Classical and quantum strategies for bit commitment schemes in the two-prover model

Jean-Raymond Simard

School of Computer Science

McGill University
Montréal, Québec
February 2007

A thesis submitted to McGill University in partial fulfilment of the requirements of the degree of Master of Science

Your file Votre référence
ISBN: 978-0-494-32783-8
Our file Notre référence
ISBN: 978-0-494-32783-8

Remerciements

Je tiens à remercier Claude Crépeau, mon superviseur, pour son soutien, sa confiance et tout le temps qu'il m'a consacré. Merci à Louis Salvail et Alain Tapp, sans qui cette recherche n'aurait probablement pas avancée si vite. Un gros merci à Simon Pierre Desrosiers, pour l'incroyable travail de correction qu'il a fait sur ce travail, ainsi que pour toutes les savoureuses discussions que nous avons eues. Merci à tous ceux qui m'ont appuyé jusqu'ici, spécialement ma famille, mes amis et professeurs. Finalement, merci à ma copine, Audrey Desautels, pour tout l'encouragement, les petits mots et tous les beaux moments passés avec moi à essayer de comprendre ce que je racontais.

Merci aussi au Conseil de recherches en sciences naturelles et en génie du Canada, et aux Fonds québécois de la recherche sur la nature et les technologies, pour m'avoir soutenu financièrement durant ces deux années.

Abstract

We show that the long-standing assumption of "no-communication" between the provers of the two-prover model is not sufficiently precise to guarantee the security of a bit commitment scheme against malicious adversaries. Indeed, we show how a simple correlated random variable, which does not allow to communicate, can be used to cheat a simplified version (sBGKW) of the bit commitment scheme of Ben-Or, Goldwasser, Kilian, and Wigderson [BGKW88]. Instead we propose a stronger notion of separation between the two provers which takes into account correlated computations. To emphasize the risk that entanglement still represents for the security of a commitment scheme despite the stronger notion of separation, we present two variations of the sBGKW scheme that can be cheated by quantum provers with probability (almost) one. A complete proof of security against quantum adversaries is then given for the sBGKW scheme. By reduction we also obtain the security of the original BGKW scheme against quantum provers. For the unfamiliar reader, basic notions of quantum processing are provided to facilitate the understanding of the proofs presented.

Résumé

Dans ce mémoire, nous montrerons que l'hypothèse traditionnelle d'impossibilité de communication faite dans le modèle à deux proveurs n'est pas suffisamment précise pour garantir la sécurité d'un protocole de mise en gage contre des prouveurs malhonnêtes. Nous montrerons comment une variable aléatoire corrélée, ne permettant pas de communiquer, peut être utilisée pour tricher une version simplifiée (sBGKW) du protocole de mise en gage de Ben-Or, Goldwasser, Kilian, and Wigderson [BGKW88]. Pour résoudre ce problème, nous proposerons une notion de séparation entre les deux prouveurs beaucoup plus forte que l'hypothèse traditionnelle. Afin de mettre en évidence le risque que constitue l'intrication pour la sécurité d'un protocole de mise en gage, nous présenterons deux variations du protocole sBGKW qui peuvent être triché par des prouveurs quantiques avec probabilité (presque) un. Une démonstration détaillée de la sécurité quantique du protocole sBGKW sera ensuite donnée. La sécurité quantique du protocole original de BGKW sera ensuite obtenue par réduction. Un bref aperçu des notions de bases d'informatique quantique sera proposé en introduction pour faciliter la compréhension des démonstrations présentées dans ce mémoire.

Contents

Introduction

The two-prover model

The two-prover model, and its generalized version with k provers, was first introduced by Ben-Or, Goldwasser, Kilian, and Wigderson [BGKW88] to prove that all NP languages have a two-prover perfect zero-knowledge interactive proof-system, without having to make intractability assumptions, such as the existence of *one-way functions* used in [GMW86] which is necessary to prove a similar result in the one-prover model. At the time, their result was of great importance since such a general statement was known to be impossible in the one-prover model, unless the polynomial-time hierarchy collapsed [For87].

Loosely speaking, an *interactive proof-system* (IPS) consists of an all powerful prover who attempts to convince a probabilistic polynomial-time bounded verifier of the truth of a proposition [GMR85]. It is termed *perfect zero-knowledge* if there exists a prover such that for any verifier there exists a stand-alone polynomial-time simulator, not interacting with anybody, whose output has the same probability distribution as the output produced by the verifier after interacting with the prover. That is, whatever can be efficiently extracted from the interaction with the prover when input a proposition, can also be efficiently extracted from the proposition itself.

Using the formalism of IPS, the setting of the two-prover model consists of two provers, Peggy and Paula, sometime taken to be computationally unbounded, who jointly agree on a strategy to convince the verifier, Vic, of the truth of an assertion under the constraint

that Peggy and Paula cannot communicate with each other once the interaction with Vic has started. This no-communication limitation is the key point which allows Vic to decide whether he should accept or not the proposition. We stress that the two-prover model is defined as a *synchronous model.* This means that, although no prover can get the content of the conversations between Vic and the other prover, a prover can see that messages are exchanged between the other two participants. The model may be depicted as in Figure 1.

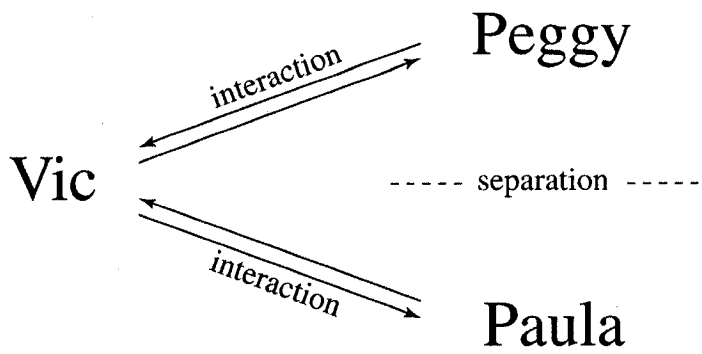

Figure 1: The two-prover model

The authors of [BGKW88] give a particularly enlightening example to illustrate the power of the two-prover model, as they note:

> *"The main novelty of our model is that the verifier can "check" its interactions with the provers "against each other". One may think of this as the process of checking the alibi of two suspects of a crime (who have worked long and hard to prepare a joint alibi), where the suspects are the provers and the verifier is the interrogator. The interrogator's conviction that the alibi is valid stems from his conviction that once the interrogation starts, the suspects can not talk to each other as they are kept in separate rooms, and since they can not anticipate the randomized questions he may ask them, he can trust his findings."*

From then on, the two-prover model has been extensively studied and numerous fundamental results in the theory of computation were found. A few years after BGKW's

results, Babai, Fortnow and Lund [BFL90] used the same model to prove that every language is in NEXP (the *non-deterministic exponential-time* complexity class) if and only if it has a many-rounds perfect zero-knowledge two-prover IPS. This result was in sharp contrast to what was previously expected since Fortnow, Rompel, and Sipser [FRS94] had shown that relative to some oracle, even the class coNP did not have a multi-prover IPS. Several refinements of [BFL90]'s result were then made [CCL90, Fei91, LS91], until Feige and Lovász [FL92] proved that a language is in NEXP if and only if it has a two-prover one-round interactive proof system with perfect completeness (if a word is in the language than the verifier always accepts) and exponentially small soundness error (if a word is not in the language than the probability of accepting it is exponentially small). This last result closed the subject on which complexity class may be achieved in the two-prover model with classical provers.

In the quantum case, the situation is filled with fuzziness. To this day, it is still not known which complexity class may be achieved with an IPS in a two-quantum-prover against a quantum-verifier situation. One promising way to tackle the problem is by first considering *one-round* IPS with a classical verifier. This means that the interaction between the verifier and a prover is limited to one round: a query and an answer. Notice that Feige and Lovász [FL92] used the classical flavor of this setting to prove their result. This special case of the two-prover model is particularly interesting to us as it corresponds to the setting of the so-called *non-local games* (see Section 1.3). Naturally, a good understanding of such games will help determine what happens when the provers share entanglement. Recently Cleve, Høyer, Toner and Watrous investigated this subject [CHTW04] from the point of view of non-locality and made clear connections with multi-prover IPS. They gave various examples of one-round multi-prover IPS which are classically sound but where entanglement seriously affects the soundness of the proof system. They also looked at the amount of entanglement required by optimal and nearly optimal quantum strategies for these games. More specifically, they showed why the known protocol which equates NEXP to the two-prover IPS breaks down if the provers can share entanglement, unless EXP=NEXP.

We claimed in the previous paragraph that it is not known which class may be achieved in a two-quantum-prover against a quantum-verifier situation. This is not completely true. For a restricted case, when the provers share only a polynomial number of qubits, it has been demonstrated by Kobayashi and Matsumoto [KM03] that the class of languages accepted by a two-prover IPS is included in NEXP. Whether the two classes are equal is still an open problem. Recently, Gavinsky [Gav06] gave a partial converse to the result of [KM03] using a new approach for bounding entanglement, and the parallel repetition theorem of [Raz95] for improving the soundness of a known classical two-prover IPS which accepts NEXP. He showed that in order to cheat, the provers require a number of entangled qubits asymptotically close to the number of parallel repetitions. Thus, by bounding the amount of shared qubits by some *a priori* fixed polynomial in the input length[1], enough repetitions can be introduced to make any cheating impossible. Formally,

Theorem [Gav06]: *Let $MIP^*_{poly(n)}$ be the model of two-prover IPS when the provers are allowed to share any entangled state over $poly(n)$ qubits, where n is the input length of the problem. Then $MIP^*_{poly(n)}$ can accept a language L if and only if $L \in NEXP$.*

In other words, the power of $MIP^*_{poly(n)}$ and that of the classical two-prover IPS (equivalent to NEXP) are the same. However, more general results with respect to MIP^*_∞ and NEXP are not known yet. The problems of integrating the zero-knowledge aspect in a two-prover IPS with quantum players and which complexity class may be reached are even less known.

[1] In [KM03] the provers are allowed a fixed number of shared qubits *per protocol.* However, in [Gav06] the provers are allowed a fixed number of shared qubits *for the whole model.* This is what makes [Gav06]'s converse only partial, since in [KM03] the provers have more freedom.

Bit commitment scheme

The cryptographic primitive known as a *commitment scheme* (often prefixed with *bit* when the committed word is a bit) has been one of the major building blocks of cryptography from its advent in the early 80's. Although it seems fair to attribute the concept to M. Blum [Blu82], the terminology of commitments, influenced by the legal vocabulary, first appeared in the contract signing protocol of S. Even [Eve82]. Commitment lies at the heart of important complex cryptographic applications such as coin tossing [Blu82], two-party computation [Kil88] and zero-knowledge proofs [GMW91, BCC88].

The general idea and security of bit commitment is often best explained from this simple example: suppose Alice wants to commit to a certain secret bit value b to Bob without him learning this value before she decides it. To do so, she writes b down on a piece of paper, puts the paper in a box which she locks with a key; she then gives the locked box to Bob (who does not have the ability to pick it). This first stage in the protocol is called *committing.* Whenever Alice consider that Bob is ready to learn her bit, she sends to him the key, he opens the box and learns the value of b. This second stage is called *unveiling.*

As illustrated in the example, there are two essential aspects to the security of a bit commitment scheme:

1. Once Alice commits to her bit, she cannot change her mind and reveal to Bob a different bit value. This is known as the *binding* property of the commitment.

2. Until unveiling starts, Bob cannot learn to which value Alice committed. This is known as the *concealing* property of the commitment.

Of course, these security characteristics naturally extend to the more general form of commitment scheme known as *string commitment.*

It has been known for long that unconditionally secure classical bit commitment is

impossible[2]. So to achieve some security properties, extra assumptions need to be made. For instance, computational assumptions can be imposed on the binding or concealing properties. Under such restrictions, commitments come in two dual flavors: binding but computationally concealing and concealing but computationally binding. The first type may be achieved from any one-way *function* [Nao91, HILL98]. Those of the second type may be achieved from any one-way *permutation* [NOVY93] or any collision-free hash function [HM96]. The problem of achieving commitments of the second type using only one-way functions is still open.

When Bennett and Brassard [BB84] brought back to life the idea of Wiesner [Wie70] to use quantum physics to achieve cryptographic tasks, a lot of hopes and efforts were put by cryptographers to revitalize the security of commitment schemes without any extra assumption. The first form of quantum bit commitment came implicitly with the BB84 coin-flipping protocol [BB84]. However, problems relating to the physical control of the quantum system made it easy to cheat for the receiver in practice. Bennett and Brassard also pointed out that it was possible, in theory, for the sender to cheat the binding property of the commitment. To solve these two problems, Brassard, Crépeau, Josza and Langlois [BCJL93] presented a new protocol, which was in fact an extension of the protocol found in [BC90], along with a "proof" of its unconditional security against quantum adversaries. For a while, most people were convinced that quantum bit commitment could be performed securely.

Unfortunately, rarely do nice things happen without any surprises. Doubts on the security of the BCJL's protocol against the sender settled in when, a couple of years after their result, Mayers found a subtle flaw in the proof and gave a specific attack to the pro-

[2]The intuition behind the proof is simple. Unconditional security requires an information theoretic argument. Let C be the random variable representing the commitment. To satisfy the binding property, C must hold a lot of information about the committed bit. However, to satisfy the concealing property, C must not hold any information on the committed bit. It is easy to see that C cannot satisfy both properties at the same time.

tocol. Mayers and the BCJL team then engaged in a battle of attacks and corrections of the protocol for about a year, until Mayers finally draw the final strike with its general impossibility theorem for quantum bit commitment [May96a, May96b]. We note that a similar result was, around the same time, independently achieved by Lo and Chau [LC97].

In their '98 paper [BCMS98], Brassard *et al.* nicely stated the disappointment:

> *"[...] In 1993 a protocol for quantum bit commitment, henceforth referred to as BCJL, was thought to be "provably secure". Because of quantum bit commitment, the future of quantum cryptography was very bright, with new applications such as the identification protocol of Crépeau and Salvail [CS95] coming up regularly. The trouble began in October 1995 when Mayers found a subtle flaw in the BCJL protocol. [...] After BCJL was shown not secure, the spontaneous attitude was to try alternative quantum bit commitment protocols by making some clever use of measurements and classical communication. However, all of these protocols were found not secure against Mayers' attack!"*

Nevertheless, the fate of quantum bit commitment is not sealed definitely. The general impossibility theorem of Mayers and Lo-Chau does not apply in all communication models. Indeed, the possibility of unconditionally secure (quantum) bit commitment has already been demonstrated in various models different from the standard noiseless communication model with two players, namely:

- the noisy communication model [CK88, Cré97, DFMS04, DKS99, CMW04],
- the multi-party computations model [BGW88, CCD88],
- the multi-prover model under some relativistic time constraint [Ken05, Ken99],
- the (quantum) memory-bounded model [CCM98, DFSS05],
- the multi-prover model under some physical separation constraints [BGKW88].

The fifth scenario, where we consider the case of two provers, is our main focus here. In [BGKW88], the authors introduced a bit commitment scheme for which they gave an

unconditional security proof against classical adversaries. Here we wish to provide a similar proof against adversaries that have full access to quantum resources.

Related Works

The starting point of this research is definitely the bit commitment scheme introduced by Ben-Or, Goldwasser, Kilian and Wigderson in [BGKW88] to provide a sufficient toolbox for their two-prover interactive proof-system to be perfect zero-knowledge. The classical security of their scheme is proven in [BGKW88].

The security of BGKW's scheme against quantum adversaries has been considered in the work of Brassard, Crépeau, Mayers and Salvail [BCMS98]. They showed that if such a bit commitment is used as a building block in the Quantum Oblivious Transfer protocol of [CK88] then the security of the commitment scheme is not sufficient to guarantee the security of the resulting QOT if the two provers can get back together at the end of the protocol. This result is in accordance with Mayers' suggestion [May97] that his version of the no-go theorem should also apply to commitment schemes based on temporary relativistic signaling constraints. However they did not address directly the question whether BGKW's bit commitment scheme is itself secure against quantum adversaries while the provers are not allowed to get back together. In the current work, we consider precisely this situation.

In a closely related work, Kent [Ken05] showed how impossibility of communication, implemented through relativistic assumptions, may be used to obtain a bit commitment scheme similar to BGKW's. Although the model he considered is essentially classical, he also discussed how his scheme behaves in a quantum setting. Kent proves the classical security of his scheme, but he remained elusive about its quantum security. Still, he proves the security of one round of his protocol (see [Ken05], Lemma 3, p. 329) against quantum adversaries, which is more or less the same as our Lemma 4.1. However, the proof he gave is erroneous in its last inequality and is not as tight as he claims. Lemma 4.1 can be viewed

as a notable clarification, and a fix for his proof. Among the differences with the scheme we present in this work, we note that his bit commitment scheme needs to be constantly updated (there is always new commitments made) to avoid cheating the first commitment made, whereas in ours we only need to maintain the physical separation assumption between the two provers for the commitment to remain secure. This particularity of his protocol translates in a constant blowup of the communication complexity proportional to the time we want to sustain the commitment, since a permanent flow of communications needs to be set between the two parties.

Another related line of research by Cleve, Høyer, Toner and Watrous [CHTW04], is one of the main inspiration of the current research as briefly discussed in the introduction. They have established nice relations between non-locality games and the two-prover model. They developed methods for establishing limits on the nonlocal behavior of such games to characterize how the soundness of two-prover IPS is affected. They also investigated the amount of entanglement required by (nearly) optimal quantum strategies to achieve these limits. However they did not consider how the zero-knowledge aspect of the studied IPS is affected by quantum adversaries.

Organization of the thesis and contributions

The remainder of the present document is organized as follows. Chapter 1 presents an overview of the basic notions of quantum mechanics needed to understand this work. We review the security definitions of a bit commitment scheme against classical and quantum adversaries, and briefly discuss a new binding definition recently introduced by Damgaard, Fehr, Salvail and Schaffner [DFSS06]. We also present some definitions and theorems that relate to non-local games. Chapter 2 introduces the original two-prover bit commitments of [BGKW88] and exposes the various problems (weakness) of the model's assumption "that the two provers are not allowed to talk to each other"; this chapter concludes with a refinement of BGKW's original assumption. In Chapter 3 we present two bit commitment

schemes in the two-prover model and show how entanglement-based strategies can be used to cheat each of them. Finally, Chapter 4 presents a variation of the bit commitment of Section 2.2 and prove its security against quantum adversaries. We obtain by reduction that the original BGKW' scheme is also secure against quantum adversaries. We conclude with some open problems. Appendix A treats of the classical and quantum optimal strategies to implement what we call the "NL-box" (see Section 2.3) and the Magic Square game (see Section3.2).

Parts of Chapter 2 (specifically sections 2.2, 2.3, and 2.4), Chapter 3, and Chapter 4 are all original contributions in which the author of the present work has intensively participated, in collaboration with Claude Crépeau, Louis Salvail, and Alain Tapp.

Chapter 1

Preliminaries and background

This chapter introduces the basic definitions and results that relate to quantum mechanics and information processing, to the security of bit commitment, and to the so-called non-local games. In no circumstances is this chapter meant to be a comprehensive introduction to the three subjects. Its sole purpose is to provide the reader with the specific tools required for the understanding of the present work. The interested reader is invited to consult [NC00] and [Bro04] for more information on these areas.

1.1 Basic notions of quantum mechanics

1.1.1 Hilbert space, the bra-ket notation and the qubit

The basic objects of linear algebra are vector spaces, themselves composed of elements called *vectors*. For instance, $\mathbb{C}^n$ is the space of all n-tuples (a.k.a. vectors) of complex numbers $(v_1, \ldots, v_n)$. A useful representation for vectors is the column matrix notation

$$\begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}. \tag{1.1}$$

Let φ be such an object. In linear algebra, the standard notation to indicate that φ is a vector is to write it toped with an arrow pointing in the right direction

$$\vec{\varphi}.$$

The type of vectors used in quantum mechanics are those of norm one. However, for historical reasons physicists have decided not to use the previous notation. Instead, in quantum mechanics the standard way to indicate that the object φ is a vector of norm one is to label it as

$$|\varphi\rangle.$$

The entire object $|\varphi\rangle$ is sometimes called a *ket*, and it is part of a set of similar labels known as the *Dirac notation*. In the same manner, we define the *bra* as the *dual vector* of $|\varphi\rangle$

$$\langle\varphi| := \begin{bmatrix} \bar{v}_1 & \dots & \bar{v}_n \end{bmatrix},$$

where $\bar{v}_i$ is the complex conjugate of v_i. One can see that a bra is simply a ket conjugated and transposed. These two transformations are usually represented using a dagger sign $\dagger$

$$\langle\varphi| \stackrel{\text{def}}{=} |\bar{\varphi}\rangle^T \stackrel{\text{def}}{=} |\varphi\rangle^\dagger.$$

Most vector spaces are not interesting unless an *inner product* function is defined on that space. For the vector space $\mathbb{C}^n$, the inner product between vectors $|\psi\rangle = [u_1, \dots, u_n]^T$ and $|\varphi\rangle = [v_1, \dots, v_n]^T$ is defined as

$$\langle\psi|\varphi\rangle := \begin{bmatrix} \bar{u}_1 & \dots & \bar{u}_n \end{bmatrix} \cdot \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} = \sum_i \bar{u}_i v_i.$$

Similarly, the outer product between vectors $|\psi\rangle$ and $|\varphi\rangle$ is defined as

$$|\psi\rangle\langle\varphi| := \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix} \cdot \begin{bmatrix} \bar{v}_1 & \dots & \bar{v}_n \end{bmatrix}.$$

In quantum mechanics' terminology, the complex vector space of dimension d equipped with such an inner product is usually referred to as a Hilbert space, denoted $\mathcal{H}^d$. For a

finite d, the Hilbert space is exactly the same as the complex inner product space. Moreover, quantum mechanics postulates that, to any isolated physical system we can associate a Hilbert space, known as the *state space*. The state of the system is completely described by a vector of norm one in that Hilbert space, known as the *state vector*. This first postulate is particularly important as it makes a connection between the physical world and the mathematical formalism of quantum mechanics. To avoid any irrelevant description of a system, from now on we assume that all the vectors in $\mathcal{H}^d$ are of norm one.

We know that a vector space of dimension d is *spanned* by a set of d vectors $|\varphi_0\rangle$ to $|\varphi_{d-1}\rangle$, such that any vector $|\varphi\rangle$ in that space can be written as a linear combination of the vectors in that set, that is,

$$|\varphi\rangle = \sum_{i=0}^{d-1} a_i |\varphi_i\rangle \quad \text{where } a_i \in \mathbb{C}.$$

This set of vectors is called a *basis* of the vector space. It is conventional to define the *computational basis* of dimension 2^d as the set $\{|i\rangle\}_{i\in\{0,1\}^d}$ where

$$|i\rangle = \begin{bmatrix} z_0 \\ \vdots \\ z_{2^d-1} \end{bmatrix} \text{ s.t. } z_j = \begin{cases} 0 & j \neq i \\ 1 & j = i \end{cases}.$$

The simplest quantum mechanical system, and the one with which we will be most concerned for quantum computation and information, is called the *qubit*. A qubit lives is a two-dimensional Hilbert space $\mathcal{H}^2$; that is, it has a two-dimensional state space. Using the computational basis $\{|0\rangle, |1\rangle\}$, we can express an arbitrary state vector $|\varphi\rangle \in \mathcal{H}^2$ of the qubit as a superposition

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle,$$

where $|\alpha|^2 + |\beta|^2 = 1$. Hence, contrary to the classical bit that can take only values zero and one, the qubit can take *any* combinations of those values in $\mathcal{H}^2$, and in particular $|0\rangle$ and $|1\rangle$.

1.1.2 The trace function

The *trace* of an arbitrary matrix $A = \{a_{ij}\}$ is defined to be the sum of its diagonal elements,

$$\mathrm{Tr}(A) \;:=\; \sum_i a_{ii}. \tag{1.2}$$

For A, B and C, arbitrary matrices, and z a complex number, the following important properties hold:

1. **Cyclic property of trace**

$$\mathrm{Tr}(ABC) \;=\; \mathrm{Tr}(BCA).$$

2. **Linearity of trace**

$$\begin{aligned} \mathrm{Tr}(A+B) &= \mathrm{Tr}(A) + \mathrm{Tr}(B), \\ \mathrm{Tr}(zA) &= z\mathrm{Tr}(A). \end{aligned}$$

Consider the operator A and a unit vector $|\varphi\rangle$, then an extremely useful corollary of the cyclic property of trace is

$$\mathrm{Tr}(A|\varphi\rangle\langle\varphi|) \;=\; \langle\varphi|A|\varphi\rangle. \tag{1.3}$$

Let A be of dimension d and $|i\rangle$ any orthonormal basis of dimension d. Using (1.3) and the *completeness relation* of the basis, $\sum_i |i\rangle\langle i| = I_d$, we can give an alternative definition for the trace function,

$$\begin{aligned} \mathrm{Tr}(A) &= \mathrm{Tr}(A \cdot I_d) = \mathrm{Tr}\left(A \sum_i |i\rangle\langle i|\right) \\ &= \sum_i \mathrm{Tr}\left(A|i\rangle\langle i|\right) \\ &= \sum_i \langle i|A|i\rangle. \end{aligned}$$

1.1.3 Tensor product

The tensor product construction is a crucial element to manipulate a multi-particle system. Indeed, the fourth postulate of quantum mechanics stipulates that the state space of a composite system is the tensor product of the state space of the component systems.

Let us first give a concrete idea of the tensor product with a matrix representation. Let A be an $m \times n$ matrix, and B a $p \times q$ matrix. The *tensor product of A with B* is defined as the $nq \times mp$ matrix

$$A \otimes B := \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix}.$$

The terms like $a_{11}B$ denote a submatrix

$$aA_{11} \cdot \begin{bmatrix} b_{11} & \dots & b_{1q} \\ \vdots & \vdots & \vdots \\ b_{p1} & \dots & b_{pq} \end{bmatrix}.$$

With that in mind, it is easier to understand the situation for Hilbert spaces, and more generally vector spaces. Let V and W be Hilbert spaces of dimension m and n respectively. If $|i\rangle$ and $|j\rangle$ are orthonormal bases for V and W respectively, then $|i\rangle \otimes |j\rangle$ is an orthonormal basis for the tensor product of V with W, also labelled $V \otimes W$. Note that the abbreviated notations $|i\rangle|j\rangle, |i, j\rangle$ or $|ij\rangle$ are often used to write the tensor product $|i\rangle \otimes |j\rangle$. So $V \otimes W$ is a mn dimensional Hilbert space and any of its elements can be represented as a combination of the basis elements.

By definition, for arbitrary $|v_1\rangle, |v_2\rangle \in V$, $|w_1\rangle, |w_2\rangle \in W$ and $z \in \mathbb{C}$, the tensor product satisfies the following properties:

1. $z(|v_1\rangle \otimes |w_1\rangle) = (z|v_1\rangle) \otimes |w_1\rangle = |v_1\rangle \otimes (z|w_1\rangle)$,

2. $(|v_1\rangle + |v_2\rangle) \otimes |w_1\rangle = |v_1\rangle \otimes |w_1\rangle + |v_2\rangle \otimes |w_1\rangle$ (distributivity),

3. $|v_1\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v_1\rangle \otimes |w_1\rangle + |v_1\rangle \otimes |w_2\rangle$ (associativity),

4. $(V \otimes W)^\dagger = V^\dagger \otimes W^\dagger$.

Let A and B be linear operators on V and W respectively, then we can define an operator $A \otimes B$ acting on $V \otimes W$ by the equation

$$(A \otimes B)\Big(\sum_i a_i |v_i\rangle \otimes |w_i\rangle\Big) \stackrel{\text{def}}{=} \sum_i a_i A|v_i\rangle \otimes B|w_i\rangle.$$

The inner product on V and W can also be used to define the inner product on $V \otimes W$. Let $|\varphi\rangle = \sum_i a_i |v_i\rangle \otimes |w_i\rangle$ and $|\psi\rangle = \sum_j b_j |v'_j\rangle \otimes |w'_j\rangle$, then

$$\langle\varphi|\psi\rangle \stackrel{\text{def}}{=} \sum_{ij} \bar{a}_i b_j \langle v_i|v'_j\rangle\langle w_i|w'_j\rangle.$$

1.1.4 Important matrix properties

In this section we review the common matrix properties found in the literature of quantum mechanics. Let A be an operator on a d-dimensional vector space V.

A is said to be a *Hermitian* or *self-adjoint* operator if it is its own adjoint,

$$A = A^\dagger.$$

An important class of Hermitian operators is the *projector*. An operator P is said to be a projector if $P = P^2$. Intuitively, this means that once a projector has been applied on a vector space, successive applications of the same projector on the resulting space will have no further effect. More interestingly, suppose W is a k-dimensional vector subspace of V such that, without loss of generality, V's orthonormal basis is $|1\rangle, \ldots, |d\rangle$ and W's orthonormal basis is $|1\rangle, \ldots, |k\rangle$. Then by definition the projector P onto the subspace W is

$$P \stackrel{\text{def}}{=} \sum_{i=1}^{k} |i\rangle\langle i|.$$

Another important class of Hermitian operators is the *positive operators.* A is said to be a positive operator if and only if

$$\forall\, |v\rangle \in V \quad \langle v|A|v\rangle \geq 0.$$

If $\forall\, |v\rangle \in V$, $\langle v|A|v\rangle > 0$ then we say that A is a *positive definite operator.*

A is said to be *normal* if $AA^\dagger = A^\dagger A$. By definition, Hermitian operators are also normal. An extremely useful representation theorem follows from the normality of an operator.

Theorem 1.1 (Spectral decomposition) *Any operator M on V is normal if and only if it is diagonal with respect to some orthonormal basis for V.*

In terms of outer product representation, it means that M can be written as the matrix $\sum_i \lambda_i |i\rangle\langle i|$, where λ_i are the eigenvalues of M and $|i\rangle$ is an orthonormal eigenbasis of V.

Finally, A is said to be unitary if $AA^\dagger = I$. Unitary transformations are fundamental to quantum mechanics as they describe the evolution of the state of a quantum system. For a closed quantum system, the state $|\varphi\rangle$ at time t_1 is related to the state $|\varphi'\rangle$ at time t_2 by a unitary operator A which depends only on t_1 and t_2, that is,

$$|\varphi'\rangle = A|\varphi\rangle.$$

Notice that a unitary operator also satisfies $A^\dagger A = I$, and so A is normal and has a spectral decomposition. Notice also that a unitary operator preserves inner products between states (or vectors):

$$\forall\, |u\rangle, |v\rangle \in V \quad \langle u|A^\dagger A|v\rangle = \langle u|I|v\rangle = \langle u|v\rangle.$$

1.1.5 Measurements

The general way of talking about a quantum measurement is by describing it with a collection $\{M_m\}$ of *measurement operators* satisfying the completeness equation

$$\sum_m M_m^\dagger M_m = I.$$

These operators act on the state space of the system being measured, and the index m refers to the measurement outcomes that may occur from the measurement. Let $|\varphi\rangle$ be the state of the quantum system immediately before the measurement takes place, then the probability that result m occurs is

$$\Pr[m] = \langle\varphi|M_m^\dagger M_m|\varphi\rangle,$$

and the state after the measurement evolves to

$$\frac{M_m|\varphi\rangle}{\sqrt{\langle\varphi|M_m^\dagger M_m|\varphi\rangle}} = \frac{M_m|\varphi\rangle}{\sqrt{\Pr[m]}}.$$

Measurement in the computational basis is often given to illustrate how measurement works. From the definition we gave in Section 1.1.1, the computational basis on one qubit is $\{|0\rangle, |1\rangle\}$. The measurement of one qubit in the computational basis is hence defined using the measurement operators $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. Measuring some state $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ with M_0 and M_1 results in a state $|\varphi'\rangle$ such that

$$|\varphi'\rangle = |0\rangle \qquad \text{with probability} \quad \Pr[0] = |\alpha|^2$$
$$|\varphi'\rangle = |1\rangle \qquad \text{with probability} \quad \Pr[1] = |\beta|^2$$

Two special cases of the previous general measurement scenario are widely used in the quantum literature and are worth seeing as they often greatly simplify the analysis of a quantum circuit for quantum computation and information: the *projective* or *von Neumann* measurements and the *POVM* measurements.

A projective measurement is described by an *observable* M, a Hermitian operator acting on the state space of the system being *observed* (note the difference with the measurement's terminology). Being a Hermitian operator, M has a spectral decomposition

$$M = \sum_m m P_m,$$

where P_m is the projector onto the eigenspace of M with eigenvalue m. The set $\{m\}$, the eigenvalues of the observables, also corresponds to the possible outcomes of the measure-

ment. As in the general definition, m occurs with probability

$$\Pr[m] = \langle\varphi|P_m|\varphi\rangle = \mathrm{Tr}[P_m|\varphi\rangle\langle\varphi|],$$

and the state immediately after measurement is

$$\frac{P_m|\varphi\rangle}{\sqrt{\Pr[m]}}.$$

One of the main reason why projective measurements are so much enjoyed is that, when augmented with the ability to perform unitary transformations, they are actually *equivalent* to the previous general description! We refer the reader to [NC00] for further details.

Whenever the statistics associated with the different possible measurement outcomes are of main interest rather than the post-measurement state, the mathematical tool known as POVM, which stands for *Positive Operator-Valued Measurement*, is particularly well adapted. We review here the important points of this formalism.

Let M_m be the measurement operator describing a measurement. We define

$$E_m = M_m^\dagger M_m.$$

Then, E_m is a positive operator such that

$$\sum_m E_m = I \quad \text{and} \quad \Pr[m] = \langle\varphi|E_m|\varphi\rangle = \mathrm{Tr}[E_m|\varphi\rangle\langle\varphi|],$$

where $|\varphi\rangle$ is the state on which the measurement is applied. The operators E_m are known as the *POVM elements* and are sufficient to determine the probabilities of the different measurement outcomes. The set $\{E_m\}$ is known as the POVM.

The interest for such a tool is best explained with a simple example. Suppose Bob is given one of two states, $|\varphi_1\rangle$ and $|\varphi_2\rangle$, such that these two states cannot be distinguished perfectly. Bob wants to determine which of the two states he has received such that whenever his technique returns an answer, he never makes an error of mis-identification. It turns

out that using the POVM formalism, it is possible for Bob to perform the measurement described by the POVM $\{E_1, E_2, E_3\}$ such that E_1 and E_2 are cleverly chosen to satisfy $\langle\varphi_1|E_1|\varphi_1\rangle = 0$ and $\langle\varphi_2|E_2|\varphi_2\rangle = 0$ (and E_3 is taken to be $I - E_1 - E_2$ for the POVM to satisfy the completeness relation). This way, whenever outcome E_1 occurs, Bob is sure that he received the state $|\varphi_2\rangle$, when outcome E_2 occurs he is sure that he received the state $|\varphi_1\rangle$, and he learns *nothing* when outcome E_3 occurs.

1.1.6 Entanglement

We finish our review of quantum mechanics with what is probably the most puzzling behavior of composite systems: *entanglement.* Let $\mathcal{H}_{2^m} \otimes \mathcal{H}_{2^n}$ be a composite system of $m+n$ qubits. A pure state $|\varphi\rangle \in \mathcal{H}_{2^m} \otimes \mathcal{H}_{2^n}$ is said to be a *product state* if there exists states $|\sigma\rangle \in \mathcal{H}_{2^m}$ and $|\psi\rangle \in \mathcal{H}_{2^n}$ such that $|\varphi\rangle = |\sigma\rangle \otimes |\psi\rangle$; otherwise $|\varphi\rangle$ is said to be an *entangled* state.

The most common entangled states present in the quantum literature are the famous two qubit *Bell states*:

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

The last state, $|\Psi^-\rangle$, is also known as the Einstein-Podolsky-Rosen (EPR) pair, or as the *singlet* state.

The best way to get the flavor of the mysterious behavior unique to entangled state is certainly with a simple example. To do so consider the entangled state $|\Phi^+\rangle$. This is a two qubit state, so let Alice have one of the qubit and Bob have the other. Then Alice and Bob are separated as far as they can be. Both are instructed to measure their respective qubit

in the computational basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. If we consider only Alices' system, her qubit is in the state with density matrix

$$\frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 1|), \tag{1.4}$$

see [NC00] page 106 for the details on how to carry such a computation. Notice that this is also the state of Bob's qubit alone.

Therefore, when Alice measures, she obtains $|0\rangle$ with probability $1/2$ and $|1\rangle$ with probability $1/2$. Without loss of generality, suppose that she obtains $|0\rangle$, then when Bob perform *his* measurement, he will also obtain $|0\rangle$. If instead Alice had obtained $|1\rangle$, then Bob would have also obtained $|1\rangle$. The strange thing is that, on one hand, as soon as Alice measures her part of $|\Phi^+\rangle$ she knows exactly that the result of Bob's measurement will be the same as hers, whether he as already measured his part or not. On the other hand, whether Alice has measured or not her state, as long as Bob does not perform his measurement, his part of $|\Phi^+\rangle$ is still, for him, in state (1.4) and from his point of view he still has probability $1/2$ to obtain either $|0\rangle$ or $|1\rangle$, even if Alice has measured! And this is true the other way around. No matter who measures first, we know for sure that Alice and Bob's respective outcomes will be the same!

No wonder why Einstein qualified this surprising feature of entanglement as "spooky action at a distance" [EPR35]. To get a glimpse why this is possible, we need to consider the global state of the two qubits. When one of the participants performs his measurement and obtains outcome $|i\rangle = |0\rangle$ or $|1\rangle$, the global state $|\Phi^+\rangle$ collapses to $|i\rangle|i\rangle$. Of course, the view of the other participant' state is still (1.4), but from the global point of view he his sure to obtain outcome $|i\rangle$ with certainty.

1.2 Security definitions

First let us define the condition on the two provers. We say that Peggy and Paula are *isolated* from one another. The intuitive meaning of this term is that Peggy and Paula cannot

communicate with each other, since this condition is explicitly imposed by the two-prover model. However, we introduce this new terminology instead of the traditional "cannot communicate with one another" because, as explained in Section 2.3 and 2.4, we noticed that the meaning of "no-communication" is too weak and must be very clearly defined to produce valid security proofs. This *isolation* will be formally defined in Section 2.4. For now, the reader may follow his intuition and picture Peggy and Paula as being separated[1] and unable to communicate with each other.

We use the following security definitions for bit commitment against a classical malicious pair Peggy-Paula. Let n be the security parameter.

Definition 1.1 *We call a function* $\mu : \mathbb{N} \to \mathbb{R}$ negligible *if for every polynomials* $p(\cdot)$ *and all sufficiently large* n*'s,*

$$\mu(n) < \frac{1}{p(n)}.$$

Henceforth, the function $\mu(n)$ will always refer to a negligible function in n.

Definition 1.2 *A bit commitment scheme is* statistically concealing *if only a negligible amount of information on the committed bit can leak to the verifier before the unveiling stage. It is* unconditionally concealing *if no information leaks.*

Definition 1.3 *A bit commitment scheme is* statistically binding *if the isolated provers Peggy and Paula successfully unveil for any other value than the one committed with negligible probability. It is* unconditionally binding *if the probability is zero.*

In this work, all the bit commitment schemes presented are unconditionally concealing and statistically binding. To lighten the lecture, we will simply use the term *concealing* and *binding*. The term *secure* will be used when both properties hold at the same time.

[1]Such a split can be implemented by physically trapping the two provers in Faraday cages or using some relativistic effects keeping them separated by a long enough distance.

In the case where the cheating pair Peggy-Paula can manipulate, share, and store quantum information, the binding condition 1.3 is too strong to be satisfied. With its general impossibility proof for quantum bit commitment, Mayers [May96a, May96b], and independently Lo and Chau [LC97], was the first to point out that the condition where either $p_0 \leq \mu(n)$ or $p_1 \leq \mu(n)$ (note that this is only a restatement of Definition 1.3), where p_b is the probability of successfully unveiling b, could never be satisfied since it was always possible to cheat by performing the honest protocol at the quantum level. Note that "quantum level" simply means that we perform the honest protocol with a superposition representing all the possible commitments. Subsequently, Dumais, Mayers and Salvail [DMS00] proposed the following weaker binding condition.

Definition 1.4 *A bit commitment scheme is statistically binding if, for $b \in \{0,1\}$, the probability p_b that isolated Peggy and Paula successfully unveil for b satisfies*

$$p_0 + p_1 \leq 1 + \mu(n). \tag{1.5}$$

As the authors noted, for classical applications, this binding condition with $\mu(n) = 0$ is as good as if the committer were permitted to honestly commit to a bit, according to the probability distribution of his choice, and only had the power to abort in view of the bit he is about to unveil. Notice also that using the language of Definition 1.4, the essential result of Mayers and Lo and Chau, that unconditionally concealing (or with probability at least $1 - q(n)$) quantum bit commitment protocols are insecure according to the binding property, can be rephrased with the equation

$$p_0 + p_1 = 2 - q(n),$$

where $q(n)$ is the probability that the concealing property is cheated. These two cases clearly define the bounds of equation (1.5) between a secure and (near-) maximally insecure scheme. It follows that the concealing and binding conditions cannot be simultaneously satisfied.

Moreover, as Kent [Ken05] argues, another reason to prefer this definition to define the security of a quantum protocol rather than Definition 1.3 is that the classical defi-

nition implies something stronger he calls *classical certification* [Ken04]. A protocol that has classical certification guarantees that its quantum inputs belong to a fixed basis, so that the inputing parties are effectively required to input classical information. If such a requirement were part of the definition of a quantum bit commitment, then showing that unconditionally secure quantum bit commitment is impossible would only require showing that no quantum protocol can prevent the commitment of superposed bits. This is a much simpler result [Ken04] which does not give any insights on the fundamental reasons[2] why unconditionally secure quantum bit commitment is impossible.

Although this work sticks to Definition 1.4 to characterize the security of quantum bit commitment, Damgård, Fehr, Salvail and Schaffner recently [DFSS06] introduced a new definition stronger than 1.4, but still weaker than its classical counterpart. This new definition is motivated by the following imaginary, but not that hard to construct, quantum bit commitment scheme: with probability 1/2, you can unveil to whatever you want and with probability 1/2, you cannot unveil at all. Of course, this is clearly not what we want, and expect, from a bit commitment scheme, at least intuitively. However, since for this example

$$p_0 + p_1 = \frac{1}{2} + \frac{1}{2} = 1 < 1 + \mu(n).$$

Existence of such a scheme is not excluded if we only require equation (1.5) to be satisfied for the commitment scheme to be binding. Instead they propose to use a stronger variant closer to the classical binding condition:

Definition 1.5 *[DFSS06] A bit commitment scheme is statistically binding if for every possibly dishonest committer there exists a binary random variable* $D \in \{0,1\}$ *such that* p_{1-D} *is negligible.*

The crucial point of their definition is that *it still allows to commit to a superposition!* The reason is that the random variable D is defined to be the outcome obtained when the

[2]E.g. if the commitment is unconditionally concealing, then we can rotate from the state representing the commitment of a zero to the state representing the commitment of a one.

superposition of commitments is measured. It then follows by definition of measurements that the information to unveil as $1-D$ is destroyed and so the value of D cannot be changed. Alternatively we might say that the dishonest committer does not control the probability distribution of D. That is, he cannot change with certainty its value from zero to one, or from one to zero. Using the same language as its classical counterpart, it boils down to saying that in Definition 1.4 the probabilities p_0 and p_1 take values *before* the superposition is measured, whereas in the new Definition 1.5 the probabilities p_0 and p_1 take values *after* the superposition has been measured. Although it has not been proven yet, it wouldn't be surprising if this new definition were the strongest possible with respect to what it means for a commitment scheme to be quantum and binding. A stronger definition would probably require a classical certification of the quantum system used for the commitment.

Moreover, as the authors of [DFSS06] point out, it is not hard to prove that committing bit by bit on a string with a scheme satisfying Definition 1.5 yields a string commitment fulfilling the same definition (adapted for strings). This natural extension was impossible using Definition 1.4.

For our matter, it is still an open problem if the quantum scheme presented in Section 4.2 is binding with respect to Definition 1.5.

1.3 Non-local games

Informally speaking, a *two-party non-local game* is a scenario where two players, Peggy and Paula, who are isolated from each other, cooperate against a verifier, Vic, in order to produce a consistent answer to a question that Vic independently asked to both Peggy and Paula. Of course, these kind of games can be cast using more than two players. Our interest in such games is that the two-prover model is exactly the setting in which these games take place. Hence, some theoretical results from this field will be quite useful to ease the classical security proofs of our protocols.

The reader familiar with the subject might already have noticed the similarities with the so-called *pseudo-telepathy games.* It is true that the framework is the same, and that when Peggy and Paula are classical players, they have an unavoidable nonzero probability of failure. However, following the definition given in [Bro04], when Peggy and Paula are quantum players, a pseudo-telepathy game is guaranteed to have a perfect winning quantum strategy. In our case, we do not need to ask so much from a quantum strategy. It is why we prefer to use the term "non-local".

The next definitions and theorems are taken from the work of A. L. Broadbent [Bro04] on pseudo-telepathy games. Let W be a predicate (a relation) on the finite sets $S \times T \times U \times V$. A two-party non-local game $G = (W, S, T, U, V)$ is defined as follows. Peggy and Paula are isolated. Vic randomly selects a pair of elements (questions) $(s, t) \in S \times T$ (he may do so according to a specific probability distribution Π on $S \times T$). Vic sends s to Peggy and t to Paula, who respond with $u \in U$ and $v \in V$ respectively, according to the pre-agreed strategy of their choice. They win if W evaluates to one on input (s, t, u, v) and lose otherwise.

Definition 1.6 *A deterministic strategy is successful in* proportion p *if the ratio of number of instances of G for which the players win and the total number of instances of G is p.*

Definition 1.7 *A strategy is successful with* probability q *if it wins any instance of G with probability at least q.*

Using the two previous definitions, we define the following bounds reached by optimal strategies.

Definition 1.8 $\widetilde{\omega}_c(G)$ *is the maximum success proportion, over all possible deterministic strategies, for classical Peggy-Paula that play the game G.*

Definition 1.9 $\omega_c(G)$ *is the maximum success probability, over all possible strategies, for classical Peggy-Paula that play the game G.*

and likewise,

Definition 1.10 *$\omega_q(G)$ is the maximum success probability, over all possible strategies, for quantum Peggy-Paula that play the game G.*

It is a common fact that for a non-local game G, to determine $\omega_c(G)$, one needs only to consider deterministic strategies. Intuitively, a shared random variable R can always be fixed to the randomness of the best strategy, hence transforming the probabilistic strategy into a deterministic one; a formal proof is given next.

Lemma 1.2 *[Bro04] For any non-local game G, $\widetilde{\omega}_c(G)$ is the maximum probability that the players win if the questions are asked uniformly at random among the set of possible questions.*

Proof: Let s be a probability distribution over a finite set of deterministic strategies $\{s_1, s_2, \ldots, s_m\}$; s represents a probabilistic strategy. Let $\Pr(s_i)$ be the probability that strategy s_i is chosen, and p_i be the success proportion of strategy s_i, then the probability that the players win the game is

$$\begin{aligned} \sum_{i=1}^{m} \Pr(s_i) p_i &\leq \sum_{i=1}^{m} \Pr(s_i) \widetilde{\omega}_c(G) \\ &= \widetilde{\omega}_c(G) \end{aligned}$$

□

Theorem 1.3 *[Bro04] For any non-local game G, $\omega_c(G) \leq \widetilde{\omega}_c(G)$.*

Proof: Consider any strategy s successful with probability $\omega_c(G)$. Let χ be the set of possible questions for G. By definition, $\forall\, x \in \chi$, the probability of winning on question x is $\Pr(win \mid x) \geq \omega_c(G)$. Let the question be chosen uniformly at random, then the probability q of winning the game using s is

$$\begin{aligned} q &= \sum_{x \in \chi} \frac{1}{|\chi|} \cdot \Pr(win \mid x) \\ &\geq \sum_{x \in \chi} \frac{1}{|\chi|} \cdot \omega_c(G) \\ &= \omega_c(G) \end{aligned} \tag{1.6}$$

By Lemma 1.2, $\widetilde{\omega}_c(G) \geq q$, and from (1.6), we get that $\omega_c(G) \leq \widetilde{\omega}_c(G)$.

□

The next lemma will also be useful.

Lemma 1.4 *[Bro04] Let $G = (W, S, T, U, V)$ be a game with $\widetilde{\omega}_c(G) < 1$, then*

$$\widetilde{\omega}_c(G) \leq \frac{|S| \cdot |T| - 1}{|S| \cdot |T|}.$$

Proof: Recall that $\widetilde{\omega}_c(G)$ is the ratio of the maximum number of questions on which the classical players can win, and the total number of questions possible. Since $\widetilde{\omega}_c(G) < 1$, and the total number of questions possible is $|S| \cdot |T|$, the next best alternative is that $\widetilde{\omega}_c(G) = \frac{|S| \cdot |T| - 1}{|S| \cdot |T|}$. So we conclude that $\widetilde{\omega}_c(G) \leq \frac{|S| \cdot |T| - 1}{|S| \cdot |T|}$.

□

Chapter 2

Bit commitment in the two-prover model

As explained in the beginning of this work, the idea of bit commitment in the two-prover model was first introduced by Ben-Or, Goldwasser, Kilian and Wigderson [BGKW88], along with the notion of Multi-Prover Interactive proofs, as an efficient way to prove that every language $L \in NP$ has a two-prover perfect zero-knowledge interactive proof system. In order to present a classically secure bit commitment scheme, which we call the "BGKW" scheme, they used the simple assumption that the two provers could not communicate with one other once the protocol had started. We show in this chapter that, stated as above, this assumption, on which the security of their scheme depends, is too weak and needs to be made more precise to preserve the soundness of their construction.

2.1 The original scheme

We now present the BGKW scheme together with some intuitive explanations of its security. We strongly refer the reader to [BGKW88] for more details.

Define the functions $\sigma_0, \sigma_1 : \{0,1,2\} \to \{0,1,2\}$ such that

1. $\forall\, i,\ \sigma_0(i) = i$,

2. $\sigma_1(0) = 0,\ \sigma_1(1) = 2,\ \sigma_1(2) = 1.$

The bit commitment for a bit b is as follows. Note that we are in the setting of BGKW, so in this case the term *isolation* means that Peggy and Paula are separated and cannot communicate with each other.

BGKW

Peggy and Paula agree on a trit $w \in \{0, 1, 2\}$. They are then isolated.

Commit to b:

- V chooses at random $r \in \{0, 1\}$ and sends it to Peggy.
- Peggy computes $z := E(r, w, b) = \sigma_r(w) + b \mod 3$ and sends it to Vic.

Unveil b:

- Paula sends to Vic the trit w.
- Vic computes $\sigma_r(w)$ and sets $b := z - \sigma_r(w) \mod 3$.

It is not hard to understand why the BGKW scheme is secure against classical adversaries. The key idea is simply that Paula does not know r and has never seen the trit $z = E(r, w, b)$. Notice however that the two-prover model allows Paula to detect when messages are transmitted between Vic and Peggy, as defined in the introduction. Therefore, the probability that Paula successfully reveals a bit value $\bar{b}$ is upper bounded by her probability to correctly determine r, which is $1/2$. More formally,

Lemma 2.1 *[BGKW88]* $\forall\ w \in \{0, 1, 2\},\ b \in \{0, 1\}$, *having that Peggy sent the trit* z, *if Paula sends to Vic the trit* $\hat{w}$ *then*

$$\Pr[\hat{w} \text{ is s.t. } \bar{b} = z - \sigma_r(\hat{w}) \mod 3] \leq \frac{1}{2}.$$

The BGKW scheme is also secure against Vic since knowing r and the trit $z = E(r, w, b)$ gives no advantage in guessing b. It is assume that the value b is selected uniformly. More formally,

Lemma 2.2 *[BGKW88] Let the variable B represents the committed bit, then* $\forall\, r \in \{0,1\}$

$$\Pr[B = 0 \mid E(r, w, 0), r] = \Pr[B = 1 \mid E(r, w, 1), r] = \frac{1}{2}.$$

Observing that independent executions of the above protocol can be performed in parallel without affecting the security, we can decrease the probability of successfully cheating to 2^{-n} by performing n independent commitments and unveils to b.

2.2 A simpler version

For a protocol to be considered cryptographically secure, its probability of successfully being cheated must be at most negligible in n, the security parameter. Hence, for cryptographic ends, we are looking at n executions of the BGKW scheme. In this context, the BGKW scheme turns out to be unnecessarily complicated. With no loss in security, it can be replaced by a far simpler and compact version, called "simplified-BGKW" (or sBGKW as a short hand), where the σ functions are removed and only one execution is needed to achieve the same security probability of 2^{-n}. For a n-bit string r and a bit b, we define the n-bit string $b \cdot r := b \wedge r_1 \ldots b \wedge r_n$.

sBGKW

Peggy and Paula agree on an n-bit string w. They are then isolated from one another.

Commit to b:

- Vic sends a random n-bit string r to Peggy,
- Peggy replies with $x := (b \cdot r) \oplus w$.

Unveil b:

- Paula announces b and an n-bit string w,
- Vic accepts iff $w = (b \cdot r) \oplus x$.

Note that at the unveiling stage, as in the original scheme it is not required that Paula be the one announcing b. It is as good to let Vic deduce b: Vic computes $Z := w \oplus x$, if $Z = 0^n$ he sets $b := 0$ and if $Z = r$ he sets $b := 1$, and otherwise rejects. Indeed, Paula may not even know b!

For obvious simplicity reasons, we use the sBGKW scheme for what follows. The assumption made in [BGKW88] is that Peggy and Paula are not allowed to communicate with each other. Based solely on that isolation constraint, the following seems a "correct proof" that the sBGKW scheme is secure classically:

Theorem 2.3 *Defining* isolation *as in [BGKW88], the* sBGKW *is secure classically.*

Proof: Vic does not know w, that is, from its point of view w is uniformly distributed among all possible n-bit strings. It follows that the two strings w and $r \oplus w$ he can receive as commitment are perfectly indistinguishable from one another. Hence, absolutely no information on the committed bit is learned by Vic before the unveiling stage. This proves that sBGKW is concealing.

Now suppose that Peggy and Paula would like to be able to unveil a certain instance of b both as 0 and as 1. To do so, Paula would like to announce $\hat{w}_b$ such that $\hat{w}_b = (b \cdot r) \oplus x$. We note that this models the two possible dishonest behaviors for Peggy and Paula: honestly commit to $\bar{b}$ and try to change to b afterwards, and commit to nothing by sending some x and decide which b they want to unveil *only* at the unveiling stage. It follows that in both scenarios, a successful cheating strategy would allow to produce the two strings $\hat{w}_0$ and $\hat{w}_1$, such that $\hat{w}_0 = x$ and $\hat{w}_1 = r \oplus x$. However, $\hat{w}_0 \oplus \hat{w}_1 = (0 \cdot r) \oplus x \oplus (1 \cdot r) \oplus x = r$ is completely unknown to Paula by the no-communication assumption. Therefore, even using unlimited computational power, her probability of issuing a valid pair $\hat{w}_0, \hat{w}_1$ is at most $1/2^n$. This proves that sBGKW is binding (see Definition 1.3).

□

Nevertheless, this result is incomplete! We noticed that the meaning of isolation as "no-communication" must be very clearly defined for the statement to be correct. Indeed,

we show next how a correlated random variable can be used to invalidate the result of Theorem 2.3 while not violating the "no-communication" assumption. This suggest that the conventional wording "no-communication" is intuitively insufficient as it is not explicit enough to cover any kind of cheating mechanism Peggy and Paula can employ.

2.3 Cheating sBGKW with a NL-box

The NL-box, short-hand for "Non-Locality box", is a device with two input bits s and t, and two output bits u and v such that u and v are individually uniformly distributed and the following relation is satisfied

$$s \wedge t = u \oplus v. \tag{2.1}$$

The pair (s, u) is on Peggy's side and the pair (t, v) is on Paula's side. Equivalently $v := u \oplus s \wedge t$. Notice that v is also uniformly distributed and $u := v \oplus s \wedge t$. Therefore, because u and v are individually uniformly distributed the NL-box does not allow Peggy and Paula to communicate.

Note that here the NL-box is taken as a black box, that is, as a workable device whose building is hidden and cannot be influenced or changed. This "non-local primitive" was first introduced as a black box by Popescu and Rohrlich [PR94, PR97] as a tool to achieve a better understanding of the non-local behavior of quantum mechanics. Appendix A covers in details the optimal classical and quantum strategy to implement this type of device, usually referred as the CHSH game in this context (which leads to the seminal CHSH *Bell inequality*).

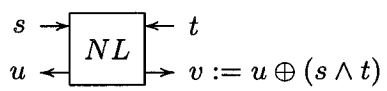

Figure 2.1: the cheating NL-box

This NL-box allows Peggy and Paula to unveil the bits committed through sBGKW in either way, at Paula's will. For each position i, $1 \leq i \leq n$, Peggy inputs in the NL-box the bit $s := r_i$ received from Vic and obtains output $x_i := u$ from the NL-box, which

corresponds to the i-th bit of the commitment string. To unveil bit b, Paula inputs $t := b$ in the NL-box and obtains the output $\hat{w}_i := v$ from the NL-box, which she sends to Vic. If $b = 0$ then $b \wedge r_i = 0$ and thus $\hat{w}_i = x_i$ which is the right value she must disclose. If $b = 1$ then $b \wedge r_i = r_i$ and thus $\hat{w}_i \oplus x_i = r_i$ or $\hat{w}_i = x_i \oplus r_i$ which is again the right value she must disclose.

2.3.1 The NL-box that breaks the original BGKW scheme

Similarly, we can define an analogous cheating box for the original BGKW scheme with two binary inputs s, t, and two uniformly generated ternary outputs x, y. We first note that the σ functions defined in Section 2.1 can be re-written as the single expression

$$\forall\, r \in \{0,1\}, w \in \{0,1,2\} \quad \sigma_r(w) = (1+r)w \mod 3. \tag{2.2}$$

So using (2.2), we want from the cheating NL-box that $u := (s+1)v - t \mod 3$ for each s, t, and uniformly chosen v. Because for any binary s, t we can easily define the inverse permutation over trits to be $v := (t+u)(s+1) \mod 3$, the following NL3-box does not allow to communicate since individually u and v are uniformly distributed.

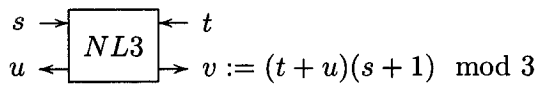

Figure 2.2: A non-local box to cheat BGKW

It is not hard to verify that the NL3-box that implements this non-local computation from s, t is exactly the one needed to cheat the original BGKW scheme. As with the NL-box, for each round i, Peggy inputs in the box $s := r_i$ and obtains the trit $x_i := u$, which she sends to Vic. If Paula wants to unveil for b, she inputs $t := b$ in the NL3-box, which

correctly outputs $\hat{w}_i := v$. Clearly, they successfully cheat since

$$\begin{aligned} \forall\, i \quad (1+r_i)\hat{w}_i - x_i \mod 3 &= (1+r_i)(b+x_i)(1+r_i) - x_i \mod 3 \\ &= (1+r_i)^2(b+x_i) - x_i \mod 3 \\ &= (b+x_i) - x_i \mod 3 \\ &= b. \end{aligned}$$

2.4 Defining isolation

The existence of such an inputs-correlated[1] random variable, which does not allow communication but allows cheating of the sBGKW two-prover bit commitment scheme sheds some light on the original assumption of Ben-Or, Goldwasser, Kilian and Wigderson:

> *"Our construction does not assume that the verifier is polynomial time bounded. The assumption that there is no communication between the two provers while interacting with the verifier, must be made in order for the verifier to believe the validity of the proofs. It need not be made to show that the interaction is perfect zero-knowledge."*

Indeed this assumption is necessary but not sufficient to guarantee the binding property of the bit commitment scheme. Among its weakness, we note that it does not explicitly force any cheating strategy to be repeatable. Still, it is not hard to see that this was something implicitly assumed in the proof of Theorem 2.3, when we wrote that in both cheating scenarios, a successful cheating end up in knowing $\hat{w}_b$ for both $b \in \{0,1\}$. The NL-box not being a repeatable process[2] gives a first understanding why we can still cheat the sBGKW

[1] We emphasize that at least one of the "inputs" to the random variable needs to be obtained once the provers are isolated, otherwise such a random variable can be shared while the provers are together, and is thus useless to cheat the sBGKW scheme.

[2] Of course, the NL-box can be repeated as often as one wants. For instance, Peggy and Paula can easily generate the output pair $(x_0, \hat{w}_0)$ from the input pair $(r, 0)$, and the output pair $(x_1, \hat{w}_1)$ from the input pair $(r, 1)$, and all these outputs are individually uniformly distributed. However, Peggy can send only one of x_0 and x_1 to Vic, and thus only the corresponding $\hat{w}$ will be valid on Paula's side for unveiling. There

despite the result of Theorem 2.3.

Clearly, to achieve the binding condition a stronger assumption must be made. However, pin-pointing it precisely is not easy. At first sight, one could require the following assumption:

> *"Once the provers are isolated, there exists no mechanism by which they may sample a joint random variable which is dependent on inputs they provide."*

We note that, among other things, this new condition excludes communication between the two provers, as desired. However, it excludes a lot more, such as shared entanglement! This last observation is somewhat constraining as it forbids to Peggy and Paula the use of some of the nicest properties of quantum mechanics. In a context where quantum processing is used but entanglement is not allowed, some results (e.g [BBKM04, KMR05]) showed that it is still possible to slightly outperform classical computations. Yet, it would be surprising that this small separation from the classical setting is enough to cheat the sBGKW scheme. Moreover, such a scenario is far fetch: to get interesting security results we need to consider entanglement. This new assumption is simply *too* strong; we need to be more subtle in the way we define this *"mechanism to sample a joint random variable"*.

It seems reasonable to believe that nature does not allow the existence of an NL-box as described in Section 2.3 (that is, as a black-box or an implementation exponentially close to a black-box). So why even ask for a stronger assumption than the no-communication assumption of [BGKW88]? Part of the answer is that Vic can play the role of the NL-box, or any other joint sampler. In no circumstances can we ignore the fact that both Peggy and Paula individually talk to Vic. Definitely, we need to consider this aspect of the protocol with great care. For instance, consider the scenario where r is sent to Peggy but committing and unveiling is not done immediately after, but rather once Vic and the two provers have been involved in other, unrelated, interactive protocols. It is perfectly conceivable

is no way for them to force the relation $x_0 = x_1$. This means that, in our context, the NL-box cannot be repeated to generate two *valid* strings $\hat{w}_0$ and $\hat{w}_1$.

that within those protocols, for each i, Peggy and Paula succeed in sending r_i and b to Vic, and then in a completely different context, or a moment of unawareness, Vic performs the required computation and output x_i and $\hat{w}_i$, which are then sent to respectively Peggy and Paula. It is obvious that if such a computation, or any alike, can take place with enough probability then Peggy and Paula would succeed in cheating the sBGKW protocol!

More generally, we must not only consider Vic but any other third party, call it Ted, to which Peggy and Paula might have access to obtain correlated information. The previous situation highlights the fact that there is a whole class of functions with inputs coming from Peggy and Paula for which Ted must not send the outputs. Intuitively, each time Ted sends a message to either Peggy or Paula, he must ensure that the message does not:

- allow Peggy and Paula to communicate;
- allow Peggy and Paula to achieve correlations better than what can be attained by local variables if Peggy and Paula are classical players, or shared entanglement if they are quantum provers.

That is, Ted must not outperform what Peggy and Paula can achieve using local variables in the sense of quantum mechanics. We wish to formulate that statement as a convenient computable criteria. A natural way to tackle the problem is to look at the entropy of the message Ted is about to send conditioned on what was previously sent from and to Ted. Suppose Ted is sending a message M to Peggy. Loosely speaking, if the uncertainty about M is the same whether Peggy has access to Paula's information or a local variable independent of Paula's information, then there is no problem sending M to Peggy because she can produce M on her own. However, if there is less uncertainty when Paula's information is available, then it means that Peggy needs some information held by Paula to produce this M with the same probability distribution. Hence, if Ted sends M, he gives to Peggy a string with a probability distribution (correlations) she could not have obtained otherwise. In the quantum case, the local variables are replaced by a quantum state, which often allows more correlations between Peggy and Paula than local variables do. At this

point, we will not consider the quantum case.

The above gives the flavor of an information theoretic approach to the problem; this is suitable as long as we stay at the variable level of a protocol. However, when Ted is involved in some computations with Peggy and Paula, he his working with *instances* of variables, and he may not know exactly, or have access to, the whole distribution from which come the instances he receives from Peggy and Paula. Of course, running the same computation multiple times on new instances would allow to re-generate the distribution of each variable, but it would be much more practical to have a criteria from which Ted can decide directly with the messages he has if he can send a message, or not. To this end, we start by introducing the following criteria.

Let Peggy be represented by P_0 and Paula by P_1. The variable $D \in \{0,1\}$ is a reference to player P_D, and $T \in \{\emptyset, \{0\}, \{1\}, \{0,1\}\}$ is a tag appended to each message that indicates to Ted the player(s) that are eligible for receiving this message, where $T = \{0,1\}$ means by both players and $T = \emptyset$ means by none of them. The message about to be sent from Ted to prover P_D is represented by $(m,T)_D$. We formalize Ted's behavior as follows.

Definition 2.1 (Practical definition) *Ted is said to be a "secure third party" if* $\forall D \in \{0,1\}$, *Ted follows these points.*

1. *A message received from player* P_D *is tagged with* $T := \{D\}$.
2. *A message generated without involving any of the previous messages, e.g. picking a random string, is tagged with* $T := \{0,1\}$.
3. *A message obtained from a computation involving previous messages is tagged with the intersection of the tags of* all *the messages involved in that computation.*
4. *A message* $(m,T)_D$ *is sent to player* P_D *only if* $D \in T$.

We now explain why Ted will not send a message that allows P_0 and P_1 to communicate or establish non-local correlations. Let $(m,T)_D$ be the message Ted is about to send to player P_D. From the fourth point of Definition 2.1, Ted will send $(m,T)_D$ only if it is tagged $T = \{D\}$ or $\{0,1\}$. Looking at the message's tag assignment rule number 3, this happens only if there is absolutely no message tagged $\{1-D\}$ or $\emptyset$ used in the computation of $(m,T)_D$. Using an induction argument, it is not hard to see that this happens only when all the variables involved in the computation of $(m,T)_D$ are independent of the information of P_{1-D}, that is, they have been themselves generated using variables tagged $\{D\}$ or $\{0,1\}$. Thus, such a message $(m,T)_D$ is also independent of the information known only to P_{1-D}. Therefore, the messages sent by Ted do not let the two players communicate.

The case of non-locality is slightly more subtle, yet pretty straightforward. Recall that in a general non-local process, both players use a message each and receive a message uniformly distributed, from their point of view, such that the four messages satisfy a certain relation. The received message does not allow to communicate with the other player. Suppose P_{1-D} receives his message first. Since from his point of view, this message is uniformly distributed, Ted *can* in fact generate a uniformly distributed message, tag it with $T := \{0,1\}$ and send it to P_{1-D}. At this point, this behavior does not violate anything because non-locality has not been created yet. Then, Ted computes the message for P_D. Because this message needs to satisfy the relation that binds together the four messages, at least a message tagged with $T \neq \{D\}$ and one tagged with $T \neq \{1-D\}$ are used in its computation (it can be the same message), so the resulting message $(m,T)_D$ will be assigned a tag $T := \emptyset$ because the intersection does not contain $\{D\}$ and $\{1-D\}$. This message $(m,\emptyset)_D$ is the one creating the non-local relation. However, from point 4 of Definition 2.1, since $D \notin \emptyset$, Ted will never send $(m,\emptyset)_D$.

As mentioned before the previous definition, we can alternatively formalize Ted's behavior in terms of entropy. Let the message about to be sent from Ted to prover P_D be represented by the variable $(M,T)_D$. The set of variables $S_{D,T}$ represents all the variables

(messages) with tag T sent by prover P_D to Ted, and the set of variables $R_{D,T}$ all the variables (messages) with tag T sent by Ted to prover P_D before $(M,T)_D$.

Definition 2.2 (Information based definition) *Ted is said to be a "secure third party" if* $\forall D \in \{0,1\}$, *Ted follows these points.*

1. *An information received from player* P_D *is tagged with* $T := \{D\}$[3].

2. *A variable* M *to be sent to* P_D *is tagged with the less restrictive tag* $T \in \{\emptyset, \{D\}, \{0,1\}\}$ *that satisfies the following relation*[4,5]. *Note that the calligraphic tag* $\mathcal{T}'$ *stands for the tag* $\{0,1\}/(T \cap \{D\})$ *and the calligraphic tag* $\mathcal{T}''$ *stands for the tag* $\{D\} \cup (T \cap \{1-D\})$.

$$\begin{aligned} & H((M,T)_D | S_{D,\{D\}}, R_{D,\{D\}}, R_{D,\{0,1\}}, S_{1-D,\mathcal{T}'}, R_{1-D,\mathcal{T}'}, R_{1-D,\{0,1\}}) \\ = \; & H((M,T)_D | S_{D,\mathcal{T}''}, R_{D,\mathcal{T}''}, R_{D,\{0,1\}}, R_{1-D,\{0,1\}}) \end{aligned} \tag{2.3}$$

3. *A variable* $(M,T)_D$ *is sent to player* P_D *only if* $D \in T$.

We warn the reader that the tags and players' variables D and $1-D$ do not play any role in the computation of the entropies; they are only present to discriminate the variables and determine which ones to include in the conditional part of the entropies. Notice also that, contrary to Definition 2.1, a variable's tag is set only when Ted consider sending it to a player, except for incoming variables. This relaxation will turn out to be the key point to explain why this generalized definition is not stronger than local variables on the players' side.

To strengthen the understanding, we first give an example of the application of this definition using the relation of the NL-box. Recall that P_0 has input X, P_1 input Y [6],

[3]This implies that the sets $S_{D,\{0,1\}}$ and $S_{1-D,\{0,1\}}$ are always empty. Therefore we did not include them in equation (2.3), but a formal expression should include them in the conditional part on both sides of the equality.

[4]In order to write a clear equation, we had to specify to which player the message is intended. As a result, we did not include $\{1-D\}$ in the set of possible tags. It turns out that the empty set tag is sufficient to cover both communication and correlation.

[5]Explanations for equation (2.3) will be provided after the example of its application.

[6]We are not using S and T for the variables' name to avoid notation conflicts with the set S and tag T used in Definition 2.2.

and they want to produce respectively a variable U and V such that the following relation holds,

$$X \wedge Y = U \oplus V.$$

Both players send their input to Ted, who tags them accordingly, i.e. $(X, \{0\})_0$ and $(Y, \{1\})_1$. Suppose U is the first message to be sent. Recall from Section 2.3 that U and V are individually uniformly distributed. Hence, Ted can pick U uniformly and send it to P_0, and U is tagged with $\{0,1\}$ [7]. Then Ted would like to send $V = U \oplus X \wedge Y$. Let's compute the left- and right-hand sides for the three possible tags. Notice that $S_{1,\{1\}} = \{(Y, \{1\})_1\}, S_{0,\{0\}} = \{(X, \{0\})_0\}, R_{0,\{0,1\}} = \{(U, \{0,1\})_0\}$, and all the other sets are empty.

- If we set $T := \emptyset$, then $T' = \{0,1\}$ and $T'' = \{1\}$. The left-hand side is

$$\begin{aligned} H((V,\emptyset)_1 | S_{1,\{1\}}, R_{1,\{1\}}, R_{1,\{0,1\}}, S_{0,\{0,1\}}, R_{0,\{0,1\}}) &= \\ H((V,\emptyset)_1 | (Y,\{1\})_1, (U,\{0,1\})_0) &= \frac{1}{2}. \end{aligned}$$

  The right-hand side is

$$\begin{aligned} H((V,\emptyset)_1 | S_{1,\{1\}}, R_{1,\{1\}}, R_{1,\{0,1\}}, R_{0,\{0,1\}}) &= \\ H((V,\emptyset)_1 | (Y,\{1\})_1, (U,\{0,1\})_0) &= \frac{1}{2}. \end{aligned}$$

- If we set $T := \{1\}$, then $T' = \{0\}$ and $T'' = \{1\}$. The left-hand side is

$$\begin{aligned} H((V,\{1\})_1 | S_{1,\{1\}}, R_{1,\{1\}}, R_{1,\{0,1\}}, S_{0,\{0\}}, R_{0,\{0\}}, R_{0,\{0,1\}}) &= \\ H((V,\{1\})_1 | (Y,\{1\})_1, (X,\{0\})_0, (U,\{0,1\})_0) &= 0. \end{aligned}$$

  The right-hand side is

$$\begin{aligned} H((V,\{1\})_1 | S_{1,\{1\}}, R_{1,\{1\}}, R_{1,\{0,1\}}, R_{0,\{0,1\}}) &= \\ H((V,\{1\})_1 | (Y,\{1\})_1, (U,\{0,1\})_0) &= \frac{1}{2}. \end{aligned}$$

[7] It is straightforward to verify that this is the less restrictive tag.

- If we set $T := \{0,1\}$, then $\mathcal{T}' = \{0\}$ and $\mathcal{T}'' = \{0,1\}$. The left-hand side is

$$\begin{aligned} H((V,\{0,1\})_1 | S_{1,\{1\}}, R_{1,\{1\}}, R_{1,\{0,1\}}, S_{0,\{0\}}, R_{0,\{0\}}, R_{0,\{0,1\}}) &= \\ H((V,\{0,1\})_1 | (Y,\{1\})_1, (X,\{0\})_0, (U,\{0,1\})_0) &= 0. \end{aligned}$$

The right-hand side is

$$\begin{aligned} H((V,\{0,1\})_1 | S_{1,\{0,1\}}, R_{1,\{0,1\}}, S_{0,\{0,1\}}, R_{0,\{0,1\}}) &= \\ H((V,\{0,1\})_1 | (U,\{0,1\})_0) &= 1. \end{aligned}$$

Thus the equation (2.3) holds only when $T := \emptyset$. It follows from point 3 that Ted won't send V to P_1, as expected.

The process of determining which tag to assign can be broken into two steps. We start with the empty tag $\emptyset$. The first step is to decide whether we can add $\{D\}$ to the tag, or not. Notice that the *right*-hand side of equation (2.3) is the same for $T \in \{\emptyset, \{D\}\}$. This results from the calligraphic tag $\mathcal{T}''$, which is equivalent to $\{D\}$ in this case. On the other hand, the calligraphic tag $\mathcal{T}'$ introduces the terms $S_{1-D,\{1-D\}}$ and $R_{1-D,\{1-D\}}$ in the *left*-hand side of equation (2.3) when $T = \{D\}$. Thus, if the result of this first step is that the tag is at least $\{D\}$, then it means that the message to be sent is independent of the private information held by P_{1-D}. However, if we find that the tag is not even $\{D\}$, then it means that the message to be sent has some dependencies with the private information of P_{1-D}, and therefore the message should not be sent.

If the first step terminates with a tag containing at least $\{D\}$, then we can move on to determine whether we can add $\{1-D\}$ to the tag, or not. We note that $\mathcal{T}'$ won't change for $T \in \{\{D\}, \{0,1\}\}$, so the *left*-hand side is invariant. However, the calligraphic tag $\mathcal{T}''$ will remove the terms $S_{D,\{D\}}$ and $R_{D,\{D\}}$ from the *right*-hand side if we consider the tag $T = \{0,1\}$. Hence, if equation (2.3) is satisfied with $T = \{0,1\}$, it means that the message to be sent is not only independent of the private information of P_{1-D} (from first step), but also of the private information of P_D. It follows naturally that this message be eligible for

distribution to both players.

The interest of Definition 2.2 is that it is more flexible in the tag assignation than the practical definition 2.1. Indeed, whenever Ted deliberately randomizes a message with new [uniformly distributed] information, the information-based tag assignment rule conclude that there is no problem to send to P_D a message that would have been tagged with $T = \{1-D\}$ or $\emptyset$ in the practical definition. We give two examples of these particular cases.

Let P_0 send to Ted a message represented by $(X, \{0\})_0$ (the variable X is tagged with $\{0\}$ and comes from P_0). Then Ted generates a uniform random variable $(W, T)_D$ (its tag and receiver have not been set yet) and produces the message $M = X \oplus W$ for P_1. Checking with equation (2.3) we see there is no problem setting M's tag to $\{1\}$, as

$$H((M, \{1\})_1 | (X, \{0\})_0) = H((W, T)_D) = H((M, \{1\})_1).$$

This is satisfied since $(W, T)_D$ is uniform and has never been sent. However, the practical definition would have assigned the tag $T := \{0\}$ since W's tag would have been $\{0, 1\}$ (by the second rule) and $\{0\} = \{0\} \cap \{0, 1\}$. Let Ted send $(M, \{1\})_1$. We now get that for *both* $D = 0$ and 1, if $T = \{D\}$ or $\{0, 1\}$ then the left-hand side of equation (2.3) for W is

$$H((W, T)_D | (X, \{0\})_0, (M, \{1\})_1) = 0,$$

and the right-hand side is respectively

$$\begin{aligned} H((W, \{0\})_0 | (X, \{0\})_0) = H((W, \{0\})_0) &= 1, \\ H((W, \{1\})_1 | (M, \{1\})_1) = H((X, \{0\})_0) &= 1, \\ H((W, \{0, 1\})_D) &= 1. \end{aligned}$$

Because equation (2.3) is not satisfied for both $T = \{D\}$ and $\{0, 1\}$, W's tag is set to $T := \emptyset$, and Ted should not send $(W, \emptyset)_D$ to neither of P_D, for $D = 0, 1$.

Similarly, we can send to P_1 a message M that would have been tagged $\emptyset$ by the practical definition. We again take the NL-box relation for example. Suppose the variables $(X, \{0\})_0$

and $(Y, \{1\})_1$ have already been sent to Ted by the players (and tagged accordingly), and $(U, \{0,1\})_0$ [8] has been sent by Ted to P_0. Let $(W,T)_D$ be a uniformly distributed random variable chosen by Ted, with $D \in \{0,1\}$. Consider the following variable for P_1,

$$V = U \oplus (W \oplus X) \wedge T,$$

that is, we randomized the variable tagged $\{0\}$ (i.e. X) in the NL-box relation. In the practical definition, because W is chosen uniformly and independently of previous variables, the second rule would have assigned a tag $\{0,1\}$ to it, and so V's tag would have been set to $\emptyset = \{0,1\} \cap \{0,1\} \cap \{0\} \cap \{1\}$. However, checking with equation (2.3), because W has not been sent yet, we get that there is no problem setting V's tag to $\{1\}$, as

$$H((V,\{1\})_1|(Y,\{1\})_1,(X,\{0\})_0,(U,\{0,1\})_0) = \frac{1}{2} = H((V,\{1\})_1|(Y,\{1\})_1,(U,\{0,1\})_0).$$

So Ted would send this message $(V, \{1\})_1$ to P_1. Is this a problem? No, because the classical limitations of non-locality have not be violated yet! The reason is simple: by randomizing completely all the [private] variables related to P_0, Ted is reducing the message he sends to P_1 to what P_1 can exactly achieve using local variables. That is to say, P_1 already has a random view of P_0's variables, so there is no problem for Ted to first randomize P_0's variables and then send this message to P_1. If we make the calculations, we see that indeed, for the variable V sent, the relation

$$V = U \oplus X \wedge Y$$

holds with probability 75%, just as in the classical scenario, and no W will never let us beat that. Of course, as in the previous example, the variable $(W,T)_D$ used to randomize can never be disclosed to *any* of the two players, and equation (2.3) agrees with that (W's tag will be set to $T := \emptyset$ for both D).

Thus, if the message intended to P_D is computed in such a way that it is independent of $S_{1-D,T}$ and $R_{1-D,T}$, for $T \in \{\{0\},\{1\},\emptyset\}$, i.e. it is randomized such that it no longer carries

[8] It is straightforward to verify that this is the less restrictive tag.

information that is known only to P_{1-D}, then the criteria of Definition 2.2 *does* let Ted send a message that would have been tagged $\{1-D\}$ or $\emptyset$ in the practical definition. However, the variables used to randomize such a message can never be disclosed to any of the players. But this is correct since it is now these variables that carry the information dependent on $S_{1-D,T}$ and $R_{1-D,T}$, for $T \in \{\{0\},\{1\},\emptyset\}$. In this sense, Definition 2.2 is more general than Definition 2.1 as it does not consider only the tag of a message to determine whether Ted should send it, but rather its relevant information content. Moreover, Definition 2.2 does let Ted send messages to the players that achieve the classical limitations of non-locality, that is, Ted never sends a message that outperforms what the players can achieve with local variables!

Henceforth, the two-prover model's assumption is based on this refined definition of isolation.

Definition 2.3 *Peggy and Paula are* isolated *from one another if they cannot communicate with one another, and for any third party Ted that interacts with Peggy and Paula, Ted is a* secure *third party.*

2.5 Fixing the proof of Theorem 2.3

We now prove the security of the sBGKW scheme with respect to this new definition. But let's first express the sBGKW scheme with the new terminology, to show that the protocol can indeed be completed in the context of the practical definition of isolation.

sBGKW

P_0 and P_1 agree on an n-bit string w. They are then isolated from one another according to Definition 2.3.

Commit to b:

- Vic sends a random n-bit string $(r,\{0,1\})_0$ to P_0,

- P_0 computes $x := (b \cdot r) \oplus w$ and sends it to Vic. Upon reception, Vic tags it $(x, \{0\})_0$.

Unveil b:

- P_1 announces b and an n-bit string w to Vic. Upon reception, Vic tags them $(b, \{1\})_1$ and $(w, \{1\})_1$.
- Let $e = 0$ if "$w = (b \cdot r) \oplus x$", and $e = 1$ otherwise. Vic accepts iff $e = 0$, and tags e with $(e, \emptyset)_D$ for both $D \in \{0, 1\}$.

Since the only communication from Vic to the provers is a random n-bit string, it is straightforward that the protocol will complete with the new isolation assumption.

Theorem 2.4 *Let Peggy (P_0) and Paula (P_1) be isolated as in Definition 2.3, then the* sBGKW *is secure classically.*

Proof: As before, the concealing condition is satisfied since Vic does not know w.

The previous section explained that in the setting of Definition 2.3, we are now *guaranteed* that any strategy that Peggy and Paula try to perform through a third party can be achieved using *only* local variables on each side. We also know from Theorem 1.3 that there's no gain for Peggy and Paula to use a probabilistic strategy; we can thus assume, without loss of generality, that a deterministic strategy is employed.

Suppose the two provers have a deterministic strategy that successfully produces w_0 when they want to unveil as $B = 0$, and w_1 when they want to unveil as $B = 1$. Because we are dealing with classical information, the instances of the local variables and the information of Peggy and Paula can be copied. From the deterministic behavior of the strategy, their classical strategy can be run on each copy of the information to output *both* $\hat{w}_0$ and $\hat{w}_1$, something we could not assert from only the no-communication assumption of [BGKW88]. Thus, any successful deterministic strategy would let Paula compute the string $\hat{w}_0 \oplus \hat{w}_1 = r$. However r is completely unknown to her by the no-communication assumption. Therefore, even using unlimited computational power, her probability of issuing a valid pair $\hat{w}_0, \hat{w}_1$ is at most $1/2^n$. This proves that sBGKW is binding.

□

Chapter 3

Intermediate schemes towards quantum secure bit commitment

We first exhibit two intermediate schemes to emphasize how shared entanglement can be used to cheat with probability one (or almost one) a classically secure two-prover bit commitment. The first protocol is a weaker version of the sBGKW scheme, called wBGKW, where the acceptance criteria of the unveiling stage is loosen to tolerate some errors. The second protocol is also a modified version of the sBGKW scheme where the acceptance criteria is based on the Magic Square game (see Section 3.2).

3.1 A weaker acceptance criteria: the wBGKW scheme

We need the following notion.

Definition 3.1 *The distance $d(x,y)$ of a pair of binary words x,y is the number of bit-positions where x and y differ.*

In this section we consider a weaker version of sBGKW, called wBGKW, where the acceptance criteria of the verifier Vic is to accept b and $\hat{w}$ if $d(\hat{w}, x \oplus (b \cdot r)) < n/5$. This means that the string $\hat{w}$ sent by Paula differs in at most $n/5$ positions from what it should be. In comparison, in sBGKW the acceptance criteria is $d(\hat{w}, x \oplus (b \cdot r)) = 0$. Note that

the choice of b is part of the expectation. The interest of such a modification is that now a cheating quantum pair Peggy and Paula, isolated as in Definition 2.3, can use the non-local property of entanglement to implement an NL-box and successfully cheat wBGKW, while, as we show next, the bit commitment is secure classically. To facilitate notation we add an index b to the string $\hat{w}$, since $\hat{w}$ is different whether we unveil zero or one. Also, define as B the random variable corresponding to the value they unveil.

Theorem 3.1 *For any classical strategy, the probability that it outputs a string $\hat{w}_0$ when $B = 0$ and $\hat{w}_1$ when $B = 1$ such that $E[d(\hat{w}_b, x \oplus (b \cdot r))] < n/5$ for both values of b, is exponentially small in n.*

Proof: Using the same arguments as in the proof of Theorem 2.4, we can assume the provers use a deterministic strategy that may produce such a $\hat{w}_0$ when $B = 0$, and $\hat{w}_1$ when $B = 1$, so they can in fact output *both* $\hat{w}_0$ and $\hat{w}_1$. Hence, Paula can compute the string $\hat{w}_0 \oplus \hat{w}_1$. Recall that when $d(\hat{w}_b, x \oplus (b \cdot r)) = 0$ then $\hat{w}_0 \oplus \hat{w}_1 = r$. We want to determine the distance between $\hat{w}_0 \oplus \hat{w}_1$ and r for this situation. From the theorem's assumption, there exists a classical strategy that outputs $\hat{w}_0$ *and* $\hat{w}_1$ such that $E[d(\hat{w}_b, x \oplus (b \cdot r))] < n/5$, for $B = 0, 1$. We easily obtain that for such a strategy, the expected distance from r is

$$E[d(\hat{w}_0 \oplus \hat{w}_1, r)] = E[d(\hat{w}_0 \oplus \hat{w}_1, x \oplus (x \oplus r))] \leq E[d(\hat{w}_0, x)] + E[d(\hat{w}_1, x \oplus r)] < 2n/5$$

by the triangular inequality. Using a standard Chernoff Bound argument, and since r is absolutely unknown to Paula, her probability of outputting a string $z = \hat{w}_0 \oplus \hat{w}_1$ such that $E[d(z, r)] < (1/2 - \epsilon) \cdot n$ is exponentially small in n for any $0 < \epsilon \leq 1/4$. Hence, because $2/5 < 1/2$, we conclude that such a strategy cannot exist except with exponentially small probability, and so unveiling *must* fail for one of the two possibilities.

□

Conversely, this scheme is almost totally insecure against quantum adversaries.

Theorem 3.2 *There exists a quantum strategy that successfully cheats the* wBGKW *scheme with probability* $1 - \mu(n)$.

Proof: We saw in Section 2.3 that the NL-box, taken as a black box, correctly produced the needed $\hat{w}_b$ to unveil as b. Using the result of Theorem A.5 of Appendix A, we get that through entanglement, Peggy and Paula can optimally simulate the NL-box such that for each i taken independently, $1 \leq i \leq n$, the NL-box produces correlated outputs with probability $\cos^2(\pi/8) \approx 0.85$. Therefore, using the standard Chernoff Bound, this independent quantum strategy yields that for both values of b

$$E[d(\hat{w}, x \oplus (b \cdot r))] = (1 - \cos^2(\pi/8)) \cdot n,$$

with probability exponentially close to one. Having that

$$(1 - \cos^2(\pi/8)) \cdot n < 0.15 \cdot n < n/5,$$

we conclude that a pair of quantum provers defeat the binding condition of the scheme with probability $1 - \mu(n)$.

□

3.2 The Magic Square

The magic square game is a two-player pseudo-telepathy game that was presented by Padmanabhan Aravind [Ara02, Ara03], who built on work by Mermin [Mer90]. The most interesting feature of this game is that it is extremely easy to show that there cannot be a classical strategy that wins with probability one (see Section A.2.1). It follows that a successful implementation of the quantum winning strategy (see Section A.2.2) would convince any observer that something classically impossible is happening, *with no need for the observer to understand why the quantum strategy works.*

3.2.1 The game

A *magic square* is a 3×3 matrix whose entries are in $\{0, 1\}$, with the property that the sum of each row is even and the sum of each column is odd. Such a square is magic because it cannot exist! Indeed, suppose we calculate the parity of the nine entries, that is, the parity

of the whole square. This value is equal to the parity of the parities of the three rows *and* equal to the parity of the parities of the three columns. However, according to the rows the parity is even, yet according to the columns, the parity is odd! This is obviously impossible.

The task that the players face while playing the game is the following. Let $x, y \in \{0, 1, 2\}$. Peggy is asked to give the entries of the x-th row, labeled $r^x := r_0^x r_1^x r_2^x$, and Paula is asked to give the entries of the y-th column, labeled $c^y := c_0^y c_1^y c_2^y$. To win the game, the parity of the row r^x must be even, the parity of the column c^y must be odd, and the intersection of the given row and column must agree, that is $r_y^x = c_x^y$.

Classical and quantum optimal strategies can be found in Section A.2 of Appendix A.

3.2.2 Magic Square bit commitment

The Magic Square bit commitment scheme, named MSBC, is an original idea due to Claude Crépeau. This scheme is particularly relevant in our study of bit commitments in the two-prover model as it is perfectly secure classically but can easily be cheated with probability one using a quantum strategy. First, define the *validity* of a square.

Definition 3.2 *A* (3×3) *matrix* S_x is valid *for bit* x *if all rows of* S_x *xor to 0 when* $x = 0$ *and all columns of* S_x *xor to 1 when* $x = 1$.

For instance the following matrix S_0 is valid for zero while S_1 is valid for one:

$$S_0 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \quad S_1 = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}. \tag{3.1}$$

The scheme is as follows.

MSBC

> Peggy and Paula agree on a random n-bit string w and an identical random square $S_i^{Peggy} = S_i^{Paula}$ for each bit w_i of w such that S_i is valid for w_i. They are then isolated as in Definition 2.3.

Commit to b:

- Vic chooses a random n-bit string a and sends it to Peggy. Label $a_0 := 0^n$, the all 0's n-bit string, and $a_1 := a$.
- Peggy computes $x := a_b \oplus w$ and sends x to Vic.

Unveil b:

- Peggy sends b to Vic.
- Vic computes $\hat{w} := a_b \oplus x$.
- Vic challenges Peggy and Paula for each bit $\hat{w}_i$ of $\hat{w}$ using a test on the squares S_i^{Peggy} and S_i^{Paula}. Vic picks a pair of random trits t_i^{Peggy} and t_i^{Paula} and asks Peggy for row number t_i^{Peggy} of S_i^{Peggy} and Paula for column number t_i^{Paula} of S_i^{Paula}.
- Vic accepts b if for each i, the row or column that should xor to $\hat{w}_i$ does, and if the intersection of the row and column is identical from both Peggy and Paula. Vic rejects otherwise.

Note that this scheme does not differ much from the sBGKW scheme. Instead of having Paula send explicitly w, both Peggy and Paula send information to Vic to allow him to reconstruct w. Indeed, we can easily see that the magic squares are just a very redundant version of w. If Vic sees all the magic squares of Peggy-Paula at unveiling, it is just repeating him what w was for each of Peggy and Paula. He can then compare this w to his $\hat{w}$ and decide whether or not he should accept b.

We now prove that the MSBC is secure classically. It is straightforward to see that the concealing property holds for Vic who does not know w.

Theorem 3.3 *Any classical strategy successfully cheats the binding property of the* MSBC *scheme with probability at most* $\left(\frac{8}{9}\right)^{n/6}$*, except with exponentially small probability.*

Proof: In order to cheat the bit commitment scheme, Peggy and Paula must be able to win a weaker form of the Magic Square pseudo-telepathy game given in Section 3.2.1, where

for each i Vic verifies only that the row or column that should xor to $\hat{w}_i$ does, instead of verifying that the row xores to zero *and* the column xores to one. Using the result of Theorem 1.3, we only need to consider deterministic strategies.

To simplify the proof, assume that Peggy *always* knows when she is being tested. The probability of successfully cheating we will obtain under this assumption will be an upper bound on the probability for any other strategy. One of the key point is that we cannot make the same assumption regarding Paula: since she doesn't know the random string $a_1 := a$ sent by Vic to Peggy, she cannot tell whether she is being tested or not. Hence, when she's asked a column that does not xor to 1, she doesn't know if she has to change one of the bit to make it xor to 1.

However, Paula is using a deterministic strategy and Peggy knows all the information possessed by Paula, except for the number t_i^{Paula} asked by Vic. This means that Peggy can do the same computations as defined by Paula's strategy to get the three possible columns that Paula could output. Note that, put together, these three columns form a square S which is *the* square that holds the most relevant information regarding Paula's choices[1]. Without lost of generality, we can thus assume that Paula always output a column that xores to 1, and if needed, modifies the first bit of the column. So Paula always succeeds her challenges. To simplify the proof further, we can assume that the last two rows of all the squares $S_i^{Peggy} = S_i^{Paula}$ they share in the beginning of the protocol always xor to 0.

Consider a challenge i where Peggy is being tested (otherwise she simply outputs the row t_i^{Peggy} asked by Vic and they succeed the challenge). As long as $t_i^{Peggy} = 1$ or 2, she can simply outputs the required row and succeed without being caught. However, with probability 1/3, $t_i^{Peggy} = 0$, and from Paula's strategy, this row xores to 1 in the square S corresponding to the three possible columns answered by Paula. So Peggy has to modify

[1]Hence, to maximize her probability of cheating, Peggy needs to base her strategy on S when returning the row asked by Vic.

one bit of the row. With probability 1/3, she will modify the bit corresponding to the column number t_i^{Paula}, and they will get caught. Therefore, for a challenge i, when Peggy is being tested, their probability of success is at most 8/9.

By independence of the challenges, we get that the success probability is at most 8/9 for each one where Peggy is being tested. Let x be the string sent by Peggy, prepared according to the strategy of her choice. Since $\hat{w}_i = x \oplus a_b$, the test will toggle between Peggy and Paula whenever $a_b = 1$. The problem for Peggy is that whenever the test toggles, she can succeed with certainty for at most only one of $b \in \{0, 1\}$. Since a is uniformly distributed, using a Chernoff argument, except with exponentially small probability, the string $a_1 := a$ contains $n/3$ 1's. Thus, there is at least one of $b \in \{0, 1\}$ for which in at least $n/6$ challenges Peggy will answer correctly with probability at most 8/9 (the sum of the challenges where she succeeds with probability at most 8/9 for 0 and those where she succeeds with probability at most 8/9 for 1 adds up to $n/3$). Therefore, their probability of successfully cheating is at most

$$\left(\frac{8}{9}\right)^{n/6}$$

for any classical strategy.

□

It follows that for n big enough, the MSBC scheme is binding. Conversely, this scheme is totally insecure against quantum adversaries.

Theorem 3.4 *There exists a quantum strategy that successfully cheats the* MSBC *scheme with probability one.*

Proof: Using the quantum strategy presented in Section A.2.2, a quantum pair Peggy-Paula can *always* produce a row and column that satisfy the winning condition of the Magic Square game (Section 3.2.1). Hence they can unveil for both values of b with probability one.

□

Chapter 4

Quantum secure bit commitment in the two-prover model

We now present the modified version of the sBGKW scheme, called the mBGKW scheme, and prove its security against quantum adversaries. Although the two schemes are almost identical, it turns out the proof against quantum provers is easier with the latter. The security of the sBGKW and BGKW schemes will follow as a corollary of mBGKW's security.

4.1 The scheme

mBGKW

Peggy and Paula agree on an n-bit string w. They are then isolated as in Definition 2.3.

Commit to b:

- Vic sends two random n-bit strings r_0, r_1 to Peggy.
- Peggy replies with $x := r_b \oplus w$.

Unveil b:

- Paula announces an n-bit string $\hat{w}$ to Vic.

- Vic computes $r := \hat{w} \oplus x$. He accepts iff $r \in \{r_0, r_1\}$ and deduces b from $r = r_b$.

4.2 mBGKW is secure against quantum adversaries

We want to show that the mBGKW scheme is secure against a quantum adversary. Clearly the commitment is concealing because Vic does not know w. This means that there exists w and w' such that $x = r_0 \oplus w = r_1 \oplus w'$, and Vic cannot determine which of w or w' has been used. This is merely an application of the One-Time Pad (Vernam Cipher). We refer the reader to [Sti05] for a complete proof of its security, which provides a nice information theoretic argument why Vic cannot learn any information about r_b.

Before diving into the formal proof that the binding property holds, let's first sketch the background intuition. We use Definition 1.4 to give the security argument for the binding property. As in Definition 1.4, let p_0 be the probability of successfully unveiling zero and p_1 be the probability of successfully unveiling one. Imagine Peggy and Paula are able to open $B = 0$ or $B = 1$ with a good probability of success. This means that Paula can announce $\hat{w}_0$ such that $r_0 = \hat{w}_0 \oplus x$ or $\hat{w}_1$ such that $r_1 = \hat{w}_1 \oplus x$, depending upon whether $B = 0$ or $B = 1$ is unveiled. We stress that, unlike in the classical scenario, even if they use a deterministic[1] quantum strategy to get $\hat{w}_0$ or $\hat{w}_1$, we cannot assert that Paula is able to generate both, since quantum states cannot be copied (see [NC00], pages 24 and 532 for details), so the process cannot be repeated exactly. It follows that with a quantum strategy, we can always hope to have $\hat{w}_0$ and $\hat{w}_1$, but not both at the same time, with non-negligible probability. We refer the reader to the introductory Section 1.2 for clarifications on this important distinction with the classical setting, particularly with Definition 1.3.

Yet, the crucial observation on which our proof relies is the same as in the classical case, namely that if Paula could simultaneously compute $(\hat{w}_0, \hat{w}_1)$, then she would learn

[1]The process (algorithm) can be deterministic, still the final result will be random, by the probabilistic nature of quantum mechanics and measurements.

$r_0 \oplus r_1 = \hat{w}_0 \oplus \hat{w}_1$. Clearly, this should not be possible with probability higher than 2^{-n} since Paula does not have any information about r_0 and r_1 [2]. However, we will not use this bound directly as the security marker, but rather as an optimal limit to upper bound the equation $p_0 + p_1$ of Definition 1.4.

Ideally, one expects that for any cheating strategy

$$p_0 + p_1 \leq 1 + \frac{1}{2^n}, \tag{4.1}$$

the bound achieved when Peggy and Paula are classical. However, it turns out this upper bound is not so easy to reach; the analysis needed to produce an upper bound that tight needs to be incredibly precise. Fortunately, as long as we get something bounded above by $1 + \mu(n)$ the binding condition is satisfied. The consequence of the next lemma gives an upper bound slightly weaker than (4.1) by about a square root distance to 1.

Define

$$p_{\oplus} := \Pr[\text{Paula determines } r_0 \oplus r_1].$$

The next lemma relates $p_{\oplus}$ to $p_0 + p_1$. We show that whenever $p_0 + p_1$ is greater than $1 + \varepsilon$, Paula can guess $r_0 \oplus r_1$ with probability at least ε^2. Then, exploiting the fact that the probability $p_{\oplus}$ to determine $r_0 \oplus r_1$ is 2^{-n}, the binding condition will naturally follows.

Lemma 4.1 *Assume Peggy and Paula have probability p_b to open b successfully such that $p_0 + p_1 \geq 1 + \varepsilon$ for $\varepsilon > 0$. Then, Paula can guess $r_0 \oplus r_1$ with probability $p_{\oplus} \geq \varepsilon^2/4$.*

Proof: Assume without loss of generality that when the unveiling phase of mBGKW starts, Paula holds the pure state $|\psi\rangle \in \mathcal{H}^N$ of dimension $N \geq 2^n$. Note that we do not need to consider the whole bipartite state between Peggy and Paula since when the unveiling phase starts, Peggy does no longer play an active role in the protocol and no communication is allowed between the two; hence her system can be traced-out of the global Hilbert space.

[2] Recall that no quantum process can send information from Peggy to Paula without communicating some classical information. Therefore $r_0 \oplus r_1$ remains uniformly distributed over $\{0,1\}^n$ during the execution of the whole protocol.

Moreover, by linearity, the proof also holds if $|\psi\rangle$ is replaced by a mixed state. Notice also that, from the new model's assumption (see Section 2.4), Peggy and Paula cannot do better using a third party than what they can achieve with entanglement; the state $|\psi\rangle$ can thus be seen as her part of the shared entangled state.

Generally speaking, Paula has two possible strategies depending upon the bit b she wants to unveil. When $B = 0$, she applies a unitary transform U_0 to $|\psi\rangle$ in order to get the state $|\psi_0\rangle := U_0|\psi\rangle$ that she measures in the computational basis $\{|w\rangle\langle w|\}_{w\in\{0,1\}^n}$ applied to the first n qubits of $|\psi_0\rangle$. When $B = 1$, she proceeds similarly with unitary transform U_1 allowing to prepare the state $|\psi_1\rangle := U_1|\psi\rangle$. She then measures $|\psi_1\rangle$ using the same measurement as for $B = 0$. All general measurement can be realized in this fashion, this is thus a general strategy for Paula. Notice that in the proof of Kent [Ken05], the use of unitary transformations U_0 and U_1 is obscured by the fact that he works with projective measurements. Notice also that the measurement on the first n qubits of $|\psi_b\rangle$ can alternatively be expressed by the measurement operators $\{|w\rangle\langle w| \otimes I_M\}_{w\in\{0,1\}^n}$ on the whole state $|\psi_b\rangle$, where I_M is the identity matrix on the system of dimension $M = N/2^n$.

From the values $r_0, r_1, x \in \{0,1\}^n$ announced by Vic and Peggy during the committing phase, we define $\hat{w}_b := r_b \oplus x$ as the string Paula has to announce in order to open b with success. We have,

$$p_b = \langle\psi_b|\hat{w}_b\rangle\langle\hat{w}_b|\psi_b\rangle, \tag{4.2}$$

which by assumption satisfies

$$p_0 + p_1 \geq 1 + \varepsilon,\ \varepsilon > 0. \tag{4.3}$$

Notice that $\langle\psi_b|\hat{w}_b\rangle$ is a generalized inner product[3] since $|\hat{w}_b\rangle$ lives in a subspace of dimension 2^n in $\mathcal{H}^N$. Therefore when $\hat{w}_b$ is obtained, there is some state left in $\mathcal{H}^N$ of dimension $N/2^n$ which we label as $|\hat{v}_b\rangle$ (i.e. $|\psi_b\rangle$ has not been completely collapsed by the measurement).

[3] If $|w\rangle \in \mathcal{H}^M$ and $|\psi\rangle \in \mathcal{H}^N$ then for $|\psi\rangle^N = \sum_i \alpha_i |a_i\rangle^M \otimes |b_i\rangle^{N/M}$ we define $\langle w|\psi\rangle = \sum_i \alpha_i \langle w|a_i\rangle|b_i\rangle$.

Thus, using (4.2) we can write $|\psi_b\rangle$ as

$$|\psi_b\rangle = \sqrt{p_b}|\hat{w}_b\rangle|\hat{v}_b\rangle + \sqrt{1-p_b}|\hat{w}_b^{\perp}\rangle, \tag{4.4}$$

where $\|\langle\hat{v}_b|\langle\hat{w}_b|\hat{w}_b^{\perp}\rangle\|^2 = 0$. Note that the "state" $|\hat{w}_b^{\perp}\rangle$ has not necessarily a physical signification. It is simply a mathematical tool that allows us to conveniently carry the statistics.

We want to determine a lower bound for the probability $p_{\oplus}$. One possible way for Paula to compute $r_0 \oplus r_1$ is to obtain $\hat{w}_0$ and $\hat{w}_1$ individually. Again, one possible way to do this is to use the following strategy:

1. Paula applies the strategy allowing to open $B = 0$ from $|\psi_0\rangle = U_0|\psi\rangle$ resulting in the state $|\tilde{\psi}_0\rangle$ after the measurement in the computational basis $\{|w\rangle\langle w|\}_{w\in\{0,1\}^n}$ has been performed on the first n qubits, and

2. Paula prepares $|\tilde{\psi}_1\rangle := U_1 U_0^{\dagger}|\tilde{\psi}_0\rangle$ before applying again the measurement in the computational basis $\{|w\rangle\langle w|\}_{w\in\{0,1\}^n}$ on the first n qubits.

Note that when preparing $|\tilde{\psi}_1\rangle$, we applied $U_0^{\dagger}$ before U_1. This is to put back the state $|\tilde{\psi}_0\rangle$ as close as possible as the original state $|\psi\rangle$. From (4.3) and for N big enough, the probability to measure $\hat{w}_0$ in the first step is not too small and so, by applying the inverse of all the unitary transformations generated by U_0, the state $|\tilde{\psi}\rangle$ we get before applying U_1 is a good enough approximation of the original $|\psi\rangle$. Similarly we can say that the fidelity $F(|\tilde{\psi}\rangle, |\psi\rangle)$ is large enough. By invariance under unitary transformation, it follows that $|\tilde{\psi}_1\rangle$ approximates $|\psi_1\rangle$ with the same fidelity $F(|\tilde{\psi}\rangle, |\psi\rangle)$.

In the strategy described above, the probability to determine $r_0 \oplus r_1$ is

$$p_0 \cdot p_{\hat{w}_1|\hat{w}_0} \cdot$$

As we said earlier, this is only *one of the* possible strategies to determine $r_0 \oplus r_1$, thus

$$p_{\oplus} \geq p_0 \cdot p_{\hat{w}_1|\hat{w}_0} \cdot$$

Let us first find a lower bound on the probability $p_{\hat{w}_1|\hat{w}_0}$ to produce $\hat{w}_1$ given that $\hat{w}_0$ has already been produced after step 1. Since $\hat{w}_0$ was obtained, the state $|\tilde{\psi}_0\rangle$ is equal to $|\hat{w}_0\rangle|\hat{v}_0\rangle$. We have,

$$\begin{aligned}
|\tilde{\psi}_1\rangle &= U_1 U_0^\dagger |\tilde{\psi}_0\rangle \\
&= U_1 U_0^\dagger |\hat{w}_0\rangle|\hat{v}_0\rangle \\
&= U_1 \left(U_0^\dagger \frac{|\psi_0\rangle}{\sqrt{p_0}} - U_0^\dagger \sqrt{\frac{1-p_0}{p_0}} |\hat{w}_0^\perp\rangle \right) && (4.5) \\
&= U_1 \frac{|\psi\rangle}{\sqrt{p_0}} - U_1 U_0^\dagger \sqrt{\frac{1-p_0}{p_0}} |\hat{w}_0^\perp\rangle && (4.6) \\
&= \frac{|\psi_1\rangle}{\sqrt{p_0}} - U_1 U_0^\dagger \sqrt{\frac{1-p_0}{p_0}} |\hat{w}_0^\perp\rangle && (4.7) \\
&= \frac{1}{\sqrt{p_0}} \left(\sqrt{p_1}|\hat{w}_1\rangle|\hat{v}_1\rangle + \sqrt{1-p_1}|\hat{w}_1^\perp\rangle - U_1 U_0^\dagger \sqrt{1-p_0}|\hat{w}_0^\perp\rangle \right), && (4.8)
\end{aligned}$$

where (4.5) follows from isolating $|\hat{w}_0\rangle|\hat{v}_0\rangle$ in (4.4), (4.6) and (4.7) are obtained by definition of U_0 and U_1 respectively, and (4.8) also follows from (4.4). At this point, Paula applies the measurement in the computational basis in order to obtain $\hat{w}_1$. Since we are interested only in finding a lower bound, the probability to obtain $\hat{w}_1$ is minimized when $U_1 U_0^\dagger |\hat{w}_0^\perp\rangle = |\hat{w}_1\rangle|\hat{v}_1\rangle$. It easily follows that,

$$\begin{aligned}
p_{\hat{w}_1|\hat{w}_0} &= \langle\tilde{\psi}_1|\hat{w}_1\rangle\langle\hat{w}_1|\tilde{\psi}_1\rangle \\
&\geq \frac{1}{p_0}\left(\sqrt{p_1} - \sqrt{1-p_0}\right)^2 && (4.9) \\
&\geq \frac{1}{p_0}\left(\sqrt{p_1} - \sqrt{p_1-\varepsilon}\right)^2 && (4.10) \\
&\geq \frac{\varepsilon^2}{4p_0}, && (4.11)
\end{aligned}$$

where (4.9) follows from (4.8), (4.10) is obtained from (4.3), and (4.11) follows from a Taylor expansion. Finally, (4.11) gives the desired result since

$$p_\oplus \geq p_0 \cdot p_{\hat{w}_1|\hat{w}_0} \geq \frac{\varepsilon^2}{4}.$$

□

Theorem 4.2 *The binding condition of* mBGKW *satisfies* $p_0 + p_1 \leq 1 + \frac{1}{\sqrt{2^{n-2}}}$.

Proof: From the isolation assumption, we have

$$p_{\oplus} = \frac{1}{2^n} .$$

Using the result from Lemma 4.1,

$$\frac{1}{2^n} \geq \frac{\varepsilon^2}{4} \quad \Longrightarrow \quad \varepsilon \leq \frac{1}{\sqrt{2^{n-2}}} . \tag{4.12}$$

It follows that the binding condition is satisfied: plugging (4.12) in (4.3), we get for any cheating strategies

$$p_0 + p_1 \leq 1 + \frac{1}{\sqrt{2^{n-2}}} .$$

□

The next corollary summarizes the security of the mBGKW against a cheating pair Peggy-Paula with access to quantum resources.

Corollary 4.3 *If there exists an algorithm A that can cheat the* mBGKW *bit commitment scheme with probabilities $p_0 + p_1 \geq 1 + 1/p(n)$, for every polynomials $p(\cdot)$ and all sufficiently large n's, then there exists an algorithm A' that can predict an unknown n-bit string $(r_0 \oplus r_1)$ with probabilities $1/4p(n)^2$, which is impossible.*

Indeed the following stronger statement is also true:

Corollary 4.4 *If there exists an algorithm A that can cheat the* mBGKW *bit commitment scheme with probabilities $p_0 + p_1 > 1 + (1/\sqrt{2})^n$ then there exists an algorithm A' that can predict an unknown n-bit string $(r_0 \oplus r_1)$ with probabilities better than $1/2^n$, which is impossible.*

Notice the square root gap between the intuitively expected binding condition $1 + \frac{1}{2^n}$ and the proven result of Corollary 4.4. This is merely the consequence of the crude lower bound we found for $p_{\oplus}$. A more precise analysis covering more strategies to compute $r_0 \oplus r_1$ and results on the maximum information we can extract from optimal measurement on $|\psi\rangle$ might close the gap. Nevertheless, this small hole is not important enough to compromise

the security of the mBGKW scheme because the binding condition is still exponentially close to one.

Notice also that the proof presented in Lemma 4.1 can easily be generalized to a whole class of bit commitment schemes with the properties that information unknown to Paula is sent to Peggy to commit, and an *exact* answer is needed from Paula to unveil successfully the committed bit. Corollary 4.4 therefore holds for a whole class of bit commitment scheme in the two-prover model.

Note finally that sBGKW is the same as mBGKW where $r_0 := 000...0$ is the all-zero string all the time. The statement and proof of Lemma 4.1 is equally valid for any fixed choice of either (but not both) r_0 or r_1 because the probability to predict $r_0 \oplus r_1$ remains exponentially small. Hence using only the model's assumption we get

Corollary 4.5 *If there exists an algorithm A that can cheat the* sBGKW *bit commitment scheme with probabilities $p_0 + p_1 > 1 + (1/\sqrt{2})^n$ then there exists an algorithm A' that can predict an unknown n-bit string r with probabilities better than $1/2^n$, which is impossible.*

4.3 Reduction to the original BGKW scheme

Building on Corollary 4.5, we can easily derive a similar result for the original BGKW scheme. Consider the following reduction from the BGKW scheme to the sBGKW scheme. First, Peggy and Paula perform their cheating algorithm for the BGKW scheme as usual. Suppose they successfully cheat for b; check Section 2.3.1 and Figure 2.2 to get a flavor of what a successful strategy is supposed to output. For each bit of the random string r and choice of bit b, Peggy receives the trit x_i and Paula receives the trit $y_i := (r_i + 1)(b + x_i) \mod 3$ from their strategy. They then convert these trits into bits to answer the sBGKW scheme, as follows:

1. Peggy sends the bit $x'_i := \big((r_i + 1)x_i \mod 3\big) \mod 2$.
2. Paula sends the bit $y'_i := \big(y_i + 2b \mod 3\big) \mod 2$.

It is straightforward to check that x' and y' are indeed the correct outputs to cheat the sBGKW scheme. When $b = 0$ then the successful strategy for BGKW outputs $y_i := (r_i+1)x_i \mod 3$. Setting $y'_i := y_i \mod 2$ yields $y'_i = x'_i$, which is the correct value to unveil as $b = 0$ in the sBGKW scheme. When $b = 1$ then $y_i := (r_i+1)x_i+r_i+1 \mod 3$. Setting $y'_i := (y_i+2 \mod 3) \mod 2$ we get

$$\begin{aligned} y'_i &= (y_i + 2 \mod 3) \mod 2 \\ &= (r_i + 1)x_i + r_i + 1 + 2 \mod 3 \mod 2 \\ &= ((r_i + 1)x_i \mod 3 \mod 2 + r_i \mod 3 \mod 2) \mod 3 \mod 2 \\ &= x'_i + r_i \mod 2. \end{aligned}$$

where we can drop the "mod 3" in the last equality since both x'_i and r_i are bits (their sum is always less than three). Again this is the correct value to unveil as $b = 1$ in the sBGKW scheme. In the black-box model, the reduction can be depicted as in Figure 4.1.

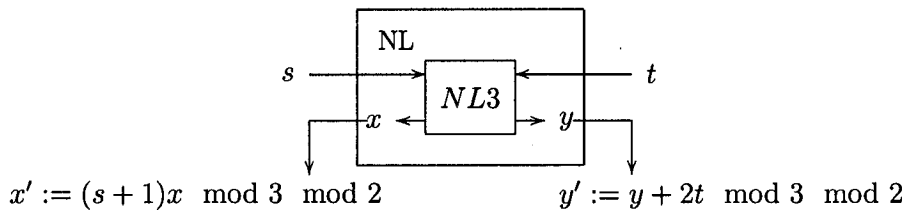

Figure 4.1: Reduction from the NL-box to the NL3-box.

Thence, from this reduction it holds that

$$p_b \stackrel{\text{def}}{=} \Pr[\text{unveil for } b \text{ in sBGKW}] \geq \Pr[\text{unveil for } b \text{ in BGKW}],$$

and we can conclude that the original BGKW scheme is also secure against quantum provers under the new model's assumption.

Corollary 4.6 *If there exists an algorithm A that can cheat the* BGKW *bit commitment scheme with probabilities $p_0 + p_1 > 1 + (1/\sqrt{2})^n$ then there exists an algorithm A' that can predict an unknown n-bit string r with probabilities better than $1/2^n$, which is impossible.*

Conclusion and open problems

In this thesis we have shown that the long-standing assumption of no-communication between the two provers was not sufficiently precise to preserve the binding property of a bit commitment scheme against all possible attacks. An extra assumption concerning the verifier, and more generally any third party the two provers may have access to, needs to be made to prevent him to send correlated messages to the provers, even if those messages do not allow to explicitly communicate. This refinement has been formally modeled with Definition 2.1.

The questions whether there exists classically secure commitment schemes that are insecure against quantum provers, and whether there exists commitment schemes secure against quantum provers, have both found affirmative answers. Once again, this highlights the fact that even in the two-prover model, the question as whether a classically secure commitment scheme is also secure against quantum adversaries is non-trivial. Indeed, we have presented two schemes, the wBGKW and MSBC schemes, that can be cheated with probability one, or exponentially close to one, if the provers share entanglement. On the other hand, we also presented a scheme, the mBGKW scheme, for which a proof that no quantum strategy can cheat the commitment was given. The security of the original BGKW commitment scheme has been proved by reduction from the security of the mBGKW scheme.

A natural question with respect to our new model's assumption is how can it be loosened. Actually, it forbids Peggy an Paula to have access to *any kind* of non-local boxes

(which may be perfectly implemented through a third party); however such a strong restriction does not necessarily need to be imposed. Take for instance the sBGKW scheme in the classical setting. Permitting Peggy and Paula to have access to a non-local box for the Magic Square game would not give them the ability to cheat the commitment scheme: if instead of the non-local box we let them have the entanglement that implements perfectly such a box (see Section A.2.2), something that makes them strictly more powerful, then we know from Lemma 4.1 that it does not help them to cheat. Still, our model's assumption does not allow such an inconsequential box! So how can the assumption be further refined? Which boxes can we allow in the assumption, and which can we not? How can we prove that a non-local box is futile without invoking Lemma 4.1?

The various applications of the sBGKW scheme also need to be studied. A direct consequence of its security against quantum adversaries is probably the possibility to elaborate *quantum zero-knowledge proofs* in the two-prover model. Using simple classical techniques from [BGG+89] and [IY87] its seems rather straightforward for the two provers to prove in zero-knowledge any statements in IP=PSPACE. However, as discussed in the introduction, up to which complexity class it is possible to do so is not known, unless the amount of entanglement shared between the provers is bounded by some a priori fixed polynomial in the input length.

Questions like is it possible to build a *quantum oblivious transfer* protocol using the construction of [CK88, Cré97], or a *quantum mutual identification* protocol as in [CS95] are also intriguing. Determining if the quantum scheme presented in Section 4.2 is binding with respect to the stronger Definition 1.5 is still an open problem.

Appendix A

Classical and quantum optimal implementation of the NL-box and the Magic Square game

Since its discovery by Einstein, Podolsky and Rosen, in the famous "thought experiment" of [EPR35], and taking all its profound fundamentality with the controversial result of John Bell in 1964 [Bel64], non-locality and its impact has been one of the major line of research in quantum mechanics. As presented in [NC00],

> *"[...] substantial experimental evidence together with the large set of inequalities generically known as the* Bell inequalities *showed that non-local correlations are a fundamental difference between classical and quantum physics, often referred as the* non-classical *property of quantum mechanics."*

On a more practical hand, in quantum computation and information, non-locality is introduced as entanglement shared between two (or more) parties. It is surprising to see how non-locality can be exploited as a resource to perform information processing task impossible using classical physic, e.g. quantum teleportation [BBC$^+$93] and superdense coding [BW92].

A.1 The CHSH game

Non-locality is often best explained in the framework of cooperative games, where two (or more) players play cooperatively against a verifier. In this section, we are mostly interested by the so-called CHSH game, after the initials of its four discovers Clauser, Horne, Shimony, and Hold [CHSH69]. The CHSH game, which leads to the well-known CHSH inequality, is among the first cooperative game ever studied for which the simple question "can we do better using entanglement" found an affirmative answer. The following shows how and by which amount we can do better than if we bound ourselves to use a classical strategy. Although it would be quite interesting to give a new technique for answering the question, elegant solutions already exist in the literature. The rest of the work presented in this chapter is heavily inspired from [CHTW04].

The structure of the CHSH game goes as follows. A verifier Vic uniformly chooses at random two bits $(s,t) \in \{0,1\} \times \{0,1\}$, then sends s to Peggy and t to Paula. Peggy responds with $u \in \{0,1\}$ and Paula responds with $v \in \{0,1\}$. To win the game, Peggy and Paula must answer (u,v) such that

$$u \oplus v = s \wedge t, \tag{A.1}$$

under the constraint that Peggy and Paula are isolated and u, alternatively v, is uniformly distributed.

It is not hard to see that winning this game corresponds exactly to the behavior we expect from the NL-box of Section 2.3. Note that using $GF(2)$ terminology, (A.1) can be expressed as

$$u + v \equiv st \pmod 2. \tag{A.2}$$

A.1.1 Optimal classical strategy for the CHSH game

Recall from Section 1.3 that ω_c is the maximum success probability over all possible strategies that the classical pair Peggy-Paula win the game. From Theorem 1.3, we get that to

upper bound ω_c, one needs only to consider deterministic strategies.

To produce u and v with a deterministic strategy, Peggy, respectively Paula, evaluates a function depending on s, respectively t. Let $u(s)$ and $v(t)$ be these functions. For instance, on input (s,t), a strategy that would output

$$u(s) = u \quad \text{and} \quad v(t) = v$$

would succeed.

Lemma A.1 $\omega_c \leq 3/4$.

Proof: From (A.2)

$$\begin{aligned} & u(s) + v(t) \equiv st \pmod 2 \\ \longrightarrow \quad & v(t) \equiv u(s) + st \pmod 2. \end{aligned}$$

For any strategy, there is two possibilities regarding the value of $u(s)$.

i. The function $u(s)$ is independent of s, that is $u(s) = u_0$ where u_0 is a constant. Thus

$$v(t) \equiv u_0 + st \pmod 2. \tag{A.3}$$

ii. The function $u(s)$ is dependent of s, that is $u(s) = u_0 + u_1 s$ where u_0, u_1 are constants. Thus

$$v(t) \equiv u_0 + s(u_1 + t) \pmod 2. \tag{A.4}$$

Peggy and Paula win on every input (s,t) only if there exists a strategy where $v(t)$ is independent of s. Clearly, from $(A.3)$ and $(A.4)$, this is not the case; Peggy and Paula cannot win every time. Because there are four possible input pairs (s,t), they can win for at most three of them. Hence $\omega_c \leq 3/4$, which proves the claim.

□

In fact it is not hard to show the stronger result:

Theorem A.2 $\omega_c = 3/4$.

Proof: Consider the truth table.

s	t	$s \wedge t$
0	0	0
0	1	0
1	0	0
1	1	1

The strategy where

$$u(s) = 0 \quad \text{and} \quad v(t) = 0$$

always output $u(s) \oplus v(s) = 0$. It is straightforward that this strategy wins the CHSH game 3/4 of the time.

□

Among other things, the result of Theorem A.2 means that the NL-box cannot be simulated perfectly using local variables on each side.

A.1.2 Optimal quantum strategy for the CHSH game

We now turn to the scenario where Peggy and Paula are allowed to use a quantum strategy. We show that sharing entanglement, Peggy and Paula *can* beat the classical bound of 3/4. As in [CHTW04], consider this specific strategy. Peggy and Paula share the entangled one qubit state

$$|\Phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

Define

$$\begin{aligned} |\psi_0(\theta)\rangle &:= \cos(\theta)|0\rangle + \sin(\theta)|1\rangle, \\ |\psi_1(\theta)\rangle &:= \sin(\theta)|0\rangle - \cos(\theta)|1\rangle. \end{aligned}$$

Given s, Peggy will perform a projective measurement determined by the measurement operators $\{X_s^u \mid u \in \{0,1\}\}$ and report u to Vic. Likewise, given t, Paula will perform a projective measurement determined by the operators $\{Y_t^v \mid v \in \{0,1\}\}$ and send v to Vic. Let the operators be

$$\begin{aligned} X_0^u &= |\psi_u(0)\rangle\langle\psi_u(0)|, \\ X_1^u &= |\psi_u(\pi/4)\rangle\langle\psi_u(\pi/4)|, \\ Y_0^v &= |\psi_v(\pi/8)\rangle\langle\psi_v(\pi/8)|, \\ Y_1^v &= |\psi_v(-\pi/8)\rangle\langle\psi_v(-\pi/8)|. \end{aligned}$$

To prove this quantum strategy outperforms ω_c, we need the following little identity.

Lemma A.3 *Let $|\varphi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ be any maximally entangled state, then for any $d \times d$ complex matrix X*

$$(X \otimes I)|\varphi\rangle = (I \otimes X^T)|\varphi\rangle.$$

Proof: Using the Schmidt decomposition, the maximally entangled state $|\varphi\rangle$ can be expressed as

$$|\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle|j\rangle.$$

Similarly, the $d \times d$ complex matrix X can be expressed as

$$X = \sum_{k=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{kl} |k\rangle\langle l| \quad \lambda_{kl} \in \mathbb{C}.$$

Using some elementary linear algebra,

$$\begin{aligned} (X \otimes I)|\varphi\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \sum_{k=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{kl} |k\rangle\langle l|j\rangle|j\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{kl} |k\rangle|l\rangle. \end{aligned} \tag{A.5}$$

And likewise,

$$\begin{aligned}(I \otimes X^T)|\varphi\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \sum_{k=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{kl} |j\rangle|l\rangle\langle k|j\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{kl} |k\rangle|l\rangle. \end{aligned} \tag{A.6}$$

Clearly (A.5) and (A.6) are equal, which conclude the claim.

□

Following the line of arguments developed in [CHTW04, Hay], we can lower bound ω_q.

Lemma A.4 $\omega_q \geq \cos^2(\pi/8)$.

Proof: Define $p(u, v \mid s, t)$ as the probability of measuring u and v given that s and t were sent. Peggy and Paula are using the projective measurements described above. Hence, the operators for the joint measurement are $\{X_s^u \otimes Y_t^v \mid u, v \in \{0, 1\}\}$. Label U the system held by Peggy and V the system held by Paula, then we get

$$\begin{aligned} p(u, v \mid s, t) &= \langle \Phi_+ | X_s^u \otimes Y_t^v | \Phi_+ \rangle & \text{(A.7)} \\ &= \langle \Phi_+ | \big(X_s^u \otimes I\big) \otimes \big(I \otimes Y_t^v\big) | \Phi_+ \rangle \\ &= \langle \Phi_+ | \big(X_s^u \otimes I\big) \otimes \big(Y_t^{v^T} \otimes I\big) | \Phi_+ \rangle & \text{(A.8)} \\ &= \langle \Phi_+ | \big(X_s^u Y_t^{v^T} \otimes I\big) | \Phi_+ \rangle \\ &= \langle \Phi_+ | \big(X_s^u Y_t^v \otimes I\big) | \Phi_+ \rangle & \text{(A.9)} \\ &= \frac{1}{2} \big(\langle 0|_U \langle 0|_V + \langle 1|_U \langle 1|_V\big) \big(X_s^u Y_t^v \otimes I\big) \big(|0\rangle_U |0\rangle_V + |1\rangle_U |1\rangle_V\big) \\ &= \frac{1}{2} \Big(\langle 0|_U X_s^u Y_t^v |0\rangle_U \langle 0|_V |0\rangle_V + \langle 0|_U X_s^u Y_t^v |1\rangle_U \langle 0|_V |1\rangle_V \\ &\quad + \langle 1|_U X_s^u Y_t^v |0\rangle_U \langle 1|_V |0\rangle_V + \langle 1|_U X_s^u Y_t^v |1\rangle_U \langle 1|_V |1\rangle_V \Big) \\ &= \frac{1}{2} \Big(\langle 0|_U X_s^u Y_t^v |0\rangle_U + \langle 1|_U X_s^u Y_t^v |1\rangle_U \Big) \\ &= \frac{1}{2} \mathrm{Tr}\big(X_s^u Y_t^v\big), \end{aligned}$$

where (A.7) is by definition of measurement, (A.8) is by applying the identity of Lemma A.3 and (A.9) is because, given our particular choice of measurement operators for Paula, Y_t^v is invariant under transpose. It is now routine to check that for every pair of inputs (s,t), Peggy and Paula give the correct answer with probability $\cos^2(\pi/8)$. As an example, we do the case where $(s,t) = (1,1)$. Because $s \wedge t = 1$, Peggy and Paula need $(u,v) \in \{(0,1),(1,0)\}$. The first pair gives

$$\begin{aligned}
p(0,1 \mid 1,1) &= \frac{1}{2}\mathrm{Tr}\big(X_1^0 Y_1^1\big) = \frac{1}{2}\mathrm{Tr}\big(|\psi_0(\pi/4)\rangle\langle\psi_0(\pi/4)||\psi_1(-\pi/8)\rangle\langle\psi_1(-\pi/8)|\big) \\
&= \frac{1}{2}|\langle\psi_0(\pi/4)|\psi_1(-\pi/8)\rangle|^2 \qquad \text{by cyclicity of the trace} \\
&= \frac{1}{2}|(\cos(\pi/4)\langle 0| + \sin(\pi/4)\langle 1|)(\sin(-\pi/8)|0\rangle - \cos(-\pi/8)|1\rangle)|^2 \\
&= \frac{1}{2}|-\cos(\pi/4)\sin(\pi/8) - \sin(\pi/4)\cos(\pi/8)|^2 \\
&= \frac{1}{2}|-\sin(\pi/4+\pi/8)|^2 = \frac{1}{2}|-\cos(\pi/2-\pi/4-\pi/8)|^2 \\
&= \frac{1}{2}\cos^2(\pi/8).
\end{aligned}$$

Doing the calculations, $(u,v) = (1,0)$ also gives $p(1,0 \mid 1,1) = 1/2\cos^2(\pi/8)$. Therefore the probability to win when $(s,t) = (1,1)$ is $\frac{1}{2}\cos^2(\pi/8) + \frac{1}{2}\cos^2(\pi/8) = \cos^2(\pi/8)$. The same holds for the three other sets of inputs (s,t).

□

Theorem A.5 $\omega_q = \cos^2(\pi/8)$.

Proof: The intuition behind what follows is that a strategy that could do better than $\cos^2(\pi/8)$ would require more "power" from entanglement. Our goal is then to show that the strategy presented above exploits entanglement's correlations to its maximum.

First, let us translate the measurement operators X_s^u, Y_t^v into observables with eigenvalues ± 1 ([NC00] p. 87). It is straightforward from its definition that the projector X_0^u corresponds exactly to a measurement in the computational basis $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$. Consider the observable Z,

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|. \tag{A.10}$$

If Peggy applies the observable Z to her part of $|\Phi_+\rangle$, if she obtains the eigenvalue 1 it means her part of $|\Phi_+\rangle$ has been projected in the state $|0\rangle\langle 0|$. On the other hand, if she obtains the eigenvalue -1 it means her part of $|\Phi_+\rangle$ has been projected in the state $|1\rangle\langle 1|$. One easily realizes that this has the same effect as applying the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$.

The measurement operator X_1^u corresponds to a measurement in the diagonal basis $\{H|0\rangle\langle 0|H, H|1\rangle\langle 1|H\}$. We know from a simple calculation ([NC00] p. 459) that

$$HZH = X.$$

Hence, using the expression for Z in (A.10),

$$X = H|0\rangle\langle 0|H - H|1\rangle\langle 1|H.$$

As it was the case for the observable Z, the eigenvalue obtained after applying the observable X has the same effect on the observed state as a measurement in the diagonal basis. Using the same type of reasoning, we get that the observable for a general rotation R_θ by angle θ is defined by

$$\begin{aligned} R_\theta Z R_\theta &= \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} \cos(\theta) & \sin(\theta) \\ \sin(\theta) & -\cos(\theta) \end{pmatrix} \\ &= \begin{pmatrix} \cos^2(\theta) - \sin^2(\theta) & 2\cos(\theta)\sin(\theta) \\ 2\cos(\theta)\sin(\theta) & -(\cos^2(\theta) - \sin^2(\theta)) \end{pmatrix} \\ &= \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}. \end{aligned}$$

Thus, the observable Y_0 associated with the measurement in basis defined by Y_0^v is

$$Y_0 = R_{\pi/8} Z R_{\pi/8} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{Z+X}{\sqrt{2}}.$$

and the observable Y_1 associated with the measurement in basis defined by Y_1^v is

$$Y_1 = R_{-\pi/8} Z R_{-\pi/8} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} = \frac{Z-X}{\sqrt{2}}.$$

To summarize, upon reception of (s,t) Peggy and Paula perform their measurement using the observables

$$X_0 = Z, \qquad Y_0 = \frac{Z+X}{\sqrt{2}},$$
$$X_1 = X, \qquad Y_1 = \frac{Z-X}{\sqrt{2}}.$$

Plugging these observables in the famous Bell inequality known as the CHSH inequality, we get

$$\langle X_0 Y_0 \rangle + \langle X_1 Y_0 \rangle + \langle X_1 Y_1 \rangle - \langle X_0 Y_1 \rangle = 2\sqrt{2}, \tag{A.11}$$

where $\langle X_i Y_j \rangle = \langle \Phi_+ | X_i \otimes Y_j | \Phi_+ \rangle$ denotes the mean value of X_i and Y_j; see [NC00] p. 116 for more details.

But wait! Using Tsirel'son [Cir80, Cir87] upper bound[1] for any observable (X_0 and X_1 being applied by Peggy and Y_0 and Y_1 by Paula)

$$\langle X_0 Y_0 \rangle + \langle X_1 Y_0 \rangle + \langle X_1 Y_1 \rangle - \langle X_0 Y_1 \rangle \leq 2\sqrt{2},$$

we get that our strategy already uses the maximum out of the correlations produced by entanglement. This conclude the theorem since no other strategy can do better.

□

A.2 The Magic Square game

A description of the Magic Square game can be found in Section 3.2.1.

For the interested reader, there are other pseudo-telepathy games that are related to the magic square game. Adán Cabello's game [Cab01b, Cab01a] does not resemble the magic square game on first approach. However, closer analysis reveals that the two games are totally equivalent! A formal proof of this claim can be found in [Bro04], along with the

[1] Although Tsirel'son proved is bound using the singlet state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$, a generalization by Wehner [Weh06] showed it holds for any bipartite state.

definition of *equivalence* between pseudo-telepathy games.

Furthermore, Aravind has generalized his own magic square idea [Ara03] to a two-player pseudo-telepathy game in which the players share n Bell states, n being an arbitrary odd number larger than one.

A.2.1 Optimal strategy for classical players

Theorem A.6 *When restricted to classical strategies, Peggy and Paula can win the Magic Square game with probability at most* $\frac{8}{9}$.

Proof: Using Theorem 1.3, we only have to consider deterministic strategies to establish a bound for $\omega_c(G)$, the maximum success probability of winning when the game G is the Magic Square game.

A deterministic classical strategy would have to assign definite binary values to each of the nine entries of the magic square. From our set of winning conditions (see Section 3.2.1), it implies that the parity of the nine entries is even according to the rows and odd according the columns. Obviously, no such set of entries can exist, so $\widetilde{\omega}_c(G) < 1$. Using Lemma 1.4, we get that $\widetilde{\omega}_c(G) \leq \frac{8}{9}$.

Consider the following square and associated deterministic strategy.

	0	1	2
0	0	0	0
1	0	0	0
2	1	1	?

The parity of rows zero and one is even, and the parity of columns zero and one is odd, so Peggy and Paula win every time for these four possible cases without changing anything. If Peggy is asked row two, then she changes the ? of entry (2,2) to zero to get an even parity, and similarly Paula changes it to one to get a odd parity for column two. It is not hard

to see that they get caught cheating only when the intersection of the answered row and column is the entry (2,2). Therefore $\widetilde{\omega}_c(G) = \frac{8}{9}$, which conclude the proof together with Lemma 1.2.

□

A.2.2 Quantum winning strategy

The quantum winning strategy for the magic square game is not as simple as the classical impossibility proof. We refer the reader to [Ara02, Bro04] for a clear and detailed proof, since we will present here only a swift overview.

Let Peggy and Paula share the entangled state

$$|\psi\rangle = \tfrac{1}{2}|0011\rangle - \tfrac{1}{2}|0110\rangle - \tfrac{1}{2}|1001\rangle + \tfrac{1}{2}|1100\rangle\,. \tag{A.12}$$

The first two qubits belong to Peggy and the last two to Paula. Upon receiving their inputs x and y from the verifier Vic, Peggy and Paula apply respectively the unitary transformation R_x and C_y, according to the following matrices. Note that, as a reminder, we used R_x as the transformation associated with the computation for the *row*, and C_y for the *column*.

$$R_0 = \frac{1}{\sqrt{2}}\begin{bmatrix} i & 0 & 0 & 1 \\ 0 & -i & 1 & 0 \\ 0 & i & 1 & 0 \\ 1 & 0 & 0 & i \end{bmatrix}, \quad R_1 = \frac{1}{2}\begin{bmatrix} i & 1 & 1 & i \\ -i & 1 & -1 & i \\ i & 1 & -1 & -i \\ -i & 1 & 1 & -i \end{bmatrix}, \quad R_2 = \frac{1}{2}\begin{bmatrix} -1 & -1 & -1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & -1 & -1 & -1 \end{bmatrix},$$

$$C_0 = \frac{1}{2}\begin{bmatrix} i & -i & 1 & 1 \\ -i & -i & 1 & -1 \\ 1 & 1 & -i & i \\ -i & i & 1 & 1 \end{bmatrix}, \quad C_1 = \frac{1}{2}\begin{bmatrix} -1 & i & 1 & i \\ 1 & i & 1 & -i \\ 1 & -i & 1 & i \\ -1 & -i & 1 & -i \end{bmatrix}, \quad C_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 0 & 0 & 1 \\ -1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix}.$$

Then, Peggy and Paula measure their qubits in the computational basis. This provides two bits to each player, which are the first two bits of their respective output r^x and c^y. Finally, Peggy and Paula determine their third output bit from the first two, so that their parity condition is satisfied. The intersection condition is also always satisfied.

Consider for example inputs $x = 1$ and $y = 2$. After Peggy and Paula apply R_1 and C_2,

respectively, the state evolves to

$$(R_1 \otimes C_2)|\psi\rangle = \tfrac{1}{2\sqrt{2}}\big[|0000\rangle - |0010\rangle - |0101\rangle + |0111\rangle \tag{A.13}$$

$$+|1001\rangle + |1011\rangle - |1100\rangle - |1110\rangle\big]\,. \tag{A.14}$$

Suppose for instance that after measurement, Peggy and Paula obtained 10 and 01. In that case, Peggy would complete with bit one so that her output $r^1 = 101$ has even parity and Paula would complete with bit zero so that her output $c^2 = 010$ has odd parity. Vic will be satisfied with the answer since both Peggy and Paula agree that the third entry of the second row is indeed the same as the second entry of the third column: $c_1^2 = r_2^1 = 1$. It is easy to check that the seven other possible answers that Peggy and Paula could have given on this example are all appropriate. The verification that this quantum strategy wins also on the other eight possible questions is tedious but straightforward.

Bibliography

[Ara02] P. K. Aravind. Bell's theorem without inequalities and only two distant observers. *Foundation of Physics Letters*, pages 397–405, 2002.

[Ara03] P. K. Aravind. A simple demonstration of Bell's theorem involving two observers and no probabilities or inequalities. *ArXiv Quantum Physics e-prints* quant-ph/0206070, 2003.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE international Conference on Computers, Systems and Signal Processing, Bangalore, India*, pages 175-179, New York, 1984. IEEE Press.

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state by dual classical and EPR channel. *Physical Review Letter*, volume 70, pages 1895–1898, 1993.

[BBKM04] E. Biham, G. Brassard, D. Kenigsberg, and T. Mor. Quantum computation without entanglement. *Theoretical Computer Science*, volume 320, pages 13–33, 2004.

[BC90] G. Brassard and C. Crépeau. Quantum bit commitment and coin tossing protocols. In *Crypto '91*, volume 537 of *Lecture Notes in Computer Science*, pages 49–61. Springer, 1990.

[BCC88] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. In *Journal of Computer System Science*, volume 37, pages 156–189, 1988.

[BCJL93] G. Brassard, C. Crépeau, R. Josza, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Proceedings of the 34th Annual IEEE Symposium on the Foundations of Computer Science*, pages 362-371, Los Alamitos, CA, 1993. IEEE Computer Science Press.

[BCMS98] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail. Defeating classical bit commitment schemes with a quantum computer. *ArXiv Quantum Physics e-prints* quant-ph/9806031, 1998.

[Bel64] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics*, volume 1, number 3, pages 195–200, 1964.

[BFL90] L. Babai, L. Fortnow, and C. Lund. Non-deterministic exponential time has two-prover interactive protocols. Technical report, Chicago, IL, USA, 1990.

[BGG+89] M. BenOr, O. Goldreich, S. Goldwasser, J. Hastad, J. Kilian, S. Micali, and P. Rogaway. Everything provable is provable in zero-knowledge. In Springer-Verlag, editor, *Advances in Cryptology, Crypto '88*, volume 403, pages 37–56, 1989.

[BGKW88] M. BenOr, S. Goldwasser, J. Kilian, and A. Widgerson. Multi-prover interactive proofs: how to remove intractability. In *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 113–131, New York, NY, USA, 1988. ACM Press.

[BGW88] M. BenOr, S. Goldwasser, and A. Widgerson. Completeness theorems for non-cryptographic fault-tolerant distributed computation. In *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 1–10, New York, NY, USA, 1988. ACM Press.

[Blu82] M. Blum. Coin flipping by telephone, a protocol for solving impossible problems. *SIGACT News*, volume 15, number 1, pages 23–27, 1982.

[Bro04] A. L. Broadbent. Quantum pseudo-telepathy games. Mémoire de Maîtrise, Université de Montréal, 2004.

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one and two particle operators on EPR states. *Physical Review Letter*, volume 69, pages 2881, 1992.

[Cab01a] A. Cabello. All versus nothing inseparability for two observers. *Physical Review Letters*, page 010403, 2001.

[Cab01b] A. Cabello. Bell's theorem without inequalities and without probabilities for two observers. *Physical Review letters*, pages 1911–1914, 2001.

[CCD88] D. Chaum, C. Crépeau, and I. Damgard Multiparty unconditionally secure protocols. In *STOC '88: Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 11–19, New York, NY, USA, 1988, ACM Press.

[CCL90] J. Cai, A. Condon, and R. Lipton. On bounded round multi-prover interactive proof systems. In *Fifth Annual conference on Structure in Complexity Theory*, pages 45–54, 1990.

[CCM98] C. Cachin, C. Crépeau, and J. Marcil. Oblivious transfer with a memory-bounded receiver. In *Foundations of Computer Science, FOCS'98*, pages 493–502, 1998.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt. Proposed experiement to test local hidden-variable theories. *Physical Review Letters*, volume 23, pages 880–884, 1969.

[CHTW04] R. Cleve, P. Høyer, B. Toner, and J. Watrous. Consequences and limits of non-local strategies. In *CCC '04: Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 236–249, Washington, DC, USA, 2004. IEEE Computer Society.

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

[Cir87] B. S. (Tsirelson) Cirel'son. Quantum analogues of the Bell inequalities: the case of two spatially separated domains. *Journal of Soviet mathematics*, volume 36, pages 557–570, 1987.

[CK88] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened secrity assumptions. In IEEE, editor, *29th Symposium on Theory of Computing, STOC'88*, pages 42–52, 1988.

[CMW04] C. Crépeau, K. Morozov, and S. Wolf. Efficient unconditional oblivious transfer from almost any noisy channel. In *Security in Communication Networks, 4th International Conference, SNC 2004, Amalfi, Italy, September 8-10, 2004, Revised Selected Papers*, pages 47–59, 2004.

[Cré97] C. Crépeau. Efficient cryptographic protocols based on noisy channels. In *EUROCRYPT*, pages 306–317, 1997.

[CS95] C. Crépeau and L. Salvail. Quantum oblivious mutual identification. In *EUROCRYPT*, pages 133–146, 1995.

[DFMS04] I. B. Damgård, S. Fehr, K. Morozov, and L. Salvail. Unfair noisy channels and oblivious transfer. In *Theory of Cryptography Conference - TCC '04*, pages 355–373, February 2004.

[DFSS05] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005)*, pages 449–458. IEEE Computer Society, 2005.

[DFSS06] I. Damgård, S. Fehr, L. Salvail, and C. Schaffner. 1-2 OT in the bounded quantum-storage model with applications. In preparation, 2005-06.

[DKS99] I. Damgård, J. Kilian, and L. Salvail. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *EUROCRYPT*, pages 56–73, 1999.

[DMS00] P. Dumais, D. Mayers, and L. Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *EUROCRYPT*, pages 300–315, 2000.

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

[Eve82] S. Even. Protocol for signing contracts. In Allen Gersho, editor, *Advances in Cryptography*, pages 148–153, Santa Barbara, California, USA, 1982.

[Fei91] U. Feige. On the success probability of two provers in one-round proof systems. In *Sixth Annual Conference on Structure in Complexity Theory*, pages 116–123, 1991.

[FL92] U. Feige and L. Lovász. Two-prover one-round proof systems: their power and their problems (extended abstract). In *Proceedings of the twenty-fourth annual ACM symposium on Theory of computing, STOC '92*, pages 733–744, New York, NY, USA, 1992. ACM Press.

[For87] L. Fortnow. The complexity of perfect zero-knowledge. In *Proceedings of the nineteenth annual ACM conference on Theory of computing, STOC '87*, pages 204–209, New York, NY, USA, 1987. ACM Press.

[FRS94] L. Fortnow, J. Rompel, and M. Sipser. On the power of multi-prover interactive protocols. *Theory of Computer Science*, volume 134, number 2, pages 545–557, 1994.

[Gav06] D. Gavinsky. On the role of shared entanglement. *ArXiv Quantum Physics e-prints* quant-ph/0604052, 2006.

[GMR85] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. In *Proceedings of the seventeenth annual ACM symposium on Theory of computing, STOC '85*, pages 291–304, New York, NY, USA, 1985. ACM Press.

[GMW86] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. In IEEE, *27th Annual IEEE Symposium on Foundations of Computer Science*, pages 174–187, New York, 1986.

[GMW91] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. In *Journal of The Association for Computing Machinery*, volume 38, pages 691–729, 1991.

[Hay] P. Hayden. Comp761 course notes, winter 2005. McGill university.

[HILL98] J. Håstad, R. Impagliazzo, L. Levin, and M. Luby. A pseudorandom generator from any one-way function. *SICOMP: SIAM journal on Computing*, volume 28, number 4, 1998.

[HM96] S. Halevi and S. Micali. Practical and provably-secure commitment schemes from collision-free hashing. In Koblitz, editor, *Advances in Cryptology: Crypto'96*, pages 201–215. Springer-Verlag, 1996.

[IY87] R. Impagliazzo and M. Yung. Direct minimum knowledge computations. In Springer-Verlag, editor, *Advances in Cryptology: Crpyto'87*, volume 293, pages 40–51, 1987.

[Ken99] A. Kent. Unconditionally secure bit commitment. *Physical Review Letters*, volume 83, pages 1447, 1999.

[Ken04] A. Kent. Promising the impossible: classical certification in a quantum world. *ArXiv Quantum Physics e-prints* quant-ph/0409029, 2004.

[Ken05] A. Kent. Secure classical bit commitment using fixed capacity communication channels. In *Journal of Cryptology*, volume 18, number 4, pages 313–335, 2005.

[Kil88] J. Kilian. Founding cryptography on oblivious transfer. In *20th ACM Symposium on theory of Computing, STOC'88*, pages 20–31. ACM, 1988.

[KM03] H. Kobayashi and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. *Journal of Computer System Science*, volume 66, number 3, pages 429–450, 2003.

[KMR05] D. Kenigsberg, T. Mor, and G. Ratsaby. Quantum advantage without entanglement. *ArXiv Quantum Physics e-prints* quant-ph/0511272, 2005

[LC97] H-K Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, volume 78, number 17, pages 3410–3413, April 1997.

[LS91] D. Lapidot and A. Shamir. Fully parallelized multi-prover protocols for nexp-time. In *32nd Annual Symposium on foundations of Computer Science, FOCS'91*, pages 13–18, 1991.

[May96a] D. Mayers. The trouble with quantum bit commitment. *ArXiv Quantum Physics e-prints* quant-ph/9603015, March 1996.

[May96b] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *ArXiv Quantum Physics e-prints* quant-ph/9605044 November 1996.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, volume 78, pages 3414–3417, 1997.

[Mer90] N. D. Mermin. Simple unified form for the major no-hidden-variables theorems. *Physical Review Letters*, volume 65, number 27, pages 3373–3376, 1990.

[Nao91] M. Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, volume 4, number 2, pages 151–158, 1991.

[NC00] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, New York, NY, USA, 2000.

[NOVY93] M. Naor, R. Ostrovsky, R. Venkatesan, and M. Yung. Perfect zero-knowledge arguments for NP can be based on general complexity assumptions. In *Advances in Cryptology: Procceedings of Crypto' 92.* Springer-Verlag, 1993.

[PR94] S. Popescu and D. Rohrlich. Nonlocality as an axiom. *Foundations of Physics*, volume 24, pages 379, 1994.

[PR97] S. Popescu and D. Rohrlich. Causality and nonlocality as axioms for quantum mechanics. In *Symposium on Causality and Locality in Modern Physics and Astronomy*, 1997.

[Raz95] R. Raz. A parallel repetition theorem. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing, STOC '95*, pages 447–456, New York, NY, USA, 1995. ACM Press.

[Sti05] D. R. Stinson. *Cryptography: Theory and Practice, Third Edition.* CRC Press, 2005.

[Weh06] S. Wehner. Tsirelson bounds for generalized Clauser-Horne-Shimony-Holt inequalities. *Physical Review A*, volume 73, pages 022110, 2006. quant-ph/0510076.

[Wie70] S. J. Wiesner. Conjugate coding. *SIGACT News*, volume 15, number 1, pages 78–88, 1983. original manuscript around 1970; subsequently published in 1983.

[Yao95] Andrew Chi-Chih Yao. Security of quantum protocols against coherent measurements. In *27th Twenty-Seventh Annual ACM Symposium on Theory of Computing, STOC '95*, pages 67–75. ACM, 1995.