Quantum attacks on classical bit commitment schemes

Gilles Brassard Claude Crépeau Dominic Mayers Louis Salvail
Université de Montréal * Princeton University † Århus Universiteit ‡

October 28, 1997

Abstract

Recent results of Mayers [] unveil a serious flaw in the proof of security of the Quantum Bit Commitment (QBC) Scheme of Brassard, Crépeau, Jozsa and Langlois [] and provide evidence that such a protocol is scritly impossible from quantum physics alone. We now investigate the power of attackers equipped with a quantum computer to break classical bit commitment scheme. We show that in certain scenarios the classical bit commitments offer little security. We also argue that certain type of proof techniques due to NOVY[] cannot be extended to the scenario of quantum computers.

1 Introduction

Quantum cryptographic protocols were born with quantum cryptography in Wiesner's seminal paper [] where he introduced "Quantum Multiplexing" later known as one-out-of-two Oblivious Transfer []. Nevertheless, in the same paper Wiesner provides an attack based on general quantum measurements against his own scheme and prove it insecure. Later Bennett and Brassard, introduced a Quantum Coin Tossing Protocol [] together with an attack based on EPR effects. Back to Oblivious Transfer, Crépeau and Kilian described a quantum protocol for this problem making the strong assumption that photon storage for long periods of time is impossible. The security of this scheme was proved recently by Crépeau []. A more realistic version of this protocol that could tolerate transmission errors was described in [].

An extension to this result was also described in []: a secure Oblivious Transfer Protocol in a model where photon storage is possible based on the existence of a Bit Commitment Scheme. The security of this protocol was proved in two steps: first Mayers and Salvail showed the security of the scheme in a model restricted to measurements of single particules and later generalized by Yao in the most general model [].

Until recently, it was implicit that the Bit Commitment Scheme used to "bootstrap" Oblivious Transfer was a Quantum Bit Commitment Scheme. Such a scheme was first offered by Brassard and Crépeau [] and later polished by Brassard, Crépeau, Jozsa and Langlois in [] who claimed a proof of the security of their scheme. Unfortunately, a flaw was recently unveiled in this proof by

* Département IRO, Université de Montréal, C.P. 6128, succursale centre-ville, Montréal (Québec), Canada H3C 3J7. e-mail: {brassard,crepeau}@iro.umontreal.ca.

†Department of Computer Science, Princeton University, Princeton, NJ 08544-2087, U.S.A.. e-mail: mayers@cs.princeton.edu.

‡Department of Computer Science,University of Århus, Ny Munkegade, building 540, DK-8000 Århus C, Denmark. e-mail: salvail@daimi.aau.dk

Mayers [] who argued quite convincingly that Quantum Bit Commitment Scheme is impossible if no limit is put on the kind of complex system and measurement the parties may use.

Although some two-party cryptographic protocols could still be found despite the result of Mayers that QBC is impossible in the most general model, all existing two-party protocols also collapse against the most general attacks allowed by quantum mechanics. The only exception to this situation is the Quantum Key Distribution protocol of Bennett and Brassard [] that is NOT a two-party protocol in the sense considered here that is still valid despite Mayers' result.

2 Bit Commitment

Assume that a party, $\mathcal{A}$, has a bit b in mind, to which she would like to be committed toward another party, $\mathcal{B}$. That is, $\mathcal{A}$ wishes, through a procedure $\mathbf{BC}(b)$, to provide $\mathcal{B}$ with a piece of evidence w that she has a bit b in mind and that she cannot change it (the commitment is *binding*). Meanwhile, $\mathcal{B}$ should not be able to tell from that evidence what b is (the commitment is *hiding*). At a later time, $\mathcal{A}$ can reveal, through an unveiling procedure $\mathbf{UN}(b,p)$, the value of b and prove through p to $\mathcal{B}$ that the piece of evidence sent earlier (w) really corresponded to that bit.

Bit commitment schemes have several applications in the field of cryptographic protocols. In particular one can implement *zero-knowledge proofs* of a variety of statements using bit commitment schemes [GMR89, GMW91, BCC88]. The first implementations of bit commitment schemes were given in a computational complexity scenario [Blu82]. Unfortunately, proofs of their (computational) security have always required an unproved assumption since otherwise they would imply very strong results such as $\mathcal{P} \neq \mathcal{NP}$.

3 NOVY Bit Commitment Scheme

In a computational scenario two techniques reduce bit commitment to very general cryptographic assumptions: the protocol of Naor [] reducing unconditionally binding–computationally hiding–bit commitment to pseudorandomness and the protocol of NOVY [] reducing computationally binding–unconditionally hiding–bit commitment to one-way permutations. We restrict our attention to this second result and first present their construction. Let $\pi : \{0,1\}^n \to \{0,1\}^n$ be a one-way permutation.

Protocol 3.1 (*NOVY/Commit*(b))

1: $\mathcal{A}$ picks $x \in_{\mathrm{R}} \{0,1\}^n$, and computes $y := \pi(x)$,

2: **for** $i \in \{1, ..., n-1\}$ **do**

3: $\mathcal{B}$ picks a hash vector $h_i \in_{\mathrm{R}} \{0,1\}^n$ and announces it to $\mathcal{A}$,

4: $\mathcal{A}$ anounces $r_i := h_i \cdot y$ to $\mathcal{B}$,

5: **endfor**

6: Let y_0, y_1 be the two solutions to $\{r_i = h_i \cdot y_*\}_{1 \le i < n}$ such that $y_0 < y_1$,

7: $\mathcal{A}$ sets a such that $y_a = y$ and anounces $a \oplus b$ to $\mathcal{B}$.

The fact that this protocol is unconditionally hiding is trivial since the commitment depends entirely on the fact that $\mathcal{A}$ knows the inverse of y_0 or y_1. Since both have a unique inverse, it is impossible to $\mathcal{B}$ o tell which one $\mathcal{A}$ knows.

Protocol 3.2 (*NOVY/Unveil*(b))

1: $\mathcal{A}$ discloses b and x to $\mathcal{B}$,

2: $\mathcal{B}$ checks that $y_{a\oplus b} = \pi(x)$.

NOVY showed that it is computationally equivalent to cheat the unveiling protocol or to inverse the one-way permutation. Any efficient algorithm to solve one problem yeilds an efficient algorithm to solve the other.

3.1 Weak Breaking of NOVY

Let $\gamma := \frac{1}{\sqrt{2}}$.

Protocol 3.3 (*NOVY/Commit*$(*)$)

1: $\mathcal{A}$ sets up a quantum register in state $\sum_{x\in\{0,1\}^n} \gamma^n |x, \pi(x)\rangle$,

2: **for** $i \in \{1, ..., n-1\}$ **do**

3: $\mathcal{B}$ picks a hash vector $h_i \in_{\mathrm{R}} \{0,1\}^n$ and announces it to $\mathcal{A}$,

4: $\mathcal{A}$ sets up her quantum register R in state $\sum_{\{x\in\{0,1\}^n | h_j\cdot\pi(x)=r_j, 1\le j<i\}} \gamma^{n-i+1} |x, \pi(x), h_i \cdot \pi(x)\rangle$,

5: $\mathcal{A}$ anounces to $\mathcal{B}$, $r_i :=$ outcome of measuring $h_i \cdot \pi(x)$, and she drops that last bit

6: **endfor**

7: Let y_0, y_1 be the two solutions to $\{r_i = h_i \cdot y_*\}_{1\le i<n}$ such that $y_0 < y_1$,

8: $\mathcal{A}$ picks a at random and announces a to $\mathcal{B}$.

Protocol 3.4 (*NOVY/Unveil*$(*)$)

1: $\mathcal{A}$ measures R, observes $|x_c, y_c\rangle$, for some bit c, discloses $b := a \oplus c$ and $x := x_c$ to $\mathcal{B}$,

2: $\mathcal{B}$ checks that $y_{a\oplus b} = \pi(x)$.

3.2 Stronger Breaking

Consider the following unitary operators:

$$U := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad X := \begin{pmatrix} I_2 & 0_2 \\ 0_2 & U \end{pmatrix}.$$

Protocol 3.5 (*NOVY/Commit*$(*)$)

...

7: Let y_0, y_1 be the two solutions to $\{r_i = h_i \cdot y_*\}_{1 \le i < n}$ such that $y_0 < y_1$, w.l.o.g. assume $y_0[n] = 0$ and $y_1[n] = 1$,

8: $\mathcal{A}$ applies $(I_{2^{n-1}} \otimes X)$ to $(R \otimes |\psi\rangle)$ and obtains $|\Xi\rangle$,

9: $\mathcal{A}$ measures the last position of $|\Xi\rangle$, observes $|a\rangle$ and announces a to $\mathcal{B}$.

At step 8 of protocol 3.5, the quantum register R starts in the state $\gamma(|x_0, y_0\rangle + |x_1, y_1\rangle)$ and assume the input state is $|\psi\rangle := \alpha|0\rangle + \beta|1\rangle$. We assume without lose of generality that $y_0[n] = 0$ and $y_1[n] = 1$. If this is not the case, position n may be swapped with any other position i where this holds and may be swapped back in place later. Thus the original state is

$$(R \otimes |\psi\rangle) = \gamma\alpha|x_0, y_0, 0\rangle + \gamma\beta|x_0, y_0, 1\rangle + \gamma\alpha|x_1, y_1, 0\rangle + \gamma\beta|x_1, y_1, 1\rangle$$

is mapped by $(I_{2^{n-1}} \otimes X)$ to

$$|\Xi\rangle = \gamma\alpha|x_0, y_0, 0\rangle + \gamma\beta|x_0, y_0, 1\rangle + \gamma\beta|x_1, y_1, 0\rangle + \gamma\alpha|x_1, y_1, 1\rangle$$

since $y_0[n] = 0$ and $y_1[n] = 1$ and thus

$$|\Xi\rangle = \gamma(\alpha|x_0, y_0, 0\rangle + \beta|x_1, y_1, 0\rangle) + \gamma(\beta|x_0, y_0, 1\rangle + \alpha|x_1, y_1, 1\rangle).$$

As a result, if the last position of $|\Xi\rangle$ is measured, bit $|a\rangle$ is observed with the property that

$$R = \begin{cases} \alpha|x_0, y_0\rangle + \beta|x_1, y_1\rangle & \text{if } |a\rangle \text{ is observed as } |0\rangle, \\ \beta|x_0, y_0\rangle + \alpha|x_1, y_1\rangle & \text{if } |a\rangle \text{ is observed as } |1\rangle, \end{cases}.$$

Another way to see this is $R = \alpha|x_a, y_a\rangle + \beta|x_{\bar{a}}, y_{\bar{a}}\rangle$.

3.2.1 When $\mathcal{A}$ Unveils

First we observe that if *NOVY/Unveil*$(*)$ takes place, then $\mathcal{B}$ is satisfied, i.e. $y_{a \oplus b} = \pi(x)$ by the simple facts that $b := a \oplus c$ and $x := x_c$. What is more interesting in this case is the fact that given a, $\mathcal{B}$ knowing $|\psi\rangle$ knows that $y_{a \oplus 0}$ should be observed by $\mathcal{A}$ with probability $||\alpha||^2$ and that $y_{a \oplus 1}$ should be observed by $\mathcal{A}$ with probability $||\beta||^2$. But this follows immediatly from the fact that $R = \alpha|x_a, y_a\rangle + \beta|x_{\bar{a}}, y_{\bar{a}}\rangle$.

3.2.2 When $\mathcal{A}$ never Unveils

Second we observe that if $NOVY/Unveil(*)$ does not take place, then $\mathcal{A}$ may recover $|\psi\rangle$ from her register R. Remembering that $R = \alpha|x_a, y_a\rangle + \beta|x_{\bar{a}}, y_{\bar{a}}\rangle$ $\mathcal{A}$ sets $|\psi\rangle := \gamma|0\rangle + \gamma|1\rangle$ and constructs a new state

$$(|\psi\rangle \otimes R) = \gamma\alpha|0, x_a, y_a\rangle + \gamma\beta|0, x_{\bar{a}}, y_{\bar{a}}\rangle + \gamma\alpha|1, x_a, y_a\rangle + \gamma\beta|1, x_{\bar{a}}, y_{\bar{a}}\rangle$$

which is mapped by $(X \otimes I_{2^{n-1}})$ to

$$|\Xi\rangle = \gamma\alpha|0, x_a, y_a\rangle + \gamma\beta|0, x_{\bar{a}}, y_{\bar{a}}\rangle + \gamma\beta|1, x_a, y_a\rangle + \gamma\alpha|1, x_{\bar{a}}, y_{\bar{a}}\rangle$$

and thus

$$|\Xi\rangle = \gamma(\alpha|0, x_a, y_a\rangle + \beta|1, x_a, y_a\rangle) + \gamma(\alpha|1, x_{\bar{a}}, y_{\bar{a}}\rangle + \beta|0, x_{\bar{a}}, y_{\bar{a}}\rangle).$$

After measuring R, if $|x_a, y_a\rangle$ is observed, then $|\psi\rangle$ is left in state $\alpha|0\rangle + \beta|1\rangle$, which achieves our goal. Otherwise $|x_{\bar{a}}, y_{\bar{a}}\rangle$ is observed and then $|\psi\rangle$ is left in state $\beta|0\rangle + \alpha|1\rangle$, which is corrected by applying the unitary operator U.

4 Two-Prover Bit Commitment Scheme

Protocol 4.1 ($2P/Commit(b)$)

1: $\mathcal{A}$ picks $r \in_{\mathrm{R}} \{0,1\}^n$, and shares it as r' with $\mathcal{A}$',

2: $\mathcal{A}$ and $\mathcal{A}$' are physically split,

3: $\mathcal{B}$ sets $m_0 := 0^n$ and picks $m_1 \in_{\mathrm{R}} \{0,1\}^n$, and announces them to $\mathcal{A}$,

4: $\mathcal{A}$ sends $z := r \oplus m_b$ to $\mathcal{B}$,

Protocol 4.2 ($2P/Unveil(b)$)

1: $\mathcal{A}$ discloses b and r to $\mathcal{B}$,

2: $\mathcal{A}$' discloses r' to $\mathcal{B}$,

3: $\mathcal{B}$ checks that $r = r'$ and that $z = r \oplus m_b$,

4.1 Cheating $2P/Commit$

Let ψ, ψ' be a pair of photons in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ shared between $\mathcal{A}$ and $\mathcal{A}$' before they are physically separated and let $\mu := \alpha|0\rangle + \beta|1\rangle$ be the particle given to $\mathcal{A}$. Consider the action of applying X to the pair (μ, ψ). Because ψ' is left untouched by this operator we may write the operator acting on the triple $(\mu, \psi, \psi') = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|100\rangle + \frac{\beta}{\sqrt{2}}|111\rangle$ as

$$X \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and thus $X \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mu, \psi, \psi') = \frac{\alpha}{\sqrt{2}}|000\rangle + \frac{\beta}{\sqrt{2}}|101\rangle + \frac{\alpha}{\sqrt{2}}|011\rangle + \frac{\beta}{\sqrt{2}}|110\rangle$. Consider now what happens if $\mathcal{A}$ measures particle ψ. With probability $\frac{||\alpha||^2}{2} + \frac{||\beta||^2}{2} = \frac{1}{2}$, she gets $\psi = |0\rangle$ and $(\mu, \psi') = \alpha|00\rangle + \beta|11\rangle$. Similarly, with probability $\frac{||\alpha||^2}{2} + \frac{||\beta||^2}{2} = \frac{1}{2}$, she gets $\psi = |1\rangle$ and $(\mu, \psi') = \alpha|01\rangle + \beta|10\rangle$. Notice that in both cases particle μ considered by itself has not changed from her original state $\alpha|0\rangle + \beta|1\rangle$. Notice also that the measured state of particle ψ indicates whether future readings of (μ, ψ') will be correlated ($\psi = |0\rangle$) or anti-correlated ($\psi = |1\rangle$).

Now let's see how we use this to cheat the protocol.

Protocol 4.3 ($2P/Commit(*)$)

1: $\mathcal{A}$ and $\mathcal{A}$' share n pairs of particles (ψ_i, ψ'_i) in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$,

2: $\mathcal{A}$ and $\mathcal{A}$' are physically split,

3: $\mathcal{B}$ sets $m_0 := 0^n$ and picks $m_1 \in_{\mathrm{R}} \{0,1\}^n$, and announces them to $\mathcal{A}$,

4: **for** $i \in \{1, ..., n\}$ **do**

5: **if** $m_1[i] = 1$ **then** $\mathcal{A}$ applies X to (μ, ψ_i),

6: $\mathcal{A}$ sets $z[i] :=$ outcome of measurement on ψ_i,

7: **endfor**

8: $\mathcal{A}$ sends z to $\mathcal{B}$.

Protocol 4.4 ($2P/Unveil(*)$)

1: $\mathcal{A}$ measures μ to get b, sets $r = z \oplus m_b$, discloses b and r to $\mathcal{B}$,

2: $\mathcal{A}$' measures $\psi'_1, ..., \psi'_n$ to get r' and discloses r' to $\mathcal{B}$,

3: $\mathcal{B}$ checks that $r = r'$ and that $z = r \oplus m_b$,

We now show that this unveiling is always succesful. For this we consider each position i individually and show that $r[i] = r'[i]$ as well as $z[i] = r[i] \oplus m_b[i]$.

Assume first that $m_1[i] = m_0[i] = 0$, then $\mathcal{A}$ sets $r[i] = z[i]$ regardless of b. Remember that $z[i]$ was obtained in protocol $2P/Commit$ as the outcome of measurement on ψ_i and $r'[i]$ was obtained in protocol $2P/Unveil$ as the outcome of measurement on ψ'_i. Because (ψ, ψ') was left in state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ both outcomes are the same and thus $r'[i] = z[i]$ as well.

Assume last that $m_1[i] = 1$ (and $m_0[i] = 0$), then $\mathcal{A}$ sets $r[i] = z[i] \oplus m_b[i] = z[i] \oplus b$. Remember that $z[i]$ was obtained in protocol $2P/Commit$ as the outcome of measurement on ψ_i after application of $X(\mu, \psi_i)$, $r'[i]$ was obtained in protocol $2P/Unveil$ as the outcome of measurement on ψ'_i and b was obtained as the outcome of measurement on μ. Because of our earlier discussion we know that $z[i]$ indicates whether later measurements of μ and ψ'_i are correlated ($r'[i] = b$ for $z[i] = 0$) or anti-correlated ($r'[i] \neq b$ for $z[i] = 1$). Thus $r'[i] \oplus b = z[i]$ and $r'[i] = z[i] \oplus b$ for $\mathcal{A}$' as well.

5 Conclusion and Open Questions

6 Acknowledgments

We thank X for support, suggestions and comments on this work.

References

[BBCS92] C. H. Bennett, G. Brassard, C. Crépeau, and M.-H. Skubiszewska. Practical quantum oblivious transfer. In *Advances in Cryptology: Proceedings of Crypto '91*, Lecture Notes in Computer Science, Vol. 576, pages 351–366. Springer-Verlag, 1992.

[BBR88] C. H. Bennett, G. Brassard, and J.–M. Robert. Privacy amplification by public discussion. *SIAM Journal on Computing*, 17(2):210–229, April 1988.

[Blu82] M. Blum. Coin flipping by telephone. In *Proceedings of IEEE Spring Computer Conference*, pages 133–137. IEEE, 1982.

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

[BC91] G. Brassard and C. Crépeau. Quantum bit commitment and coin tossing protocols. In *Advances in Cryptology: Proceedings of Crypto '90*, Lecture Notes in Computer Science, Vol. 537, pages 49–61. Springer-Verlag, 1991.

[Cré90] C. Crépeau. *Correct and Private Reductions among Oblivious Transfers*. PhD thesis, Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, 1990.

[CK88] C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *29th Symposium on Foundations of Computer Science*, pages 42–52. IEEE, 1988.

[GMW91] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity, or All languages in $\mathcal{NP}$ have zero-knowledge proof systems. *Journal of the ACM*, 38:691–729, 1991.

[GMR89] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof-systems. *SIAM Journal on Computing*, 18:186–208, 1989.

[Kra86] E. Kranakis. Primality and cryptography. John Wiley and Sons, 1986.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[Shi84] A.N. Shiryayev. Probability. Springer-Verlag, 1984.

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983. Manuscript written *circa* 1970, unpublished until it appeared in SIGACT News.

Contents