Classical and Quantum Strategies for Two-Prover Bit Commitments

Claude Crépeau[1⋆], Louis Salvail[2], Jean-Raymond Simard[1], and Alain Tapp[3]

[1] School of Computer Science, McGill University,
Montréal, QC, Canada. {crepeau,jrsimard}@cs.mcgill.ca
[2] BRICS, Dept. of Computer Science,
Århus University, Århus, Denmark. salvail@brics.dk
[3] Département d'Informatique et R.O., Université de Montréal,
Montréal, QC, Canada. tappa@iro.umontreal.ca

Abstract. First we show that the assumption behind the Two-Prover Zero-knowledge Interactive proof of BenOr, Goldwasser, Kilian and Wigderson [5] is too weak and need be made more precise to preserve soundness of their construction. Secondly, we introduce a Two-Prover Zero-knowledge Interactive proof similar to theirs and demonstrate that classically it is equally secure as the original but however, we later show that if the provers are allowed to share quantum entanglement, they are able to successfully prove false statements to the verifier with probability nearly one. Then we show that another variation of the original scheme of BGKW is secure against quantum provers. Finally we investigate the possibility of using this two-prover bit commitment scheme in order to achieve three applications : zero-knowledge proofs, quantum Oblivious Transfer and mutual identification.

1 Introduction

The notion of Multi-Prover Interactive proofs was introduced by BenOr, Goldwasser, Kilian and Wigderson [5] together with the Zero-knowledge property of such proofs. In the Two-prover scenario, we have two provers, Peggy and Paula, that are allowed to share arbitrary information before the proof, but they become physically separated and isolated during the execution of the proof in order to prevent them from communicating.

The Two-prover Interactive proofs of BGKW rely on their construction of a bit commitment scheme, information theoretically secure under the assumption that the provers cannot communicate. We refer the reader to their paper [5] to understand the application of this bit commitment scheme to construction of Two-prover Interactive proofs. We solely focus on their bit commitment scheme.

Despite the impossibility theorems of Mayers [19] and of Lo and Chau [18] the possibility of information theoretically secure bit commitment schemes in the two-prover model is *not* excluded in the quantum model while the provers cannot communicate. Indeed, the computations required to cheat the binding condition of a quantum bit commitment scheme cannot in general be performed by the two provers without ability to communicate classically or exchange quantum systems.

In this paper we consider two important questions regarding two-prover bit commitment schemes. The first is whether certain bit commitment schemes are secure classically but insecure if the provers are allowed to share quantum entanglement. The second is whether bit commitment schemes may be secure despite the fact that the provers can share quantum entanglement and perform arbitrary local quantum computations.

⋆ Supported in part by Québec's MDER, FQRNT, Canada's NSERC, MITACS, CIAR and the Bell University Laboratories.

We answer both questions in the affirmative. We start by reviewing existing two-prover bit commitment schemes in Section 2 and inspired from those, exhibit in Section 4 such a scheme that is information theoretically secure classically, but totally insecure when the two-provers are allowed to share quantum entanglement. Again, this does not mean that no such scheme is secure in the quantum model, but only that we found one which is definitely insecure. Indeed we then demonstrate in Section 5 that an existing bit commitment scheme remains secure under quantum attacks of the provers.

Back to the classical model, the authors of BGKW asserted: "that there is no communication between the two provers while interacting with the verifier". We show is Section 3 that, although this assumption *must be made*, it is however too weak, because the scheme we exhibit is binding classically but it is not at all binding if the provers are allowed to share entanglement. It is a very well known result that entanglement does not allow to communicate. Although it is true that they can cheat if they can communicate, it is also true that they can cheat without communicating. Therefore the assumption that the provers cannot communicate is too weak. This situation can be turned into a purely classical situation by providing the two provers with a correlated source of randomness that does not allow them to communicate but that allows them to cheat the binding condition of the bit commitment scheme. This peculiar source of randomness may replace the entanglement used by our attack.

Finally we investigate the possibility of using this two-prover bit commitment scheme in order to achieve three applications : zero-knowledge proofs, quantum Oblivious Transfer and mutual identification.

1.1 Related work

The security of a two-prover bit commitment scheme against quantum adversaries has been considered in the past in the work of Brassard, Crépeau, Mayers and Salvail [7]. They showed that if such a bit commitment scheme is used in combination to the Quantum Oblivious Transfer protocol of [7] it 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.

Another related line of research by Cleve, Høyer, Toner and Watrous [8] is the main inspiration of the current paper. They have established some relations between so called "non-locality games" and Two-prover Interactive Proofs but did not consider the Zero-Knowledge aspect.

A very different set of results [26] relate non-locality boxes and two party protocols such as bit commitment and oblivious transfer. These are only marginally connected to the current research.

2 Preliminaries

2.1 Two-prover bit commitment schemes

In the BGKW bit commitment scheme, Peggy and Paula have pre-agreed on an n-trit string w. After they are physically isolated, Peggy commits a bit b to Vic as follows:

BGKW–commit to b:

- Vic sends a random n-bit strings r to Peggy,
- Peggy replies with x such that $x_i = \sigma_{r_i}(w_i) + b \bmod 3$ for each position i,

where $\sigma_z(t) = (-1)^z t \bmod 3$ or simply

σ	0	1	2
0	0	1	2
1	0	2	1

where z is a bit and t is a trit.

BGKW–unveil b:
- Paula announced b and an n-bit string $\hat{w}$,
- Vic accepts iff $b = \sigma_{r_i}(\hat{w}_i) - x_i \bmod 3$ for each position i.

The authors of the above protocol prove that in each position i, the probability of successfully unveiling $\bar{b}$ instead of b using a $\hat{w}_i$ instead of w_i is no more than $1/2$. They also prove that each x_i carries no information about b. Combination of these two results yields that their bit-commitment scheme perfectly conceals the bit b, while statistically binding Peggy-Paula to a unique bit except with probability no greater than 2^{-n}.

Our first observation is that the BGKW bit-commitment scheme is unnecessarily complicated and can be replaced with no loss in security by a much simpler protocol we call "Simplified-BGKW" (or sBGKW as a short hand). This commitment scheme may be seen as Naor's bit-commitment scheme [21] (from a pseudo-random bit generator) in an information theoretical setting.

In the sBGKW bit commitment scheme, Peggy and Paula have pre-agreed on an n-bit string w. After they are physically separated, Peggy commits a bit b to Vic as follows:

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

sBGKW–unveil b:
- Paula announced b and an n-bit string $\hat{w}$,
- Vic accepts iff $\hat{w} = (b \cdot r) \oplus x$.

Now imagine that Peggy and Paula would like to be able to unveil a certain instance of b both as 0 and as 1. Our only assumption is that Paula knows nothing about r.

Peggy announces b to Vic and Paula would like to announce $\hat{w}$ such that $\hat{w} = (b \cdot r) \oplus x$. Indeed to successfully cheat she would need to know two strings $\hat{w}_0, \hat{w}_1$ such that $\hat{w}_0 = x$ and $\hat{w}_1 = r \oplus x$. However, $\hat{w}_0 \oplus \hat{w}_1 = r$ is completely unknown to Paula. Therefore, her probability of issuing a valid pair $\hat{w}_0, \hat{w}_1$ is at most $1/2^n$.

2.2 Non-locality boxes: the CHSH game

The CHSH game has been one on the first studied two players cooperative game for which it was proven that a quantum strategy outperforms any classical strategy. The game involves two physically separated players, $P1$ and $P2$, and one verifier V, and goes as follows : V selects at random two bits, a and b, and sends them to $P1$ and $P2$, respectively. Upon reception of their input, $P1$ and $P2$ each output a bit, s and t, and send them to the V who computes the following predicate

$$s \oplus t = a \wedge b.$$

$P1$ and $P2$ win the game if the predicate holds, and lose otherwise.

The maximum success probability of a classical strategy for the CHSH game is $3/4$. One simple way to determine this bound is by considering exhaustively all deterministic strategies : $P1$ and $P2$ can return four different output sets to V, that is $(s,t) \in \{(0,0),(1,1),(0,1),(1,0)\}$. For the two

first sets, they can win as long as $(a, b) \neq (1, 1)$, and for the two last sets, they can win only when $(a, b) = (1, 1)$. Therefore on each output set they cannot win for more than 3/4 of the input sets, and their best strategy is to set $s = y$ so they can achieve this probability of winning.

In the quantum setting, it turns out the maximum success probability of a quantum strategy for the CHSH game can be increased to $cos^2(\pi/8) \approx 0.85$. Here's a nice quantum strategy presented in [8] that achieves this bound. First, let $P1, P2$ share the entanglement $|\Phi^-\rangle = \frac{1}{\sqrt{2}}\big(|00\rangle - |11\rangle\big)$. Define

$$|\phi_0(\theta)\rangle = cos(\theta)|0\rangle + sin(\theta)|1\rangle$$
$$|\phi_1(\theta)\rangle = -sin(\theta)|0\rangle + cos(\theta)|1\rangle$$

and let P_1 and P_2's measurement be given as

$$X_0^a = |\phi_a(0)\rangle\langle\phi_a(0)|$$
$$X_1^a = |\phi_a(\pi/4)\rangle\langle\phi_a(\pi/4)|$$
$$Y_0^b = |\phi_b(\pi/8)\rangle\langle\phi_b(\pi/8)|$$
$$Y_1^b = |\phi_b(-\pi/8)\rangle\langle\phi_b(-\pi/8)|$$

for $a, b \in \{0, 1\}$. Each of these matrix are projective measurement and are thus positive semidefinite. Given our particular choice of entanglement, we have

$$\langle\Phi^-|X \otimes Y|\Phi^-\rangle = \frac{1}{2}\mathrm{Tr}(X^T Y)$$

for arbitrary X and Y. Because each of the matrices X_s^a and Y_t^b is real and symmetric, the probability that $P1$ and $P2$ answer (s, t) on input (a, b) is $\frac{1}{2}\mathrm{Tr}(X_s^a Y_t^b)$. It is then easily verified by an exhaustive check that, in every case, the correct answer is given with probability $cos^2(\pi/8)$ and the incorrect answer is given with probability $sin^2(\pi/8)$.

The fact that this probability of success is optimal follows from Tsirelson's Inequality [16][24].

3 Cheating sBGKW with a NL-box

Consider the following NL-box with input bits a and b. The box's outputs are two bits x and y such that x is uniformly distributed and $y := x \oplus b \wedge a$. First notice that y is also uniformly distributed and $x := y \oplus b \wedge a$. Therefore, the NL-box does not allow Peggy and Paula to communicate. However this NL-box allows them to unveil the bits committed through sBGKW in either way.

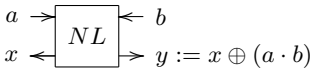

Fig. 1. the cheating NL-box

For each position i, Peggy inputs bit r_i received from Vic and obtains x_i from the NL-box. To unveil bit b Paula discloses this value to Vic and $\hat{x}_i$ is obtained from the NL-box with input b. If $b = 0$ then $b \wedge r_i = 0$ and thus $\hat{x}_i = x_i$ which is the right value she must disclose. If $b = 1$ then $b \wedge r_i = r_i$ and thus $\hat{x}_i \oplus x_i = r_i$ or $\hat{x}_i = x_i \oplus r_i$ which is again the right value she must disclose.

The existence of such a correlated 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. To achieve the binding condition a stronger assumption must be made: "there exists no mechanism by which the provers may sample a joint random variable which is dependent on inputs they provide." Notice that, among other things, this new condition excludes communication between the provers. However, it excludes a lot more, such as shared entanglement.

4 Cheating wBGKW using entanglement

Let the distance $d(x, y)$ of a pair of binary words x, y be the number of bit-positions where x and y differ. Consider a modified version of sBGKW, called wBGKW, where the acceptance criteria of the verifier Vic is to accept b and $\hat{w}$ if $d(\hat{w}, x \oplus (b \cdot r)) < n/5$. In sBGKW the criteria was $d(\hat{w}, x \oplus (b \cdot r)) = 0$.

It is clear (but formally proved below) that the classical optimal strategy yields $\mathbb{E}\{d(\hat{w}, x \oplus (b \cdot r))\} = n/4 > n/5$ (the choice of b is part of the expectation) and therefore the probability that $d(\hat{w}, x \oplus (b \cdot r)) < n/5$ for both values of b is exponentially small in n.

Conversely, the independent quantum strategy yields $\mathbb{E}\{d(\hat{w}, x \oplus (b \cdot r))\} < 0.15n < n/5$ for both values of b. In other words, the probability that $d(\hat{w}, x \oplus (b \cdot r)) \geq n/5$ is exponentially small in n when the provers use the strategy discussed above with the NL-box and the NL-box is simulated through entanglement. Thus a pair of quantum provers defeat the binding condition of the scheme with probabilities nearly 1.

4.1 Analysis of the classical case

We prove the following,

Theorem 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 $d(\hat{w}_b, x \oplus (b \cdot r)) < n/5$ for both values of b is exponentially small in n. Thus unveiling must fail for one of the two possibilities except with exponentially small probability.*

Proof. The result follows from first observing that any classical strategy that may produce such a $\hat{w}_0$ when $b = 0$ and $\hat{w}_1$ when $b = 1$ may output BOTH $\hat{w}_0$ and $\hat{w}_1$. In other words, classical strategies may always be parallelized (however, quantum strategies cannot!). Then we conclude that the assumption implies existence of a classical strategy that outputs $\hat{w}_0$ and $\hat{w}_1$ such that $d(\hat{w}_b, x \oplus (b \cdot r)) < n/5$. However, this is very unlikely because we easily obtain that $d(\hat{w}_0 \oplus \hat{w}_1, r) < 2n/5$ by the triangular inequality. But r is absolutely unknown to Paula and therefore her probability of outputting a string $z = \hat{w}_0 \oplus \hat{w}_1$ such that $d(z, r) < (1/2 - \epsilon)n$ is exponentially small in n for any $\epsilon > 0$ (and $2/5 < 1/2$ of course).

□

5 A quantumly secure variation

In the mBGKW bit commitment scheme, Peggy and Paula have pre-agreed on an n-bit string w. After they are physically separated, Peggy commits a bit b to Vic as follows:

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

mBGKW–unveil b:
- Paula announces $\hat{w}$ to Vic,
- Vic accepts b iff $r_b = \hat{w} \oplus x$.

We want to show that the mBGKW scheme is secure against a quantum adversary. Clearly the commitment is concealing for Vic does not know w. The binding property holds for the following reason.

Let p_0 be the probability of successfully unveiling 0 and p_1 be the probability of successfully unveiling 1. Imagine Peggy and Paula are able to open $b = 0$ or $b = 1$ with 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 wether $b = 0$ or $b = 1$ is unveiled. If she could simultaneously compute $(\hat{w}_0, \hat{w}_1)$ then she would learn $r_0 \oplus r_1 = \hat{w}_0 \oplus \hat{w}_1$. Clearly, this should not be possible with probability better than 2^{-n} since Paula does not have any information about (r_0, r_1) and therefore $r_0 \oplus r_1$ remains uniformly distributed over $\{0,1\}^n$ during the execution of the protocol. The next lemma shows that whenever $p_0 + p_1 > 1 + \varepsilon$, Paula can guess $r_0 \oplus r_1$ with success probability about ε^2.

Lemma 1. *Assume Peggy and Paula have probability p_b to open b with success 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 pure state $|\psi\rangle \in \mathcal{H}_N$ of dimension $N \geq 2^n$. She 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 than for $b = 0$. It is easy to verify that this corresponds to the most general strategy for Paula. From $r_0, r_1, x \in \{0,1\}^n$ 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,

$$p_b = \langle\psi_b|\hat{w}_b\rangle\langle\hat{w}_b|\psi_b\rangle, \tag{1}$$

which by assumption satisfies

$$p_0 + p_1 \geq 1 + \varepsilon, \varepsilon > 0. \tag{2}$$

Notice that $\langle\psi_b|\hat{w}_b\rangle$ is a generalized inner product since $|\hat{w}_b\rangle$ lives in a subspace of dimension 2^n in $\mathcal{H}_N$[4]. Using (1), we can write $|\psi_b\rangle$ as,

$$|\psi_b\rangle = \sqrt{p_b}|\hat{w}_b\rangle|\hat{v}_b\rangle + \sqrt{1-p_b}|\hat{w}_b^\perp\rangle, \tag{3}$$

where $\|\langle\hat{w}_b|\hat{w}_b^\perp\rangle\|^2 = 0$.

[4] 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 $\langle w|\psi\rangle = \sum_i \alpha_i \langle w|a_i\rangle|b_i\rangle$.

We want to determine a lower bound for the probability $p_\oplus$ for Paula to obtain $(\hat{w}_0, \hat{w}_1)$ using 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 canonical basis has been performed, and
2. Paula prepares $|\tilde{\psi}_1\rangle = U_1 U_0^\dagger |\tilde{\psi}_0\rangle$ before applying the measurement in the canonical basis.

Instead of computing directly $p_\oplus$, we 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 $|\tilde{\psi}_0\rangle = |\hat{w}_0\rangle|\hat{v}_0\rangle$. We have,

$$\begin{aligned}
|\tilde{\psi}_1\rangle &= U_1 U_0^\dagger |\tilde{\psi}_0\rangle \\
&= U_1 U_0^\dagger |\hat{w}_0\rangle|\hat{v}_0\rangle \\
&= U_1 \left(U_0^\dagger \frac{|\psi_0\rangle}{\sqrt{p_0}} - U_0^\dagger \sqrt{\frac{1-p_0}{p_0}} |\hat{w}_0^\perp\rangle \right) && (4) \\
&= U_1 \frac{|\psi\rangle}{\sqrt{p_0}} - U_1 U_0^\dagger \sqrt{\frac{1-p_0}{p_0}} |\hat{w}_0^\perp\rangle && (5) \\
&= \frac{|\psi_1\rangle}{\sqrt{p_0}} - U_1 U_0^\dagger \sqrt{\frac{1-p_0}{p_0}} |\hat{w}_0^\perp\rangle && (6) \\
&= \frac{1}{\sqrt{p_0}} \left(\sqrt{p_1}|\hat{w}_1\rangle|\hat{v}_1\rangle + \sqrt{1-p_1}|\hat{w}_1^\perp\rangle - U_1 U_0^\dagger \sqrt{1-p_0}|\hat{w}_0^\perp\rangle \right), && (7)
\end{aligned}$$

where (4) follows from (3), (5) and (6) are obtained by definition of U_0 and U_1 respectively, and (7) also follows from (3). At this point, Paula applies the measurement in the canonical basis in order to obtain $\hat{w}_1$. 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,

$$\begin{aligned}
p_{\hat{w}_1|\hat{w}_0} &= \langle\tilde{\psi}_1|\hat{w}_1\rangle\langle\hat{w}_1|\tilde{\psi}_1\rangle \\
&= \langle\hat{v}_0|\langle\hat{w}_0|U_0 U_1^\dagger|w_1\rangle\langle w_1|U_1 U_0^\dagger|\hat{w}_0\rangle|\hat{v}_0\rangle \\
&\geq \frac{1}{p_0}\left(\sqrt{p_1} - \sqrt{1-p_0}\right)^2 && (8) \\
&\geq \frac{1}{p_0}\left(\sqrt{p_1} - \sqrt{p_1-\varepsilon}\right)^2 && (9) \\
&\geq \frac{\varepsilon^2}{4p_0}, && (10)
\end{aligned}$$

where (8) follows from (7), (9) is obtained from (2), and (10) follows from a Taylor expansion. Finally, (10) gives the desired result since

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

□

Corollary 1. *If there exists an algorithm A that can cheat the bit commitment scheme with probabilities $p_0 + p_1 \geq 1 + 1/poly$ then there exists an algorithm A' that can predict an unknown n-bit string $(r_0 \oplus r_1)$ with probabilities $1/poly' = 1/4poly^2$, which is impossible.*

Indeed the following stronger statement is also true:

Corollary 2. *If there exists an algorithm A that can cheat the bit commitment scheme with probabilities $p_0 + p_1 > 1 + 4/2^{n/2}$ 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.*

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 1 is equally valid for any fixed choice of either (but not both) r_0 or r_1 because $r_0 \oplus r_1$ remains unlikely to predict.

6 Applications of a quantumly secure sBGKW

In this section we discuss three applications of a quantumly secure sBGKW bit commitment scheme. These are, two-prover zero-knowledge proofs, two-prover Oblivious Transfer and two-prover mutual identification.

6.1 Quantum Zero-Knowledge Proofs

The most obvious application of a two-prover bit commitment scheme secure against quantum adversaries is the elaboration of Zero-Knowledge proof, secure against quantum provers and verifier. Having a secure bit commitment scheme yields immediately zero-knowledge proofs for any language in NP using the classical constructions of either [13] or [6]. The zero-knowledge property immediate follows from the construction of the commitments because a simulator is able to unveil any bit commitment either way, because he issues fake messages from both provers. Thus simulation is straight forward, requires no rewinding, even if the verifier uses a quantum auxiliary input [15].

Moreover, using simple classical techniques put forward by [4] and [14] it is rather straightforward also for the two-provers to prove in zero-knowledge any statement in IP=PSPACE ([23]). It is sufficient in this case to demonstrate that a classical verifier would accept wen speaking with the prover. This is summarized as follows.

Theorem 2. *Using the* sBGKW *bit commitment scheme, there exists a statistical zero-knowledge proof for every statement in IP=PSPACE, even against a polytime quantum verifier.*

However, classically the two-prover scenario allows for much larger complexity classes: Babai, Fortnow and Lund [1] showed that any language in NEXP can be proven in zero-knowledge to a polytime verifier. Nevertheless, in the quantum case it is not even known what complexity class may be achieved in a two-quantum-provers vs quantum-verifier situation (consult [25, 17]). The complexity class that may be reached in zero-knowledge is even less known ! This is an intriguing open question.

6.2 Quantum Oblivious Transfer

The goal of an *Oblivious Transfer* (OT) [22] is as follows. Vic has a secret bit β drawn from a certain distribution. At the end of the protocol, either Peggy learns the value β (and knows it) or Peggy gains no further information about the value of β, with each event occurring with probability 1/2. Vic learns nothing about which event takes place. It is a folklore result that in the classical setting OT cannot be achieved securely (without extra assumptions). Moreover, it is not known whether

classically the two-prover model allows for a secure OT between Peggy-Paula and Vic while Peggy and Paula are separated.

It is well known from previous work [3][20][27] that in the quantum world, a protocol to achieve OT can be obtained from a bit commitment scheme. However, in the one prover model, Mayers [19] and independently Lo and Chau [18] showed that quantum-secure bit commitment was impossible. Since OT can be used to construct a bit commitment [9], their result forces any OT protocol to be insecure against a quantum adversary. Interestingly, it turns out that in the two-prover model, the quantum-secure scheme presented in section 5 can be used to build an OT secure against a quantum adversary. This is what we show here. For our purpose, we consider the same canonical oblivious transfer protocol as the one presented in [3][27].

OT protocol:
Let $U = \{+, \times\}^n \times \{0,1\}^n$, where $+, \times$ stand for the rectilinear and diagonal bases respectively.

Step 1: Vic pics a random uniformly chosen $u = (a, g) \in U$, and sends to Peggy photons i, $1 \leq i \leq n$, with polarizations given by bases $a[i]$ and bits $g[i]$, that is the qubits sent are random bits encoded using the BB84 coding scheme [2].

Step 2: Peggy picks a random uniformly chosen $b \in \{+, \times\}^n$, measures photons i in bases $b[i]$ and records the results as $h[i] \in \{0,1\}$. Peggy then makes a commitment of all n pairs $(b[i], h[i])$ to Vic.

Step 3: Vic picks a random uniformly chosen subset $R \subseteq \{1, 2, \ldots, n\}$, and tests the commitment made by Peggy at positions in R. If any $i \in R$ reveals $a[i] = b[i]$ and $g[i] \neq h[i]$, then Vic stops the protocol; otherwise the protocol continues.

Step 4: Vic announces the basis a to Peggy. Let T_0 be the set of all $1 \leq i \leq n$ with $a[i] = b[i]$, and let T_1 be the set of all $1 \leq i \leq n$ with $a[i] \neq b[i]$. Peggy chooses $I_0, I_1 \subseteq T_0 - R, T_1 - R$ with $\mid I_0 \mid = \mid I_1 \mid = 0.24n$, and sends $\{I_0, I_1\}$ in random order to Vic.

Step 5: Vic picks a random $s \in \{0,1\}$, and sends $s, \beta_s = \beta \oplus_{i \in I_s} g[i]$ to Bob. Bob computes $\beta = \beta_s \oplus_{i \in I_s} h[i]$, if $I_s \subseteq T_0$; otherwise does nothing.

Let the bit commitment of Step 2 be the sBGKW scheme. Therefore Peggy is split in two physically separated provers, Peggy and Paula, that cannot communicate with each other, and share some information $w[i]$ for each i. At Step 3, Vic ask Paula to unveil the positions in R.

As shown in [27], if each qubit i received by Peggy is measured, then the construction is secure against coherent measurement, and because the sBGKW scheme is secure against a quantum adversary, the OT protocol will be secure against a quantum adversary.

Based on the proof of Yao we claim the following without further proof

Theorem 3. *Using the* sBGKW *bit commitment scheme, there exists a statistically secure implementation of OT in the scenario where two parties Peggy-Paula are physically separated.*

However, Peggy might not measure the qubits she receives. It raises the question of whether or not it is possible for her to fake the measurement of her qubits, succeed Vic's test and then recover

the qubits for each position where the commitment was not opened. If it is the case then when the basis a will be disclosed, all she needs to do to obtain β is measure each qubit i according to $a[i]$ to get the correct $g[i]$.

Brassard, Crépeau, Mayers and Salvail [7] have shown a quantum attack, named "BCMS' attack", in the context where a two-prover bit commitment is used to force the other party to perform a measurement on a quantum system, which is exactly the task Peggy and Paula want to achieve. The attack is to make the bit commitment at quantum level, in a superposition entangled to the qubit to be measured. However, to take advantage of this attack, Peggy and Paula must get back together to recover the original qubit. Thus we must keep in mind that while the OT protocol is secure while Peggy and Paula are physically separated, it is completely insecure as soon as they get back together. This seriously limits the set of applications where such a protocol is relevant.

Another detail must be dealt with: since Peggy does not participate in the unveiling stage, how can Paula and Peggy agree on which bits Vic asked them to unveil ? This information is necessary for Peggy to know the set R in order to compute T_0 and T_1.

Of course, we cannot trust Vic to send R to Peggy because he may be dishonest. The only solution possible is to use Vic as an intermediary between Peggy and Paula. Paula may send the indexes of the bits unveiled in an *authenticated* message to Peggy through Vic. A concern is that Peggy-Paula may have shared entanglement before being separated, allowing them to use the bits of the authentication tag and the channel through Vic to teleport some quantum states. These quantum states may allow them to successfully carry the attack of BCMS. Thus, we need to restrict the size of this tag to prevent them from cheating. Note that the message sent is not encrypted, so the bits representing R cannot be used to send cheating information because Vic can check the validity of the information. If the set R is wrong, then Vic aborts the protocol.

We can therefore conclude that in order to make the OT protocol quantum-secure against the BCMS attack using the sBGKW bit commitment scheme, the following modifications need to be made

- Once separated, Peggy and Paula must never be put together again.
- At the end of Step 3, Paula will communicate the bits unveiled to Peggy through Vic, using an authenticated message with an authentication tag significantly smaller than the security parameter n used for the OT protocol.

We do not claim to have a complete proof of security of this application. Our purpose is to exhibit an application of the sBGKW commitment scheme with convincing arguments that it is secure. Work in progress is to complete this proof.

6.3 Quantum Mutual Identification

An alternative application of quantum cryptography was explored by Crépeau and Salvail [10]: mutual identification. In this cryptographic situation, two players Peggy and Vic share a common secret string w and would like to check that they mutually know this string in such a way that

- if both parties are honest, they always succeed
- a dishonest party who does not know w will only gain exponentially small amount of information each time he/she runs the protocol with an honest party.

Although the above paper suggests some quantum solutions to this problem, to this day, no proof of security has been discovered for their protocol. On the other hand, it is obvious that such a

solution may be obtained from a secure Oblivious Transfer protocol since the latter is universal for two-party computations. Nevertheless, more direct solutions have been developed by Fagin, Naor and Winkler [12] and Crépeau-Salvail [11].

As a consequence, a rather efficient solution may be obtained from the OT constructed in the previous sub-section. If one party, say Peggy, is split into two provers Peggy-Paula instead of a single party, it becomes possible to obtain sBGKW bit commitments, QOT, and finally an efficient mutual identification protocol.

In the honest case, when both Peggy and Vic know w they will succeed and all is fine.

In the dishonest case however, if Peggy (and Paula) did not know the secret string w, when they get back together after the identification protocol, they would be able to cheat all the QOTs (à la BCMS [7]) and actually obtain the string w completely ! This may seem like a rather serious problem, but in fact, it is not.

If Vic finds out that Peggy-Paula fail the identification protocol, he is safe as long as Peggy and Paula cannot get back together ever again! For instance, Vic may be an ATM while Peggy-Paula are a pair of smartcards. Only Peggy needs to know w, but not Paula. If Peggy-Paula succeed the identification then the user gets both cards back at the end of the interaction. If the identification fails, only the main card (Peggy) is given back to the user. The secondary card (Paula) is kept (or destroyed) by Vic. Since Paula's part in all these protocol is rather minor, it is a trivial business to make sure it forgets all its memory as the protocol evolves. If a dishonest Vic keeps the Paula-card dishonestly, the user knows that there is no useful data that may be recovered from it and so security is preserved. If an ATM keeps the card of an honest user, then the user knows the ATM is dishonest but need not contact his bank. Only if both cards are stolen must the user contact his bank, which is more or less unavoidable.

7 Conclusion

We have shown that the question as whether two-prover bit commitment schemes that are secure classically are also secure quantumly is non-trivial. We have presented a two-prover bit commitment scheme that classically secure, but insecure if the provers share entanglement. We have also presented a two-prover bit commitment scheme that is both classically secure, and secure if the provers share entanglement. We have discussed several applications of such a scheme.

Acknowledgements

We thank Richard Cleve, Barbara Terhal, and John Watrous for various discussions on this work.

References

1. L. Babai, L. Fortnow, and C. Lund. Nondeterministic exponential time has two-prover interactive protocols. In *Proceedings of the 31st Annual Symposium on Foundations of Computer Science*, volume 1, 1990, pp.16-25.
2. 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*, December 1984, pp. 175 - 179.
3. C.H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer protocols. In *Advances in Cryptology: Proceedings of Crypto '91* , volume 576 of Lecture Notes in Computer Science , pages 351-366. Springer-Verlag, 1992.
4. M. Ben-Or, O. Goldreich, S.Goldwasser, J. Hastad, J. Kilian, S. Micali, P. Rogaway. Everything provable is provable in zero-knowledge. In *Advances in Cryptology : Proceedings of Crypto '88*, volume 403 of Lecture Notes in Computer Science, Springer-Verlag, 1989, pp. 37-56.
5. M. Ben-Or, S. Goldwasser, J. Kilian, and A. Wigderson, Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions. In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC'88)*,Chicago, Illinois, pages 113-122, May 1988.
6. G. Brassard, D. Chaum and C. Crépeau. Minimum disclosure proofs of knowledge. In *Journal of Computer and System Sciences*, Vol. 37, no. 2, 1988, pp. 156-189.
7. G. Brassard, C. Crépeau, D. Mayers and L. Salvail, Defeating classical Bit Commitment Schemes with a Quantum Computer. Posted as paper 9806031 on quant-ph archive , 13 pages, June 1998.
8. R. Cleve, P. Høyer, B. Toner, J. Watrous. Consequences and Limits of Nonlocal Strategies *Proceedings of the 19th Annual Conference on Computational Complexity*, pages. 236-249, 2004
9. C. Crépeau, F. Légaré and L. Salvail. How to convert the flavor of a quantum bit commitment. In *Advances in Cryptology: Proceedings of Eurocrypt '0l.*, Springer-Verlag, pages 60-77, 2001.
10. C. Crépeau, and L. Salvail. Quantum oblivious mutual identification. In *Advances in Cryptology: Proceedings of Eurocrypt '95*, May 1995, pp. 133-146.
11. C. Crépeau and L. Salvail. Oblivious Verification of Common String. In *CWI Quarterly*, volume 8, no. 2, June 1995, pp. 97-109.
12. R. Fagin, M. Naor and P. Winkler. Comparing Information without leaking it. In *Journal of Communications of the ACM*, volume 39, no. 5, 1996, pp. 77-85.
13. Goldreich, O., S. Micali, and A. Wigderson. Proofs that Yield Nothing but their Validity or All Language in NP Have Zero-Knowledge Proof Systems. In *Journal of the ACM*, vol. 38, no 1, 1991, pp. 691-729.
14. R. Impagliazzo,and M. Yung. Direct minimum knowledge computations. In *Advances in Cryptology : Proceedings of Crypto '87*, volume 293 of Lecture Notes in Computer Science, Springer-Verlag, 1987, pp. 40-51.
15. J. van de Graaf. Towards a Formal Definition of Security for Quantum Protocols. Ph.D. thesis, Computer Science and Operational Research Department, Université de Montréal, 1997.
16. L. A. Khalfin, B. S. (Tsirelson) Tsirel'son. Quantum and quasi-classical analogs of Bell inequalities. In P. Lahti and P. Mittelstaedt, editors, *Symposium on the Foundations of Modern Physics*, pp. 441-460. World Scientific, 1985.
17. H . Kobayashi, and K. Matsumoto. Quantum multi-prover interactive proof systems with limited prior entanglement. In *Journal of Computer System Science*, volume 66, no. 3, 2003, pp. 429-450.
18. H.-K. Lo and H. F. Chau. Is Quantum Bit Commitment Really Possible ? manuscript posted on Los Alamos reprint archive quant-ph, March 96.
19. D. Mayers. The trouble with Quantum Bit Commitment. manuscript posted on Los Alamos reprint archive quant-ph, March 96.
20. D. Mayers,L. Salvail. Quantum Oblivious Transfer is Secure Against All Individual Measurements. In *Proceedings of the workshop on Physics and Computation*, PhysComp '94, Dallas, Nov 1994, pp. 69-77.
21. M. Naor. Bit Commitment Using Pseudo-randomness. In *Journal of Cryptology*, Volume 4, pp. 151-158.
22. Rabin, M. O., "How to exchange secrets by oblivious transfer", Technical Memo TR–81, Aiken Computation Laboratory, Harvard University, 1981.
23. A. Shamir. IP = PSPACE. In *Journal of ACM*, volume 39, no. 4, 1992, pp. 869-877.
24. B. S. (Tsirelson) Tsirel'son. Quantum analogues of the Belle inequalities: The case of two spatially separated domains. In *Journal of Soviet Mathematics*, vol. 36, pp. 557-570,1987.
25. J. Watrous. PSPACE Has Constant-Round Quantum Interactive Proof Systems. In *Proceedings of IEEE Symposium on Foundations of Computer Science*, 1999, pp. 112-119.
26. S. Wolf, J. Wullschleger. Oblivious transfer and quantum non-locality quant-ph 0502030
27. A. C.-C. Yao Security of Quantum Protocols Against Coherent Measurements. In *Proceedings of the 26th Symposium on the Theory of Computing*, June 1995, pp. 67-75.