Optimal bounds for quantum bit commitment*

André Chailloux
LRI
Université Paris-Sud
andre.chailloux@gmail.fr

Iordanis Kerenidis†
CNRS - LIAFA
Université Paris 7
jkeren@liafa.jussieu.fr

1 Introduction

Quantum information has given us the opportunity to revisit information theoretic security in cryptography. The first breakthrough result was a protocol of Bennett and Brassard [BB84] that showed how to securely distribute a secret key between two players in the presence of an omnipotent eavesdropper. Thenceforth, a long series of work has focused on which other cryptographic primitives are possible with the help of quantum information. Unfortunately, the subsequent results were not positive. Mayers and Lo, Chau proved the impossibility of secure quantum bit commitment and oblivious transfer and consequently of any type of two-party secure computation [May97, LC97, DKSW07]. However, several weaker variants of these primitives have been shown to be possible [HK04, BCH$^+$08].

The main primitives that have been studied are coin flipping, bit commitment and oblivious transfer. Coin flipping is a cryptographic primitive that enables two distrustful and far apart parties, Alice and Bob, to create a random bit that remains unbiased even if one of the players tries to force a specific outcome. It was first proposed by Blum [Blu81] and has since found numerous applications in two-party secure computation. In the classical world, coin flipping is possible under computational assumptions like the hardness of factoring or the discrete log problem. However, in the information theoretic setting, it is not hard to see that in any classical protocol, one of the players can always bias the coin to his or her desired outcome with probability 1.

Aharonov et al. [ATVY00] provided a quantum protocol where no dishonest player could bias the coin with probability higher than 0.9143. Then, Ambainis [Amb01] described an improved protocol whose cheating probability was at most 3/4. Subsequently, a number of different protocols have been proposed [SR01, NS03, KN04] that achieved the same bound of 3/4. On the other hand, Kitaev [Kit03], using a formulation of quantum coin flipping protocols as semi-definite programs proved a lower bound of 1/2 on the product of the two cheating probabilities for Alice and Bob (for a proof see *e.g.* [ABDR04]). In other words, no quantum coin flipping protocol can achieve a cheating probability less than $1/\sqrt{2}$ for both Alice and Bob. Recently, we resolved the question of whether 3/4 or $1/\sqrt{2}$ is ultimately the right bound for quantum coin flipping by constructing a strong coin-flipping protocol with cheating probability $1/\sqrt{2} + \varepsilon$ ([CK09]).

The protocol in [CK09] is in fact a *classical* protocol that uses the primitive of weak coin flipping as a subroutine. In the setting of weak coin flipping, Alice and Bob have a priori a desired coin

*A technichal version can be found on the arxiv quant-ph: 1102.1678v1

†We acknowledge financial support from the ANR through projects CRYQ (ANR-09-JCJC-0067-01) and QRAC (ANR-08-EMER-012), and from the European Union through project QCS (grant 255961).

outcome, in other words the two values of the coin can be thought of as 'Alice wins' and 'Bob wins'. We are again interested in bounding the probability that a dishonest player can win this game. Weak coin flipping protocols with cheating probabilities less than 3/4 were constructed in [SR02, Amb02, KN04]. Finally, a breakthrough result by Mochon resolved the question of the optimal quantum weak coin flipping. First, he described a protocol with cheating probability 2/3 [Moc04, Moc05] and then a protocol that achieves a cheating probability of $1/2 + \varepsilon$ for any $\varepsilon > 0$ [Moc07].

In other words, in coin flipping, the power of quantum really comes from the ability to perform weak coin flipping. If there existed a classical weak coin flipping protocol with arbitrarily small bias, then this would have implied a classical strong coin flipping protocol with cheating probability arbitrarily close to $1/\sqrt{2}$ as well.

2 Our contribution

In this paper, we turn our attention to bit commitment. Even though this primitive is closely related to coin flipping we will see that actually the results are surprisingly different. A bit commitment protocol consists of two phases: in the commit phase, Alice commits to a bit b; in the reveal phase, Alice reveals the bit to Bob. We are interested in the following two probabilities: Alice's cheating probability is the average probability of revealing both bits during the reveal phase, and Bob's cheating probability is the probability he can guess the bit b after the commit phase.

Using the known results about coin flipping we can give the following bounds on these probabilities. First, most of the suggested coin flipping protocols with cheating probability 3/4 were using some form of imperfect bit commitment scheme. More precisely, Alice would quantumly commit to a bit a, Bob would announce a bit b and then Alice would reveal her bit a. The outcome of the coin flip would be $a \oplus b$. Hence, we already know bit commitment protocols that achieve cheating probability equal to 3/4. Note also that Ambainis had proved a lower bound of 3/4 for any protocol of this type. On the other hand, a bit commitment protocol with cheating probability p immediately gives a strong coin flipping protocol with the same cheating probability (by the above mentioned construction) and hence Kitaev's lower bound of $1/\sqrt{2}$ still holds.

The question of the optimal cheating probability for bit commitment remained unresolved, similar to the case of coin flipping that was answered in [CK09]. Here, we find the optimal cheating probability for quantum bit commitment, which surprisingly is neither of the above mentioned constants. In fact, we show that it is approximately 0.739.

We start by providing a lower bound for any quantum bit commitment protocol. In order to do so, we describe an explicit cheating strategy for Alice and Bob in any protocol. In high level, let $|\psi_b\rangle$ be the joint state of Alice and Bob after the commit phase and σ_b Bob's density matrix, when Alice honestly commits to bit b. It is well known that there exists a cheating strategy for Bob that succeeds with probability

$$P_B^* \geq \frac{1}{2} + \frac{\Delta(\sigma_0, \sigma_1)}{2}$$

where $\Delta(\cdot, \cdot)$ denotes the trace distance between two density matrices.

For Alice, we consider the following cheating strategy. Instead of choosing a bit b in the beginning of the protocol, she goes into a uniform superposition of the two possible values and controlled on this qubit she performs honestly the commit phase. Then, after the commit phase, when she wants to reveal a specific bit b, she first performs a unitary operation on her part to transform the joint state to one which is as close as possible to the honest state $|\psi_b\rangle$ (the unitary is given by Uhlmann's theorem) and then performs the reveal phase honestly.

It is not hard to see that Alice's cheating probability is at least

$$P_A^* \geq \frac{1}{2}\left(F^2(\sigma_+, \sigma_0) + F^2(\sigma_+, \sigma_1)\right)$$

where $F(\cdot,\cdot)$ denotes the fidelity between two states and $\sigma_+ = \frac{1}{2}(\sigma_0 + \sigma_1)$.

In order to conclude we prove our main technical lemma

Proposition 1 *Let σ_0, σ_1 any two quantum states. Let $\sigma_+ = \frac{1}{2}(\sigma_0 + \sigma_1)$. We have*

$$\frac{1}{2}\left(F^2(\sigma_+, \sigma_0) + F^2(\sigma_+, \sigma_1)\right) \geq (1 - (1 - \frac{1}{\sqrt{2}})\Delta(\sigma_0, \sigma_1))^2$$

By equalizing the two lower bounds that are expressed in terms of the trace distance we conclude that

Theorem 1 *In any quantum bit commitment protocol with cheating probabilities P_A^* and P_B^* we have $\max\{P_A^*, P_B^*\} \geq \frac{-11+6\sqrt{2}+\sqrt{21-12\sqrt{2}}}{4(2\sqrt{2}-3)} \approx 0.739$.*

Then, we provide a matching upper bound. We describe a quantum bit commitment protocol that achieves a cheating probability arbitrarily close to 0.739. Out protocol uses a weak coin flipping protocol with cheating probability $1/2 + \epsilon$ as a subroutine and achieves a cheating probability for the bit commitment of approximately $0.739 + O(\epsilon)$.

Theorem 2 *There exists a quantum bit commitment protocol that uses a weak coin flipping protocol with cheating probability $1/2 + \epsilon$ as a subroutine and achieves cheating probabilities less than $\frac{-11+6\sqrt{2}+\sqrt{21-12\sqrt{2}}}{4(2\sqrt{2}-3)} + O(\epsilon) \approx 0.739 + O(\epsilon)$.*

We note that our protocol is in fact quantum even beyond the weak coin flip subroutine. This is in fact necessary. We show that any classical bit commitment protocol with access to a perfect weak coin (or even strong) cannot achieve cheating probability less than $3/4$.

Theorem 3 *Any classical bit commitment protocol with access to perfect weak (or strong) coin flipping cannot achieve cheating probabilities less than $3/4$.*

Unlike the case of quantum strong coin flipping that is derived classically when one has access to a weak coin flipping protocol, the optimal quantum bit commitment takes advantage of quantum effects beyond the weak coin flipping subroutine.

References

[ABDR04] Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Rohrig. Multiparty quantum coin flipping. In *CCC '04: Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259, Washington, DC, USA, 2004. IEEE Computer Society.

[Amb01] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. In *STOC '01: Proceedings of the thirtieth annual ACM symposium on Theory of computing*, Washington, DC, USA, 2001. IEEE Computer Society.

[Amb02] Andris Ambainis. Lower bound for a class of weak quantum coin flipping protocols, 2002. quant-ph/0204063.

[ATVY00] Dorit Aharonov, Amnon Ta-Shma, Umesh V. Vazirani, and Andrew C. Yao. Quantum bit escrow. In *STOC '00: Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 705–714, New York, NY, USA, 2000. ACM.

[BB84] Bennett and Brassard. Quantum cryptography: Public key distribution and coin tossing. in Proc. Of IEEE Inter. Conf. on Computer Systems and Signal Processing, Bangalore, Kartarna, (Institute of Electrical and Electronics Engineers, New York, 1984.

[BCH+08] Harry Buhrman, Matthias Christandl, Patrick Hayden, Hoi-Kwong Lo, and Stephanie Wehner. Possibility, impossibility and cheat-sensitivity of quantum bit string commitment. *Physical Review A*, 78:022316, 2008.

[Blu81] Manuel Blum. Coin flipping by telephone. In *CRYPTO*, pages 11–15, 1981.

[CK09] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. *Foundations of Computer Science (FOCS)*, pages 527–533, 2009.

[DKSW07] Giacomo Mauro D'Ariano, Dennis Kretschmann, Dirk Schlingemann, and Reinhard F. Werner. Reexamination of quantum bit commitment: the possible and the impossible. *Physical Review A*, 76:032328, 2007.

[HK04] Lucien Hardy and Adrian Kent. Cheat sensitive quantum bit commitment. *Physical Review Letters*, 92:157901, 2004.

[Kit03] A Kitaev. Quantum coin-flipping. presentation at the 6th workshop on quantum information processing (QIP 2003), 2003.

[KN04] I. Kerenidis and A. Nayak. Weak coin flipping with small bias. *Inf. Process. Lett.*, 89(3):131–135, 2004.

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

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

[Moc04] Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *FOCS '04: Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, pages 2–11, Washington, DC, USA, 2004. IEEE Computer Society.

[Moc05] C. Mochon. Large family of quantum weak coin-flipping protocols. *Phys. Rev. A*, 72(2):022341–+, August 2005.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias, 2007. quant-ph:0711.4114.

[NS03] Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Phys. Rev. A*, 67(1):012304, Jan 2003.

[SR01] R. W. Spekkens and T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65:012310, 2001.

[SR02] Robert Spekkens and Terry Rudolph. Quantum protocol for cheat-sensitive weak coin flipping. *Phys. Rev. Lett.*, 89(22):1–4, Nov 2002.