Optimal bounds for quantum bit commitment

André Chailloux[*]
LRI
Université Paris-Sud
andre.chailloux@lri.fr

Iordanis Kerenidis[*]
CNRS - LIAFA
Université Paris 7
jkeren@liafa.jussieu.fr

February 9, 2011

Abstract

Bit commitment is a fundamental cryptographic primitive with numerous applications. Quantum information allows for bit commitment schemes in the information theoretic setting where no dishonest party can perfectly cheat. The previously best-known quantum protocol by Ambainis achieved a cheating probability of at most 3/4 [Amb01]. On the other hand, Kitaev showed that no quantum protocol can have cheating probability less than $1/\sqrt{2}$ [Kit03] (his lower bound on coin flipping can be easily extended to bit commitment). Closing this gap has since been an important and open question.

In this paper, we provide the optimal bound for quantum bit commitment. We first show a lower bound of approximately 0.739, improving Kitaev's lower bound. We then present an optimal quantum bit commitment protocol which has cheating probability arbitrarily close to 0.739. More precisely, we show how to use any weak coin flipping protocol with cheating probability $1/2 + \varepsilon$ in order to achieve a quantum bit commitment protocol with cheating probability $0.739 + O(\varepsilon)$. We then use the optimal quantum weak coin flipping protocol described by Mochon [Moc07]. To stress the fact that our protocol uses quantum effects beyond the weak coin flip, we show that any classical bit commitment protocol with access to perfect weak (or strong) coin flipping has cheating probability at least 3/4.

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 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.

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 $\max\{P_A^*, P_B^*\} \geq 0.739$.*

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 $0.739 + O(\epsilon)$.

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 $0.739 + O(\epsilon)$.*

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 $3/4$.

3

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.

2 Preliminaries

2.1 Useful facts about trace distance and fidelity of quantum states

We start by stating a few properties of the trace distance Δ and fidelity F between two quantum states.

Definition 1 *For any two quantum states ρ, σ, the trace distance Δ between them is given by $\Delta(\rho, \sigma) = \Delta(\sigma, \rho) = \frac{1}{2} tr(|\rho - \sigma|)$ where $|A| = \sqrt{A^\dagger A}$ for a matrix A*

Proposition 2 *For any two states ρ, σ such that $\rho = \sum_i p_i |i\rangle\langle i|$ and $\sigma = \sum_i q_i |i\rangle\langle i|$, we have*

$$\Delta(\rho, \sigma) = \sum_i \frac{1}{2}|p_i - q_i| = \sum_{i:p_i \geq q_i} (p_i - q_i) = 1 - \sum_i \min\{p_i, q_i\} = \sum_i \max\{p_i, q_i\} - 1$$

Proof: Since $\sum_i p_i = \sum_i q_i = 1$, we have $\sum_{i:p_i \geq q_i}(p_i - q_i) = \sum_{ip_i < q_i}(q_i - p_i)$ and $\sum_i \max\{p_i, q_i\} + \min\{p_i, q_i\} = 2$ hence

$$\Delta(\rho, \sigma) = \sum_i \frac{1}{2}|p_i - q_i| = \frac{1}{2}\left(\sum_{i:p_i \geq q_i}(p_i - q_i) + \sum_{i:p_i < q_i}(q_i - p_i)\right) = \sum_{i:p_i \geq q_i}(p_i - q_i)$$

$$\Delta(\rho, \sigma) = \sum_i \frac{1}{2}|p_i - q_i| = \frac{1}{2}\sum_i(\max\{p_i, q_i\} - \min\{p_i, q_i\}) = 1 - \sum_i \min\{p_i, q_i\} = \sum_i \max\{p_i, q_i\} - 1$$

■

Proposition 3 *For any two states ρ, σ, and a POVM $E = \{E_1, \ldots, E_m\}$ with $p_i = tr(\rho E_i)$ and $q_i = tr(\sigma E_i)$, we have $\Delta(\rho, \sigma) \geq \frac{1}{2}\sum_i |p_i - q_i|$. There is a POVM (even a projective measurement) for which this inequality is an equality.*

Proposition 4 *[Hel67] Suppose Alice has a bit $c \in_R \{0,1\}$ unknown to Bob. Alice sends a quantum state ρ_c to Bob. We have*

$$\Pr[\text{Bob guesses } c] \leq \frac{1}{2} + \frac{\Delta(\rho_0, \rho_1)}{2}$$

Definition 2 *For any two states ρ, σ, the fidelity F between them is given by $F(\rho, \sigma) = F(\sigma, \rho) = tr(\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}})$*

Proposition 5 *For any two states ρ, σ, and a POVM $E = \{E_1, \ldots, E_m\}$ with $p_i = tr(\rho E_i)$ and $q_i = tr(\sigma E_i)$, we have $F(\rho, \sigma) \leq \sum_i \sqrt{p_i q_i}$. There is a POVM for which this inequality is an equality.*

4

Proposition 6 (Uhlmann's theorem) *For any two states ρ, σ, there exist a purification $|\phi\rangle$ of ρ and a purification $|\psi\rangle$ of σ such that $|\langle\phi|\psi\rangle| = F(\rho, \sigma)$*

Proposition 7 *For any two states ρ, σ and a completely positive trace preserving operation Q, we have $F(\rho, \sigma) \leq F(Q(\rho), Q(\sigma))$.*

2.2 Definition of quantum bit commitment

Definition 3 *A quantum commitment scheme is an interactive protocol between Alice and Bob with two phases, a Commit phase and a Reveal phase.*

- *In the* commit *phase, Alice interacts with Bob in order to commit to b.*

- *In the* reveal *phase, Alice interacts with Bob in order to reveal b. Bob decides to accept or reject depending on the revealed value of b and his final state. We say that Alice successfully reveals b, if Bob accepts the revealed value.*

We define the following security requirements for the commitment scheme.

- Completeness: *If Alice and Bob are both honest then Alice always successfully reveals the bit b she committed to.*

- Binding property: *For any cheating Alice and for honest Bob, we define Alice's cheating probability as*

$$P_A^* = \frac{1}{2}\left(\Pr[\text{ Alice successfully reveals } b = 0] + \Pr[\text{ Alice successfully reveals } b = 1]\right)$$

- Hiding property: *For any cheating Bob and for honest Alice, we define Bob's cheating probability as*

$$P_B^* = \Pr[\text{ Bob guesses } b \text{ after the Commit phase }]$$

Remark: The definition of quantum bit commitment we use is the standard one when one studies stand-alone cryptographic primitives. In this setting, quantum bit commitment has a clear relation to other fundamental primitives such as coin flipping and oblivious transfer [ATVY00, Amb01, Kit03, Moc07, CKS10]. Moreover, the study of such primitives sheds light on the physical limits of quantum mechanics and the power of entanglement. Recently there have been some stronger definitions of Quantum Bit Commitment protocols that suit better practical uses (see for example [DFR$^+$07]). Notice that using our weaker definition of quantum bit commitment only strengthens our lower bound which also holds for the stronger ones.

We now describe more in detail the different steps on a quantum bit commitment protocol. We consider protocols where Alice reveals b at the beginning of the decommit phase. Note that this doesn't help Bob and can only harm a cheating Alice. Proving a lower bound for such protocols will hence be a lower bound for all bit commitment protocols.

We assume here that Alice and Bob are both honest. Let $\mathcal{A}$ Alice's space and $\mathcal{B}$ Bob's space.

The commit phase: Alice wants to commit to a bit b. Alice and Bob communicate with each other and perform some quantum operations. This can be seen as a joint quantum operation which depends on b. We can suppose wlog that this operation is a quantum unitary U_b^C (by increasing Alice and Bob's quantum space). At the end of the commit phase, Alice and Bob share the quantum state $|\psi_b\rangle$. Let $\sigma_b = \text{Tr}_{\mathcal{A}}|\psi_b\rangle\langle\psi_b|$ the state that Bob has after the commit phase.

The reveal phase: Alice wants to reveal b to Bob. Alice reveals b at the beginning of the decommit phase. Similarly to the commit phase, we can suppose that the decommit phase is equivalent to Alice and Bob performing a joint unitary U_b^D on their shared state ($|\psi_b\rangle$ if they were honest in the Commit phase). At the end, Bob performs a check to see whether Alice cheated or not. In the honest case, Bob always accepts.

2.3 Definitions of Coin flipping

We provide the formal definitions of all the different variants of coin flipping protocols that we are going to use.

In a coin flipping protocol, we call a round of communication one message from Alice to Bob and one message from Bob to Alice. We suppose that Alice always sends the first message and Bob always sends the last message. The protocol is quantum if we allow the parties to send quantum messages and perform quantum operations. A player is honest if he or she follows the protocol. A cheating player can deviate arbitrarily from the protocol but still outputs a value at the end of it. There are two important variants of coin flipping that have been studied.

Strong Coin Flipping

A strong coin flipping protocol between two parties Alice and Bob is a protocol where Alice and Bob interact and at the end, Alice outputs a value $c_A \in \{0, 1, \text{Abort}\}$ and Bob outputs a value $c_B \in \{0, 1, \text{Abort}\}$. If $c_A = c_B$, we say that the protocol outputs $c = c_A$. If $c_A \neq c_B$ then the protocol outputs $c = \text{Abort}$.

A strong coin flipping protocol with bias ε ($SCF(\varepsilon)$) has the following properties

- If Alice and Bob are honest then $\Pr[c = 0] = \Pr[c = 1] = 1/2$

- If Alice cheats and Bob is honest then $P_A^* = \max\{\Pr[c = 0], \Pr[c = 1]\} \leq 1/2 + \varepsilon$.

- If Bob cheats and Alice is honest then $P_B^* = \max\{\Pr[c = 0], \Pr[c = 1]\} \leq 1/2 + \varepsilon$

The probabilities P_A^* and P_B^* are called the cheating probabilities of Alice and Bob respectively. The cheating probability of the protocol is defined as $\max\{P_A^*, P_B^*\}$. We say that the coin flipping is *perfect* if $\varepsilon = 0$. This is because a player that want to Abort can always declare victory rather than aborting without reducing the security of the protocol(see [Moc07]).

Weak coin flipping

A weak coin flipping protocol between two parties Alice and Bob is a protocol where Alice and Bob interact and at the end, Alice outputs a value $c_A \in \{0, 1\}$ and Bob outputs a value $c_B \in \{0, 1\}$. If $c_A = c_B$, we say that the protocol outputs $c = c_A$. If $c_A \neq c_B$ then the protocol outputs $c = \text{Abort}$. The difference with Strong coin flipping is that the players do not Abort. This is

because a player that wants to Abort can always declare victory rather than aborting without reducing the security of the protocol.

A (balanced) weak coin flipping protocol with bias ε ($WCF(1/2, \varepsilon)$) has the following properties

- If $c = 0$, we say that Alice wins. If $c = 1$, we say that Bob wins.

- If Alice and Bob are honest then $\Pr[\text{ Alice wins }] = \Pr[\text{ Bob wins }] = 1/2$

- If Alice cheats and Bob is honest then $P_A^* = \Pr[\text{ Alice wins }] \leq 1/2 + \varepsilon$

- If Bob cheats and Alice is honest then $P_B^* = \Pr[\text{ Bob wins }] \leq 1/2 + \varepsilon$

Similarly, P_A^* and P_B^* are the cheating probabilities of Alice and Bob. The cheating probability of the protocol is defined as $\max\{P_A^*, P_B^*\}$.

We can also define weak coin flipping for the case where the winning probabilities of the two players in the honest case are not equal.

Unbalanced weak coin flipping

A weak coin flipping protocol with parameter z and bias ε ($WCF(z, \varepsilon)$) has the following properties.

- If $c = 0$, we say that Alice wins. If $c = 1$, we say that Bob wins.

- If Alice and Bob are honest then $\Pr[\text{ Alice wins }] = z$ and $\Pr[\text{ Bob wins }] = 1 - z$

- If Alice cheats and Bob is honest then $P_A^* = \Pr[\text{ Alice wins }] \leq z + \varepsilon$

- If Bob cheats and Alice is honest then $P_B^* = \Pr[\text{ Bob wins }] \leq (1 - z) + \varepsilon$

Reformulation of Quantum weak coin flipping protocol   We reformulate here the definition of a quantum weak coin flipping to take into account the fact that Alice and Bob are quantum players that perform unitary operations during the protocol and at the end they perform a measurement on a quantum register in order to get their classical output. More precisely, let $\mathcal{O}_A$ (resp. $\mathcal{O}_B$) be Alice's (resp. Bob's) one-qubit output register. At the end of the protocol Alice (resp. Bob) has a state ρ_A in $\mathcal{O}_A$ (resp. ρ_B in $\mathcal{O}_B$). They also share some garbage state. The players get their output value by measuring their output qubit in the computational basis. Let ρ_{AB} the joint output state of Alice and Bob in $\mathcal{O}_A \otimes \mathcal{O}_B$. In this setting, a weak coin flipping has the following properties.

- The 0 outcome corresponds to Alice winning. The 1 outcome corresponds to Bob winning.

- If Alice and Bob are honest then $\langle 00|\rho_{AB}|00\rangle = \langle 11|\rho_{AB}|11\rangle = 1/2$

- If Alice cheats and Bob is honest then $P_A^* = \langle 0|\rho_B|0\rangle \leq 1/2 + \varepsilon$

- If Bob cheats and Alice is honest then $P_B^* = \langle 1|\rho_A|1\rangle \leq 1/2 + \varepsilon$

Notice that Alice's cheating probability depends only on Bob's output. This is because a cheating Alice will always claim that she won, so she wins when Bob outputs 'Alice wins'. We have the same behavior for a cheating Bob.

Similarly, we can define an unbalanced weak coin flipping in this setting.

- The 0 outcome corresponds to Alice winning. The 1 outcome corresponds to Bob winning.

- If Alice and Bob are honest then $\langle 00|\rho_{AB}|00\rangle = z$; $\langle 11|\rho_{AB}|11\rangle = 1 - z$

- If Alice cheats and Bob is honest then $P_A^* = \langle 0|\rho_B|0\rangle \le z + \varepsilon$

- If Bob cheats and Alice is honest then $P_B^* = \langle 1|\rho_A|1\rangle \le (1 - z) + \varepsilon$

We will use the following result by Mochon.

Proposition 8 [Moc07] *For every $\varepsilon > 0$, there exists a quantum $WCF(1/2, \varepsilon)$ protocol P.*

Note also that this construction can be extended to the unbalanced case. A procedure to use balanced WCF protocols to unbalanced ones has been presented in [CK09]. This procedure was presented in the classical setting but can be easily extended to the quantum definitions of unbalanced weak coin.

Proposition 9 (CK09) *Let P be a $WCF(1/2, \varepsilon)$ protocol with N rounds. Then, $\forall z \in [0, 1]$ and $\forall k \in \mathbb{N}$, there exists a $WCF(x, \varepsilon_0)$ protocol Q such that:*

- *Q uses $k \cdot N$ rounds.*

- *$|x - z| \le 2^{-k}$.*

- *$\varepsilon_0 \le 2\varepsilon$.*

3 Proof of the Lower Bound

To prove the lower bound, we will show some generic cheating strategies for Alice and Bob that work for any kind of bit commitment scheme. We will then show that these cheating strategies give a cheating probability of approximately 0.739 for any protocol.

3.1 Description of cheating strategies

We denote by $|\psi_b\rangle$ the quantum state Alice and Bob share at the end of the commit phase. Let $\sigma_b = \mathrm{Tr}_{\mathcal{A}}|\psi_b\rangle\langle\psi_b|$ the state that Bob has after the commit phase when Alice honestly commits to bit b.

3.1.1 Bob's cheating strategy

The cheating strategy of Bob is the following:

- Perform the Commit phase honestly.

- Guess b by performing on the state at the end of the commit phase the optimal discriminating measurement between σ_0 and σ_1.

First note that an all-powerful Bob can always perform this strategy, since he knows the honest states σ_0 and σ_1 and can hence compute and perform the optimal measurement. Let us analyze this strategy. We know [Hel67] that Bob can guess b with probability $\frac{1}{2} + \frac{\Delta(\sigma_0, \sigma_1)}{2}$ and hence

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

8

3.1.2 Alice's cheating strategy

The cheating strategy of Alice is the following

- Perform a quantum strategy so that at the end of the commit phase, Bob has the state $\sigma_+ = \frac{1}{2}(\sigma_0 + \sigma_1)$.

- In order to reveal a specific value b, send b then apply a local quantum operation such that the actual joint state of the protocol, $|\phi_b\rangle$, satisfies $|\langle\phi_b|\psi_b\rangle| = F(\sigma_+, \sigma_b)$. Perform the rest of the reveal phase honestly.

First note that an all-powerful Alice can perform this strategy. An honest Alice has a strategy to make Bob's state after the commit phase equal to σ_b for both $b = 0$ and $b = 1$. A cheating Alice creates a qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Conditioned on 0 (resp. 1), she applies the strategy that will give Bob the state σ_0 (resp. σ_1). By doing this Bob's state at the end of the commit phase is exactly σ_+. Moreover, by Uhlmann's theorem, Alice can compute and perform the local unitary in the beginning of the reveal phase to create a state $|\phi_b\rangle$ that satisfies $|\langle\phi_b|\psi_b\rangle| = F(\sigma_+, \sigma_b)$.

For the analysis, since Bob accepts b with probability 1 when the joint state of the protocol is $|\psi_b\rangle$, he accepts with probability at least $|\langle\phi_b|\psi_b\rangle|^2 = F^2(\sigma_+, \sigma_b)$ when the joint state of the protocol is $|\phi_b\rangle$. From this cheating strategy, we have that

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

3.2 Showing the Lower Bound

We have the following bounds for cheating Alice and cheating Bob.

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

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

We now use the following inequality that will be proved in the next section

Proposition 10 *Let σ_0, σ_1 any two quantum states. Let $\sigma_+ = \frac{1}{2}(\sigma_0 + \sigma_1)$. We have*

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

Let $t = \Delta(\sigma_0, \sigma_1)$. From the above Proposition, we have the following bounds.

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

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

We get the optimal cheating probability by equalizing these two bounds, *ie.*

$$\left(1 - (1 - \frac{1}{\sqrt{2}})t\right)^2 = \frac{1 + t}{2}$$

Notice that the same cheating probabilities appeared in the analysis of a weak coin flipping protocol in [KN04]. Solving the equation gives $t \approx 0.4785$ and hence we have

Theorem 1 *In any quantum bit commitment protocol with cheating probabilities P_A^* and P_B^* we have* $\max\{P_A^*, P_B^*\} \geq 0.739$.

3.3 Proof of the fidelity Lemma

In this Section, we show Proposition 10.

Proof of Proposition 10:   We will prove this Lemma in three steps. Let σ_0, σ_1 two quantum states and let $\sigma_+ = \frac{1}{2}(\sigma_0 + \sigma_1)$.

Step 1   We first consider the states $\rho_0 = \frac{1}{2}|0\rangle\langle 0| \otimes \sigma_0 + \frac{1}{2}|1\rangle\langle 1| \otimes \sigma_1$ and $\rho_+ = \frac{1}{2}|0\rangle\langle 0| \otimes \sigma_+ + \frac{1}{2}|1\rangle\langle 1| \otimes \sigma_+$. We compute the trace distance and fidelity of these states

$$\Delta(\rho_0, \rho_+) = \frac{1}{2}\left(\Delta(\sigma_0, \sigma_+) + \Delta(\sigma_1, \sigma_+)\right) = \frac{1}{2}\Delta(\sigma_0, \sigma_1) \tag{1}$$

In order to calculate the fidelity we note first that $\rho_+^{\frac{1}{2}} = \frac{1}{\sqrt{2}}\left(|0\rangle\langle 0| \otimes \sigma_+^{\frac{1}{2}} + |1\rangle\langle 1| \otimes \sigma_+^{\frac{1}{2}}\right)$. From the definition of fidelity we have

$$
\begin{aligned}
F(\rho_0, \rho_+) &= tr\left(\sqrt{\rho_+^{\frac{1}{2}}\rho_0\rho_+^{\frac{1}{2}}}\right) \\
&= tr\left(\sqrt{\frac{1}{4}|0\rangle\langle 0| \otimes \sigma_+^{\frac{1}{2}}\sigma_0\sigma_+^{\frac{1}{2}} + \frac{1}{4}|1\rangle\langle 1| \otimes \sigma_+^{\frac{1}{2}}\sigma_1\sigma_+^{\frac{1}{2}}}\right) \\
&= tr\left(\frac{1}{2}|0\rangle\langle 0| \otimes \sqrt{\sigma_+^{\frac{1}{2}}\sigma_0\sigma_+^{\frac{1}{2}}} + \frac{1}{2}|1\rangle\langle 1| \otimes \sqrt{\sigma_+^{\frac{1}{2}}\sigma_1\sigma_+^{\frac{1}{2}}}\right) \\
&= \frac{1}{2}tr\left(\sqrt{\sigma_+^{\frac{1}{2}}\sigma_0\sigma_+^{\frac{1}{2}}}\right) + \frac{1}{2}tr\left(\sqrt{\sigma_+^{\frac{1}{2}}\sigma_1\sigma_+^{\frac{1}{2}}}\right) \\
&= \frac{1}{2}\left(F(\sigma_0, \sigma_+) + F(\sigma_1, \sigma_+)\right)
\end{aligned}
$$

Hence, by Cauchy-Schwartz we conclude that

$$F^2(\rho_0, \rho_+) \leq \frac{1}{2}F^2(\sigma_0, \sigma_+) + \frac{1}{2}F^2(\sigma_1, \sigma_+) \tag{2}$$

Step 2   Consider the POVM $E = \{E_1, \ldots, E_m\}$ with $p_i = tr(\rho_0 E_i)$ and $q_i = tr(\rho_+ E_i)$ such that $F(\rho_0, \rho_+) = \sum_i \sqrt{p_i q_i}$ (Prop. 5). We consider the states $D_0 = \sum_i p_i |i\rangle\langle i|$ and $D_+ = \sum_i q_i |i\rangle\langle i|$. For the trace distance and fidelity of these states, we have

$$\Delta(D_0, D_+) = \frac{1}{2}\sum_i |p_i - q_i| \leq \Delta(\rho_0, \rho_+) = \frac{1}{2}\Delta(\sigma_0, \sigma_1) \qquad \text{by Prop. 2, 3 and Eq. 1} \tag{3}$$

$$F(D_0, D_+) = F(\rho_0, \rho_+) = \sum_i \sqrt{p_i q_i} \tag{4}$$

Step 3 Let us define k such that $k/2 = \Delta(D_0, D_+)$. We now consider the states $T_0 = k|0\rangle\langle 0| + (1-k)|2\rangle\langle 2|$ and $T_+ = \frac{k}{2}|0\rangle\langle 0| + \frac{k}{2}|1\rangle\langle 1| + (1-k)|2\rangle\langle 2|$. We calculate the trace distance and fidelity of these states

$$\Delta(T_0, T_+) = \frac{k}{2} = \Delta(D_0, D_+) \leq \frac{\Delta(\sigma_0, \sigma_1)}{2} \tag{5}$$

$$F(T_0, T_+) = \left(1 - k + \frac{k}{\sqrt{2}}\right) \geq \left(1 - (1 - \frac{1}{\sqrt{2}})\Delta(\sigma_0, \sigma_1)\right) \tag{6}$$

The only thing remaining is to show that $F(T_0, T_+) \leq F(D_0, D_+)$. To prove this, we construct a completely positive trace preserving operation Q such that $Q(T_0) = D_0$ and $Q(T_+) = D_+$. We can then conclude using Proposition 7.

We define $D_1 = \sum_i r_i |i\rangle\langle i|$ with $p_i + r_i = 2q_i$. This means that $D_+ = \frac{1}{2}D_0 + \frac{1}{2}D_1$ and $\Delta(D_0, D_1) = k$.

Let $A = \{i : p_i \geq r_i\}$ and $B = \{i : p_i < r_i\}$. Let $w_i = \min\{p_i, r_i\}$ We consider the following Q

$$Q(|0\rangle\langle 0|) = \sum_{i \in A} \frac{1}{k}(p_i - r_i)|i\rangle\langle i|$$

$$Q(|1\rangle\langle 1|) = \sum_{i \in B} \frac{1}{k}(r_i - p_i)|i\rangle\langle i|$$

$$Q(|2\rangle\langle 2|) = \sum_{i} \frac{1}{1-k}w_i|i\rangle\langle i|$$

$$Q(|i\rangle\langle j|) = 0 \quad \text{for } i \neq j$$

Since $\Delta(D_0, D_1) = k$, we have in particular that $\sum_i w_i = 1 - k$; $\sum_{i \in A}(p_i - r_i) = \sum_{i \in B}(r_i - p_i) = k$ (see Proposition 2). Q is hence a completely positive trace preserving operation. We now have:

$$Q(T_0) = k \sum_{i \in A} \frac{1}{k}(p_i - r_i)|i\rangle\langle i| + (1-k)\sum_{i} \frac{1}{1-k}w_i|i\rangle\langle i|$$

$$= \sum_{i \in A}(p_i - r_i)|i\rangle\langle i| + \sum_{i} w_i|i\rangle\langle i|$$

$$= \sum_{i \in A}(p_i - r_i + r_i)|i\rangle\langle i| + \sum_{i \in B} p_i|i\rangle\langle i|$$

$$= \sum_{i} p_i|i\rangle\langle i| = D_0$$

Similarly, we have

$$Q(T_+) = \frac{k}{2}\sum_{i \in A} \frac{1}{k}(p_i - r_i)|i\rangle\langle i| + \frac{k}{2}\sum_{i \in B} \frac{1}{k}(r_i - p_i)|i\rangle\langle i| + (1-k)\sum_{i} \frac{1}{1-k}w_i|i\rangle\langle i|$$

$$= \sum_{i \in A} \frac{p_i - r_i}{2}|i\rangle\langle i| + \sum_{i \in B} \frac{r_i - p_i}{2}|i\rangle\langle i| + \sum_{i} w_i|i\rangle\langle i|$$

$$= \sum_{i \in A}(r_i + \frac{p_i - r_i}{2})|i\rangle\langle i| + \sum_{i \in B}(p_i + \frac{r_i - p_i}{2})|i\rangle\langle i|$$

$$= \sum_{i} q_i|i\rangle\langle i| = D_+$$

From this, we conclude that

$$F(D_0, D_+) = F(Q(T_0), Q(T_+)) \geq F(T_0, T_+). \tag{7}$$

Putting everything together, we have using equations (2),(4),(6),(7)

$$\frac{1}{2}\left(F^2(\sigma_0, \sigma_+) + F^2(\sigma_1, \sigma_+)\right) \geq F^2(\rho_0, \rho_+) = F^2(D_0, D_+) \geq F^2(T_0, T_+) \geq \left(1 - (1 - \frac{1}{\sqrt{2}})\Delta(\sigma_0, \sigma_1)\right)^2$$

$\blacksquare$

4 Proof of the Upper Bound

In this section we describe and analyze a protocol that proves the optimality of our bound.

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 $0.739 + O(\epsilon)$.*

Our protocol is a quantum improvement of the following simple protocol that achieves cheating probability $3/4$. Alice commits to bit b by preparing the state $1/\sqrt{2}(|bb\rangle + |22\rangle)$ and sending the second qutrit to Bob. In the reveal phase, she sends the first qutrit and Bob checks that the pure state is the correct one. It is not hard to prove that both Alice and Bob can cheat with probability $3/4$ [Amb01, KN04]. The main idea in order to reduce the cheating probabilities for both players is the following: first we increase a little bit the amplitude of the state $|22\rangle$ in this superposition. This decreases the cheating probability of Bob. However, now Alice can cheat even more. To remedy this, we use the quantum procedure of a weak coin flipping so that Alice and Bob jointly create the above initial state (with the appropriate amplitudes) instead of having Alice create it herself. We present now the details of the protocol.

4.1 The protocol

Commit phase, Step 1 Alice and Bob perform an unbalanced weak coin flipping procedure (without measuring the final outcome), where Alice wins with probability $1 - p$ and Bob with probability p. As we said, we can think of this procedure as a big unitary operation that creates a joint pure state in the space of Alice and Bob. Moreover, Alice and Bob have each a special 1-qubit register that they can measure at the end of the protocol in order to read the outcome of the weak coin flipping. Here, we assume that they don't measure anything and that at the end Alice sends back to Bob all her garbage qubits. In other words, in the honest case, Alice and Bob share the following state at the end of the weak coin protocol

$$|\Omega\rangle = \sqrt{p}|L\rangle_{\mathcal{A}} \otimes |L, G_L\rangle_{\mathcal{B}} + \sqrt{1 - p}|W\rangle_{\mathcal{A}} \otimes |W, G_W\rangle_{\mathcal{B}}$$

where W corresponds to the outcome "Alice wins" and L corresponds to the outcome "Alice loses". The spaces $\mathcal{A}, \mathcal{B}$ correspond to Alice's and Bob's private quantum space. The garbage states $|G_W\rangle, |G_L\rangle$ are known to both players.

Commit phase, Step 2 After the end of the weak coin flipping procedure, Alice does the following. Conditioned on her qubit being W, she creates two qutrits in the state $|22\rangle$ and sends the second to Bob. Conditioned on her qubit being L, she creates two qutrits in the state $|bb\rangle$ where b is the bit she wants to commit to and sends the second to Bob. If the players are both honest, they share the following state:

$$|\Omega_b\rangle = \sqrt{p}|L, b\rangle_{\mathcal{A}} \otimes |L, b, G_L\rangle_{\mathcal{B}} + \sqrt{1-p}|W, 2\rangle_{\mathcal{A}} \otimes |W, 2, G_W\rangle_{\mathcal{B}}$$

Reveal phase In the reveal phase, Alice sends b and all her remaining qubits in space $\mathcal{A}$ to Bob. Bob checks that he has the state $|\Omega_b\rangle$.

4.2 Analysis

If Alice and Bob are both honest then Alice always successfully reveals the bit b she committed to.

Cheating Bob Bob is not necessarily honest in the weak coin flipping protocol, however the weak coin flipping has small bias ϵ. Since Alice is honest, Bob has all the qubits expect the one qubit which is in Alice's output register. At the end of the first step of the Commit phase, Alice and Bob share a state

$$|\Omega^*\rangle = \sqrt{p'}|L\rangle_{\mathcal{A}}|\Psi_L\rangle_{\mathcal{B}} + \sqrt{1-p'}|W\rangle_{\mathcal{A}}|\Psi_W\rangle_{\mathcal{B}}$$

for some states $|\Psi_L\rangle, |\Psi_W\rangle$ held by Bob. Recall that the outcome L in Alice's output register corresponds to the outcome where Alice loses the weak coin flipping protocol. Hence, for any cheating Bob, since our coin flipping has bias ε, we have $p' \leq p + \varepsilon$. At the end of the commit phase, depending on Alice's committed bit b, the joint state is

$$|\Omega_b^*\rangle = \sqrt{p'}|L, b\rangle_{\mathcal{A}}|b, \Psi_L\rangle_{\mathcal{B}} + \sqrt{1-p'}|W, 2\rangle_{\mathcal{A}}|2, \Psi_W\rangle_{\mathcal{B}}$$

and Bob's density matrix is

$$\sigma_b^* = p'|b, \Psi_L\rangle\langle b, \Psi_L| + (1-p')|2, \Psi_W\rangle\langle 2, \Psi_W|.$$

By Proposition 4, we have

$$P_B^* = \Pr[\text{ Bob guesses } b] \leq \frac{1}{2} + \frac{\Delta(\sigma_0^*, \sigma_1^*)}{2} = \frac{1}{2} + \frac{p'}{2} \leq \frac{1+p}{2} + \frac{\varepsilon}{2}$$

Cheating Alice Let σ_b be Bob's reduced state at the end of the commit phase when both players are honest. Let $|\bar{x}\rangle = |L, x, G_L\rangle$ for $x \in \{0, 1\}$ and $|\bar{2}\rangle = |W, 2, G_W\rangle$. We have

$$\sigma_b = p|\bar{b}\rangle\langle\bar{b}| + (1-p)|\bar{2}\rangle\langle\bar{2}|$$

Let ξ be Bob's state at the end of the commit phase for a cheating Alice. Let $r_i = \langle\bar{i}|\xi|\bar{i}\rangle$ for $i \in \{0, 1, 2\}$. From the characterization of the fidelity in Proposition 7, we have that

$$F(\xi, \sigma_b) \leq \sqrt{pr_b} + \sqrt{(1-p)r_2}$$

13

From standard analysis of bit commitment protocol (for example [KN04]), we have using Uhlmann's Theorem that

$$P_A^* \leq \frac{1}{2} \left(F^2(\xi, \sigma_0) + F^2(\xi, \sigma_1) \right)$$
$$\leq \frac{1}{2} \left(\sqrt{pr_0} + \sqrt{(1-p)r_2} \right)^2 + \frac{1}{2} \left(\sqrt{pr_1} + \sqrt{(1-p)r_2} \right)^2$$

In order to get a tight bound for the above expression, we use here the property of the weak coin flipping. Recall that $|\overline{2}\rangle = |W, 2, G_W\rangle$ has its first register as W (this corresponds to Alice winning the coin flip). On the other hand, $|\overline{0}\rangle$ and $|\overline{1}\rangle$ have L as their first register, corresponding to the case where Bob wins. For any cheating Alice, she can win the weak coin flip with probability smaller than $1 - p + \varepsilon$ and hence this means in particular that $r_2 \leq 1 - p + \varepsilon$. Moreover, $r_0 + r_1 + r_2 \leq 1$. For $\varepsilon < p(1 - \frac{1}{2-p})$, we can show that this quantity is maximal when r_2 is maximal and $r_0 = r_1 = (p - \varepsilon)/2$ (proven in Appendix A). This gives us

$$P_A^* \leq \left(\sqrt{p \cdot \frac{p - \varepsilon}{2}} + \sqrt{(1-p)(1-p+\varepsilon)} \right)^2 \leq \left(1 - (1 - \frac{1}{\sqrt{2}})p \right)^2 + O(\varepsilon)$$

Putting it all together   Except for the terms in ε, we obtain exactly the same quantities as in our lower bound. By equalizing these cheating probabilities, we have

$$\max\{P_A^*, P_B^*\} \approx 0.739 + O(\varepsilon)$$

Since we can have ε arbitrarily close to 0 (Proposition 8) and we can have an unbalanced weak coin flipping protocol with probability arbitrarily close to p (Proposition 9), we conclude that our protocol is arbitrarily close to optimal.

5   Proof of the classical lower bound

In this Section, we show a 3/4 lower bound for classical bit commitment schemes when players additionally have the power to perform perfect (strong or weak) coin-flipping. This will show that unlike strong coin flipping, quantum and classical bit commitment are not alike in the presence of weak coin flipping.

We first describe such protocols in Section 5.1. In Section 5.2, we construct a cheating strategy for Alice and Bob for these protocols such that one of the players can cheat with probability at least 3/4.

5.1   Description of a classical bit commitment protocol with perfect coin flips

We describe classical bit commitment schemes when players additionally have the power to perform perfect (strong or weak) coin-flipping. The way we deal with the coin is the following: when Alice and Bob are honest, they always output the same random value c and both players know this value. We can suppose equivalently that a random coin c is given publicly to both Alice and Bob each time they perform coin flipping. We describe any BC protocol with coins as follows:

- Alice and Bob have some private randomness R_A and R_B respectively.

- *Commit phase:* Alice wants to commit to some value x. Let N the number of rounds of the commit phase. For $i = 1$ to N: Alice sends a message a_i, Bob sends a message b_i, Alice and Bob flip a coin and get a public $c_i \in_R \{0, 1\}$.

- *Reveal phase:* Alice wants to decommit to some value y ($= x$ if Alice is honest).

  1. Alice first reveals y. This is a restriction for the protocol but showing a lower bound for such protocols will show a lower bound for all protocols since this can only limit Alice's cheating possibilities without helping Bob.

  2. Let M the number of rounds of the reveal phase. For $i = 1$ to M: Alice sends a message a_i', Bob sends a message b_i', Alice and Bob flip a coin and get a public $c_i' \in_R \{0, 1\}$.

  3. Bob has an accepting procedure Acc to decide whether he accepts the revealed bit or whether he aborts (if Bob catches Alice cheating).

We denote the commit phase transcript by $t_C = (a_1, b_1, c_1, \ldots, a_N, b_N, c_N)$. If Alice and Bob are honest, then we can write $t_C = T_C(R_A, R_B, c, x)$ where T_C is a function fixed by the protocol that takes as input Alice and Bob's private coins R_A, R_B, the outcomes of the public coin flips $c = (c_1, \ldots, c_N)$ as well as the bit x Alice wants to commit to and outputs a commit phase transcript t_C. If we can write $t_C = T_C(R_A, R_B, c, x)$ for some R_A, R_B, c, x, we say that t_C is an honest commit phase transcript.

Similarly, we define the decommit phase transcript by $t_D = (a_1', b_1', c_1', \ldots, a_M', b_M', c_M')$. If Alice and Bob are honest, we can write $t_D = T_D(R_A, R_B, c', y, t_C)$, where T_D is a function fixed by the protocol that takes as input Alice and Bob's private coins R_A, R_B, the outcomes of the public coin flips $c' = (c_1', \ldots, c_M')$, the bit y Alice reveals as well as the commit phase transcript t_C and outputs a reveal phase transcript t_D. If we can write $t_D = T_D(R_A, R_B, c', y, t_C)$ for some R_A, R_B, c', y and some honest commit phase transcript t_C, we say that t_D is an honest reveal phase transcript.

Whether Bob accepts at the end of the protocol depends on both transcripts t_C, t_D of the commit and reveal phase, the bit y Alice reveals as well as Bob's private coins. We write that $Acc(t_C, t_D, y, R_B) = 1$ when Bob accepts.

Note that in the honest case, Bob always accepts Alice's deommitment. This means that we can transform Alice's honest strategy in the reveal phase to a deterministic strategy which will also be always accepted. This fact will be useful in the proof.

5.2   Proof of the classical lower bound

In this Section, we construct cheating strategies for Alice and Bob such that one of the players will be able to cheat with probability greater than $3/4$. We only consider cheating strategies where Alice and Bob are honest during the coin flips so again, they will be modeled as public and perfectly random coins. Moreover, Alice and Bob will always be honest during the commit phase.

Before describing the cheating strategies we need some definitions. More particularly, we consider a cheating Alice who cheats during the reveal phase by following a deterministic strategy A^*. For a fixed honest commit phase transcript t_C, we can write the transcript of the reveal phase as a function of A^*, R_B, c', y, t_C, more precisely $T_D^*(A^*, R_B, c', y, t_C)$.

Definition 4 *We say that R_B is consistent with t_C if and only if there exist R_A, c, x such that $t_C = T_C(R_A, R_B, c, x)$.*

Definition 5 *Let t_C an honest commit phase transcript. We say that $t_C \in A_y$ if and only if*

$$\exists A^* \text{ s.t. } \forall c' \text{ and } \forall R_B \text{ consistent with } t_C, Acc(t_C, T_D^*(A^*, R_B, c', y, t_C), y, R_B) = 1$$

Intuitively, $t_C \in A_y$ means that if Alice and Bob output an honest commit phase transcript t_C, there is a deterministic strategy A^* for Alice that allows her to reveal y without Bob aborting, independently of Bob's private coins R_B. Since there is always a deterministic honest strategy for Alice in the reveal phase (when Alice and bob have been honest in the commit phase), we have

$$\forall \ R_A, R_B, c, x \quad t_C = T_C(R_A, R_B, c, x) \in A_x$$

Notice also that for any honest commit phase transcript t_C, both players Alice and Bob can compute whether $t_C \in A_u$ for both $u = 0$ and $u = 1$.

Definition 6 *We define the probability*

$$p_u = \Pr[t_C = T_C(R_A, R_B, c, u) \in A_{\overline{u}}] \quad \text{where the probability is taken over uniform } R_A, R_B, c.$$

Consider that Bob is honest. p_u is the probability that if Alice behaves honestly in the commit phase and commits to u, she has a deterministic cheating strategy to reveal $\overline{u}$ which always succeeds (independently of c', R_B).

We can now describe and analyze our cheating strategies for Alice and Bob and prove our theorem

Theorem 3 *For any classical bit commitment protocol with access to public perfect coins, one of the players can cheat with probability at least $3/4$.*

Proof: Let us fix a bit commitment protocol. We describe cheating strategies for Alice and Bob.

Cheating Alice

- Commit phase: Alice picks $x \in_R \{0, 1\}$ and she honestly commits to x during the commit phase.

- Reveal phase: if Alice wants to reveal x, she just remains honest during the reveal phase. By completeness of the protocol, this strategy succeeds with probability 1. If Alice wants to reveal $\overline{x}$, we know by definition of p_x that she succeeds with probability at least p_x. This gives us:

$$P_A^* \geq \frac{1}{2} + \frac{p_x}{2}$$

since Alice chooses x at random, we have:

$$P_A^* \geq \frac{1}{2} + \frac{p_0 + p_1}{4}$$

16

Cheating Bob As Alice, Bob is honest in the commit phase. Let x the bit Alice committed to. Since Alice and Bob are honest the commit-phase transcript is $t_C = T_C(R_A, R_B, c, x)$ for uniformly random R_A, R_B, c. As said before, we know that $t_C \in A_x$.

At the end of the commit phase, Bob wants to guess the bit x Alice commits to and he performs the following strategy: if $t_C \in A_0 \cap A_1$ he guesses x at random. If $\exists! \, u$ s.t. $t_C \notin A_u$ he guesses $x = \overline{u}$.

We know that Bob succeeds in cheating with probability $1/2$ if $t_C \in A_{\overline{x}}$ and with probability 1 if $t_C \notin A_{\overline{x}}$. This gives us $P_B^* \geq p_x \cdot \frac{1}{2} + (1 - p_x) \cdot 1 = 1 - \frac{p_x}{2}$. Since again, Alice's bit x is uniformly random, we have

$$P_B^* \geq 1 - \frac{p_0 + p_1}{4}$$

Putting it all together Taking Alice and Bob cheating probabilities together, we have $P_A^* + P_B^* \geq 3/2$ which gives $\max\{P_A^*, P_B^*\} \geq 3/4$.

■

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] Andre Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:527–533, 2009.

[CKS10]   André Chailloux, Iordanis Kerenidis, and Jamie Sikora. Lower bounds for Quantum Oblivious Transfer. In Kamal Lodaya and Meena Mahajan, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2010)*, volume 8 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 157–168, Dagstuhl, Germany, 2010. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[DFR$^+$07]   Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. A tight high-order entropic quantum uncertainty relation with applications. In *Proceedings of the 27th annual international cryptology conference on Advances in cryptology*, CRYPTO'07, pages 360–378, Berlin, Heidelberg, 2007. Springer-Verlag.

[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.

[Hel67]   C. W. Helstrom. Detection theory and quantum mechanics. 10(3):254–291, 1967.

[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. WCF, 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.

A   Proof of $r_0 = r_1$ and r_2 maximal in the quantum lower bound

In this Section, we show the following:

Proposition 11 *Let*

$$P_A^* \le \frac{1}{2}\left(\sqrt{pr_0} + \sqrt{(1-p)r_2}\right)^2 + \frac{1}{2}\left(\sqrt{pr_1} + \sqrt{(1-p)r_2}\right)^2$$

with the constraints: $r_0, r_1, r_2 \ge 0$, $r_0 + r_1 + r_2 \le 1$ and $r_2 \le 1 - p + \varepsilon$ for $\varepsilon < p(1 - \frac{1}{2-p})$. This cheating probability is maximized for $r_0 = r_1 = \frac{p-\varepsilon}{2}$ and $r_2 = 1 - p + \varepsilon$.

Proof: First note that the maximal cheating probability is achieved for $r_0 + r_1 + r_2 = 1$ since this cheating probability is increasing in r_0, r_1, r_2.

We first show that $r_0 = r_1$. Let's fix r_2. This means that $S = r_0 + r_1 = 1 - r_2$ is fixed. Let $u = \sqrt{(1-p)r_2}$. We have

$$P_A^* \le f(r_0) = \frac{1}{2}\left(\sqrt{pr_0} + u\right)^2 + \frac{1}{2}\left(\sqrt{p(S - r_0)} + u\right)^2 .$$

Taking the derivative, we have

$$
\begin{aligned}
f'(r_0) &= \frac{1}{2}\left(2\sqrt{p}\frac{1}{2\sqrt{r_0}}(\sqrt{pr_0} + u) - 2\sqrt{p}\frac{1}{2\sqrt{(S - r_0)}}(\sqrt{p(S - r_0)} + u)\right) \\
&= \frac{1}{2}\left(p + \frac{u\sqrt{p}}{\sqrt{r_0}} - p - \frac{u}{\sqrt{p}}\sqrt{S - r_0}\right) \\
&= \frac{u\sqrt{p}}{2}\left(\frac{1}{\sqrt{r_0}} - \frac{1}{\sqrt{S - r_0}}\right)
\end{aligned}
$$

We have $f'(r_0) > 0$ for $r_0 < S/2$; $f'(r_0) = 0$ for $r_0 = S/2$; $f'(r_0) < 0$ for $r_0 > S/2$. This means that the maximum of f is achieved for $r_0 = S/2$ *i.e.* $r_0 = r_1$.

We now show that $r_2 = 1 - p + \varepsilon$ gives the maximal cheating probability if ε is not too big. Since P_A^* is maximal for $r_0 = r_1$ and for $r_0 + r_1 + r_2 = 1$, we have

$$
\begin{aligned}
P_A^* &\le \frac{1}{2}\left(\sqrt{pr_0} + \sqrt{(1-p)r_2}\right)^2 + \frac{1}{2}\left(\sqrt{pr_0} + \sqrt{(1-p)r_2}\right)^2 \\
&\le (\sqrt{pr_0} + \sqrt{(1-p)r_2})^2 \\
&\le \left(\sqrt{p(\frac{1 - r_2}{2})} + \sqrt{(1-p)r_2}\right)^2 = g(r_2)
\end{aligned}
$$

Again, we take the derivative of g.

$$g'(r_2) = \left(-\frac{\sqrt{p}}{\sqrt{2(1 - r_2)}} + \frac{\sqrt{1 - p}}{\sqrt{r_2}}\right) \cdot \left(\sqrt{p(\frac{1 - r_2}{2})} + \sqrt{(1-p)r_2}\right)$$

From this, we have

$$g'(r_2) \geq 0 \Leftrightarrow \left(-\frac{\sqrt{p}}{\sqrt{2(1 - r_2)}} + \frac{\sqrt{1 - p}}{\sqrt{r_2}} \right) \geq 0$$

$$\Leftrightarrow \sqrt{\frac{p}{2(1 - r_2)}} \leq \sqrt{\frac{1 - p}{r_2}}$$

$$\Leftrightarrow pr_2 \leq 2(1 - r_2)(1 - p)$$

$$\Leftrightarrow r_2 \leq 1 - \frac{p}{2 - p}$$

For $\varepsilon < p(1 - \frac{1}{2-p})$, we have $1 - p + \varepsilon < 1 - \frac{p}{2-p}$, so when $\varepsilon < p(1 - \frac{1}{2-p})$, $g(r_2)$ is always increasing when $r_2 \leq 1 - p + \varepsilon$ and is maximal when $r_2 = 1 - p + \varepsilon$, which concludes the proof. ∎