Improved Loss-Tolerant Quantum Coin Flipping

André Chailloux

March 15, 2011

Abstract

In this paper, we present a loss-tolerant quantum strong coin flipping protocol with bias $\varepsilon \approx 0.359$. This is an improvement over Berlin *et al.* 's protocol [BBBG08] which achieves a bias of 0.4. To achieve this, we extend Berlin *et al.* 's protocol by adding an encryption step that hides some information to Bob until he confirms that he successfully measured. We also show using numerical analysis that a we cannot improve this bias by considering a k-fold repetition of Berlin *et al.* 's protocol for $k > 2$.

1 Introduction

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.

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 case of coin flipping is one of the most intriguing ones. Even though the results of Mayers and of Lo and Chau exclude the possibility of perfect quantum coin flipping, it still remained open whether one can construct a quantum protocol where no player could bias the coin with probability 1. A few years later, Aharonov et al. [ATVY00] provided such a 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. Finally, it was shown in [CK09] how to achieve a strong coin flipping with cheating probability $\frac{1}{\sqrt{2}}$ using a weaker coin flipping primitive developed by Mochon [Moc07].

The results mentioned earlier don't take into account practical issues such as losses, noise or other imperfections in the quantum apparatus used. In 2008, Berlin *et al.* presented a loss-tolerant quantum coin flipping with bias 0.4. In this protocol, honest players don't always succeed when they perform a measurement (the measurement sometimes abort) but when they do succeed, they always output the correct value. This is in contrast with noise tolerance where an honest player could perform a measure with a wrong outcome without knowing it. Recently, Aharon *et al.* [AMS10] created a loss-tolerant quantum coin flipping protocol with bias $\varepsilon \approx 0.3975$. In another flavor, Barrett and Massar [BM04] showed how to do bit-string generation (a weaker notion of coin flipping) in the presence of noise.

In this paper, we continue the study of loss-tolerant quantum coin flipping protocol. We construct such a protocol with bias $\varepsilon \approx 0.359$. To achieve this bias, we extend Berlin *et al.* 's protocol by adding an encryption step that hides some information to Bob as long as he doesn't confirm that he successfully measured. Notice that we improve the bias of the protocol by adding only a classical layer on top of Berlin *et al.* 's protocol. Let us emphasize that in this paper we only look at information theoretic security and we do not discuss computational security or security in restricted models like the bounded-storage or noisy-storage model [DFSS08, WST08].

It would be interesting whether to see whether such techniques can be used to deal with loss-tolerance in other practical models such as the bounded/noisy storage model. Moreover, finding a noise-tolerant quantum coin flipping with information theoretic security and small bias remains an interesting open question.

2 Our work

We continue [BBBG08]'s work and try to create practical quantum coin flipping protocols. As their protocol, we ask Alice and Bob to send several copies of single qubit states. Moreover, we don't require honest players to have any quantum memories. On the other hand, we consider cheating players as being all powerful.

As explained in [BBBG08], one of the main difficulties in creating a bit-commitment based coin flipping lies in the states you send to Bob. The existence of a conclusive measurement between the states sent to Bob allows him to cheat perfectly even if the states are close. Berlin *et al.* 's protocol is of the following form.

- Alice sends a state σ to Bob.
- Bob measures this state in some basis B (possibly dependent on some of his private coins). If Bob successfully measures then they continue the protocol. Otherwise, they start again

In this protocol, the state σ is chosen very carefully such that a cheating Bob cannot take advantage of the fact, that he can reset the protocol. This strongly limits the good choices for σ. To partially overcome this problem, we use the following high-level scheme

- Alice picks $r \in_R \{0, 1\}$ and sends $E_r(\sigma)$ where E_r is some quantum operation that hides some information about σ
- Bob measures in some basis B. If Bob successfully measures then they continue the protocol. Otherwise, they start again
- Alice reveals r and then they continue the protocol

While doing this, one must be careful that an honest Bob will still be able to exploit the measurement of the encrypted state and that Alice cannot use this to cheat.

Applying this scheme on a two-fold parallel repetition of Berlin *etal*'s protocol, we show the following

Theorem 2.1 *There is a loss-tolerant quantum coin flipping protocol with bias* $\varepsilon \approx 0.359$

Notice that without this encryption step extra step, the resulting scheme would not be loss-tolerant but the bias would remain the same.

3 Preliminaries

3.1 Definitions

The statistical distance over classical distributions is defined as $\Delta(\{X_i\}_{i\in\{0,1\}^n}, \{Y_i\}_{i\in\{0,1\}^n}) = \frac{1}{2}\sum_i |X_i - Y_i|$

Following [NC00], we define the fidelity and the trace distance for any quantum states ρ, σ as follows

$$\begin{aligned} D(\rho,\sigma) &= \frac{1}{2}|\sigma-\rho| \quad \text{with } |A| = \sqrt{A^\dagger A} \\ F(\rho,\sigma) &= tr(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}) \end{aligned}$$

Note that the fidelity is sometimes defined as $(tr(\sqrt{\rho^{1/2}\sigma\rho^{1/2}}))^2$.

For two quantum 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 $D(\rho,\sigma) = \Delta(\{X_i\},\{Y_i\})$ and $F(\rho,\sigma) = \sum_i \sqrt{p_i q_i}$.

Definition 3.1 *Let* E *and* F *any two ensembles of quantum states and let* ρ *any quantum state. We define:*

$$\begin{aligned} F(\rho,E) &= \max_{\sigma\in E} F(\rho,\sigma) \\ F(E,F) &= \max_{\sigma\in E,\sigma'\in F} F(\sigma,\sigma') \end{aligned}$$

Finally, we define a (strong) coin flipping protocol

Definition 3.2 *A coin flipping protocol with bias* ε *consists of instructions given to Alice and Bob and an outcome* $x \in \{0,1,\perp\}$ *(*$\perp$ *corresponds to aborting the protocol) such that*

- *If Alice and Bob are honest then* $\Pr[x=0] = \Pr[x=1] = 1/2$
- *For any cheating Alice* $P_A^* = \max\{\Pr[x=0], \Pr[x=1]\} \leq 1/2 + \varepsilon$
- *For any cheating Bob* $P_B^* = \max\{\Pr[x=0], \Pr[x=1]\} \leq 1/2 + \varepsilon$

For completeness, we also define weak coin-flipping protocols

Definition 3.3 *A weak coin flipping protocol with bias* ε *consists of instructions given to Alice and Bob and an outcome* $x \in \{0,1,\perp\}$ *(*$\perp$ *corresponds to aborting the protocol) such that*

- *If Alice and Bob are honest then* $\Pr[x=0] = \Pr[x=1] = 1/2$
- *For any cheating Alice* $P_A^* = \Pr[x=0] \leq 1/2 + \varepsilon$
- *For any cheating Bob* $P_B^* = \Pr[x=1] \leq 1/2 + \varepsilon$

Intuitively, $x = 0$ *corresponds to the fact that Alice wins and* $x = 1$ *to the fact that Bob wins. Note that a cheating player can win with probability less than* $1/2 + \varepsilon$ *but can lose with probability* 1.

3.2 Useful facts

Proposition 3.4 *[NC00] For any two states* ρ_0, ρ_1 *and any pure state* $|\phi\rangle$*, we have*

$$D(\rho_0, \rho_1) \geq |\langle\phi|\rho_0|\phi\rangle - \langle\phi|\rho_1|\phi\rangle|$$

Proposition 3.5 *[NC00] For any two states* ρ, σ *such that* $\rho = \sum_i p_i |\phi_i\rangle\langle\phi_i|$ *and* $\sigma = \sum_i q_i |\phi_i\rangle\langle\phi_i|$*, we have*

$$D(\rho, \sigma) \leq \Delta(\{X_i\}, \{Y_i\})$$

Proposition 3.6 *[FG99] For any quantum states* ρ, σ*, we have*

$$1 - F(\rho, \sigma) \leq D(\rho, \sigma) \leq \sqrt{1 - F^2(\rho, \sigma)}$$

Proposition 3.7 *[KN04] For any quantum states* ρ, σ_0, σ_1*, we have*

$$F^2(\rho, \sigma_0) + F^2(\rho, \sigma_1) \leq 1 + F(\sigma_0, \sigma_1)$$

Proposition 3.8 *[Joz94] For any quantum states* ρ, σ_0, σ_1*, we have*

$$F^2(\rho, \sum_i p_i \sigma_i) \geq \sum_i p_i F^2(\rho, \sigma_i)$$

Proposition 3.9 *[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*

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

4 The protocol

4.1 Quantum states used

Consider the two orthonormal basis $\mathcal{B}^0(\lambda) = \{|\phi_0^0(\lambda)\rangle, |\phi_1^0(\lambda)\rangle\}$ and $\mathcal{B}^1(\lambda) = \{|\phi_0^1(\lambda)\rangle, |\phi_1^1(\lambda)\rangle\}$ for any $\lambda \in \mathbb{R}$ with:

$$\begin{aligned} |\phi_0^0(\lambda)\rangle &= \sqrt{\lambda}|0\rangle + \sqrt{1-\lambda}|1\rangle \\ |\phi_1^0(\lambda)\rangle &= \sqrt{1-\lambda}|0\rangle - \sqrt{\lambda}|1\rangle \end{aligned}$$

and

$$\begin{aligned} |\phi_0^1(\lambda)\rangle &= \sqrt{\lambda}|0\rangle - \sqrt{1-\lambda}|1\rangle \\ |\phi_1^1(\lambda)\rangle &= \sqrt{1-\lambda}|0\rangle + \sqrt{\lambda}|1\rangle \end{aligned}$$

$|\phi_c^b\rangle$ corresponds to the encoding of bit c in basis b.
Finally, we define

$$\rho_c = \frac{1}{2}\sum_i |\phi_c^i\rangle\langle\phi_c^i| = \lambda|c\rangle\langle c| + (1-\lambda)|1-c\rangle\langle 1-c|$$

4.2 Berlin *etal*'s protocol

Berlin *etal*'s protocol (parameter λ omitted)

1. Alice chooses at random $b \in_R \{0,1\}$ and $c \in_R \{0,1\}$ and sends $|\phi_c^b\rangle$ to Bob.
2. Bob chooses $b' \in_R \{0,1\}$ and measures the qubit he receives in basis $B_{b'}$. If his measurement fails, he announces it to Alice and they repeat the protocol from step 1. If the measurement succeeds continue.
3. Bob picks $c' \in_R \{0,1\}$ and sends c' to Alice
4. Alice reveals b, c
5. If $b = b'$, Bob checks that what he measured corresponds to $|\phi_c^b\rangle$. If it doesn't match, he aborts.
6. The outcome of the protocol is $x = c \oplus c'$.

This protocol is loss tolerant in the sense that a cheating Bob cannot gain advantage in the fact that he can restart the protocol when his measurement fails. This protocol has the following security parameters:

1. $P_A^* = \frac{3}{4} + \frac{\sqrt{\lambda(1-\lambda)}}{2}$
2. $P_B^* = \lambda$

By taking $\lambda = 0.9$, we have $P_A^* = P_B^* = 0.9$ and their protocol achieve a bias of 0.4.

4.3 Our protocol

Our protocol

1. Alice chooses at random $b_1, b_2 \in_R \{0,1\}$; $c \in_R \{0,1\}$ and $r_1, r_2 \in_R \{0,1\}$ sends two quantum registers $|\phi^{b_i}_{c\oplus r_i}\rangle$ for $i \in \{1,2\}$ to Bob.
2. Bob chooses $b'_1, b'_2 \in_R \{0,1\}$ and measures each register i he receives in basis $B_{b'_i}$. If one of his measurements fails, he announces it to Alice and they repeat the protocol from step 1. If the measurement succeeds, Bob announces this fact to Alice and they continue.
3. Alice sends r_1, r_2 to Bob.
4. Bob picks $c' \in_R \{0,1\}$ and sends c' to Alice
5. Alice reveals b_1, b_2, c
6. For each register i for which $b_i = b'_i$, Bob checks that what he measured corresponds to $|\phi^{b_i}_{c\oplus r_i}\rangle$. If one of the measurements does not match, he aborts.
7. The outcome of the protocol is $x = c \oplus c'$.

This protocol is closely related to a two-fold parallel repetition of Berlin *etal*'s protocol. Such a repetition would directly improve the bias if we did not require loss tolerance. We add an additionnal step in this protocol. Alice hides some information about the state she sends using 2 private bits r_1, r_2 that she reveals as soon as Bob confirms that he measured successfully. As we will show, this makes the protocol loss-tolerant again.

5 Security proofs

If Alice and Bob are honest then Bob never aborts and $x = c \oplus c'$ is random. We now analyse separately cheating Alice and cheating Bob.

5.1 Cheating Alice

We consider a cheating Alice and an honest Bob.

5.1.1 General framework for checking Bob

The way Bob checks is closely related to the following procedure

- Alice sends a state σ in space $\mathcal{Y}$
- At a later stage, Alice sends a bit i to Bob in space $\mathcal{X}$
- Bob checks that the first state Alice sends in $\mathcal{Y}$ is the state $|\psi_i\rangle$ for some state $|\psi_i\rangle$.

We want to show the following:

Proposition 5.1

$$\Pr[\textit{ Alice passes Bob's test }] \leq F^2(\sigma, L)$$

where $L = \{\sum_j p_i|\phi_j\rangle\langle\phi_j| : \sum_j p_j = 1\}$

Proof: Let σ the first state in $\mathcal{Y}$ sent by Alice and let $\widetilde{\sigma}$ the state in $\mathcal{XY}$ after Alice reveals i. Since Bob immediately measures the register $\mathcal{X}$ in the computational basis, there is an state $\widetilde{\sigma}$ which will give the best cheating probability of the form $\widetilde{\sigma} = \sum_i p_i|i\rangle\langle i| \otimes |\psi_i\rangle\langle\psi_i|$ and

$$\Pr[\text{ Alice passes Bob's test }] = \sum_i ||\psi_i\rangle\langle\phi_i||^2$$

Similarly, if we fix $\widetilde{\sigma} = |\Omega\rangle\langle\Omega|$ where $|\Omega\rangle = \sum_i \sqrt{p_i}|i, \phi_i\rangle$, we get that Pr[Alice passes Bob's test] = $\sum_i ||\psi_i\rangle\langle\phi_i||^2$ This means that we can suppose w.log that after the last step, the state in $\mathcal{XY}$ is pure.

Let $\widetilde{\sigma} = |\Omega\rangle\langle\Omega|$ where $|\Omega\rangle = \sum_i \sqrt{p_i}|i, \phi_i\rangle$. Let K subspace of quantum pure states spanned by $\{|i\rangle \otimes |\phi_i\rangle\}$. Let $P_K = \sum_i |i\rangle\langle i| \otimes |\phi_i\rangle\langle\phi_i|$ the projection on subspace K. Bob's check is equivalent to projecting on the subspace K.

$$\begin{aligned}
\Pr[\text{ Alice passes Bob's test }] &= tr(P_K\widetilde{\sigma}P_K) \\
&= tr(P_K|\Omega\rangle\langle\Omega|P_K) = \max_{|u\rangle\in L} |\langle\Omega|u\rangle|^2 \\
&\leq \max_{|u\rangle\in K} F^2(\mathrm{Tr}_{\mathcal{X}}(|\Omega\rangle\langle\Omega|), \mathrm{Tr}_{\mathcal{X}}|u\rangle\langle u|) \\
&\leq \max_{|u\rangle\in K} F^2(\sigma, \mathrm{Tr}_{\mathcal{X}}|u\rangle\langle u|) \\
&\leq F^2(\sigma, L) \quad \text{since } \forall|u\rangle \in K,\ \mathrm{Tr}_{\mathcal{X}}|u\rangle\langle u| \in L
\end{aligned}$$

■

5.2 Proof of security for cheating Alice

We consider a cheating Alice and an honest Bob. For the sake of the analysis, we can suppose that honest Bob doesnt' have losses when he measures (this does not help Alice). Our protocol says that Bob measures each register i in a random basis $B_{b'_i}$ and performs a check if this basis corresponds to the basis B_{b_i} in which Alice encoded c. Similarly, we could say that Bob performs this measurement at the very end (still picking b'_i at random). In this case, we are in the framework of the previous subsection except that with some probability, Bob chooses the wrong basis and does not check anything.

Suppose Alice wants to reveal c in our protocol. Let ξ the state in $\mathcal{XY}$ she sends at state 1. Let $\xi_X = \mathrm{Tr}_{\mathcal{Y}}\xi$ and $\xi_Y = \mathrm{Tr}_{\mathcal{X}}\xi$. Let $L_c = \{\sum_{i\in\{0,1\}} p_i|\phi^i_c\rangle\langle\phi^i_c|\}$

We have the following cases:

- Bob flipped $b'_1 \neq b_1$ and $b'_2 \neq b_2$. Bob does nt check anything Alice successfully reveals c with probability 1.
- Bob flipped $b'_1 = b_1$ and $b'_2 \neq b_2$. Bob checks the first register. From Proposition 5.1, Alice successfully reveals c with probability no greater than $F^2(\xi_X, L_c)$.

- Bob flipped $b'_1 \neq b_1$ and $b'_2 = b_2$. Bob checks the second register. Similarly, Alice successfully reveals c with probability no greater than $F^2(\xi_Y, L_c)$.
- Bob flipped $b'_1 = b_1$ and $b'_2 = b_2$. Bob checks both registers. In the same way, Alice successfully reveals c with probability no greater than $F^2(\xi, L_c^{\otimes 2})$.

This gives us

$$\Pr[\text{ Alice successfully reveals } c] = \frac{1}{4}\left(1 + F^2(\xi_X, L_c) + F^2(\xi_Y, L_c) + F^2(\xi, L_c \otimes 2)\right)$$

We will now need the following Lemma

Lemma 5.2

$$F(L_0, L_1) \leq 2\sqrt{\lambda(1-\lambda)}$$

Proof: Let $\rho_0 \in L_0$ and $\rho_1 \in L_1$ such that $F(\rho_0, \rho_1) = F(L_0, L_1)$. By definition of L_0, we have $\langle 0|\rho_0|0\rangle = \lambda$ and $\langle 0|\rho_1|0\rangle = 1 - \lambda$. This gives us $D(\rho_0, \rho_1) \geq 2\lambda - 1$. Using Proposition 3.7, we have

$$\begin{aligned} F(\rho_0, \rho_1) &\leq \sqrt{1 - D^2(\rho_0, \rho_1)} \\ &\leq \sqrt{1 - 4\lambda^2 + 4\lambda - 1} \\ &\leq 2\sqrt{\lambda(1-\lambda)} \end{aligned}$$

■

We can now prove our main statement

Proposition 5.3

$$P_A^* \leq \frac{1}{2} + \frac{1}{2}\left(\frac{1 + f(\lambda)}{2}\right)^2$$

where $f(\lambda) = 2\sqrt{\lambda(1-\lambda)}$

Proof: We suppose w.log that Alice wants final outcome $x = 0$. This means that she has to reveal $c = c'$. Let ξ the state sent by Alice and let $\xi_X = \mathrm{Tr}_{\mathcal{Y}}\xi$ and $\xi_X = \mathrm{Tr}_{\mathcal{Y}}\xi$. Since c' is random, we have

$$\begin{aligned} P_A^* &= \frac{1}{2}\sum_{c\in\{0,1\}} \Pr[\text{ Alice successfully reveals } c] \\ &\leq \frac{1}{2}\sum_{c\in\{0,1\}} \frac{1}{4}\left(1 + F^2(\xi_X, D_c) + F^2(\xi_Y, D_c) + F^2(\xi, DD_c)\right) \\ &\leq \frac{1}{8}\left(2 + 1 + F(D_0, D_1) + 1 + F(D_0, D_1) + 1 + F(DD_0, DD_1)\right) \quad (\textit{Proposition } 3.6) \\ &\leq \frac{1}{2} + \frac{1}{2}\left(\frac{1}{4} + \frac{1}{2}F(D_0, D_1) + \frac{1}{4}F^2(D_0, D_1)\right) \\ &\leq \frac{1}{2} + \frac{1}{2}\left(\frac{1 + f(\lambda)}{2}\right)^2 \quad (f(\lambda) \geq F(D_0, D_1) \text{ from Lemma } 5.2) \end{aligned}$$

■

5.3 Cheating Bob

The main part here is to show the loss-tolerance of the protocol. This means that a cheating Bob cannot take advantage of the fact that he's allowed to reset the protocol in case one of his measurements failed.

5.4 Cheat Sensitivity

For a fixed c and r_1, r_2, let $\xi_c^{r_1,r_2}$ sent by Alice. We have

$$\begin{aligned}\xi_c^{r_1,r_2} &= \frac{1}{4}\sum_{b_1,b_2\in\{0,1\}} |\phi^{b_1}_{c\oplus r_1}\phi^{b_2}_{c\oplus r_2}\rangle\langle\phi^{b_1}_{c\oplus r_1}\phi^{b_2}_{c\oplus r_2}| \\ &= \rho_{c\oplus r_1}\otimes\rho_{c\oplus r_2} \\ &= \sum_{u,v\in\{0,1\}} p^{u,v}_{c\oplus r_1,c\oplus r_2}|u,v\rangle\langle u,v|\end{aligned}$$

where: if $x = y$ then $p_x^y = \lambda$; if $x \neq y$ then $p_x^y = 1-\lambda$ and $p^{u,v}_{c\oplus r_1,c\oplus r_2} = p^u_{c\oplus r_1}\cdot p^v_{c\oplus r_2}$.

When receiving ξ, Bob performs a quantum operation

$$A(|u,v\rangle) = \alpha_{u,v}|\psi_{u,v}\rangle|0\rangle_{\mathcal{O}} + \beta_{u,v}|\omega_{u,v}\rangle|1\rangle_{\mathcal{O}}$$

where $\mathcal{O}$ is the space that Bob measures to determine whether he should announce that he succeeded the measurement or not. The outcome 0 in space $\mathcal{O}$ corresponds to the outcome where the protocol continues. In a way, the cheating Bob postselects on the outcome being 0 since if he obtains 1, he decides to start the protocol again. Once Bob successfully measured and after Alice sends r_1, r_2, Bob has the following state depending on the operation A he performed averaging on r_1, r_2.

$$\xi_c^A = \frac{1}{S}\sum_{\substack{r_1,r_2\in\{0,1\}\\u,v\in\{0,1\}}} p^{u,v}_{c\oplus r_1,c\oplus r_2}\Gamma_{u,v}|r_1,r_2,\psi_{u,v}\rangle\langle r_1,r_2,\psi_{u,v}|$$

where

- The $\Gamma_{u,v}$'s are arbitrary real numbers. These numbers depend on the $\alpha_{u,v}$'s. We assume that Bob can choose any value for these numbers.
- The $|\psi_{u,v}\rangle$'s are not necessarily orthogonal.
- S is a normalization factor.

Proposition 5.4 *$\forall A$, $D(\xi_0^A,\xi_1^A) \leq D(\xi_0,\xi_1)$ where $\xi_c = \rho_c^{\otimes 2}$.*

Proof: Let's fix A. We have

$$D(\xi_0^A,\xi_1^A) = \frac{1}{S}D\Big(\sum_{\substack{r_1,r_2\in\{0,1\}\\u,v\in\{0,1\}}} p^{u,v}_{r_1,r_2}\Gamma_{u,v}|r_1,r_2,\psi_{u,v}\rangle\langle r_1,r_2,\psi_{u,v}|, \sum_{\substack{r_1,r_2\in\{0,1\}\\u,v\in\{0,1\}}} p^{u,v}_{1\oplus r_1,1\oplus r_2}\Gamma_{u,v}|r_1,r_2,\psi_{u,v}\rangle\langle r_1,r_2,\psi_{u,v}|\Big)$$

from convexity of the statistical distance (Proposition 3.5) , we have

$$\begin{aligned} D(\xi_0^A, \xi_1^A) &\leq \frac{1}{S}\Delta\left(\{p^{u,v}_{r_1,r_2}\Gamma_{u,v}\}_{\substack{r_1,r_2\in\{0,1\}\\u,v\in\{0,1\}}}, \{p^{u,v}_{1\oplus r_1,1\oplus r_2}\Gamma_{u,v}\}_{\substack{r_1,r_2\in\{0,1\}\\u,v\in\{0,1\}}}\right) \\ &\leq \frac{1}{2S}\sum_{\substack{r_1,r_2\in\{0,1\}\\u,v\in\{0,1\}}} |p^{u,v}_{r_1,r_2}\Gamma_{u,v} - p^{u,v}_{1\oplus r_1,1\oplus r_2}\Gamma_{u,v}| \\ &\leq \frac{1}{2S}\sum_{u,v}\Gamma_{u,v}\sum_{r_1,r_2}|p^{u,v}_{r_1,r_2} - p^{u,v}_{1\oplus r_1,1\oplus r_2}| \end{aligned}$$

To calculate this sum, if $(r_1, r_2) = (u, v)$ then $p^{u,v}_{r_1,r_2} = \lambda^2$ and $p^{u,v}_{1\oplus r_1,1\oplus r_2} = (1-\lambda)^2$. If $(r_1, r_2) = (\overline{u}, \overline{v})$ then $p^{u,v}_{r_1,r_2} = (1-\lambda)^2$ and $p^{u,v}_{1\oplus r_1,1\oplus r_2} = \lambda^2$. In the other cases, $p^{u,v}_{r_1,r_2} = p^{u,v}_{1\oplus r_1,1\oplus r_2}$. This gives us

$$\begin{aligned} D(\xi_0^A, \xi_1^A) &\leq \frac{1}{2S}\sum_{u,v} 2\Gamma_{u,v}\left(\lambda^2 - (1-\lambda)^2\right) \\ &\leq 2\lambda - 1 \end{aligned}$$

Since, $\xi_c = \lambda^2|cc\rangle\langle cc| + \lambda(1-\lambda)(|01\rangle\langle 01| + |10\rangle\langle 10|) + (1-\lambda)^2|\overline{c}\ \overline{c}\rangle\langle\overline{c}\ \overline{c}|$, we have $D(\xi_0, \xi_1) = (\lambda^2 - (1-\lambda)^2) = 2\lambda - 1$, which allows us to conclude. ■

We can now prove our main Claim

Proposition 5.5 $P_B^* \leq \lambda$

Proof: Suppose w.log that Bob wants outcome $x = 0$. He wants to pick $c' = c$. Before picking c', he has the state ξ_c^A. We have

$$\begin{aligned} P_B^* &= \Pr[\text{ Bob guesses } c] \\ &= \frac{1}{2} + \frac{D(\xi_0^A, \xi_1^A)}{2} \\ &\leq \lambda \end{aligned}$$

■

Theorem 5.6 *There is a loss-tolerant quantum coin flipping protocol with bias* $\varepsilon \approx 0.359$

Proof: We just need to find λ that minimizes $\max(P_A^*, P_B^*)$. The maximum is achieved for $\lambda \approx 0.859$ which gives $P_A^* = P_B^* \approx 0.859$ which gives a bias $\varepsilon \approx 0.359$. ■

6 Further discussion

Optimality of the bias The bias that we show here is actually not optimal for the protocol. The reason is the following: in the analysis of cheating Alice (Section 5.2), we consider the cheating probability for Alice depending on whether Bob checks the first bit, the second bit or both bits. For each of these cases, we upper bound Alice's cheating probability. But it appears that the cheating probabilities for each of these cases is different and that Alice cannot cheat optimally for all these cases at the same time. This slightly decreases Alice's cheating probability. We can numerically calculate calculate in this case that for $\lambda \approx 0.858$, we have $P_A^* = P_B^* \approx 0.858$. This gives a bias of $\varepsilon \approx 0.858$ which is a slight improvement over what is shown.

Multiple repetition Our protocol consists of a two-fold repetition of Berlin *et al.* 's protocol. What happens if we consider a k-fold repetition? Even if it is difficult to calculate the exact cheating probabilities of Alice and Bob in the case of multiple repetitions, these probabilities can be easily upper and lower bounded. We use the following bounds. Let $P_A^*(k,\lambda)$ the cheating probability for Alice (resp. Bob) with a k-fold repetition of Berlin *et al.* 's protocol with parameter λ. Let $P(k) = \min_\lambda(\max\{P_A^*(k,\lambda), P_B^*(k,\lambda)$. $P(k)$ corresponds to the best cheating probability when consider a k-fold repetition of the protocol. We need to lower bound $P_A^*(k,\lambda)$. We have

$$P_A^*(k,\lambda) \leq f(k,\lambda) = \frac{1}{2} + \frac{1}{2}\left(\frac{1}{2} + \sqrt{\lambda(1-\lambda)}\right)^k$$

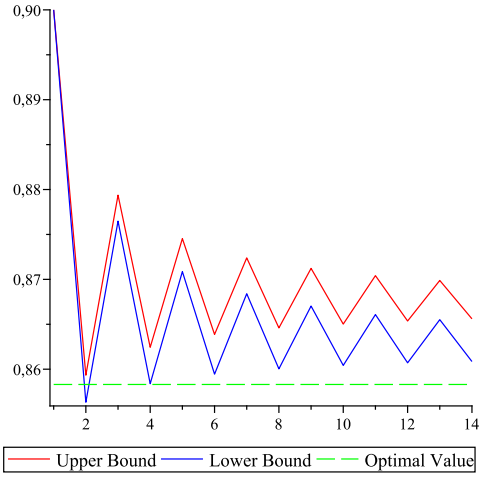
This is a generalization of the upper bound we use to show that $\varepsilon \approx 0.359$. Intuitively, this corresponds to the case where Alice knows if Bob measured in the correct basis' or not. When we consider Alice's cheating strategies where she uses separate (non entangled) strategies for each of the k repetitions, we have the following lower bound.

$$P_A^*(k,\lambda) \geq g(k,\lambda) = (\frac{3}{4} + \frac{\sqrt{\lambda(1-\lambda)}}{2})^k$$

On the other hand, it possible to calculate exactly Bob's cheating probability since

$$P_B^*(k,\lambda) = 1/2 + D(\rho_0^{\otimes k}, \rho_1^{\otimes k})/2$$

Using these bounds, we get the following diagram for cheating probabilities of Alice and Bob which shows that the optimal value is achieved using a 2-fold repetition of the protocol. The x-axis corresponds to the number of repetition k. The y-axis corresponds to the minimal cheating probability $P(k)$ when using lower/upper bounds for P_A^*.



7 Conclusion and open questions

In this work, we presented a loss-tolerant quantum coin flipping protocol with bias $\varepsilon \approx 0.359$. To do this, we presented a general method to disallow cheating Bob to take advantage of the fact that he can reset the protocol when one of his measurement fails. It would be interesting to see whether such techniques can be used for other protocols which have information theoretic security or not. Moreover, what is the best bias that can be achieved for such loss-tolerant protocols and can such protocols also be noise-tolerant?

References

[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.

[AMS10] N. Aharon, S. Massar, and J. Silman. A family of loss-tolerant quantum coin flipping protocols. 2010. quant-ph:0711.4114.

[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.

[BBBG08] Guido Berlin, Gilles Brassard, Felix Bussieres, and Nicolas Godbout. Loss-tolerant quantum coin flipping. In *ICQNM '08: Proceedings of the Second International Conference on Quantum, Nano and Micro Technologies (ICQNM 2008)*, pages 1–9, Washington, DC, USA, 2008. IEEE Computer Society.

[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.

[BM04] Jonathan Barrett and Serge Massar. Security of quantum bit-string generation. *Phys. Rev. A*, 70(5):052310, Nov 2004.

[CK09] Andre Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. *Foundations of Computer Science, Annual IEEE Symposium on*, 0:527–533, 2009.

[DFSS08] Ivan B. Damgard, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM J. Comput.*, 37(6):1865–1890, 2008.

[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.

[FG99] Christopher A. Fuchs and Jeroen Van De Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inform. Theory 45. No*, pages 45–1216, 1999.

[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.

[Joz94] R Jozsa. Fidelity for mixed quantum states. *J Modern Optics*, pages 2315–2324, December 1994.

[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.

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

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

[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.

[WST08] Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100(22):220502, Jun 2008.