

We start by considering how some of the non-communicating schemes discussed in Chapter 3 can be implemented in the relativistic setting. Since the communication constraints imposed by relativity are temporary, the resulting commitment schemes cannot guarantee everlasting security.[2] Understanding exactly the "mode of failure", i.e. how different commitment schemes "expire", provides valuable insight into the power of relativistic cryptography.

The only realistic implementation of a relativistic protocol involves stationary agents exchanging information at the speed of light. The protocol specifies a set of locations and each party is required to delegate a (stationary) agent to each location. All communication between Alice and Bob occurs locally, i.e. between agents occupying the same location, and for simplicity we assume that all local communication is instantaneous.[3] Communication between distinct agents of the same party is unrestricted (and assumed to be secure) but must respect the speed-of-light constraint (for simplicity we take $c = 1$).[4]

[2] Unless the parties keep communicating, see Section 4.3 for more details.

[3] Note that this is the only reasonable model. If an agent of Alice were to send a message to a far-away agent of Bob, she would either have to "escort" the message until it reaches the agent of Bob (which is equivalent to placing an extra agent at the receiving end as in our model) or she would let the message out unguarded, in which case there is no guarantee that the message will not be intercepted by some other agent of Bob at some earlier location.

[4] Security of internal communication can be ensured by using teleportation to transmit quantum states and information-theoretic encryption (one-time pad) for classical information. Alternatively, we can assume that distinct agents occupy different locations within the same laboratory (e.g. the model of two long laboratories in a single spatial dimension as in Section 1.7.2 and Fig. 1.6 of Ref. [Col06]).

All examples considered in this thesis take place in a single spatial dimension labelled by x and as usual time is labelled by t. All considerations in this chapter extend in a straightforward fashion to more spatial dimensions but we are not aware of any examples in which this gives any advantage. We label the locations by integers and refer to the agents occupying Location k as Alice_k and Bob_k. For convenience we define the following three locations.

Location 0	$x = 0$
Location 1	$x = -1$
Location 2	$x = 1$

It is important to bear in mind that in relativistic protocols all the interactions are performed by agents occupying well-defined locations. We avoid referring to the main party (whose location during the protocol is not specified) as it might create the impression that there exists some higher form of life that is able to instantaneously communicate with all its agents. The existence of such a being is forbidden by relativity and would indeed render all the relativistic protocols insecure.

Let us first present a relativistic variant of Protocol 2. Before the protocol begins Alice_1 and Alice_2 must be provided with a random bit $a \in \{0, 1\}$ (e.g. generated by Alice_0 at $t = -1$).

Protocol 5: `Bit commitment from secret sharing (relativistic)`

1. (commit) At $t = 0$, Alice_1 sends $x_1 = d \oplus a$ to Bob_1 and Alice_2 sends $x_2 = a$ to Bob_2. Bob_1 and Bob_2 immediately send x_1 and x_2 to Bob_0.
2. (open and verify) At $t = 1$, Bob_0 receives x_1 and x_2 and computes the commitment as $d = x_1 \oplus x_2$.

In a sense this protocol is easier to understand than the original, non-communicating version (cf. the spacetime diagram in Fig. 4.1). It is clear that Alice becomes committed at $t = 0$ (the commitment point) and that the commitment becomes known to Bob (Bob_0 to be more specific) at $t = 1$ (the opening point), hence, the commitment is valid for $t \in (0, 1)$. On the other hand, in the non-communicating variant it is not a priori clear when (and why!) communication constraints vanish and the commitment opens. Just like in Protocol 4, Alice_1 can single-handedly decide on the commitment and the choice can be delayed until $t = 0$.

Our second example is a relativistic variant of Protocol 4. This time Alice_1 and Alice_2 must share a random n-bit string $a \in \{0, 1\}^n$.

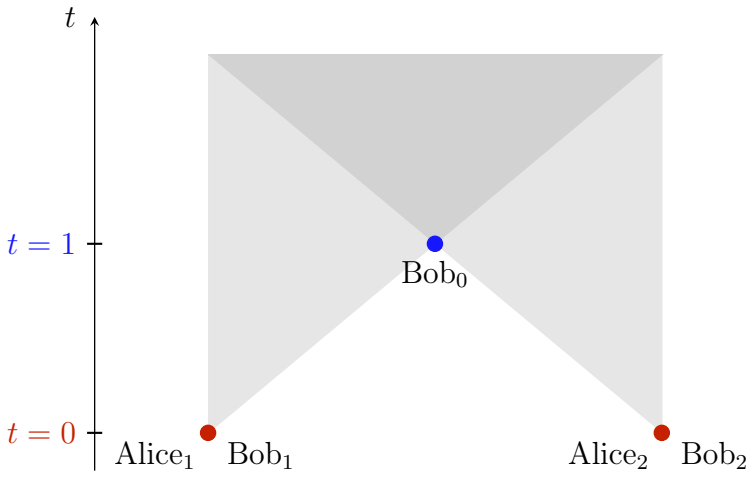

Fig. 4.1: Spacetime diagram for Protocol 5. The red dots represent the commit phase while the blue dot represents the open phase. The shaded areas correspond to the future light cones of the interactions in the commit phase.

Protocol 6: `Simplified-BGKW (relativistic)`

1. (commit) At $t = 0$, Bob_1 sends $y_1 = b$ to Alice_1 and she replies with $x_1 = d \cdot y_1 \oplus a$. Bob_1 immediately sends x_1 to Bob_2.
2. (open) At $t \in (0, 2)$, Alice_2 reveals $x_2 = a$ to Bob_2.
3. (verify) At $t = 2$, Bob_2 receives x_1 and verifies that $x_1 \oplus x_2 = d \cdot b$.

Just like in Protocol 4, Alice_1 can choose the value of the commitment single-handedly and this choice can be delayed until $t = 0$ (Alice_2 does not need to know it). The requirement that the open phase happens at $t < 2$ ensures that no signals can be sent between the commit and open phases (cf. Fig. 4.2). It is easy to see that Alice_2 could cheat perfectly if she knew b so the timing must be chosen such that b, which is announced by Bob_1 at $t = 0$, is not available to Alice_2 during the open phase. Under this condition the relativistic protocol and the original, non-communicating version are equivalent as far as security is concerned.

Note that in this relativistic scheme there is always a non-zero delay in verifying the commitment but it can be made arbitrarily small.[5] Whether this constitutes a severe limitation or not depends on the particular application but this feature, which appears often in relativistic protocols, should be always kept in mind, especially

[5]The possibility of immediate verification of the opening would imply that the commit phase and the open phase are *not* space-like separated. Then, there would have been enough time for b to reach Alice_2, which would render the protocol insecure.

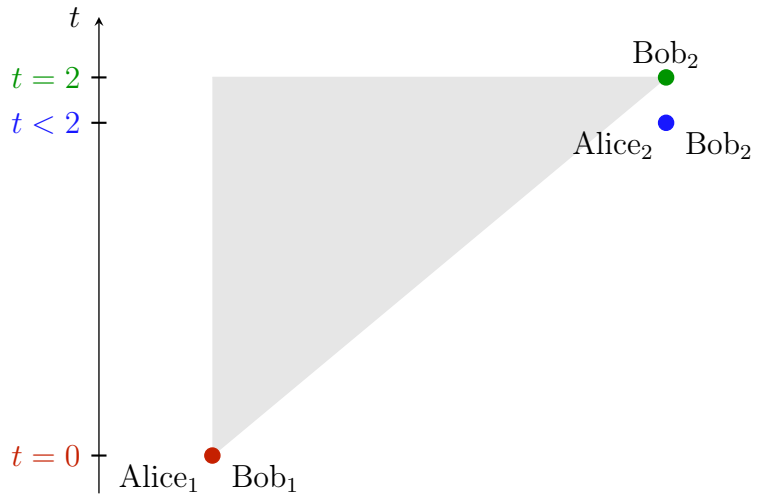

Fig. 4.2: Spacetime diagram for Protocol 6. The red dot represents the commit phase, the blue dot represents the open phase, the green dot corresponds to the point at which Bob_2 verifies the commitment.

when considering composability (i.e. executing a relativistic scheme as a subroutine in a longer procedure).

It is instructive to consider what happens if for some reason the open phase does not happen in the interval $t \in (0, 2)$. At $t = 2$ dishonest Alice_2 receives b (sent by dishonest Alice_1 at $t = 0$) and at this point she can provide a valid proof for either value of d, which makes the protocol completely insecure. In other words, the commitment expires at $t = 2$ and no opening should be accepted at (or after) that point. If Alice_2 does not perform the opening during $t \in (0, 2)$, Bob will never find out whether Alice_1 made an honest commitment, let alone its value.

Having presented two cases in which non-communicating protocols can be turned in a straightforward manner into relativistic protocols, let us briefly discuss one case in which such a simple translation is not possible. Recall Protocol 1 for distributed oblivious transfer presented in Section 3.2. Security of this protocol hinges on the assumption that Bob_1 and Bob_2 cannot communicate from the beginning of the protocol until the end of time. We know that permanent communication constraints cannot be enforced by relativity so we cannot hope for everlasting security but temporary security is not immediately ruled out. To restrict communication between Bob_1 and Bob_2 we would have to place them at distant locations, as usual accompanied by their communication partners Alice_1 and Alice_2. During the protocol each Alice receives a single message and the message that they actually want to obtain is the `XOR` of the two. Unfortunately, the earliest point at which the transmitted message might be reconstructed coincides with the point at which the information gathered by Bob_1 and Bob_2 can be recombined to reveal which message Alice chose to retrieve (the spacetime diagram is essentially identical to the one shown in Fig. 4.1).

We could have hoped for some finite interval during which Alice already knows the message but Bob still remains ignorant about her choice but in case of Protocol 1 this is not possible. This shows that not all non-communicating protocols can be mapped directly onto the relativistic setting in a meaningful way.

4.2 Explicit analysis of relativistic protocols

We have seen how simple non-communicating protocols can be implemented in the relativistic setting but so far the security analysis was rather ad hoc. While this is sufficient for simple schemes, for more complex protocols (involving more agents and/or multiple rounds, which might be necessary to achieve improved security features, e.g. longer commitment time) a systematic approach is desirable. In this section we provide a solution to a subclass of these problems and discuss the complications arising while dealing with the most general case.

A relativistic protocol is classical if all the messages exchange between agents of Alice and agents of Bob are classical. A protocol is quantum if there is at least one quantum message. Since classical protocols are designed to be executed by classical parties they should not require the agents of Alice or Bob to perform quantum operations *in the honest scenario*. However, this cannot be ruled out in the dishonest case and it is natural to study the security of classical protocols against quantum adversaries.

We first consider classical protocols and we show that analysing the dishonest scenario is equivalent to a certain multiplayer game with *partial communication constraints*[6] played by the agents of the dishonest party.[7] In Section 4.2.1 we show that if the agents are restricted to classical strategies, the situation is equivalent to a multiplayer game of non-communicating players. In Section 4.2.2 we mention some complications that arise when analysing such games against quantum players. Finally, in Section 4.2.3 we discuss briefly the problems related to quantum relativistic protocols.

For the sake of concreteness let us consider the case of honest Alice. Since the agents of Alice follow the protocol, we might think of them as an omnipresent referee, who interacts with the agents of Bob. The following simple procedure explains how to turn a relativistic protocol into a multiplayer game (similar to those described in Section 2.3) such that winning the game is equivalent to cheating in the protocol.

1. Identify all points of spacetime at which the agents of Alice and Bob interact,

[6] Similar models have been previously studied from the foundational point of view under the name of *time-ordered models* [GWC+14] or *correlation scenarios* [Fri12, Fri14].

[7] Note that this procedure is not specific to commitment schemes and applies to any relativistic protocol in which cheating can be cast as a game.

order them by their time coordinate and label by (positive) integers.[8] Without loss of generality we assume that every interaction consists of a *challenge* from Alice followed by a *response* from Bob, which for the j^{th} interaction are denoted by c_j and r_j, respectively.[9] Let (x_j, t_j) be the spacetime coordinates of the j^{th} interaction and let n be the total number of interactions in the protocol. Construct the *communication graph* $G = ([n], E)$, in which each vertex corresponds to an interaction and the set of (directed) edges is determined by the causality constraints. More precisely, (j, k) is an edge iff k is in the future light cone of j

$$(j,k) \in E \iff |x_k - x_j| \leq t_k - t_j.$$

Note that G is an oriented and acyclic graph.

2. Without loss of generality the challenge issued by Alice in the j^{th} interaction is a deterministic function of some pre-shared randomness (represented by a random variable Z) and the previous responses of Bob. For a particular value of the random variable $Z = z$ we have

$$c_j = f_j(z, r_1, r_2, \ldots, r_{j-1}).$$

(Clearly, f_j might not depend on the responses which do not belong to the past light cone of the j^{th} interaction but to keep the notation simple we do not indicate this restriction explicitly.) The collection of functions $f_1, f_2, \ldots, f_n$ together with the probability distribution of Z fully determines the distribution of challenges issued by Alice.

3. Deciding whether a cheating attempt is successful, i.e. the predicate function for the game, might without loss of generality be taken to depend only on the initial randomness and the responses from Bob, i.e. $V(z, r_1, r_2, \ldots, r_n)$.

This procedure provides us with three components: the communication graph, the distribution of challenges and the predicate function. Clearly, this triple defines a multiplayer game in which communication, instead of being completely forbidden, is restricted. More specifically, we can identify the j^{th} interaction with a player $\mathcal{P}_j$ and starting from $j = 1$ every player takes part in the following procedure.

1. Player $\mathcal{P}_j$ receives messages sent by previous players.

2. Player $\mathcal{P}_j$ receives a challenge c_j and issues a response r_j.

3. Player $\mathcal{P}_j$ might send a message to any player $\mathcal{P}_k$ such that $(j, k) \in E$.

[8] For interactions occurring at the same time the order does not matter.

[9] If the protocol requires more rounds of communications in a sequence, consider them as separate interactions.

At the end all the answers are collected and the predicate function V is evaluated to determine whether the game is won or lost.

Since quantum communication can be implemented by teleportation (and we do not impose any restrictions on the amount of entanglement shared by the players) we can assume all communication to be classical.

Let us summarise what we have accomplished so far. We have started from a classical relativistic protocol and we have turned it into an equivalent classical multiplayer game with communication constraints. Note that by classical we mean that all the challenges and responses are classical but this does not prevent the players from using quantum systems to generate them. As discussed in the next section, the case of quantum players (i.e. players using quantum systems to generate their classical responses) is significantly harder to analyse than the case of classical players.

Note that multiplayer games with communication constraints include many interesting scenarios as special cases. For example if $E = \emptyset$ (i.e. the communication graph G has no edges) we recover the standard scenario of multiplayer non-communicating games. The other extreme case is when the players satisfy a "total order", i.e. $(j, k) \in E \iff k > j$, which is equivalent to a single player responding to a sequence of challenges. This is exactly the scenario that arises in classical non-relativistic two-party cryptography.[10]

4.2.1 Classical players

Any strategy available to classical players can be expressed as a convex combination of deterministic strategies. Since randomness can be shared among the players in advance and their goal is to achieve the optimal winning probability (which is determined by a fixed and known function), we might restrict our attention to deterministic strategies. What is the most general strategy of $\mathcal{P}_j$, i.e. what is his response allowed to depend on? Clearly, it might depend on the challenge that he receives c_j but it might also depend on messages received by him from the "previous" players. This seems to complicate the situation, since these might be arbitrary and depend on anything that was available to the sender, etc. However, a simple observation allows us to simplify this seemingly complicated structure. Since the message sent by a particular player is a function of the data available to him, he could alternatively send the whole data set to the receiver, who can then generate the

[10] These two special cases have also been studied if the challenges and/or responses are quantum. For some recent results on two-player quantum games see Refs. [RV13, CJPPG15] while for sequential quantum games see papers on quantum non-relativistic two-party cryptography listed in Section 1.3.

message himself. This leads to the simple conclusion that it is optimal[11] to broadcast any challenge received from the referee to all eligible players. Then the response of $\mathcal{P}_j$ becomes a deterministic function of all the challenges *in his past*. If we supply every player with these additional inputs, they no longer need to communicate. This reduction works because there exists a trivial but optimal communication strategy for the players, namely "broadcast everything".

OBSERVATION 4.1. *Let $\mathcal{G}_1$ be the game in which $\mathcal{P}_j$ receives c_j and the allowed communication pattern is specified by $G = ([n], E)$. Let $\mathcal{G}_2$ be the game in which $\mathcal{P}_j$ receives $\{c_k\}_{k\in\mathcal{S}_j}$ where*

$$\mathcal{S}_j := \{k \in [n] : (k, j) \in E\}$$

and no communication is allowed $G = ([n], \emptyset)$. The sets of strategies available to the classical players in games $\mathcal{G}_1$ and $\mathcal{G}_2$ are identical.

This observation plays a crucial role in the analysis of a multiround classical relativistic bit commitment protocol in Chapter 6.

4.2.2 Quantum players

We have seen that for classical players games with communication constraints can be reduced to fully non-communicating games. What happens if we attempt such a reduction for quantum players?

As one might expect the quantum case is not so simple and it is instructive to consider the following example. Consider a game of three players where G contains only one edge, $E = \{(1, 2)\}$. Clearly, $\mathcal{P}_3$ cannot communicate with the other players but his presence is necessary to hope for a quantum advantage.[12] The response of $\mathcal{P}_1$ is determined by some measurement he performs on his quantum system (and the measurement setting depends on the challenge c_1). Then he passes whatever is left of the quantum system along with the classical messages c_1 and r_1 to $\mathcal{P}_2$ who then receives c_2 and completely measures the quantum system to obtain r_2.

This scenario is difficult to analyse because the measurement performed by $\mathcal{P}_1$ affects how much information $\mathcal{P}_2$ (who learns a new piece of information c_2) might extract from the state. This problem goes under the name of sequential measurements and is currently an active area of research [HM15]. Note that in the classical setting such trade-offs do not exist: generating the response for the current round does not affect the information that might be sent to other players.

[11] Optimal in the sense of spreading information to the largest number of players, certainly not in terms of efficiency.

[12] Without $\mathcal{P}_3$ we would have a game equivalent to asking a sequence of classical questions to a single player and in such games no quantum advantage is possible.

To the best of our knowledge, this is the simplest example in which finding the quantum value of a classical game cannot be reduced to any of the previously studied models. Interestingly enough, this is precisely the scenario which arises when analysing security of the multiround protocol presented in Chapter 6 against quantum adversaries.

4.2.3 Quantum relativistic protocols

While presenting the procedure to map a relativistic protocol onto a communication-constrained model, we have explicitly restricted ourselves to classical protocols. This was mainly to avoid the trouble of specifying the most general way in which the referee may choose the challenge. While this is conceptually not difficult, formalising these notions would be quite cumbersome. In particular, we would need to explicitly define the Hilbert spaces corresponding to the referee's memory, the "message" space, define the class of operations the referee might use to prepare the challenge, argue what the new predicate is, etc.[13]

While mapping a quantum relativistic protocol onto a quantum game is not difficult, we do not know how to analyse the resulting "quantum" games. Without aiming for full generality let us just sketch out two quantum games, which demonstrate difficulties that might arise in these scenarios.

The first game is a variation on the example presented in the previous section. Basically, by making the first challenge c_1 quantum we can eliminate $\mathcal{P}_3$ without trivialising the problem. Consider a game of two players $\mathcal{P}_1, \mathcal{P}_2$ such that $E = \{(1,2)\}$. The challenge received by $\mathcal{P}_1$ is an unknown quantum state and he is required to give a classical response r_1. $\mathcal{P}_1$ passes the remaining quantum state together with his classical response to $\mathcal{P}_2$, who receives a new (classical) challenge and must produce another classical response. Clearly, the information extractable in the second round depends on the measurement performed in the first one, hence, the two rounds cannot be decoupled and mapped onto a non-communicating model. Games of this type arise when considering quantum non-relativistic protocols.

The second game is arguably the simplest manifestation of no-cloning. Consider a game of three players whose communication graph contains two edges: $E = \{(1,2),(1,3)\}$. The challenge issued to $\mathcal{P}_1$ is an unknown quantum state and no response is required. Players $\mathcal{P}_2$ and $\mathcal{P}_3$ are then challenged to unveil one out of two incompatible properties of the original state. Clearly, this would be easy if each of them could hold a copy of the original state but this is forbidden by the no-cloning theorem. One solution is for $\mathcal{P}_1$ to measure one of the two properties and send the classical outcomes to $\mathcal{P}_2$ and $\mathcal{P}_3$. However, this only allows them to

[13] Note that as a special case we must recover the standard model for quantum protocols of Yao [Yao95], which puts a lower bound on the complexity of the description.

answer one of the challenges correctly. This is exactly the quantum feature used in Kent's quantum relativistic bit commitment protocol [Ken12b], whose complete analysis can be found in Chapter 5.

4.3 Limitations of relativistic cryptography

We have made contributions towards understanding of relativistic commitment schemes but in general the exact power of relativistic cryptography is not yet completely understood. The goal of this section is to summarise what is known to be possible and what the known limitations are. It turns out that between the two there is a sizeable piece of land yet to be discovered.

Let us start with the simplest task: coin tossing. The trivial classical protocol (described for example as Protocol 2.3 in Ref. [Col06]), in which Alice_1 sends a random bit to Bob_1 and simultaneously Bob_2 sends a random bit to Alice_2 and the outcome of the coin toss is the `XOR` of the two bits, achieves perfect security and is easily implemented in the simplest relativistic model with just two locations. More sophisticated flavours of coin tossing, in which Alice and Bob can partially influence the bias of the coin, are also possible [Col06].

The situation becomes a bit more complicated when it comes to bit commitment. All the commitment protocols we have discussed so far expire in some way: in case of Protocol 5 the commitment automatically opens, in case of Protocol 6 the commitment vanishes. In principle these commitments can be made arbitrarily long but only at the price of increasing the spatial separation between the sites. This is clearly not a desirable solution, since in practice we are restricted to a fixed region of space (we have easy access to the surface of the Earth but going beyond that seems somewhat impractical). Can we achieve an arbitrarily long commitment while performing the protocol in a finite region of space? Let us first consider protocols in which the commit phase only requires a finite amount of communication, i.e. at some point the communication stops and no more messages need to be exchanged until the open phase. It is clear that at that point both parties could bring all their systems together and within some period of time (proportional to the size of the accessible region of space) we would be back in the standard scenario, in which the usual trade-offs apply. Hence, arbitrarily long commitment cannot be achieved by a protocol with a bounded number of messages in the commit phase. What about protocols in which the agents keep communicating? The multiround scheme presented in Chapter 6 belongs to this class and implements bit commitment which is secure against classical adversaries and can be made arbitrarily long. We conjecture that the protocol remains secure against quantum adversaries but we currently do not have a proof.

Commitments with a finite period of validity (which at some point expire) have been previously studied under the name of *timed commitments*. For example Boneh and Naor [BN00] study commitments which fail in the same way as Protocol 5, i.e. after some fixed time the committed value is revealed to Bob.[14] They show that such commitments can be used for contract signing or honesty-preserving auctions. Generally speaking, such temporary secrecy is sufficient if the goal is to force parties to act simultaneously (in the sense that their respective actions should not depend on each other) even if the communication model is sequential. Broadbent and Tapp considered the task of secure voting, for which such commitments would be sufficient [BT08]. Timed commitments that vanish (i.e. the commitment is no longer valid but the committed value, if there was one, remains secret) can be used in similar situations if we want to give Alice more power to protect her privacy. This type of commitment might also be used in multiparty protocols which are robust against a certain fraction of dishonest parties (then any party that refuses to open the commitment would be declared dishonest).

To see the limitations of relativistic commitment schemes it is instructive to investigate whether they can be used to implement other, more powerful primitives. For example, a well-known construction shows how to use bit commitment and quantum communication to implement oblivious transfer [BBCS92, Yao95]. Are relativistic schemes suitable for this canonical construction? Without going into too many details let us describe one important feature of this construction. At some point of the procedure Bob is required to make several commitments. Later, Alice asks Bob to open a random subset of them but the rest he keeps untouched. Security for Bob hinges on the fact that some commitments remain closed, which rules out relativistic schemes that expire by opening (like Protocol 5). The commitments that vanish without revealing any information (like Protocol 6) might seem perfectly suited for the task. However, a simple conceptual problem referred to as *classical certification* or *retractability* arises [Ken12c, Col06]. Basically, the canonical construction implicitly assumes that every commitment (including the unopened ones) *has a value*. While it might not be immediately clear what it means for an unopened commitment to have a value, this concept can be made rigorous and it is possible to show that relativistic protocols do not satisfy this property. A more detailed discussion on the issue of classical certification of relativistic commitment schemes and an explicit example how it renders the canonical construction insecure can be found in Appendix A. While this is by no means a proof that no relativistic commitment scheme can be used for the canonical construction, we have at least ruled out the ones considered so far.

[14] Their motivation comes from schemes which only offer computational security. Such schemes can always be forced open given enough time and computational power.

What about implementing relativistic oblivious transfer directly without going through canonical construction? This possibility seems unlikely due to the following informal argument. In every (correct) oblivious transfer protocol at some fixed point Alice must receive the chosen message. At this point the knowledge of Alice (or Bob) might be scattered among all their agents but in an attempt to cheat it can be (within some finite time) gathered at one location and then the usual impossibility results apply. Investigating whether this intuition can be turned into a rigorous argument would be an interesting research problem for two reasons: it would require us to propose a meaningful definition of relativistic oblivious transfer and the actual impossibility result (if true) would determine an important boundary point of quantum relativistic cryptography. Alternatively, one can relax the requirements and look for a protocol whose security is only guaranteed for a finite period of time. Such protocols might exist and it would be interesting to know how useful they are.

Chapter 5

Bit commitment by transmitting measurement outcomes

This chapter is based on

- **Experimental bit commitment based on quantum communication and special relativity** [arXiv:1306.4801]
  T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner and H. Zbinden
  Physical Review Letters **111**, 180504 (2013).
  (presented at *QCrypt '13*)

In the previous chapters we have seen why non-communicating models are useful in cryptography and how such models can be implemented using relativity. In this chapter we use the tools introduced before and present a complete analysis of a particular quantum relativistic bit commitment protocol proposed by Kent [Ken12b]. Our initial approach to this problem, presented in Ref. [KTHW13], relied on some tools from non-asymptotic quantum information theory and a recently discovered uncertainty relation [TR11, Tom12]. Later, however, we found another, simpler approach (which does not explicitly use any uncertainty relation), which we then extended to apply to experimental implementations [LKB+13]. In this chapter we only present the latter, superior method. Note that similar techniques found applications to other interesting problems in quantum cryptography [TFKW13]. (During the lifetime of these projects an independent security analysis of the same protocol was provided by Croke and Kent [CK12] and an independent experiment was performed by Liu, Cao, Curty, Liao, Wang, Cui, Li, Lin, Sun, Li, Zhang, Zhao, Chen, Peng, Zhang, Cabello and Pan [LCC+14]).

Outline: We start by proving security of the original protocol. Our methods are robust, as they also apply to the case of imperfect state preparation and noisy transmission. This would be sufficient to prove security of an implementation that

uses a single-photon source, a lossless quantum channel and perfect detectors (or devices which are good approximations thereof). Unfortunately, such devices are not available at the moment, hence, we modify the protocol so it can be implemented using currently available devices, in our case a weak-coherent source and inefficient and noisy detectors. We describe the new security model, extend the previous security analysis and determine the minimum requirements on the honest devices that allow for a secure implementation of the protocol. We also present an explicit calculation of the security parameter of the protocol. We finish this chapter by giving a brief overview of an experiment performed between Geneva and Singapore in collaboration with an experimental group at the University of Geneva.

5.1 The original protocol

We use the following notation for the BB84 states

$$|\psi_x^\theta\rangle = H^\theta |x\rangle, \tag{5.1}$$

where $x, \theta \in \{0,1\}$. For a sequence of BB84 states described by $x, \theta \in \{0,1\}^n$ we use

$$|x^\theta\rangle = \bigotimes_{k=1}^{n} |\psi_{x_k}^{\theta_k}\rangle. \tag{5.2}$$

For a particular basis string $\theta \in \{0,1\}^n$ we define S and T to be the rounds in which Alice encoded her qubits in the computational and Hadamard basis, respectively,

$$S = \{k \in [n] : \theta_k = 0\},$$
$$T = \{k \in [n] : \theta_k = 1\}.$$

The protocol proposed by Kent [Ken12b] uses the same locations as described in Section 4.1 and Fig. 5.1 shows the relevant spacetime diagram. The parameter $n \in \mathbb{N}$ determines the usual cost vs. security trade-off (see Section 2.4), while $\delta \in [0,1)$ specifies the noise tolerance of the protocol. Recall that $\mathrm{d_H}(\cdot,\cdot)$ is the fractional Hamming distance (defined in Section 2.1.1).

Protocol 7: `Bit commitment by transmitting measurement outcomes`

1. (commit) At $t = 0$, Bob_0 chooses $x, \theta \in \{0,1\}^n$ uniformly at random, creates $|x^\theta\rangle$ and sends it to Alice_0. Alice_0 measures all the incoming qubits in the same basis (computational if $d = 0$ and Hadamard if $d = 1$) to

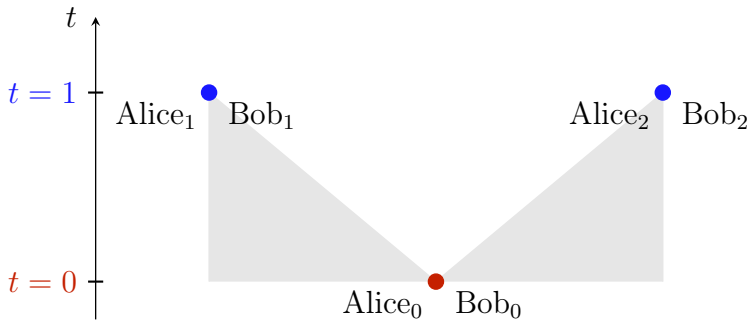

Fig. 5.1: Spacetime diagram for Protocol 7. The red dot represents the commit phase while the blue dots represent the open phase. The shaded area corresponds to the past light cones of the events of the open phase.

produce $y \in \{0,1\}^n$ (the string of measurement outcomes), which she then sends to Alice_1 and Alice_2.

2. (open) At $t = 1$, Alice_1 and Alice_2 simultaneously send d and y to Bob_1 and Bob_2, respectively.

3. (verify) Bob_1 and Bob_2 pass all the information to Bob_0, who verifies that:

   - Alice_1 and Alice_2 have attempted to unveil the same value
   - Alice_1 and Alice_2 have provided exactly the same string y
   - the string y is consistent with the BB84 states initially prepared by Bob_0 up to the error threshold δ

$$\begin{aligned} \mathrm{d_H}(x_S, y_S) &\leq \delta \quad \text{for} \quad d = 0, \\ \mathrm{d_H}(x_T, y_T) &\leq \delta \quad \text{for} \quad d = 1. \end{aligned}$$

If all three conditions are satisfied, Bob_0 accepts the commitment.

Before we proceed with a complete analysis let us mention a couple of unusual features of the protocol.

First of all, it seems that Alice becomes committed without actually sending any information to Bob (no communication from Alice to Bob happens until the open phase). Is that possible? How can Bob be sure that for $t > 0$ Alice is indeed committed?

To answer this question it is instructive to consider a slight variation on Protocol 7, in which the open phase is delayed until $t = 2$. Clearly, in this case Alice_0 could keep the quantum states untouched until $t = 1$ and only then perform the

measurement. For this modified protocol Alice only becomes committed at $t = 1$, which does not occur *immediately after* the communication in the commit phase is over (as was the case in all the previous protocols).

This quantum protocol challenges the preconception that the timing of the commitment point is determined by the interactions in the commit phase. Strangely enough, in this case the commitment point is determined by the timing of and locations used in the open phase. In fact, it is easy to see that the commitment point is determined by the latest point in the common past of the openings performed by Alice_1 and Alice_2.

Protocols discussed in Section 4.1 result in commitments which are only valid for a finite amount of time (in case of Protocol 5 the commitment at some point automatically opens while in case of Protocol 6 at some point security for honest Bob is lost). It is interesting to note that the quantum commitment scheme we consider now does not expire. A commitment initiated at $t = 0$ may be opened at any $t = t_{\text{open}} > 1$ but a successful opening only demonstrates that Alice was committed for $t \in (t_{\text{open}} - 1, t_{\text{open}})$. It is important to stress that at $t = t_{\text{open}} - 1$ Alice is not yet committed, so we must take the commitment point to be $t = t_{\text{open}} - 1 + r$, where $r > 0$ is an arbitrarily small (but non-zero) constant.

Finally, let us point out that verifying whether an opening should be accepted or not is not immediate. Moreover, in contrast to Protocol 6, the delay cannot be made arbitrarily small. Since the conditions that Bob needs to verify depend on data unveiled at both opening locations, the delay is proportional to the distance between them.

5.1.1 Correctness

Correctness in the noiseless setting is clear by inspection while for an experimental implementation the only relevant quantity turns out to be the total bit-flip error rate between (honest) Alice and Bob (this rate includes contributions coming from imperfect state preparation, transmission noise and measurement errors). For simplicity we assume that noise acts independently on every qubit. Let err be the bit-flip error rate, i.e. the probability of obtaining the wrong outcome despite the qubit having been prepared and measured in the same basis.[1] The protocol is asymptotically correct (i.e. the probability of honest parties aborting decays exponentially in n) if

$$\text{err} < \delta. \tag{5.3}$$

[1] If the error probabilities are different for the two bases, we take the larger value to be on the safe side.

Note that this depends solely on the numerical value of err and not on the exact effects that contribute to it.

5.1.2 Security for honest Alice

Since Bob receives no information before the open phase, he remains completely ignorant about Alice's commitment and so the protocol is hiding.

5.1.3 Security for honest Bob

To investigate security for honest Bob we first turn the original prepare-and-measure scheme of Kent into an entanglement-based scheme (equivalence for security purposes was explained in Section 2.2.3). In the entanglement-based formulation instead of generating BB84 states Bob_0 generates EPR pairs, he keeps one half of each (to be measured later) and sends the other halves to Alice_0. The most general attack performed by Alice_0 during the commit phase is to perform an isometry that "splits up" the entire quantum system received from Bob_0 into two parts, which she then sends to Alice_1 and Alice_2. In the open phase, Alice_1 and Alice_2 measure their respective quantum systems and pass the outcomes to Bob_1 and Bob_2, respectively.

Since we want to prove security with respect to the global command variant of Definition 3.2 let us spell out how this definition applies to the protocol.[2]

First, we need to characterise the set of states that Alice_0 might enforce at the commitment point. While at $t = 0$ the state is (without loss of generality) only shared between Alice_0 and Bob_0, at the commitment point ($t = r > 0$) the share of Alice_0 is already explicitly split up into two parts (that will reach Alice_1 and Alice_2 in time for the open phase) and this partitioning is essential to determine the commitment. We denote the relevant subsystems by A_1 and A_2 (even if at the commitment point these subsystems are not with the agents Alice_1 and Alice_2 yet). It is straightforward to see that at the commitment point any tripartite state $\sigma_{BA_1A_2}$ can be enforced as long as the marginal state held by Bob_0 remains unchanged, i.e.

$$\operatorname{tr}_{A_1A_2} \sigma_{BA_1A_2} = \left(\frac{\mathbb{1}}{2}\right)^{\otimes n}.$$

Interestingly enough, our proof does not make use of this property. In other words, the protocol remains secure even if Alice_0 were allowed to provide an arbitrary tripartite state compatible with the measurements that Bob_0 will later perform (i.e. the subsystem of Bob_0 must consist of n qubits).

In the open phase Alice_1 and Alice_2 must provide proofs, which are just classical strings of length n. Hence, the opening maps correspond to measurements. Each

[2] Security in the local command can be achieved by the trivial Protocol 3, cf. Section 3.3.

of Alice_1 and Alice_2 has two different measurements used to unveil the two different values of the commitment and we denote the measurement operators of Alice_1 (Alice_2) attempting to unveil d by $\{P_y^d\}_{y\in\{0,1\}^n}$ $\left(\{Q_y^d\}_{y\in\{0,1\}^n}\right)$. Since we do not impose any constraints on the local dimensions of A_1 and A_2 we may without loss of generality assume that these measurements are projective. The fact that Alice_2 might use different measurements for $d = 0$ and $d = 1$ indicates that we work in the global command model.

If $\theta \in \{0,1\}^n$ is the basis string (picked by Bob_0 uniformly at random), then his measurement is described by operators $\{|x^\theta\rangle\langle x^\theta|\}_{x\in\{0,1\}^n}$ as defined in Eq. (5.2). The commitment is accepted if the strings supplied by Alice_1 and Alice_2 are consistent with the classical outcomes obtained by Bob_0. This condition can be written as a projector acting on the original tripartite state and it is easy to see that the projector Π_d^θ corresponding to Bob_0 accepting the unveiling of d for a particular basis string θ equals

$$\Pi_0^\theta = \sum_{x\in\{0,1\}^n} |x^\theta\rangle\langle x^\theta| \otimes \sum_{\substack{y\in\{0,1\}^n \\ \mathrm{d_H}(x_S,y_S)\leq\delta}} P_y^0 \otimes Q_y^0,$$
$$\Pi_1^\theta = \sum_{x\in\{0,1\}^n} |x^\theta\rangle\langle x^\theta| \otimes \sum_{\substack{y\in\{0,1\}^n \\ \mathrm{d_H}(x_T,y_T)\leq\delta}} P_y^1 \otimes Q_y^1,$$

and the three registers correspond to the subsystems held by Bob_0, Alice_1 and Alice_2, respectively (and the latter two result from an isometry applied by Alice_0 to subsystem A_0, which she received in the commit phase). These projectors require that Alice_1 and Alice_2 unveil the same string, which on the relevant subset (S for $d = 0$ and T for $d = 1$) is δ-close (in terms of fractional Hamming distance) to the string obtained by Bob. To calculate the probability of successfully unveiling d we must average over all possible basis choices

$$p_d = 2^{-n} \sum_{\theta\in\{0,1\}^n} \mathrm{tr}(\Pi_d^\theta \sigma_{BA_1A_2}).$$

In fact, our technique allows us to generalise the definition (5.1) to any pair of bases on a qubit

$$\langle\psi_0^0|\psi_1^0\rangle = \langle\psi_0^1|\psi_1^1\rangle = 0.$$

This requirement comes directly from the fact that the equivalence between prepare-and-measure and entanglement-based schemes as presented in Section 2.2.3 only applies if the average state is fully mixed. It turns out that the final bound depends

only on the overlap between the bases

$$c := \max_{x,y} |\langle \psi_x^0 | \psi_y^1 \rangle|, \tag{5.4}$$

which is a well-known measure of incompatibility used extensively in the study of uncertainty relations [Deu83, MU88, BCC+09, TR11].

PROPOSITION 5.1. *Let*

$$\lambda_0 = \frac{1+c}{2} \quad \textit{and} \quad \lambda_1 = \frac{1-c}{2},$$

where c is the overlap as defined in Eq. (5.4). For any strategy of dishonest Alice, the probabilities of Bob accepting the commitment satisfy

$$p_0 + p_1 \leq 1 + \varepsilon,$$

for

$$\varepsilon = \begin{cases} \lambda_0^n & \text{for } \delta = 0, \\ \exp\left(-\frac{1}{2}\left(\sqrt{\lambda_1} - \frac{\delta}{\sqrt{\lambda_1}}\right)^2 n \right) & \text{for } 0 < \delta < \lambda_1. \end{cases} \tag{5.5}$$

Proof. Let us write the sum out explicitly

$$p_0 + p_1 = 2^{-n} \sum_{\theta} \operatorname{tr}\left([\Pi_0^\theta + \Pi_1^\theta] \sigma_{BA_1A_2} \right). \tag{5.6}$$

Adding up the two projectors (for a particular value of θ) gives

$$\Pi_0^\theta + \Pi_1^\theta = \sum_x |x^\theta\rangle\langle x^\theta| \otimes \left[\sum_{\substack{y \\ \mathrm{d_H}(x_S, y_S) \leq \delta}} P_y^0 \otimes Q_y^0 \quad + \sum_{\substack{y \\ \mathrm{d_H}(x_T, y_T) \leq \delta}} P_y^1 \otimes Q_y^1 \right].$$

The terms in the square bracket can be upper bounded by replacing one of the measurement operators by the identity matrix. Therefore,

$$\begin{aligned} \sum_{\substack{y \\ \mathrm{d_H}(x_S, y_S) \leq \delta}} P_y^0 \otimes Q_y^0 \quad + \sum_{\substack{y \\ \mathrm{d_H}(x_T, y_T) \leq \delta}} P_y^1 \otimes Q_y^1 &\leq \sum_{\substack{y \\ \mathrm{d_H}(x_S, y_S) \leq \delta}} P_y^0 \otimes \mathbb{1} \quad + \mathbb{1} \otimes \sum_{\substack{y \\ \mathrm{d_H}(x_T, y_T) \leq \delta}} Q_y^1 \\ &\leq \mathbb{1} \otimes \mathbb{1} \quad + \sum_{\substack{y \\ \mathrm{d_H}(x_S, y_S) \leq \delta}} P_y^0 \otimes \sum_{\substack{z \\ \mathrm{d_H}(x_T, z_T) \leq \delta}} Q_z^1, \end{aligned}$$

where the last step follows from the following operator inequality

$$A \otimes \mathbb{1} + \mathbb{1} \otimes B = \mathbb{1} \otimes \mathbb{1} + A \otimes B - (\mathbb{1} - A) \otimes (\mathbb{1} - B) \leq \mathbb{1} \otimes \mathbb{1} + A \otimes B, \tag{5.7}$$

which holds for any $0 \leq A, B \leq \mathbb{1}$. Therefore,

$$\Pi_0^\theta + \Pi_1^\theta \leq \sum_x |x^\theta\rangle\langle x^\theta| \otimes \mathbb{1} \otimes \mathbb{1} + \Pi_c^\theta = \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1} + \Pi_c^\theta, \tag{5.8}$$

where

$$\Pi_c^\theta = \sum_x |x^\theta\rangle\langle x^\theta| \otimes \sum_{\substack{y \\ \mathrm{d_H}(x_S, y_S) \leq \delta}} P_y^0 \otimes \sum_{\substack{z \\ \mathrm{d_H}(x_T, z_T) \leq \delta}} Q_z^1$$

is a projector for the "cross-game", in which Alice_1 has to unveil a string consistent with $d = 0$ and Alice_2 has to unveil a string consistent with $d = 1$.[3] Combining Eqs. (5.6) and (5.8) gives

$$p_0 + p_1 \leq 1 + 2^{-n} \sum_\theta \mathrm{tr}\left(\Pi_c^\theta \sigma_{BA_1A_2}\right) = 1 + \mathrm{tr}\left(\langle \Pi_c^\theta \rangle \sigma_{BA_1A_2}\right) \leq 1 + \|\langle \Pi_c^\theta \rangle\|,$$

where $\langle \cdot \rangle$ denotes averaging over θ, i.e. $\langle \Pi_c^\theta \rangle = 2^{-n} \sum_\theta \Pi_c^\theta$, and $\| \cdot \|$ denotes the Schatten ∞-norm (defined in Section 2.2.1). Changing the order of summation in Π_c^θ gives

$$\Pi_c^\theta = \sum_{y,z} \sum_{\substack{x \\ \mathrm{d_H}(x_S, y_S) \leq \delta \\ \mathrm{d_H}(x_T, z_T) \leq \delta}} |x^\theta\rangle\langle x^\theta| \otimes P_y^0 \otimes Q_z^1.$$

Now, it is clear that only the x-dependent part needs to be averaged:

$$\langle \Pi_c^\theta \rangle = 2^{-n} \sum_\theta \Pi_c^\theta = \sum_{y,z} B_{yz} \otimes P_y^0 \otimes Q_z^1,$$

where

$$B_{yz} = 2^{-n} \sum_\theta \sum_{\substack{x \\ \mathrm{d_H}(x_S, y_S) \leq \delta \\ \mathrm{d_H}(x_T, z_T) \leq \delta}} |x^\theta\rangle\langle x^\theta|.$$

Since the product $P_y^0 \otimes Q_z^1$ yields orthogonal projectors, we have

$$\|\langle \Pi_c^\theta \rangle\| = \max_{y,z} \|B_{yz}\|. \tag{5.9}$$

To identify values of y and z which maximise the norm we take a closer look at the matrices B_{yz}. For every θ define $u(\theta)$ to be the string that satisfies $[u(\theta)]_S = y_S$ and

[3] Our security analysis goes through a thought experiment in which Alice_1 and Alice_2 are challenged to unveil *different* bits and in the current method this connection is made through the operator inequality (5.7). Interestingly enough, our previous method relies on the same idea but expressed at the level of no-signalling probability distributions (see Lemma V.1 of Ref. [KTHW13]).

$[u(\theta)]_T = z_T$. Relabelling $x \mapsto x \oplus u(\theta)$ yields

$$B_{yz} = 2^{-n} \sum_{\theta} \sum_{\substack{x \\ \mathrm{w_H}(x_S) \leq \delta \\ \mathrm{w_H}(x_T) \leq \delta}} |(x \oplus u(\theta))^\theta\rangle\langle(x \oplus u(\theta))^\theta|.$$

The constraints on the second sum can be relaxed by noting that $\mathrm{w_H}(x_S) \leq \delta$ and $\mathrm{w_H}(x_T) \leq \delta$ imply $\mathrm{w_H}(x) \leq \delta$. Therefore,

$$B_{yz} \leq B'_{yz} = 2^{-n} \sum_{\theta} \sum_{\substack{x \\ \mathrm{w_H}(x) \leq \delta}} |(x \oplus u(\theta))^\theta\rangle\langle(x \oplus u(\theta))^\theta|,$$

which makes the second sum independent of θ. Hence, the summation over θ can be performed first and due to the tensor product structure we have

$$|x^\theta\rangle\langle x^\theta| = \bigotimes_{k=1}^{n} |\psi^{\theta_k}_{x_k}\rangle\langle\psi^{\theta_k}_{x_k}|$$

and

$$\sum_{\theta} \ldots \iff \bigotimes_{k=1}^{n} \sum_{\theta_k \in \{0,1\}} \ldots.$$

Therefore,

$$2^{-n} \sum_{\theta} |(x \oplus u(\theta))^\theta\rangle\langle(x \oplus u(\theta))^\theta| = \bigotimes_{k=1}^{n} \rho_{x_k \oplus y_k, x_k \oplus z_k}.$$

where

$$\rho_{b,c} = \frac{1}{2}(|\psi^0_b\rangle\langle\psi^0_b| + |\psi^1_c\rangle\langle\psi^1_c|)$$

for $b, c \in \{0,1\}$. Note that $\rho_{b,c} + \rho_{1-b,1-c} = \mathbb{1}$ so they are diagonal in the same basis. Therefore, without loss of generality we can write

$$\rho_{b,c} = \sum_{t \in \{0,1\}} \lambda^{b \oplus c}_t |e^{b \oplus c}_t\rangle\langle e^{b \oplus c}_t|,$$

for $b, c \in \{0,1\}$, where $\lambda^{b \oplus c}_0 + \lambda^{b \oplus c}_1 = 1$. In particular, we have

$$\Big(\bigotimes_{k=1}^{n} \rho_{x_k \oplus y_k, x_k \oplus z_k}\Big)\Big(\bigotimes_{k=1}^{n} |e^{y_k \oplus z_k}_{v_k}\rangle\Big) = \bigotimes_{k=1}^{n} \lambda^{y_k \oplus z_k}_{x_k \oplus y_k \oplus v_k} |e^{y_k \oplus z_k}_{v_k}\rangle.$$

Therefore, we also know the eigenbasis of

$$B'_{yz} = \sum_{\substack{x \\ \mathrm{w_H}(x) \leq \delta}} \bigotimes_{k=1}^{n} \rho_{x_k \oplus y_k, x_k \oplus z_k},$$

and the largest eigenvalue equals

$$\|B'_{yz}\| = \max_v \sum_{\substack{x \\ \mathrm{w_H}(x)\leq\delta}} \prod_{k=1}^{n} \lambda_{x_k\oplus y_k\oplus v_k}^{y_k\oplus z_k}.$$

Recall from Eq. (5.9) that the expression we want to bound is

$$\max_{y,z} \|B'_{yz}\| = \max_{v,y,z} \sum_{\substack{x \\ \mathrm{w_H}(x)\leq\delta}} \prod_{k=1}^{n} \lambda_{x_k\oplus y_k\oplus v_k}^{y_k\oplus z_k} = \max_{a,b} \sum_{\substack{x \\ \mathrm{w_H}(x)\leq\delta}} \prod_{k=1}^{n} \lambda_{x_k\oplus b_k}^{a_k}.$$

It is clear that every bit of a and b should be chosen to satisfy $\lambda_{b_k}^{a_k} = \max_{s,t} \lambda_s^t := \lambda_0$. Then

$$\max_{y,z} \|B'_{yz}\| = \sum_{\substack{x \\ \mathrm{w_H}(x)\leq\delta}} \prod_{k=1}^{n} \lambda_{x_k} = \sum_{k=0}^{\lfloor\delta n\rfloor} \binom{n}{k} \lambda_0^{n-k}\lambda_1^k,$$

where $\lambda_1 = 1 - \lambda_0$. Finally, since we know that

$$\|\langle\Pi_c^\theta\rangle\| = \max_{y,z} \|B_{yz}\| \leq \max_{y,z} \|B'_{yz}\|,$$

we obtain the security guarantee of the form

$$\varepsilon = \sum_{k=0}^{\lfloor\delta n\rfloor} \binom{n}{k} \lambda_0^{n-k}\lambda_1^k.$$

For $\delta = 0$ there is only one term in the sum while for $0 < \delta < \lambda_1$ we use the Chernoff bound (Lemma 2.2) to obtain the final result of the lemma. □

The protocol is secure as long as $\delta < \lambda_1$, which combined with Eq. (5.3) implies that correctness and security is possible as long as

$$\mathrm{err} < \lambda_1.$$

This allows us to check whether a particular experimental setup (characterised by err and λ_1) allows for a secure implementation of the protocol. For example, if the source emits perfect BB84 states (or, in fact, any two mutually unbiased bases on a qubit) we can tolerate up to 14.6% of errors.

5.2 Modelling imperfect devices

While we have allowed our states to be imperfect and undergo some noise process in transit, we have implicitly assumed that every time Bob_0 pushes a button a qubit

in a well-defined state is sent towards Alice_0, who always detects it to obtain a particular classical outcome. As of today there is no physical system which matches this idealised description to a reasonable degree. Therefore, in collaboration with an experimental group at the University of Geneva, we have developed a new version of the protocol, which can be implemented using currently available devices.

First of all, instead of a single-photon source we use a weak-coherent source with phase randomisation[4], which emits pulses of light in which the number of photons is a Poisson-distributed random variable. Let $|r\rangle$ be the Fock state of r photons and μ be the average number of photons per pulse (an adjustable parameter of the source). Then, the ensemble emitted by a weak-coherent source can be written as

$$\rho = \sum_{r=0}^{\infty} p_r |r\rangle\langle r| \quad \text{for} \quad p_r = e^{-\mu} \cdot \frac{\mu^r}{r!}.$$

A direct consequence of this model is that some pulses might contain more than one photon and we refer to those as *multiphoton emissions*. Such pulses constitute a deadly threat to our protocol since Alice_0 could measure the first photon in the computational basis, the second photon in the Hadamard basis and, hence, obtain enough information to open either value with certainty. Clearly, multiphoton emissions do not contribute to security and so their number must be rigorously controlled.

Besides the imperfections of the source, there is also a certain probability that a photon might be lost either in transit or during the detection process. Let η be the *detection efficiency*, i.e. the probability that a photon sent by Bob_0 is detected by Alice_0. We assume that the loss process affects every photon independently so the number of photons detected by Alice_0 is, again, a Poisson-distributed random variable. The probability of detecting r photons equals

$$p_r(\mu, \eta) = e^{-\mu\eta} \cdot \frac{(\mu\eta)^r}{r!}. \tag{5.10}$$

We assume that the detection efficiency depends neither on the measurement setting nor on the incoming state. Note that while this is a natural assumption from the theoretical point of view, it does not always hold for an experimental setup (it is common to have slightly different detection efficiencies for measurements in different bases) and this issue needs to be addressed while analysing experimental data as explained in Section 5.4. Moreover, it has recently been demonstrated that strong pulses of light might allow Bob to learn some information about Alice's basis setting

[4]We have decided to use phase randomisation because then the number of photons in a pulse can be modelled as a classical random variable, which turns out to be convenient for the security analysis.

[LWW+10], which is not included in our analysis.

We follow the standard approach (presented in Section 2.4), i.e. we assume that the devices used by the honest party are trusted (their characterisation including any imperfections is known) but the dishonest party is limited only by the laws of physics. The following table lists the models used for each of the three distinct scenarios.

Alice	Bob	source	losses	errors
honest	honest	weak-coherent source	yes	yes
honest	dishonest	perfect	detectors only	N/A
dishonest	honest	weak-coherent source	no	no

5.3 Protocol with backreporting

If we try to implement the original protocol using the equipment described above, we run into a very simple problem: in most rounds Alice_0 simply does not see a click (either because the photon was never emitted or it was not detected). What is she supposed to do then? One solution would be to simply generate a random bit and act as if this was the outcome of the measurement. This solution works as long as losses are infrequent and can be "hidden" within the error threshold. However, in the experimental setup described above losses are extremely common. In fact, it is the detection events that are rare. Therefore, flipping a coin for every loss is not a feasible solution.

We solve this problem using a standard technique known as *backreporting*, which requires Alice_0 to inform Bob_0 at the end of the quantum exchange which rounds were successful (i.e. a photon was detected) and only these rounds are used for the protocol (all the remaining data is discarded). This clearly restores correctness but, unfortunately, it opens a new security loophole as dishonest Alice_0 might also backreport single-photon rounds in order to increase the contribution of multiphoton emissions, which she can win with certainty. To avoid this threat Bob_0 must carefully monitor the number of rounds backreported by Alice. Let $\mathcal{M}$ be the set of rounds in which Alice_0 observed a click, which we call *the valid set*. Bob_0 only continues with the protocol if the size of the valid set exceeds a certain threshold, $m := |\mathcal{M}| \geq \gamma n$, where $\gamma \in [0, 1)$ is an adjustable parameter of the protocol called the *detection threshold*.

Protocol 8: `Bit commitment by transmitting measurement outcomes with backreporting`

1. (commit) At $t = 0$, Bob_0 chooses $x, \theta \in \{0,1\}^n$ uniformly at random, creates $|x^\theta\rangle$ and sends it to Alice_0. Alice_0 measures all the incoming qubits in the same basis (computational if $d = 0$ and Hadamard if $d = 1$) . The rounds in which a click was observed form $\mathcal{M}$ and $y \in \{0,1\}^m$ is the string of outcomes. Alice_0 announces $\mathcal{M}$ to Bob_0. Bob_0 continues with the protocol only if $m \geq \gamma n$.

2. (open) At $t = 1$, Alice_1 and Alice_2 simultaneously send d and y to Bob_1 and Bob_2, respectively.

3. (verify) Bob_1 and Bob_2 pass all the information to Bob_0, who verifies that:

   - Alice_1 and Alice_2 have attempted to unveil the same value
   - Alice_1 and Alice_2 have provided exactly the same string y
   - the string y is consistent with the BB84 states initially prepared by Bob_0 up to the error threshold δ

$$\begin{aligned} \mathrm{d_H}(x_{S\cap\mathcal{M}}, y_{S\cap\mathcal{M}}) &\leq \delta \quad \text{for} \quad d = 0, \\ \mathrm{d_H}(x_{T\cap\mathcal{M}}, y_{T\cap\mathcal{M}}) &\leq \delta \quad \text{for} \quad d = 1. \end{aligned}$$

   If all three conditions are satisfied, Bob_0 accepts the commitment.

5.3.1 Correctness

To guarantee correctness we must first ensure that Alice registers a sufficient number of clicks. Asymptotically, we simply require that the probability of seeing a click (i.e. detecting at least one photon) is larger than the detection threshold

$$\sum_{r=1}^{\infty} p_r = 1 - p_0 > \gamma.$$

Using Eq. (5.10) to express p_0 in terms of μ and η gives

$$e^{-\mu\eta} + \gamma < 1.$$

Since in our model errors are independent of losses or multiphoton emissions, the second correctness condition remains the same as before, i.e. Eq. (5.3).

5.3.2 Security for honest Alice

Since backreporting introduces communication from Alice_0 to Bob_0 in the commit phase, security for honest Alice is no longer unconditionally true. To make sure that the valid set $\mathcal{M}$ does not contain any information about the commitment we must ensure that the detection efficiencies do not depend on the basis choice regardless of the state that the dishonest Bob_0 sends in. We assume that the detection system used by Alice satisfies these properties (see Section 5.2).

5.3.3 Security for honest Bob

Security analysis for honest Bob is an extension built on top of the previous argument. We take advantage of the fact that all the experimental imperfections (e.g. multiphoton emissions or no-detection events) can be modelled as classical random variables and that for particular values of these random variables Proposition 5.1 provides an explicit security bound.

In every round a certain number of photons (between 0 and ∞) is emitted (recall that in this case we assume that Alice_0 has perfect detectors, i.e. $\eta = 0$). Pulses with no photons affect correctness but do not constitute a security threat. Pulses with one photon is what the original protocol calls for and what we analysed in the previous section. Finally, multiphoton pulses are a serious threat as they allow Alice_0 to obtain sufficient information to successfully open both values of the commitment. To simplify our analysis we replace all the zero-photon emissions by single-photon emissions (which only gives Alice more power). Eq. (5.10) with $\eta = 0$ implies that the probability of a multiphoton emission in a particular round equals

$$p_m = 1 - e^{-\mu}(1 + \mu).$$

The number of multiphoton rounds N_m is a binomially-distributed random variable

$$\Pr[N_m = k] = \binom{n}{k} p_m^k (1 - p_m)^{n-k}. \tag{5.11}$$

The optimal strategy of dishonest Alice_0 is to discard as many single-photon rounds as possible. It is clear that if she can discard all of them, she is left with multiphoton emissions only and no security can be guaranteed. Therefore, the necessary condition for security is that the number of multiphoton rounds is lower than the detection threshold

$$N_m < \lceil \gamma n \rceil.$$

After using up the entire backreporting allowance the number of valid rounds equals $m = \lceil \gamma n \rceil$ but there are only $\lceil \gamma n \rceil - N_m$ (which is now guaranteed to be a positive

number) single-photon rounds among them. Honest Bob believes that they are performing a bit commitment protocol of $\lceil \gamma n \rceil$ rounds but there is a certain number of multiphoton ones, which Alice can win "for free". Hence, she can concentrate her error allowance on the single-photon rounds and the security we achieve is that of playing a game of $\lceil \gamma n \rceil - N_m$ rounds with the absolute (non-fractional) error allowance of $\delta \lceil \gamma n \rceil$, which gives the effective (fractional) error allowance of

$$\delta' = \frac{\delta \lceil \gamma n \rceil}{\lceil \gamma n \rceil - N_m}. \tag{5.12}$$

The proof in Section 5.1.3 is valid only if the effective (fractional) error allowance, δ', satisfies

$$\delta' < \lambda_1,$$

where λ_1 measures the incompatibility of the measurements performed by Bob_0. Hence, in our case we require

$$\delta \lceil \gamma n \rceil < (\lceil \gamma n \rceil - N_m)\lambda_1. \tag{5.13}$$

In the asymptotic limit it is sufficient to look at the expectation value

$$\mathbb{E}[N_m] = p_m n = [1 - e^{-\mu}(1+\mu)]n,$$

which substituted into Eq. (5.13) gives

$$e^{-\mu}(1+\mu) + (1 - \delta/\lambda_1)\gamma > 1.$$

5.3.4 Requirements on the honest devices

Having derived explicit criteria for correctness and security we can check whether a given experimental setup allows for a secure implementation of the protocol. The correctness and security constraints are

$$\begin{gathered} e^{-\mu\eta} + \gamma < 1, \\ \mathrm{err} < \delta, \\ e^{-\mu}(1+\mu) + (1 - \delta/\lambda_1)\gamma > 1. \end{gathered}$$

It is clear that δ and γ (parameters of the protocol) can be taken arbitrarily close to the values which would turn the first two conditions into equalities. This leaves us with only one, but rather complicated, condition

$$e^{-\mu}(1+\mu) + (1 - \mathrm{err}/\lambda_1)(1 - e^{-\mu\eta}) > 1.$$

This expression allows us to check whether for devices of certain quality (quantified by λ_1, err and η) there exists a value of μ that makes the protocol both correct and secure.[5]

5.3.5 Explicit security calculation

The asymptotic analysis is relevant as $n \to \infty$ but in any practical scenario the number of rounds is finite. Therefore, we want to explicitly calculate security guarantees as a function of n. Since correctness is verified experimentally and security for honest Alice is perfect by assumption, we only need to calculate security for honest Bob.

Let E denote the event that Alice successfully cheats in the bit commitment protocol. We have shown in Eq. (5.12) that the probability of cheating successfully depends on the number of multiphoton emissions. Therefore, let us write

$$\Pr[E] = \sum_{k=0}^{n} \Pr[E|N_m = k] \Pr[N_m = k]. \tag{5.14}$$

Equation (5.5) allows us to bound $\Pr[E|N_m = k]$ as long as the number of multiphoton emissions is below the threshold. For $k < k_t := \gamma n(1 - \delta/\lambda_1)$ we have

$$\Pr[E|N_m = k] \leq \exp\left(-\frac{1}{2}\left(\sqrt{(\gamma n - k)\lambda_1} - \frac{\delta\gamma n}{\sqrt{(\gamma n - k)\lambda_1}}\right)^2\right).$$

On the other hand, for $k \geq k_t$ there is no security and the trivial bound, $\Pr[E|N_m = k] \leq 1$, is the best we can hope for. The second term is given by Eq. (5.11). Performing the summation (5.14) for any particular values of the parameters is a straightforward exercise in any package for numerical calculations (e.g. Octave [EBH09]).

5.4 Experimental implementation

Protocol 8 requires the use of three equidistant locations on a line. This is clearly quite difficult to do if we want to take maximal advantage of the size of the Earth. Therefore, we have implemented a modified protocol, in which only two locations are used. The experiment is performed between Geneva (Location 1) and Singapore (Location 2) and achieves secure commitment for 15.6 ms (the maximal duration achievable on the Earth, corresponding to antipodal locations on the surface, equals

[5] Note that changing the mean photon number μ affects the physical aspect of the protocol so it might influence other physical parameters like the error rate. On the other hand, parameters like δ or γ, which are only relevant for the post-processing, do not have such an effect.

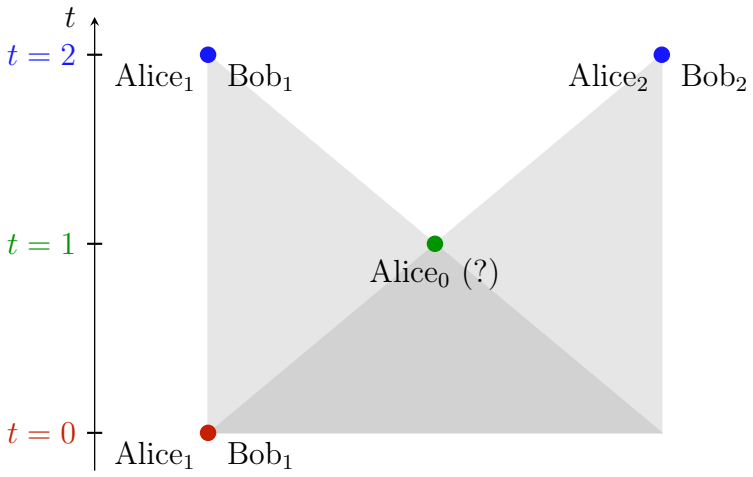

Fig. 5.2: Spacetime diagram for the experimental implementation of Protocol 8. The red dot represents the commit phase while the blue dots represent the open phase. The shaded area corresponds to the past light cones of the events of the open phase. The green dot determines the commitment point, i.e. the *latest* point at which Alice can still perform an honest commitment.

21.2 ms). As explained in Section 5.1 the maximal commitment time equals *half* the time it takes to travel at lightspeed between the two opening locations (we cannot rule out the possibility that dishonest Alice deployed an extra agent exactly in between the two locations, who receives the quantum states at $t = 1$ and only then performs the measurements, cf. Fig. 5.2).

Each location hosts one agent for each player synchronised to universal time using a global positioning system (GPS) clocks. The protocol consists of two parts: (i) exchange of quantum information in the commit phase and (ii) exchange of classical information in the open phase. Phase (i) was implemented using a commercial quantum key distribution system Vectis 5100 from ID Quantique located at the University of Geneva (see Fig. 5.3). This system is based on the two-way "Plug&Play" configuration [MHH+97]: strong optical pulses travel from Alice_1 to Bob_1, who uses them to encode the BB84 states. Moreover, he attenuates the optical power down to single photon level and sends these weak-coherent pulses back to Alice_1. Trojan-horse attacks on Bob's side are particularly effective against the "Plug&Play" configuration so the power of the incoming beam is continuously monitored by Bob_1. To use the quantum key distribution system for bit commitment some software changes must be made, in particular communication from Alice_1 to Bob_1 is restricted to backreporting only. As discussed in Section 5.3.2 extra care has to be taken to ensure that the backreported data does not leak any information about the choice of measurements performed by Alice_1. In our experimental setup the two bases exhibit slightly different detection probabilities so the raw data must

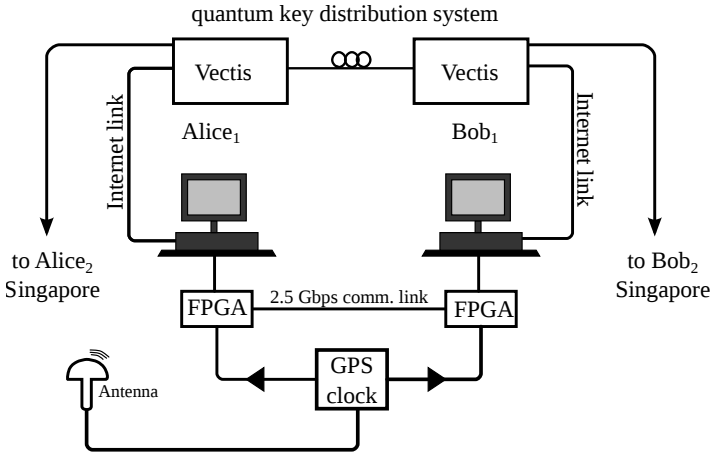

Fig. 5.3: Experimental setup located in Geneva. The setup located in Singapore is identical except that Alice_1 and Bob_1 are replaced by Alice_2 and Bob_2, and that there is no quantum key distribution system (the protocol only requires quantum interactions in the commit phase which as explained in Section 5.4 happens in Geneva). Figure reproduced with permission from Tommaso Lunghi.

be artificially "equalised".[6]

The duration of the commitment is ultimately limited by the distance between the locations under the assumption that all local communication is instantaneous. However, since the exchange of quantum states in the commit phase takes a considerate amount of time, which would reduce the achievable commitment time, we have performed a *delayed commitment*. In a delayed commitment scheme Alice_1 first commits to a random bit r and only later announces $d \oplus r$, which initiates the actual commitment (and determines its value). This allows us to perform all the quantum information exchange in advance, which maximises the commitment time.

Classical information needed by Alice_2 in Singapore to open the commitment was transmitted in advance through the internet (one-time-pad encrypted using pre-shared keys generated by a quantum random generator from ID Quantique). The classical information exchange in the open phase was performed using stand-alone computers equipped with field-programmable gate array (FPGA) to make the transmission time negligible relative to the commitment time (around 3 μs).

[6] More specifically, with probability p we discard an outcome obtained for the more efficient setting, where p is chosen to make the expected number of detections backreported for both settings equal.

Chapter 6

Multiround relativistic bit commitment protocol

This chapter is based on

- **Practical relativistic bit commitment** [arXiv:1411.4917]
  T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner and H. Zbinden
  Physical Review Letters **115**, 030502 (2015).
  (presented at *QCrypt '14*)

The quantum protocol discussed in the previous chapter implements secure bit commitment in the β-split model (one of the minimal splits, in which, as discussed in Section 3.3, no classical protocol can give security). This demonstrates that quantum protocols are strictly more powerful and in this particular case the extra power results from the no-cloning theorem. However, a weak point of that scheme is the length of the commitment, which is limited by the spatial separation of the two opening sites. In particular, for a protocol taking place on the Earth, the commitment time is limited to 21 ms. While this might be sufficient for some purposes, extending the commitment time would be highly desirable. It is clear that if the spatial arrangement is fixed, the only manner to extend the commitment time is to introduce additional rounds of communication. In fact, this idea was proposed by Kent quite early on [Ken99, Ken05], where instead of *opening* the commitment Alice *commits* to the information she *would have used* in the unveiling. The original way of "chaining" commitments has the drawback that the communication required grows exponentially with the number of rounds [Ken99]. This was later rectified by adding a compression scheme on top of the protocol [Ken05]. Security of such a chained scheme would follow directly if the individual commitments were com-

posably secure[1]. However, we do not know how to prove composable security of relativistic commitment schemes and there is evidence that this might indeed be impossible (e.g. in Appendix A we show that the classical relativistic `sBGKW` scheme is not secure according to the usual composable definition). Therefore, the security proof must explicitly consider all the intermediate commitments. Security argument against classical adversaries presented by Kent [Ken05] is of asymptotic nature and, therefore, not sufficient for implementation purposes.

Outline: With the goal of finding a new classical multiround protocol in mind we first revisit the two-round protocol proposed in Ref. [Sim07, CSST11] and show that security for honest Bob relies on the difficulty of a certain non-local game, whose quantum value was recently investigated by Sikora, Chailloux and Kerenidis [SCK14]. This completes the security analysis and shows that the two-round protocol is secure against quantum adversaries.[2] With the two-round scheme as our starting point we propose a new classical multiround protocol (with constant communication rate) and analyse its security against *classical* adversaries.[3] Correctness can be verified by inspection, security for honest Alice is intuitively obvious (nevertheless formalising it requires some work) and security for honest Bob turns out to be more involved but we eventually derive an explicit and easily computable security bound. Unfortunately, the bound suffers from rather undesirable scaling in the number of rounds (which is proportional to the length of the commitment). While the commitment time is not subject to any fundamental limitations, an implementation using standard digital equipment only allows modest commitment times. In collaboration with the Geneva group we have implemented the protocol to achieve a secure commitment of 2 ms.[4]

Note added: After the completion of this work, two groups independently provided security proofs that give significantly improved security bounds [FF15b, CCL15]. These results imply that Protocol 9 can be used to realise long-lasting commitments with very modest resources, hence, making it truly practical.

[1] In fact, this is exactly the idea of composable security: the protocol is indistinguishable from the ideal primitive in *all possible scenarios*.

[2] Security for honest Alice is obvious against classical Bob. Security against quantum Bob follows from a simple observation that if only one agent (Bob_1) is involved in the commit phase of a classical protocol, no advantage can be gained by using quantum systems (cf. footnote 12 in Section 4.2.2).

[3] For more than two rounds security analysis against quantum adversaries becomes rather involved as explained in Section 4.2.2.

[4] An attentive reader might be puzzled that the new multiround protocol yields commitment time which is significantly shorter than the one previously achieved by the quantum protocol. The solution of this conundrum is that while the previous experiment was performed between Geneva and Singapore, the new multiround one was (for practical reasons) executed between two locations within Switzerland. Performing the multiround protocol between Geneva and Singapore would give a commitment time of 156 ms (a tenfold improvement over the quantum protocol).

6.1 Two-round protocol

Since the two-round protocol has already been discussed in Section 4.1 let us go directly to the security analysis. Recall that the protocol requires two sites labelled Location 1 and Location 2. To simplify notation in this chapter we assume that these locations are separated by $(1+\epsilon)$ units of length for some $\epsilon > 0$. Therefore, one unit of time is *not* sufficient to transmit information between them.

Protocol 6: `Simplified-BGKW (relativistic)`

1. (commit) At $t = 0$, Bob_1 sends $y_1 = b$ to Alice_1 and she replies with $x_1 = d \cdot y_1 \oplus a$. Bob_1 immediately sends x_1 to Bob_2.
2. (open) At $t = 1$, Alice_2 reveals $x_2 = a$ to Bob_2.
3. (verify) At $t = 1 + \epsilon$, Bob_2 receives x_1 and verifies that $x_1 \oplus x_2 = d \cdot b$.

(Note that the verification step could be performed slightly earlier using an agent positioned somewhere in between Bob_1 and Bob_2 but since ε is chosen to be essentially 0 this makes no difference.)

Correctness is straightforward to check and security for honest Alice comes from the fact that the message that Bob_1 receives in the commit phase is one-time-padded with a uniformly random string.

Security for honest Bob is quantified using Definition 3.2. Since only one agent (Alice_2) is involved in the open phase, the distinction between local and global command does not arise. As explained in Section 2.5.1 it is often helpful to explicitly state the cheating game that Alice attempts to win. In the commit phase Alice_1 receives $b \in \{0,1\}^n$ (chosen uniformly at random) and in the open phase Alice_2 receives nothing from Bob but she is challenged to open $d \in \{0,1\}$ chosen uniformly at random. In each phase she is required to output an n-bit string, which we denote by x_1 and x_2, respectively. Since there is no communication between Alice_1 and Alice_2 this is equivalent to a two-player game which (using the formalism presented in Section 2.3) is specified by the uniform input distribution $p(b,d) = \frac{1}{2} \cdot \frac{1}{2^n}$ and the predicate function

$$V(b, x_1, d, x_2) = \begin{cases} 1 & \text{if } \; x_1 \oplus x_2 = d \cdot b, \\ 0 & \text{otherwise.} \end{cases}$$

Since this game can be seen as a generalisation of the CHSH game (which corre-

sponds to $n = 1$), let us call it CHSH_n after Ref. [SCK14]. Calculating the classical value is straightforward but let us do it explicitly for completeness.

As explained in Section 2.3 we might without loss of generality assume that Alice_1 and Alice_2 employ deterministic strategies, which we denote by functions $f_1(b)$ and $f_2(d)$. Define H_d as the event over B (private randomness of Bob) that the opening of d is accepted

$$H_d \iff d \cdot B = f_1(B) \oplus f_2(d). \tag{6.1}$$

Since both H_0 and H_1 are defined over B it is meaningful to talk about $H_0 \vee H_1$ and $H_0 \wedge H_1$.[5] Note that $\Pr[H_0] + \Pr[H_1] = \Pr[H_0 \vee H_1] + \Pr[H_0 \wedge H_1] \leq 1 + \Pr[H_0 \wedge H_1]$. The event $H_0 \wedge H_1$ happens when condition (6.1) is satisfied for both values of d. Define K to be the event that the `XOR` of the two is satisfied

$$K \iff B = f_2(0) \oplus f_2(1).$$

Since the left-hand side is a uniformly distributed random variable and the right-hand side is a constant $\Pr[K] = 2^{-n}$. Moreover, as $H_0 \wedge H_1 \implies K$ we have $\Pr[H_0 \wedge H_1] \leq \Pr[K]$. Combining the two statements implies that for any strategy of classical Alice we have $\Pr[H_0] + \Pr[H_1] \leq 1 + 2^{-n}$ which leads to

$$\omega(\mathrm{CHSH}_n) \leq \frac{1}{2} + \frac{1}{2^{n+1}}.$$

It is easy to check that the trivial strategy of always outputting $x_1 = x_2 = 0^n$ saturates this bound. Intuitively this game should be difficult because unveiling $d = 0$ and $d = 1$ requires Alice_2 to know x_1 and $x_1 \oplus b$, respectively. She cannot guess both of these too well since b is chosen uniformly at random by Bob_1.

Applying this reasoning to quantum adversaries is not so straightforward because Alice_2 might have two distinct measurements that reveal x_1 and $x_1 \oplus b$, respectively, but they might be incompatible so the implications on her ability to guess b are not so obvious. Fortunately, the following bound on the quantum value was recently proven [SCK14]

$$\omega^*(\mathrm{CHSH}_n) \leq \frac{1}{2} + \frac{1}{\sqrt{2^{n+1}}}.$$

This is sufficient for our purposes as it implies that

$$p_0 + p_1 \leq 1 + \sqrt{2} \cdot 2^{-n/2}$$

for all strategies of dishonest quantum Alice. Therefore, the protocol is ε-binding with $\varepsilon = 2^{(1-n)/2}$ decaying exponentially in n (but note that the decay rate is half

[5] This is exactly where the argument breaks down when applied to the quantum world, in which H_0 and H_1 are not in general defined *simultaneously*.

of the decay rate against classical adversaries).

This is a prime example that analysing classical protocols against quantum adversaries is *not always* a futile task and sometimes leads to interesting observations. An immediate question arises regarding super-quantum adversaries: what if Alice_1 and Alice_2 have access to stronger-than-quantum correlations? It is straightforward to see that the protocol is completely insecure against Alice_1 and Alice_2 who have access to no-signalling correlations [Sim07, CSST11]. In fact, it was shown recently that in this particular model it is not possible to have a protocol secure against no-signalling adversaries [FF15a]. This is a consequence of the fact that in this context the hiding property coincides with the definition of no-signalling and so if the protocol is hiding then there exists a perfect cheating strategy consistent with no-signalling. This is yet another example of how classical and quantum theories are qualitatively different from the no-signalling world.

6.2 Multiround protocol

To extend the commitment time we must introduce additional rounds of communication, which keep the commitment "alive" (the sustain phase). If Alice and Bob require the commitment to be valid for m units of time (for some $m \in \mathbb{N}$) they need to execute the following protocol of $m+1$ rounds. We use k as a label for the round under consideration and since the rounds alternate between the two locations we define

$$l(k) = \begin{cases} 1 & \text{if } k \equiv 1 \pmod 2, \\ 2 & \text{if } k \equiv 0 \pmod 2. \end{cases}$$

We use a_k and b_k to denote private strings (chosen uniformly at random) of Alice and Bob, respectively and x_k and y_k to denote messages announced by Alice and Bob, respectively, in the k^{th} round of the protocol. All the n-bit strings are interpreted as elements of the finite field $\mathbb{F}_{2^n}$ and "$*$" denotes the finite field multiplication.

Protocol 9: `Multiround bit commitment`

1. (commit, $k = 1$) At $t = 0$, Bob_1 sends $y_1 = b_1$ to Alice_1. Alice_1 returns $x_1 = d \cdot y_1 \oplus a_1$.
2. (sustain, $2 \leq k \leq m$) At $t = k - 1$, $\text{Bob}_{l(k)}$ sends $y_k = b_k$ to $\text{Alice}_{l(k)}$. $\text{Alice}_{l(k)}$ returns $x_k = (y_k * a_{k-1}) \oplus a_k$.
3. (open, $k = m + 1$) At $t = m$, $\text{Alice}_{l(m+1)}$ sends d and $x_{m+1} = a_m$ to $\text{Bob}_{l(m+1)}$.

4. (verify) At $t = m + \epsilon$, $\text{Bob}_{l(m+1)}$ receives x_m and accepts the opening if

$$\begin{aligned} x_{m+1} \;=\; & x_m \;\oplus\; b_m * x_{m-1} \;\oplus\; b_m * b_{m-1} * x_{m-2} \;\oplus\; \ldots \\ & \ldots \;\oplus\; b_m * b_{m-1} * \ldots * b_2 * x_1 \;\oplus\; d \cdot b_m * b_{m-1} * \ldots * b_1. \end{aligned} \tag{6.2}$$

It is easy to see that the timing is chosen precisely to make every two consecutive rounds space-like separated. In the formalism presented in Section 4.2 there are $m + 1$ interactions and the communication graph is

$$\begin{aligned} G &= ([m+1], E) \quad \text{for} \\ E &= \{(j,k) \in [m+1]^2 : j + 2 \leq k\}. \end{aligned} \tag{6.3}$$

Correctness of the protocol is straightforward to check by substituting the honest responses of Alice_1 and Alice_2 into the acceptance condition (6.2).

6.2.1 Security for honest Alice

Security for honest Alice is a direct consequence of the fact that every message she announces is one-time-padded with a fresh secret n-bit string. Hence, we would intuitively expect the transcripts corresponding to $d = 0$ and $d = 1$ to be statistically indistinguishable. We prove this statement by considering an arbitrary adaptive attack (consistent with relativity) that classical Bob_1 and Bob_2 might implement. While we do not believe that Bob_1 and Bob_2 can gain anything by using quantum systems, we currently do not have a rigorous argument to justify this belief.

We start with a lemma which formalises the intuition that if we take an arbitrary random variable taking values in $\mathbb{F}_q$ and add it to a uniform and uncorrelated random variable (over $\mathbb{F}_q$) then there will be no correlations between the input and the output (or any function thereof). More specifically, in the following lemma Y is a random variable from which the input is generated using function g, X is the fresh (finite field) randomness and h is a function allowing us to condition on a certain subset of values of Y.

LEMMA 6.1. *Let $\mathcal{X} = \mathbb{F}_q$ and $\mathcal{Y}, \mathcal{Z}$ be arbitrary finite sets. Let X and Y be two random variables taking values in $\mathcal{X}$ and $\mathcal{Y}$, respectively, such that X is uniform and independent from Y*

$$\Pr[X = x, Y = y] = q^{-1} \cdot \Pr[Y = y], \tag{6.4}$$

for all $x \in \mathcal{X}$ and $y \in \mathcal{Y}$. Then for arbitrary functions $g : \mathcal{Y} \to \mathcal{X}$, $h : \mathcal{Y} \to \mathcal{Z}$ and

arbitrary fixed $x \in \mathcal{X}$, $z \in \mathcal{Z}$ it holds that

$$\Pr[X + g(Y) = x \,|\, h(Y) = z] = q^{-1}.$$

Proof. Note that

$$\Pr[X + g(Y) = x, h(Y) = z] = \sum_{y \in \mathcal{Y}} \Pr[X = x - g(y), h(y) = z, Y = y]$$
$$= \sum_{\substack{y \in \mathcal{Y} \\ h(y) = z}} \Pr[X = x - g(y), Y = y] = \sum_{\substack{y \in \mathcal{Y} \\ h(y) = z}} q^{-1} \cdot \Pr[Y = y] = q^{-1} \cdot \Pr[h(Y) = z],$$

where the second last equality follows from applying the assumption (6.4) to every term of the sum. □

Lemma 6.1 allows us to prove security for honest Alice.

PROPOSITION 6.1. *If Alice is honest then the protocol is hiding.*

Proof. We want to show that the transcripts for $d = 0$ and $d = 1$ at the opening point (i.e. after the last sustain round) are indistinguishable, i.e.

$$\Pr[X_1 = x_1, X_2 = x_2, \ldots, X_m = x_m | d = 0] = \Pr[X_1 = x_1, X_2 = x_2, \ldots, X_m = x_m | d = 1]$$

for all $x_1, x_2, \ldots, x_m$. In fact, we show a stronger statement, namely

$$\Pr[X_1 = x_1, X_2 = x_2, \ldots, X_t = x_t | d = c] = 2^{-nt}, \tag{6.5}$$

for all $t \in [m]$ and both values of $c \in \{0, 1\}$.

Honest Alice follows the protocol, which means that $\{A_k\}_{k=1}^m$ are drawn independently, uniformly at random from $\{0,1\}^n$ and so Alice's message in the k^{th} round (represented as a random variable) equals

$$X_k = \begin{cases} d \cdot Y_1 \oplus A_1 & \text{for } \; k = 1, \\ (Y_k * A_{k-1}) \oplus A_k & \text{for } \; 2 \leq k \leq m. \end{cases} \tag{6.6}$$

Bob_1 and Bob_2, on the other hand, are only limited by the causal constraints, which means that the message in the k^{th} round might depend on some pre-shared randomness denoted by R_B and all the responses of Alice_1 and Alice_2 which belong to the past of the k^{th} round. Therefore, without loss of generality the message in the k^{th} round is

$$Y_k = f_k(R_B, X_1, X_2, \ldots X_{k-2}) \tag{6.7}$$

for some arbitrary function f_k (we include all randomness used by Bob in R_B so f_k is deterministic).

In this scenario the full transcript is a deterministic function of Alice's commitment d, her private randomness $\{A_k\}_{k=1}^m$ and Bob's pre-shared randomness R_B. For every string announced by Alice and Bob we can explicitly find the subset of random variables it may depend on as listed in the table below

message	random variables it might depend on
Y_1	R_B
Y_2	R_B
Y_3	d, R_B, A_1
$\vdots$	$\vdots$
Y_k	$d, R_B, A_1, A_2, \ldots, A_{k-2}$
$\vdots$	$\vdots$
Y_m	$d, R_B, A_1, A_2, \ldots, A_{m-2}$
X_1	d, R_B, A_1
X_2	d, R_B, A_1, A_2
X_3	d, R_B, A_1, A_2, A_3
$\vdots$	$\vdots$
X_k	$d, R_B, A_1, A_2, \ldots, A_k$
$\vdots$	$\vdots$
X_m	$d, R_B, A_1, A_2, \ldots, A_m$

First, we verify that condition (6.5) holds for $t = 1$

$$\Pr[X_1 = x_1 | d = c] = \Pr[b \cdot Y_1 \oplus A_1 = x_1] = \Pr[b \cdot f_1(R_B) \oplus A_1 = x_1] = 2^{-n},$$

where the first two equalities follow from Eqs. (6.6) and (6.7), respectively. The last equality is a direct consequence of Lemma 6.1 (in a simplified form: no conditioning) applied to $X = A_1$, $Y = (c, R_B)$, $g(Y) = c \cdot f_1(R_B)$. Now, suppose that Eq. (6.5) holds for $t = k$. Then

$$\begin{aligned}
&\Pr[X_1 = x_1, \ldots, X_{k+1} = x_{k+1} | d = c] \\
&\quad = \Pr[X_{k+1} = x_{k+1} | d = c, X_1 = x_1, \ldots, X_k = x_k] \cdot \Pr[X_1 = x_1, \ldots, X_k = x_k | d = c] \\
&\quad = \Pr[(Y_{k+1} * A_k) \oplus A_{k+1} = x_{k+1} | d = b, X_1 = x_1, \ldots, X_k = x_k] \cdot 2^{-nk} \\
&\quad = 2^{-n} \cdot 2^{-nk} = 2^{-(n+1)k},
\end{aligned}$$

where the second last inequality follows from applying Lemma 6.1 to

$$\begin{aligned} X &= A_{k+1}, \\ Y &= (c, R_B, A_1, \ldots, A_k), \\ g(Y) &= Y_{k+1} * A_k, \\ h(Y) &= (X_1, X_2, \ldots, X_k). \end{aligned} \tag{6.8}$$

Note that it is not immediately obvious and the reader should verify (using the table presented above) that the quantities on the right-hand side of Eq. (6.8) are functions of Y alone, and therefore satisfy the assumptions of the lemma. This shows that Eq. (6.5) holds for $t = k + 1$ and so by induction it must hold for all $t \in [m]$. This shows that even at the opening point the transcript contains no information about Alice's commitment, which implies that the protocol is hiding. □

6.2.2 Security for honest Bob

Security for honest Bob is where the framework developed in Section 4.2 comes in useful. We immediately identify the case of honest Bob as a game of $m + 1$ players $\mathcal{P}_1, \ldots, \mathcal{P}_{m+1}$ whose communication is restricted by G defined in Eq. (6.3). Player $\mathcal{P}_k$ (for $1 \leq k \leq m$) receives a uniformly random n-bit string represented by the random variable B_k. Moreover, all the players except for $\mathcal{P}_1$ receive d (the value they are challenged to unveil) chosen uniformly at random. It is clear that d must not be available to $\mathcal{P}_1$ (this would correspond to an honest commitment) but it must be available to all the other players. This is important as it fixes the commitment point to occur immediately after $t = 0$, i.e. allows us to claim that Alice becomes committed immediately after the first round.

Having explicitly determined the inputs received by each player and the communication constraints we apply Observation 4.1 to turn this scenario into a non-communicating game. It is easy to verify that the output of $\mathcal{P}_1$ denoted by X_1 can be written as

$$X_1 = f_1(R_A, B_1),$$

where R_A corresponds to any randomness shared by the players. For $\mathcal{P}_k$ for $2 \leq k \leq m$ we have

$$X_k = f_k(R_A, B_1, B_2, \ldots, B_{k-2}, B_k, d).$$

Finally, for $\mathcal{P}_{m+1}$ we have

$$X_{m+1} = f_{m+1}(R_A, B_1, B_2, \ldots, B_{m-1}, d).$$

This allows us to prove security for honest Bob.

PROPOSITION 6.2. *If Bob is honest then the protocol is ε-binding for $\varepsilon = \omega_m$ defined in Eq. (2.4).*

Proof. The argument is essentially identical to the one presented in Section 6.1 and we use the same definitions for the events H_0, H_1 and K. Since K is defined as the XOR of Eq. (6.2) for $d = 0$ and $d = 1$ we have

$$K \iff B_1 * B_2 * \ldots * B_m = g_{m+1}(R_A, B_1, B_2, \ldots, B_{m-1}) \oplus g_m(R_A, B_1, B_2, \ldots, B_{m-2}, B_m) \bigoplus_{k=2}^{m-1} B_m * B_{m-1} * \ldots * B_{k+1} * g_k(R_A, B_1, B_2, \ldots, B_{k-2}, B_k),$$

where

$$g_k(R_A, B_1, B_2, \ldots, B_{k-2}, B_k) = f_k(R_A, B_1, B_2, \ldots, B_{k-2}, B_k, d = 0) \oplus f_k(R_A, B_1, B_2, \ldots, B_{k-2}, B_k, d = 1).$$

To bound $\Pr[K]$ note that the right-hand side contains exactly m terms, but each of them depends on $(m-1)$ B's; none of the terms depends on *all B's simultaneously*. The terms corresponding to $2 \leq k \leq m-1$ have some internal structure (e.g. the dependence on B_m is *not* arbitrary) but we can relax the problem to the case where the k^{th} term is an arbitrary function of all the B's except for B_k denoted by h_k. The winning condition for the relaxed game is

$$B_1 * B_2 * \ldots * B_m = \bigoplus_{k=1}^{m} h_k(B_{[m]\setminus\{k\}}).$$

In Section 2.3.3 we define the optimal winning probability for this game to be ω_m, which concludes the proof since

$$p_0 + p_1 \leq 1 + \Pr[K] \leq 1 + \omega_m. \qquad \square$$

The recursive argument presented in Section 2.3.5 allows us to obtain explicit upper bounds on ω_m. In particular, we have $\omega_m \leq c_m$, where

$$c_m = \begin{cases} 2^{-n} & \text{for } \; m = 1, \\ \frac{1}{2^{n+1}} + \sqrt{c_{m-1}} & \text{for } \; m \geq 2. \end{cases} \tag{6.9}$$

For large n, to a good approximation we have $c_m \approx 2^{-n/2^m}$. The decay is exponential in n but since the decay rate strongly depends on m, security deteriorates rapidly as we increase the number of rounds. The tightness of these bounds is an interesting open problem and is briefly discussed in Appendix B.5 of Ref. [LKB+15]. No explicit

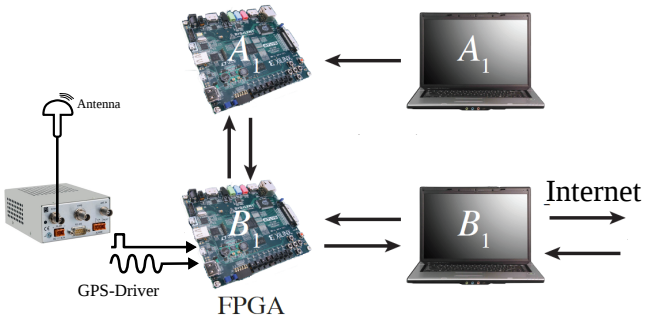

Fig. 6.1: Experimental setup at Location 1 where A_1 and B_1 represent Alice_1 and Bob_1, respectively. Figure reproduced with permission from Tommaso Lunghi.

cheating strategy is known, whose winning probability would approach our security bounds.

6.3 Experimental implementation

Both the two-round and the multiround protocols have been implemented between University of Geneva and University of Berne. The straight-line distance between these two locations is $s = 131$ km, which corresponds to $\Delta t = 437\mu$s. Each classical agent consists of a standalone computer equipped with a FPGA and the agents are connected by an optical link (see Fig. 6.1). Synchronisation to universal time is achieved via a GPS clock. While the task of exchanging classical information is on its own quite straightforward, the challenge in our case is to take maximal advantage of the relativistic constraints. To maximise the commitment time, it is crucial to ensure that the devices are synchronised up to high accuracy and that classical data manipulation (communication with an external memory to load and store data, data exchange between the two agents and local computation) are optimised to produce the highest feasible rate.

The protocol was implemented with $n = 512$ bits, which for the two-round protocol gives the security parameter of $\varepsilon \approx 10^{-77}$ (against quantum adversaries). The multiround protocol was implemented with $m + 1 = 6$ rounds which gives the security parameter of $\varepsilon \approx 2.3 \times 10^{-10}$ (against classical adversaries). The total commitment time was 2 ms but placing exactly the same setup at the antipodes of the Earth would allow for commitment time of 212 ms. Of course, the commitment time could be made longer by employing more sophisticated hardware, which allows us to exchange more data within the relativistic constraints, but since our main goal was to demonstrate the feasibility of implementing multiround schemes we decided not to do it.

Chapter 7

Conclusions

The central theme of this thesis is the study of how communication constraints can be used in classical and quantum cryptography, with a particular focus on commitment schemes. Communication constraints resulting from fundamental physical principles (like the fact that the speed of light is finite) are of particular interest. While relativity does not permit to implement the ideal commitment functionality, some weaker variants are possible and understanding similarities and differences between these schemes lies at the heart of this thesis.

It seems fair to claim that we now have a good understanding of relativistic commitment schemes, in particular the simplest class, in which no messages are exchanged when the commitment is valid. The main drawback of such schemes is the limitation on the commitment time, which is proportional to the distance between the agents. In order to increase the length of the commitment (without moving the agents further apart) one needs to resort to multiround schemes and we have presented a particular classical protocol along with a security proof against classical adversaries. This shows that in the classical world one can achieve arbitrary long commitments even if the agents are forced to occupy a finite region of space.

A natural follow-up question is to ask whether this statement remains true in the quantum world. Security analysis of the aforementioned multiround protocol against quantum adversaries is currently out of reach but we conjecture that the protocol remains secure against quantum adversaries (although with weaker security guarantees). Moreover, security analysis of relativistic protocols against quantum adversaries leads to a new, interesting class of problems: multiplayer games with communication constraints, which have not been studied before (except for a few special cases) and might be of independent interest. Note that multiround commitment schemes against no-signalling adversaries have recently been shown to be impossible [FF15a].

Having understood the features and limitations of relativistic commitment schemes, the next step would be to look at more powerful primitives and oblivious transfer

would be a natural choice. While we know that perfect oblivious transfer is not possible, one might think of weaker variants which have not been ruled out. We do not see a straightforward way of translating distributed oblivious transfer protocols into the relativistic setting (see Section 4.1 for details) and, to the best of our knowledge, no explicitly relativistic schemes have been proposed. Investigating the possibility of relativistic oblivious transfer would constitute an important step towards characterising the exact power of quantum relativistic cryptography.

Bibliography

[Aar05] S. Aaronson. NP-complete Problems and Physical Reality. *ACM SIGACT News*, 36, 2005.
DOI: 10.1145/1052796.1052804.

[AK15a] E. Adlam and A. Kent. Deterministic Relativistic Quantum Bit Commitment. 2015.
arXiv: 1504.00943.

[AK15b] E. Adlam and A. Kent. Device-Independent Relativistic Quantum Bit Commitment. 2015.
arXiv: 1504.00944.

[ATVY00] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. C.-C. Yao. Quantum Bit Escrow. *Proc. 32nd ACM STOC*, 2000.
DOI: 10.1145/335305.335404.

[Bab85] L. Babai. Trading group theory for randomness. *Proc. 17th ACM STOC*, 1985.
DOI: 10.1145/22145.22192.

[Bab90] L. Babai. E-mail and the unexpected power of interaction. *Proc. 5th Annual Structure in Complexity Theory Conference*, 1990.
DOI: 10.1109/SCT.1990.113952.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proc. IEEE Conference on Computers, Systems and Signal Processing*, 1984.
Online: http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf.

[BBB+92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *J. Cryptology*, 5(1), 1992.
DOI: 10.1007/BF00191318.

[BBBW83] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner. Quantum cryptography, or unforgeable subway tokens. *Advances in Cryptology:*

Proc. CRYPTO '82, 1983.
DOI: 10.1007/978-1-4757-0602-4_26.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels. *Phys. Rev. Lett.*, 70(13), 1993.
DOI: 10.1103/PhysRevLett.70.1895.

[BBCS92] C. H. Bennett, G. Brassard, C. Crépeau, and M. H. Skubiszewska. Practical Quantum Oblivious Transfer. *Advances in Cryptology: Proc. CRYPTO '91, LNCS*, 576, 1992.
DOI: 10.1007/3-540-46766-1_29.

[BBM92] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum Cryptography without Bell's Theorem. *Phys. Rev. Lett.*, 68(5), 1992.
DOI: 10.1103/PhysRevLett.68.557.

[BC91] G. Brassard and C. Crépeau. Quantum Bit Commitment and Coin Tossing Protocols. *Advances in Cryptology: Proc. CRYPTO '90, LNCS*, 537, 1991.
DOI: 10.1007/3-540-38424-3_4.

[BC96] G. Brassard and C. Crépeau. Cryptology column – 25 years of quantum cryptography. *ACM SIGACT News*, 27(3), 1996.
DOI: 10.1145/235666.235669.

[BCC88] G. Brassard, D. Chaum, and C. Crépeau. Minimum Disclosure Proofs of Knowledge. *J. Comput. System Sci.*, 37(2), 1988.
DOI: 10.1016/0022-0000(88)90005-0.

[BCC+09] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. *Nat. Phys.*, 6, 2009.
DOI: 10.1038/nphys1734.

[BCF+11] H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-based quantum cryptography: impossibility and constructions. *Advances in Cryptology: Proc. CRYPTO '11, LNCS*, 6841, 2011.
DOI: 10.1007/978-3-642-22792-9_24.

[BCH+06] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner. Security of Quantum Bit String Commitment Depends on the Information

Measure. *Phys. Rev. Lett.*, 97(25), 2006.
DOI: 10.1103/PhysRevLett.97.250501.

[BCH+08] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Phys. Rev. A*, 78(2), 2008.
DOI: 10.1103/PhysRevA.78.022316.

[BCJL93] G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. *Proc. 34th IEEE FOCS*, 1993.
DOI: 10.1109/SFCS.1993.366851.

[BCMS97] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail. A brief review on the impossibility of quantum bit commitment. 1997.
arXiv: quant-ph/9712023.

[BCP+14] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner. Bell nonlocality. *Rev. Mod. Phys.*, 86(2), 2014.
DOI: 10.1103/RevModPhys.86.419.

[BCS12] H. Buhrman, M. Christandl, and C. Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Phys. Rev. Lett.*, 109(16), 2012.
DOI: 10.1103/PhysRevLett.109.160501.

[BCU+06] H. Buhrman, M. Christandl, F. Unger, S. Wehner, and A. Winter. Implications of superstrong non-locality for cryptography. *Proc. R. Soc. A*, 462, 2006.
DOI: 10.1098/rspa.2006.1663.

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1, 1964.

[Bel11] S. M. Bellovin. Frank Miller: Inventor of the One-Time Pad. *Cryptologia*, 35(3), 2011.
DOI: 10.1080/01611194.2011.583711.

[BFL91] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. *Comput. Complex.*, 1(1), 1991.
DOI: 10.1007/BF01200056.

[BFW14] M. Berta, O. Fawzi, and S. Wehner. Quantum to Classical Randomness Extractors. *IEEE Trans. Inf. Theory*, 60(2), 2014.
DOI: 10.1109/TIT.2013.2291780.

[BGKW88] M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson. Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions. *Proc. 20th ACM STOC*, 1988.
DOI: 10.1145/62212.62223.

[Bha97] R. Bhatia. *Matrix Analysis*. Springer New York, 1997.

[Bha09] R. Bhatia. *Positive Definite Matrices*. Princeton University Press, 2009.

[Blu81] M. Blum. Coin Flipping by Telephone. *Advances in Cryptology: A Report on CRYPTO '81*, 1981.
DOI: 10.1145/1008908.1008911.

[BM05] H. Buhrman and S. Massar. Causality and Tsirelson's bounds. *Phys. Rev. A*, 72(5), 2005.
DOI: 10.1103/PhysRevA.72.052103.

[BN00] D. Boneh and M. Naor. Timed Commitments. *Advances in Cryptology: Proc. CRYPTO '00, LNCS*, 1880(3), 2000.
DOI: 10.1007/3-540-44598-6_15.

[Bor26] M. Born. On The Quantum Mechanics Of Collisions. *Zeitschrift für Physik*, 37(12), 1926.

[BS98] C. H. Bennett and P. W. Shor. Quantum Information Theory. *IEEE Trans. Inf. Theory*, 44(6), 1998.
DOI: 10.1109/18.720553.

[BS15] M. Bavarian and P. W. Shor. Information Causality, Szemerédi-Trotter and Algebraic Variants of CHSH. *Proc. Conference on Innovations in Theoretical Computer Science*, 2015.
DOI: 10.1145/2688073.2688112.

[BT08] A. Broadbent and A. Tapp. Information-Theoretically Secure Voting Without an Honest Majority. *Proc. IAVoSS Workshop on Trustworthy Elections*, 2008.
arXiv: 0806.1931.

[Can01] R. Canetti. Universally Composable Security: A New Paradigm for Cryptographic Protocols. *Proc. 42nd IEEE FOCS*, 2001.
DOI: 10.1109/SFCS.2001.959888.

[CCL15] K. Chakraborty, A. Chailloux, and A. Leverrier. Arbitrarily long relativistic bit commitment. 2015.
arXiv: arXiv:1507.00239.

[CDP+13] G. Chiribella, G. M. D'Ariano, P. Perinotti, D. Schlingemann, and R. F. Werner. A short impossibility proof of quantum bit commitment. *Phys. Lett. A*, 377(15), 2013.
DOI: 10.1016/j.physleta.2013.02.045.

[CFL83] A. K. Chandra, M. L. Furst, and R. J. Lipton. Multi-party protocols. *Proc. 15th ACM STOC*, 1983.
DOI: 10.1145/800061.808737.

[Che52] H. Chernoff. A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations. *Ann. Math. Statist.*, 23, 1952.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15), 1969.
DOI: 10.1103/PhysRevLett.23.880.

[CHTW04] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and Limits of Nonlocal Strategies. *Proc. IEEE Comput. Comp. '04*, 2004.
DOI: 10.1109/CCC.2004.1313847.

[CJPPG15] T. Cooney, M. Junge, C. Palazuelos, and D. Pérez-García. Rank-one quantum games. *Comput. Complex.*, 24, 2015.
DOI: 10.1007/s00037-014-0096-x.

[CK06] R. Colbeck and A. Kent. Variable-bias coin tossing. *Phys. Rev. A*, 73(3), 2006.
DOI: 10.1103/PhysRevA.73.032320.

[CK11] A. Chailloux and I. Kerenidis. Optimal bounds for quantum bit commitment. *Proc. 52nd IEEE FOCS*, 2011.
DOI: 10.1109/FOCS.2011.42.

[CK12] S. Croke and A. Kent. Security details for bit commitment by transmitting measurement outcomes. *Phys. Rev. A*, 86(5), 2012.
DOI: 10.1103/PhysRevA.86.052309.

[Col06] R. Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2006.
arXiv: 0911.3814.

[Col07] R. Colbeck. Impossibility of secure two-party classical computation. *Phys. Rev. A*, 76(6), 2007.
DOI: 10.1103/PhysRevA.76.062308.

[Cré88] C. Crépeau. Equivalence Between Two Flavours of Oblivious Transfers. *Advances in Cryptology: Proc. CRYPTO '87, LNCS*, 293, 1988.
DOI: 10.1007/3-540-48184-2_30.

[Cré96] C. Crépeau. What is going on with Quantum Bit Commitment? *Proc. Pragocrypt '96: 1st International Conference on the Theory and Applications of Cryptology*, 1996.
Online: http://www.cs.mcgill.ca/~crepeau/PS/Cre96a.ps.

[Cré97] C. Crépeau. Efficient Cryptographic Protocols Based on Noisy Channels. *Advances in Cryptology: Proc. EUROCRYPT '97, LNCS*, 1233, 1997.
DOI: 10.1007/3-540-69053-0_21.

[Cré11] C. Crépeau. Commitment. *Encyclopedia of Security and Cryptography*, 2011.
DOI: 10.1007/978-1-4419-5906-5_239.

[CSST11] C. Crépeau, L. Salvail, J.-R. Simard, and A. Tapp. Two provers in isolation. *Advances in Cryptology: Proc. ASIACRYPT '11, LNCS*, 7073, 2011.
DOI: 10.1007/978-3-642-25385-0_22.

[Deu83] D. Deutsch. Uncertainty in Quantum Measurements. *Phys. Rev. Lett.*, 50(9), 1983.
DOI: 10.1103/PhysRevLett.50.631.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing principle and the universal quantum computer. *Proc. R. Soc. Lond. A*, 400, 1985.
DOI: 10.1098/rspa.1985.0070.

[DFR+07] I. B. Damgård, S. Fehr, R. Renner, L. Salvail, and C. Schaffner. A Tight High-Order Entropic Quantum Uncertainty Relation with Applications. *Advances in Cryptology: Proc. CRYPTO '07, LNCS*, 2007.
DOI: 10.1007/978-3-540-74143-5_20.

[DFSS05] I. B. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography In the Bounded Quantum-Storage Model. *Proc. 46th IEEE FOCS*, 2005.
DOI: 10.1109/SFCS.2005.30.

[Dir39] P. A. Dirac. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, 35(03), 1939.
DOI: 10.1017/S0305004100021162.

[DKSW07] G. M. D'Ariano, D. Kretschmann, D. Schlingemann, and R. F. Werner. Reexamination of quantum bit commitment: The possible and the impossible. *Phys. Rev. A*, 76(3), 2007.
DOI: 10.1103/PhysRevA.76.032328.

[DLTW08] A. C. Doherty, Y.-C. Liang, B. Toner, and S. Wehner. The Quantum Moment Problem and Bounds on Entangled Multi-prover Games. *Proc. IEEE Comput. Comp. '08*, 2008.
DOI: 10.1109/CCC.2008.26.

[EBH09] J. W. Eaton, D. Bateman, and S. Hauberg. *GNU Octave version 3.0.1 manual: a high-level interactive language for numerical computations*. CreateSpace Independent Publishing Platform, 2009.
Online: http://www.gnu.org/software/octave/.

[Eke91] A. K. Ekert. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett.*, 67(6), 1991.
DOI: 10.1103/PhysRevLett.67.661.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.*, 47, 1935.

[ER14] A. K. Ekert and R. Renner. The ultimate physical limits of privacy. *Nature*, 507(7493), 2014.
DOI: 10.1038/nature13132.

[Fey82] R. P. Feynman. Simulating Physics with computers. *International Journal of Theoretical Physics*, 21(6-7), 1982.
DOI: 10.1007/BF02650179.

[FF15a] S. Fehr and M. Fillinger. Multi-Prover Commitments Against Non-Signaling Attacks. *Advances in Cryptology: Proc. CRYPTO '15, LNCS*, 2015.
DOI: 10.1007/978-3-662-48000-7_20.

[FF15b] S. Fehr and M. Fillinger. On the Composition of Two-Prover Commitments, and Applications to Multi-Round Relativistic Commitments. 2015.
arXiv: 1507.00240.

[Fri12] T. Fritz. Beyond Bell's theorem: correlation scenarios. *New J. Phys.*, 14, 2012.
DOI: 10.1088/1367-2630/14/10/103001.

[Fri14] T. Fritz. Beyond Bell's Theorem II: Scenarios with arbitrary causal structure. 2014.
arXiv: 1404.4812.

[FRS94] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. *Theoretical Computer Science*, 134(2), 1994.
DOI: 10.1016/0304-3975(94)90251-8.

[Gas04] W. Gasarch. A survey on private information retrieval. *Bull. Eur. Assoc. Theor. Comput. Sci.*, 82, 2004.

[GIKM00] Y. Gertner, Y. Ishai, E. Kushilevitz, and T. Malkin. Protecting Data Privacy in Private Information Retrieval Schemes. *J. Comput. System Sci.*, 60(3), 2000.
DOI: 10.1006/jcss.1999.1689.

[GKR08] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum. One-time Programs. *Advances in Cryptology: Proc. CRYPTO '08, LNCS*, 5157, 2008.
DOI: 10.1007/978-3-540-85174-5_3.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff. The Knowledge Complexity of Interactive Proof Systems. *Proc. 17th ACM STOC*, 18(1), 1985.
DOI: 10.1137/0218012.

[GMW86] O. Goldreich, S. Micali, and A. Wigderson. Proofs that Yield Nothing But their Validity and a Methodology of Cryptographic Protocol Design. *Proc. 27th ACM STOC*, 1986.
DOI: 10.1109/SFCS.1986.47.

[Gol08] O. Goldreich. Probabilistic Proof Systems: A Primer. 2008.
Online: http://www.wisdom.weizmann.ac.il/~oded/PS/pps5.pdf.

[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. *Proc. 28th ACM STOC*, 1996.
DOI: 10.1145/237814.237866.

[GWC+14] R. Gallego, L. E. Würflinger, R. Chaves, A. Acín, and M. Navascués. Nonlocality in sequential correlation scenarios. *New J. Phys.*, 16(3), 2014.
DOI: 10.1088/1367-2630/16/3/033037.

[Hel76] C. W. Helstrom. *Quantum detection and estimation theory*. Academic Press, New York, USA, 1976.

[HK04] L. Hardy and A. Kent. Cheat Sensitive Quantum Bit Commitment. *Phys. Rev. Lett.*, 92(15), 2004.
DOI: 10.1103/PhysRevLett.92.157901.

[HM12] P. Hayden and A. May. Summoning Information in Spacetime, or Where and When Can a Qubit Be? 2012.
arXiv: 1210.0913.

[HM15] T. Heinosaari and T. Miyadera. Universality of Sequential Quantum Measurements. *Phys. Rev. A*, 022110, 2015.
DOI: 10.1103/PhysRevA.91.022110.

[Hol73] A. S. Holevo. Statistical problems in quantum physics. *Proc. 2nd Japan-USSR Symposium on Probability Theory, LNCS*, 330, 1973.
DOI: 10.1007/BFb0061483.

[KdW04] I. Kerenidis and R. de Wolf. Quantum symmetrically-private information retrieval. *Inform. Process. Lett.*, 90(3), 2004.
DOI: 10.1016/j.ipl.2004.02.003.

[Ken99] A. Kent. Unconditionally Secure Bit Commitment. *Phys. Rev. Lett.*, 83(7), 1999.
DOI: 10.1103/PhysRevLett.83.1447.

[Ken05] A. Kent. Secure Classical Bit Commitment Using Fixed Capacity Communication Channels. *J. Cryptology*, 18(4), 2005.
DOI: 10.1007/s00145-005-0905-8.

[Ken11] A. Kent. Unconditionally secure bit commitment with flying qudits. *New J. Phys.*, 13, 2011.
DOI: 10.1088/1367-2630/13/11/113015.

[Ken12a] A. Kent. Quantum tasks in Minkowski space. *Class. Quantum Grav.*, 29(22), 2012.
DOI: 10.1088/0264-9381/29/22/224013.

[Ken12b] A. Kent. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. *Phys. Rev. Lett.*, 109(13), 2012.
DOI: 10.1103/PhysRevLett.109.130501.

[Ken12c] A. Kent. Why classical certification is impossible in a quantum world. *Quant. Inf. Proc.*, 11(2), 2012.
DOI: 10.1007/s11128-011-0262-x.

[Ken13] A. Kent. A no-summoning theorem in relativistic quantum theory. *Quant. Inf. Proc.*, 12(2), 2013.
DOI: 10.1007/s11128-012-0431-6.

[Kil88] J. Kilian. Founding Cryptography on Oblivious Transfer. *Proc. 20th ACM STOC*, 1988.
DOI: 10.1145/62212.62215.

[KM02] H. Kobayashi and K. Matsumoto. Quantum Multi-prover Interactive Proof Systems with Limited Prior Entanglement. *Proc. ISAAC '02, LNCS*, 2518, 2002.
DOI: 10.1007/3-540-36136-7_11.

[KMS11] A. Kent, W. J. Munro, and T. P. Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84(1), 2011.
DOI: 10.1103/PhysRevA.84.012326.

[KTHW13] J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner. Secure Bit Commitment From Relativistic Constraints. *IEEE Trans. Inf. Theory*, 59(7): 4687–4699, 2013.
DOI: 10.1109/TIT.2013.2247463.

[KWW12] R. König, S. Wehner, and J. Wullschleger. Unconditional Security From Noisy Quantum Storage. *IEEE Trans. Inf. Theory*, 58(3), 2012.
DOI: 10.1109/TIT.2011.2177772.

[LC97] H.-K. Lo and H. Chau. Is Quantum Bit Commitment Really Impossible? *Phys. Rev. Lett.*, 78(17), 1997.
DOI: 10.1103/PhysRevLett.78.3410.

[LCC+14] Y. Liu, Y. Cao, M. Curty, S. K. Liao, J. Wang, K. Cui, Y. H. Li, Z. H. Lin, Q. C. Sun, D. D. Li, H. F. Zhang, Y. Zhao, T. Y. Chen, C. Z. Peng, Q. Zhang, A. Cabello, and J. W. Pan. Experimental unconditionally secure bit commitment. *Phys. Rev. Lett.*, 112(1), 2014.
DOI: 10.1103/PhysRevLett.112.010504.

[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. *Phys. Rev. Lett.*, 111(18), 2013.
DOI: 10.1103/PhysRevLett.111.180504.

[LKB+15] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden. Practical Relativistic Bit Commitment. *Phys. Rev. Lett.*, 115(3), 2015.
DOI: 10.1103/PhysRevLett.115.030502.

[Lo97] H.-K. Lo. Insecurity of Quantum Secure Computations. *Phys. Rev. A*, 56(2), 1997.
DOI: 10.1103/PhysRevA.56.1154.

[LWW+10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Phot.*, 4(686), 2010.
DOI: 10.1038/NPHOTON.2010.214.

[Mal00] T. Malkin. *A Study of Secure Database Access and General Two-Party Computation*. PhD thesis, Massachusetts Institute of Technology, 2000.

[Mau91] U. M. Maurer. A Provably-Secure Strongly-Randomized Cipher. *Advances in Cryptology: Proc. EUROCRYPT '90, LNCS*, 473, 1991.
DOI: 10.1007/3-540-46877-3_33.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17), 1997.
DOI: 10.1103/PhysRevLett.78.3414.

[MHH+97] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. "Plug and play" systems for quantum cryptography. *App. Phys. Lett.*, 70(793), 1997.
DOI: 10.1063/1.118224.

[MM07] G. L. Mullen and C. Mummert. *Finite Fields and Applications*. Amer. Math. Soc., 2007.

[Moc07] C. Mochon. Quantum weak coin flipping with arbitrarily small bias. 2007.
arXiv: 0711.4114.

[MU88] H. Maassen and J. B. M. Uffink. Generalized Entropic Uncertainty Relations. *Phys. Rev. Lett.*, 60(12), 1988.
DOI: 10.1103/PhysRevLett.60.1103.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[NP00] M. Naor and B. Pinkas. Distributed Oblivious Transfer. *Advances in Cryptology: Proc. ASIACRYPT '00, LNCS*, 2000.
DOI: 10.1007/3-540-44448-3_16.

[NPA07] M. Navascués, S. Pironio, and A. Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98(1), 2007.
DOI: 10.1103/PhysRevLett.98.010401.

[PR94] S. Popescu and D. Rohrlich. Quantum Nonlocality as an Axiom. *Foundations of Physics*, 24(3), 1994.
DOI: 10.1007/BF02058098.

[RG15] J. Ribeiro and F. Grosshans. A Tight Lower Bound for the BB84-states Quantum-Position-Verification Protocol. 2015.
arXiv: 1504.07171.

[Riv99] R. L. Rivest. Unconditionally Secure Commitment and Oblivious Transfer Schemes Using Private Channels and a Trusted Initializer. 1999.
Online: http://people.csail.mit.edu/rivest/pubs/Riv99d.pdf.

[RKKM14] I. Radchenko, K. Kravtsov, S. Kulik, and S. N. Molotkov. Relativistic quantum cryptography. *Laser Phys. Lett.*, 11, 2014.
DOI: 10.1088/1612-2011/11/6/065203.

[RUV13] B. W. Reichardt, F. Unger, and U. Vazirani. Classical command of quantum systems. *Nature*, 496(7446), 2013.
DOI: 10.1038/nature12035.

[RV13] O. Regev and T. Vidick. Quantum XOR games. *Proc. IEEE Comput. Comp. '13*, 2013.
DOI: 10.1109/CCC.2013.23.

[Sal98] L. Salvail. Quantum Bit Commitment From a Physical Assumption. *Advances in Cryptology: Proc. CRYPTO '98, LNCS*, 1462, 1998.
DOI: 10.1007/BFb0055740.

[Sca12] V. Scarani. The device-independent outlook on quantum physics. *Acta Phys. Slov.*, 62(4), 2012.
arXiv: 1303.3081.

[Sch95] B. Schumacher. Quantum coding. *Phys. Rev. A*, 51(4), 1995.
DOI: 10.1103/PhysRevA.51.2738.

[Sch10] C. Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Phys. Rev. A*, 82(3), 2010.
DOI: 10.1103/PhysRevA.82.032308.

[SCK14] J. Sikora, A. Chailloux, and I. Kerenidis. Strong connections between quantum encodings, nonlocality, and quantum cryptography. *Phys. Rev. A*, 89(2), 2014.
DOI: 10.1103/PhysRevA.89.022334.

[Sha48] C. E. Shannon. A Mathematical Theory of Communication. *Bell System Technical Journal*, 27(3-4), 1948.
DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[Sha49] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 28(4), 1949.
DOI: 10.1002/j.1538-7305.1949.tb00928.x.

[Sho94] P. W. Shor. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Proc. 35th ACM STOC*, 1994.
DOI: 10.1109/SFCS.1994.365700.

[Sim07] J.-R. Simard. *Classical and Quantum Strategies for Bit Commitment Schemes in the Two-Prover Model*. Master's thesis, McGill University, 2007.
Online: http://crypto.cs.mcgill.ca/~crepeau/PDF/memoire-JR.pdf.

[SR01] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Phys. Rev. A*, 65, 2001.
DOI: 10.1103/PhysRevA.65.012310.

[SR02] R. W. Spekkens and T. Rudolph. Quantum Protocol for Cheat-Sensitive Weak Coin Flipping. *Phys. Rev. Lett.*, 89(22), 2002.
DOI: 10.1103/PhysRevLett.89.227901.

[TFKW13] M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New J. Phys.*, 15(10), 2013.
DOI: 10.1088/1367-2630/15/10/103002.

[Tom12] M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zurich, 2012.
arXiv: 1203.2142.

[TR11] M. Tomamichel and R. Renner. Uncertainty Relation for Smooth Entropies. *Phys. Rev. Lett.*, 106(11), 2011.
DOI: 10.1103/PhysRevLett.106.110506.

[Tsi80] B. S. Tsirelson. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.*, 4(2), 1980.
DOI: 10.1007/BF00417500.

[Uhl76] A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.*, 9(2), 1976.
DOI: 10.1016/0034-4877(76)90060-4.

[Unr14] D. Unruh. Quantum Position Verification in the Random Oracle Model. *Advances in Cryptology: Proc. CRYPTO '14, LNCS*, 8617, 2014.
DOI: 10.1007/978-3-662-44381-1_1.

[Vid13] T. Vidick. Three-player entangled XOR games are NP-hard to approximate. *Proc. 54th IEEE FOCS*, 2013.
DOI: 10.1109/FOCS.2013.87.

[Weh06] S. Wehner. Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. *Phys. Rev. A*, 73, 2006.
DOI: 10.1103/PhysRevA.73.022110.

[Wer89] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40(8), 1989.
DOI: 10.1103/PhysRevA.40.4277.

[Wie83] S. Wiesner. Conjugate coding. *ACM SIGACT News*, 15(1), 1983.
DOI: 10.1145/1008908.1008920.

[Wil13] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

[WNI03] A. Winter, A. C. A. Nascimento, and H. Imai. Commitment Capacity of Discrete Memoryless Channels. *Cryptography and Coding, LNCS*, 2898, 2003.
DOI: 10.1007/978-3-540-40974-8_4.

[WST08] S. Wehner, C. Schaffner, and B. Terhal. Cryptography from Noisy Storage. *Phys. Rev. Lett.*, 100(22), 2008.
DOI: 10.1103/PhysRevLett.100.220502.

[WTHR11] S. Winkler, M. Tomamichel, S. Hengl, and R. Renner. Impossibility of growing quantum bit commitments. *Phys. Rev. Lett.*, 107(9), 2011.
DOI: 10.1103/PhysRevLett.107.090502.

[WWW11] S. Winkler, J. Wullschleger, and S. Wolf. Bit Commitment From Nonsignaling Correlations. *IEEE Trans. Inf. Theory*, 57(3), 2011.
DOI: 10.1109/TIT.2011.2104471.

[WŻ82] W. K. Wootters and W. H. Żurek. A single quantum cannot be cloned. *Nature*, 299(5886), 1982.
DOI: 10.1038/299802a0.

[Yao82] A. C.-C. Yao. Protocols for secure computations. *Proc. 23rd IEEE FOCS*, 1982.
DOI: 10.1109/SFCS.1982.38.

[Yao95] A. C.-C. Yao. Security of Quantum Protocols Against Coherent Measurements. *Proc. 27th ACM STOC*, 1995.
DOI: 10.1145/225058.225085.

Appendix A

Classical certification of relativistic bit commitment

In 1992 Bennett et al. proposed how to construct oblivious transfer by combining bit commitment with quantum communication [BBCS92]. This was later formalised and proven secure by Yao [Yao95], who refers to it as "the canonical construction". At that point the quantum bit commitment protocol by Brassard et al. [BCJL93] was considered secure so the canonical construction uses it as a black box. While quantum bit commitment was later proven impossible, the canonical construction remains interesting because classically we do not know whether bit commitment can be used to implement oblivious transfer.

Attempts to use relativistic commitment schemes in the canonical construction led to some interesting insight. It turns out that the construction implicitly assumes a certain property of the commitment scheme known as *classical certification*, which in the quantum world should not be taken for granted. In fact, Kent showed that classical certification is generally impossible in case of quantum protocols [Ken12c].

In this appendix we show that classical certification is not determined solely by the protocol but depends also on the exact power of the adversary. More specifically, we show that the (classical relativistic) `sBGKW` scheme is classically-certifiable against classical adversaries but not against quantum adversaries. We discuss why lack of classical certification completely breaks the canonical construction and present an explicit cheating strategy.

A.1 Classical certification of the `sBGKW` scheme

Classical certification should be thought of as a stronger variant of the binding property and to make this connection clear we call it the *strongly-binding property*. Since the goal here is to flesh out the difference between the two notions and we al-

ready have a particular example in mind, we use definitions tailored to that concrete scenario. For completeness, let us restate the protocol first.

Protocol 4: `Simplified-BGKW`

1. (commit) Bob sends $y_1 = b$ to Alice$_1$ and she replies with $x_1 = d \cdot y_1 \oplus a$.
2. (open) Alice$_2$ reveals $x_2 = a$ to Bob.
3. (verify) Bob verifies that $x_1 \oplus x_2 = d \cdot b$.

Note that no communication is required between the commitment point and the opening point (so the two are operationally equivalent) and that only Alice$_2$ is involved in the open phase.

DEFINITION A.1. *Let $\sigma_{A_1A_2B}$ be a state that Alice$_1$ and Alice$_2$ can enforce at the commitment point and let $(\Phi^0_{A_2\to P}, \Phi^1_{A_2\to P})$ be opening maps performed by Alice$_2$.*

*A multiagent bit commitment protocol is ε-**binding** if for all states and all maps we have*

$$p_0 + p_1 \leq 1 + \varepsilon,$$

where

$$p_d = \mathrm{tr}\left(M_{\mathrm{accept}}\left[\Phi^d_{A_2\to P}(\sigma_{A_2B})\right]\right).$$

*A multiagent bit commitment protocol is ε-**strongly-binding** if every state $\sigma_{A_1A_2B}$ can be supplemented by a binary random variable D*

$$\sigma_{DA_1A_2B} = |0\rangle\langle 0|_D \otimes \sigma^0_{A_1A_2B} + |1\rangle\langle 1|_D \otimes \sigma^1_{A_1A_2B}$$

such that the subnormalised states $\sigma^d_{A_1A_2B}$ satisfy

$$\mathrm{tr}\left(M_{\mathrm{accept}}\left[\Phi^d_{A_2\to P}(\sigma^d_{A_2B})\right]\right) \leq \varepsilon \tag{A.1}$$

for $d \in \{0, 1\}$.

Intuitively, the random variable D tells us which value Alice$_2$ cannot unveil. More precisely, inequality (A.1) states that the probability of $D = d$ *and* Bob accepting the unveiling of d is at most ε. As the random variable D could be given to an external observer, it captures the notion that the commitment has an objective value, which is beyond Alice's influence. It is a simple exercise to show that every protocol which is ε-strongly-binding is also ε-binding.

In Chapter 6 we showed that Protocol 4 is ε-binding with

$$\varepsilon = 2^{-n} \qquad \text{(against classical adversaries)},$$
$$\varepsilon = \sqrt{2} \cdot 2^{-n/2} \quad \text{(against quantum adversaries)}.$$

While there is clearly a quantitative difference, qualitatively the situation is the same: in both cases the protocol is secure and the security guarantee decays exponentially in n.

The situation turns out to be quite different when we consider the stronger definition. We start by showing that Protocol 4 is ε-strongly-binding with $\varepsilon = 2^{-n/2}$ against classical adversaries. However, we then prove that against quantum adversaries, the protocol does not satisfy the strongly-binding definition for any $\varepsilon < \frac{1}{4}$ regardless of how large n is.

To show that the protocol is strongly-binding in the classical case we explicitly construct the random variable D. It suffices to provide a construction for deterministic strategies of Alice (any non-deterministic strategy can be written as a convex combination of deterministic strategies). The deterministic strategy of Alice_1 is a function $f : \{0,1\}^n \to \{0,1\}^n$, while for Alice_2 we have $g : \{0,1\} \to \{0,1\}^n$, where the argument of g is the value d that she is trying to unveil. Then, the condition for successfully unveiling d becomes

$$f(b) \oplus g(d) = d \cdot b.$$

PROPOSITION A.1. *Protocol 4 is ε-strongly-binding against classical adversaries with $\varepsilon = 2^{-n/2}$.*

Proof. Under the assumption that Alice_1 and Alice_2 behave deterministically the state of the protocol at the commitment point is completely described by two variables: b and $f(b)$, which can be used to define the random variable D. For $c \in \{0,1\}^n$ let

$$\mathcal{S}(c) := \{b \in \{0,1\}^n : f(b) = c\}$$

and

$$\mathcal{T}_0 := \{c \in \{0,1\}^n : |\mathcal{S}(c)| \leq 2^{n/2}\},$$
$$\mathcal{T}_1 := \{c \in \{0,1\}^n : |\mathcal{S}(c)| > 2^{n/2}\}.$$

Note that $|\mathcal{T}_1| < 2^{n/2}$ since

$$2^n = \sum_c |\mathcal{S}(c)| \geq \sum_{c \in \mathcal{T}_1} |\mathcal{S}(c)| > 2^{n/2} \sum_{c \in \mathcal{T}_1} 1 = 2^{n/2} |\mathcal{T}_1|.$$

We define the random variable D as a deterministic function of b

$$D := \begin{cases} 0 & \text{if } f(b) \in \mathcal{T}_0, \\ 1 & \text{if } f(b) \in \mathcal{T}_1. \end{cases}$$

Now we check that this definition satisfies the conditions. For $D = 0$ we have

$$\begin{aligned} \Pr[D = 0 \wedge \text{unveil } 0] &= \Pr[D = 0 \wedge f(b) \oplus g(0) = 0^n] \\ &= 2^{-n} |\{b \in \{0,1\}^n : f(b) \in \mathcal{T}_0 \wedge f(b) = g(0)\}| \\ &= 2^{-n} |\{b \in \{0,1\}^n : g(0) \in \mathcal{T}_0 \wedge f(b) = g(0)\}| \\ &= 2^{-n} \left|\mathcal{S}\big(g(0)\big)\right| \cdot I[g(0) \in \mathcal{T}_0] \leq 2^{-n} 2^{n/2} = 2^{-n/2}, \end{aligned}$$

where $I[\cdot]$ denotes the indicator function[1]. For $D = 1$ we have

$$\begin{aligned} \Pr[D = 1 \wedge \text{unveil } 1] &= \Pr[D = 1 \wedge f(b) \oplus g(1) = b] \\ &= 2^{-n} |\{b \in \{0,1\}^n : f(b) \in \mathcal{T}_1 \wedge f(b) \oplus g(1) = b\}| \\ &= 2^{-n} \sum_{c \in \mathcal{T}_1} |\{b \in \{0,1\}^n : f(b) = c \wedge f(b) \oplus g(1) = b\}| \\ &\leq 2^{-n} \sum_{c \in \mathcal{T}_1} |\{b \in \{0,1\}^n : c \oplus g(1) = b\}| \\ &\leq 2^{-n} \sum_{c \in \mathcal{T}_1} 1 = 2^{-n} |\mathcal{T}_1| < 2^{-n} \cdot 2^{n/2} = 2^{-n/2}. \end{aligned}$$

□

To prove that this stronger notion of security is not possible in the quantum case, we propose an explicit attack and show that the resulting state cannot be supplemented by an additional random variable satisfying the criteria.

PROPOSITION A.2. *Protocol 4 does not satisfy the ε-strongly-binding property against quantum adversaries for any $\varepsilon < \frac{1}{4}$.*

Proof. Suppose that at the beginning of the protocol Alice_1 and Alice_2 share the maximally entangled state of $2n$ qubits

$$|\Psi_{2^n}\rangle_{A_1 A_2} = 2^{-n/2} \sum_x |x\rangle_{A_1} |x\rangle_{A_2}.$$

Let C be an auxiliary control register held by Alice_1, initially prepared in the state

[1] The indicator function is defined to satisfy $I[\text{true statement}] = 1$ and $I[\text{false statement}] = 0$.

$|+\rangle$. When Alice$_1$ receives b, she applies the following unitary $U^b_{A_1C}$

$$\begin{aligned} U^b_{A_1C}|x\rangle_{A_1}|0\rangle_C &= |x\rangle_{A_1}|0\rangle_C, \\ U^b_{A_1C}|x\rangle_{A_1}|1\rangle_C &= |x\oplus b\rangle_{A_1}|1\rangle_C. \end{aligned} \tag{A.2}$$

Then, the tripartite state $|\psi\rangle_{A_1A_2C}$ becomes

$$\begin{aligned} |\psi\rangle_{A_1A_2C} &= (U^b_{A_1C}\otimes \mathbb{1}_{A_2})|\Psi_{2^n}\rangle_{A_1A_2}|+\rangle_C \\ &= 2^{-(n+1)/2}\Big[\sum_x |x\rangle_{A_1}|x\rangle_{A_2}|0\rangle_C + \sum_x |x\oplus b\rangle_{A_1}|x\rangle_{A_2}|1\rangle_C\Big] \\ &= 2^{-(n+1)/2}\Big[\sum_x |x\rangle_{A_1}|x\rangle_{A_2}|0\rangle_C + \sum_x |x\rangle_{A_1}|x\oplus b\rangle_{A_2}|1\rangle_C\Big] \\ &= 2^{-(n+1)/2}\sum_x |x\rangle_{A_1}\Big[|x\rangle_{A_2}|0\rangle_C + |x\oplus b\rangle_{A_2}|1\rangle_C\Big]. \end{aligned}$$

Now, Alice$_1$ measures A_1 in the computational basis to obtain a classical random variable X_1 and it is easy to verify that the state $\sigma_{X_1A_2C}$ is

$$\sigma_{X_1A_2C} = 2^{-n}\sum_x |x\rangle\langle x|_{X_1}\otimes|\alpha_{x,b}\rangle\langle\alpha_{x,b}|_{A_2C},$$

where

$$|\alpha_{x,b}\rangle_{A_2C} = \frac{1}{\sqrt{2}}\big(|x\rangle_{A_2}|0\rangle_C + |x\oplus b\rangle_{A_2}|1\rangle_C\big).$$

Recall that b is drawn uniformly at random by Bob and we should explicitly include it in the state. The state $\sigma_{X_1BA_2C}$ represents a complete description of the state of the protocol at the commitment point

$$\sigma_{X_1BA_2C} = 2^{-2n}\sum_{x,b} |x\rangle\langle x|_{X_1}\otimes|b\rangle\langle b|_B\otimes|\alpha_{x,b}\rangle\langle\alpha_{x,b}|_{A_2C}.$$

Our goal now is to show that regardless of how we define the auxiliary random variable D, it will not meet the desired criteria. The most general form of the state with the additional random variable is

$$\sigma_{DX_1BA_2C} = \sum_{d,x,b} |d\rangle\langle d|_D\otimes|x\rangle\langle x|_{X_1}\otimes|b\rangle\langle b|_B\otimes\sigma^{dxb}_{A_2C},$$

where $\sigma^{dxb}_{A_2C}$ are subnormalised quantum states. However, since tracing out D must give us back $\sigma_{X_1BA_2C}$ and the states on A_2C (conditional on particular values of X_1 and B) are pure, we conclude that for all d, x, b

$$\sigma^{dxb}_{A_2C} \propto |\alpha_{x,b}\rangle\langle\alpha_{x,b}|_{A_2C}.$$

Therefore, without loss of generality we can write

$$\sigma_{DX_1BA_2C} = \sum_{d,x,b} p_{dxb} |d\rangle\langle d|_D \otimes |x\rangle\langle x|_{X_1} \otimes |b\rangle\langle b|_B \otimes |\alpha_{x,b}\rangle\langle\alpha_{x,b}|_{A_2C},$$

where $p_{dxb} = \Pr[D = d, X_1 = x, B = b]$ is a probability distribution over D, X_1 and B. Now, we need to evaluate the probability of Alice_2 unveiling the commitment successfully. Since Alice_1 does not play a role in the open phase, we trace out subsystem C. The unveiling strategy of Alice_2 is simply to measure her subsystem in the computational basis (regardless of the value she is trying to unveil). If we represent her measurement outcome by X_2 we obtain the following (fully classical) state

$$\sigma_{DX_1BX_2} = \sum_{d,x,b} p_{dxb} |d\rangle\langle d|_D \otimes |x\rangle\langle x|_{X_1} \otimes |b\rangle\langle b|_B \otimes \frac{1}{2}\big(|x\rangle\langle x|_{X_2} + |x \oplus b\rangle\langle x \oplus b|_{X_2}\big).$$

This allows us to evaluate the

$$\begin{aligned}
\Pr[D = d \wedge \text{unveil d}] &= \Pr[D = d \wedge X_1 \oplus X_2 = d \cdot B] \\
&= \sum_{xb} \frac{p_{dxb}}{2}\big(1 + I[b = 0]\big) \\
&\geq \frac{1}{2}\sum_{xb} p_{dxb} = \frac{1}{2}\Pr[D = d].
\end{aligned}$$

Since $\Pr[D = 0] + \Pr[D = 1] = 1$, we must have $\Pr[D = d \wedge \text{unveil d}] \geq \frac{1}{4}$ for at least one value of d. Hence, the security requirement cannot hold for any $\varepsilon < \frac{1}{4}$. □

It is clear that register C determines the commitment value and if C was a classical register the protocol would satisfy the strongly-binding definition. However, since C is a quantum register kept in a coherent superposition, it does not have a well-defined value. We cannot think of the value of the commitment as a classical random variable and no meaningful definition of D is possible. In the next section we show that this feature makes the scheme unsuitable for the canonical construction.

A.2 Consequences for the canonical construction

The canonical construction requires Bob to generate random BB84 states and send them to Alice, who measures every incoming state in a random basis (computational or Hadamard). After all the states have been measured Bob announces the basis he used for every state. If Alice has followed the protocol she has learnt (on average) half of the (logical) bits. Note that Bob does not know which bits she has learnt.

An obvious problem with this construction comes from the fact that Alice can

store the quantum states and only measure them once the basis information is available. In this way she will learn the entire string, which renders the scheme completely insecure.

To defeat this cheating strategy Alice is required to prove that she has really measured all the systems by making a certain commitment. More specifically, for every received BB84 state she is required to commit two bits: the basis used and the outcome observed.

Later Bob asks Alice to open commitments corresponding to a random subset of the rounds. He expects that whenever she claims to have measured in the correct basis, she should have obtained the correct outcome. Classical intuition tells us that if Alice succeeds on a randomly chosen subset, then the other commitments (with high probability) must also correspond to honest measurements. In that case we conclude that she has followed the protocol, the BB84 states have been measured so the attack described above is no longer a threat.

The classical intuition implicitly assumes that the commitments contain specific values, which are well-defined regardless of whether the commitment is ultimately opened or not. This is exactly the notion of classical certification, which is generally not satisfied in the quantum setting. Here, we show that if the `sBGKW` scheme is used in the construction, there exists a quantum cheating strategy for Alice with the following two properties.

- If Alice is challenged to open the commitment, she can produce statistics indistinguishable from the honest execution of the protocol.

- If the commitment is not opened and Alice_1 and Alice_2 are allowed to recombine their systems, they can recover the original BB84 states.

Let $|\phi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ be the state that Alice_1 has received from Bob and suppose she stores it in register C. Alice_1 picks the measurement basis $\theta \in \{0, 1\}$ uniformly at random and makes an honest commitment to it. If $\theta = 0$ she leaves $|\phi\rangle$ unchanged, if $\theta = 1$ she applies a Hadamard transform to it. For simplicity in the following argument we assume $\theta = 0$ (the case of $\theta = 1$ is analogous). For the second commitment (to the outcome of the measurement) Alice_1 follows the dishonest procedure outlined in the previous section and it is easy to verify that at the commitment point the state is

$$\sigma_{X_1 A_2 C} = 2^{-n} \sum_x |x\rangle\langle x|_{X_1} \otimes |\alpha'_{x,b}\rangle\langle\alpha'_{x,b}|_{A_2 C},$$

where

$$|\alpha'_{x,b}\rangle_{A_2 C} = \alpha_0|x\rangle_{A_2}|0\rangle_C + \alpha_1|x \oplus b\rangle_{A_2}|1\rangle_C. \tag{A.3}$$

If Alice$_2$ is challenged to unveil this round, she honestly unveils the basis information ($\theta = 0$), while for the second commitment she simply measures her system in the computational basis and obtains the correct string to unveil d with probability at least $|\alpha_d|^2$. It is easy to see that identical statistics would be obtained if Alice$_1$ made a measurement in the computational basis at the beginning and honestly committed to the classical outcome. Picking $\theta \in \{0, 1\}$ uniformly at random leads to statistics which is indistinguishable from honestly measuring in a random basis.

On the other hand, if the commitment is not opened we can still recover the original state. Conditional on $X_1 = x$ and $B = b$ the state on A_2C is $|\alpha'_{x,b}\rangle_{A_2C}$ given by Eq. (A.3). Note that C is with Alice$_1$ while A_2 is with Alice$_2$ but if we bring the systems together we can apply a unitary $U^b_{A_2C}$ (as in Eq. (A.2) except that it acts on A_2 instead of A_1) to obtain

$$U^b_{A_2C}|\alpha'_{x,b}\rangle_{A_2C} = \alpha_0|x\rangle_{A_2}|0\rangle_C + \alpha_1|x\rangle_{A_2}|1\rangle_C = |x\rangle_{A_2} \otimes |\phi\rangle_C.$$

Therefore, we have recovered the original state.

It is interesting to note that in this procedure the state $|\phi\rangle$ received by Alice$_1$ becomes "delocalised" between Alice$_1$ and Alice$_2$ at the commitment point. In other words, Alice$_1$ cannot recover it by acting on her own subsystem alone. This is not surprising as Alice$_1$ through the procedure has in some sense allowed Alice$_2$ to remotely perform a measurement on $|\phi\rangle$ so in order to reconstruct it we must combine the two systems together.

Since in the relativistic setting all communication constraints are temporary we cannot prohibit Alice$_1$ and Alice$_2$ from recovering the original state at some later point and once the basis information is available, they will perform the right measurement to obtain the correct outcome. Therefore, no uncertainty can be guaranteed on the rounds that have not been opened, which renders the construction completely insecure.

Index