Optimal quantum strong coin flipping

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

Iordanis Kerenidis*
CNRS - LRI
Université Paris-Sud
jkeren@lri.fr

April 9, 2009

Abstract

Coin flipping is a fundamental cryptographic primitive that enables two distrustful and far apart parties to create a uniformly random bit [Blu81]. Quantum information allows for protocols 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]. Closing this gap has been one of the important open questions in quantum cryptography.

In this paper, we resolve this question by presenting a quantum strong coin flipping protocol with cheating probability arbitrarily close to $1/\sqrt{2}$. More precisely, we show how to use any weak coin flipping protocol with cheating probability $1/2 + \varepsilon$ in order to achieve a strong coin flipping protocol with cheating probability $1/\sqrt{2} + O(\varepsilon)$. The optimal quantum strong coin flipping protocol follows from our construction and the optimal quantum weak coin flipping protocol described by Mochon [Moc07].

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

*Supported in part by ANR CRAQ and AlgoQP grants of the French Ministry and in part by the European Commission under the Integrated Project Qubit Applications (QAP) funded by the IST directorate as Contract Number 015848.

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, i.e. where the resulting coin is perfectly unbiased, 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.

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.

The question of whether 3/4 or $1/\sqrt{2}$ is ultimately the right bound for quantum coin flipping has been open since then. In fact, there had been "evidence" suggesting both cases. First, Kitaev's semi-definite program formulation of coin flipping seems to be a natural one and using this semi-definite program one cannot hope to prove a better lower bound. On the other hand, most of the suggested coin flipping protocols 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 $a \oplus b$. However, Ambainis had proved a lower bound of 3/4 for any protocol of this type and even though more complicated protocols based on similar ideas had been proposed, they all seemed to get stuck at the same 3/4 bound.

During the study of quantum coin flipping, a weaker variant was introduced that is referred to as *weak coin flipping* in opposition to the original *strong coin flipping*. In this setting, 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]. The best achieved bound was in fact $1/\sqrt{2}$, a strange coincidence, since Kitaev's lower bound of $1/\sqrt{2}$ does not apply in the case of weak coin flipping. The only lower bound that carries over from the case of strong coin flipping is a bound by Ambainis that shows that in order to achieve a cheating probability of $1/2 + \varepsilon$ the protocol must have at least $O(\log\log\frac{1}{\varepsilon})$ rounds [Amb02]. We refer to ε as the bias of the protocol.

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]. Kitaev's formalism and Mochon's optimal weak coin flipping protocol delve heavily into the theory of convex cones and operator monotone functions.

In this work, we resolve the question of the optimal quantum strong coin flipping protocol. We present a general method on how to use any weak coin-flipping protocol with cheating probability $1/2+\varepsilon$ in order to construct a strong coin-flipping protocol with cheating probability $1/\sqrt{2}+O(\varepsilon)$.

Our protocol uses roughly the same number of rounds as the weak coin flipping protocol. Combining our construction with Mochon's quantum weak coin flipping protocol that achieves arbitrarily small bias, we conclude that it is possible to construct a quantum strong coin flipping protocol with cheating probability arbitrarily close to $\frac{1}{\sqrt{2}}$.

Let us make a few remarks about our protocol. First, it is a *classical* protocol that uses a weak coin flipping as a subroutine. 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. Moreover, our protocol has the advantages of being very easy to describe and having a straightforward analysis, assuming, of course, the existence of a weak coin flipping protocol.

Using weak coin flipping in order to perform strong coin flipping is not a new idea. There is a trivial protocol that uses a perfect weak coin flipping and achieves strong coin flipping with cheating probability 3/4: Alice and Bob run the weak coin flipping protocol and whoever wins, flips a random coin $c \in_R \{0,1\}$.

Our protocol can be thought of as a refinement of the abovementioned one. There are two simple ideas that we use. First, we will have Alice flip and announce the outcome of her random coin *before* Alice and Bob perform the weak coin flipping protocol. Second, we will use an "unbalanced" weak coin flipping, where in the honest case, Alice wins with probability z and Bob with probability $1-z$.

We can now describe informally our protocol

Strong Coin Flipping Protocol

- Alice flips a random coin a and sends a to Bob.
- Alice and Bob run an unbalanced weak coin flipping protocol where honest Alice wins with probability z and honest Bob with probability $1-z$.
- If Alice wins, the output is a.
- If Bob wins, he outputs a with probability p and $\overline{a}$ with probability $1-p$.

In Section 4, we first show how to construct "unbalanced" weak coin flipping protocols for any z and bias $O(\varepsilon)$, assuming the existence of a "balanced" weak coin flipping protocol with bias ε. Then, we optimize the parameters z and p in order to make the cheating probability of our protocol at most $1/\sqrt{2} + O(\varepsilon)$.

2 Definitions

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

A 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 $c = \text{Abort}$.

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.

Weak coin flipping

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 $P_B^* = \Pr[\text{ Bob wins }] \leq 1/2 + \varepsilon$

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 $\varepsilon = 0$.

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 $P_B^* = \Pr[\text{ Bob wins }] \leq (1 - z) + \varepsilon$

Strong coin flipping

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 $P_B^* = \max\{\Pr[c = 0], \Pr[c = 1]\} \leq 1/2 + \varepsilon$

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 will also use the following result by Mochon

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

3 An optimal strong coin flipping protocol

In this section, we describe how to construct an optimal strong coin flipping protocol from any weak coin flipping protocol. Let us try to give some intuition for our protocol before we actually describe and analyze it. For this high level discussion, we assume the existence of a perfect weak coin flipping protocol. As we said, there exists a trivial protocol that uses a weak coin flipping in order to achieve strong coin flipping:

SCF(3/4) protocol using a perfect weak coin flipping protocol P

- Alice and Bob run the protocol P
- The winner chooses a random $c \in_R \{0,1\}$, and sends c to the other player, c being the outcome of the protocol.

Let us analyze this protocol more closely. Let Alice be dishonest and her desired value for the coin be 0. Her strategy will be to try and win the WCF protocol, which happens with probability 1/2 and then output 0. However, even if she loses the weak coin flipping, there is still a probability 1/2 that the honest Bob will output 0. Hence, Alice's (and by symmetry Bob's) cheating probability is 3/4.

In order to reduce this bias, we would like to eliminate the situation where the honest player, after winning the WCF, still helps the dishonest player cheat with probability 1/2. One can try to resolve this problem by having Alice flip and announce her random coin c before running the WCF protocol. In this case: first, Alice announces a bit a. Then, Alice and Bob perform a WCF. If Alice wins the outcome is a; if Bob wins then the outcome is $\overline{a}$.

In this case, Bob never outputs a. However, there is a simple cheating strategy for Alice. If she wants 0, she sets $a = 1$, loses the WCF (which she can do with probability 1) and therefore Bob always outputs 0. Hence, Bob's choice when he wins the WCF must be probabilistic. Let us now consider the following protocol:

Improved SCF protocol using a perfect weak coin flipping protocol P

- Alice picks a random bit $a \in_R \{0,1\}$ and sends a to Bob.
- Alice and Bob run P.
- If Alice wins then the outcome is a.
- If Bob wins then he outputs a with probability p and $\overline{a}$ with probability $1-p$.

First note that Bob's cheating probability is 3/4, independent of p. Namely, if Alice picks the value Bob wants, then he just loses the WCF; if Alice picks the opposite value then he tries to win the WCF in order to pick his desired value. On the other hand, let us calculate Alice's cheating probability. Alice can pick a to be equal to her desired outcome, in which case the final outcome is a with probability $\frac{1}{2} \cdot 1 + \frac{1}{2} \cdot p$. She may also pick a to be the opposite of her desired outcome, in which case she always loses the WCF and hence, the final outcome is $\overline{a}$ with probability $1-p$. Alice's cheating probability is the maximum of the two cases. By choosing $p = 1/3$ the probabilities in the two cases are equal and we conclude that Alice's cheating probability is 2/3.

Hence, using any balanced WCF protocol, we can have a strong coin flipping protocol that achieves cheating probability 3/4 for Bob and 2/3 for Alice. This in some sense already beats the best previously known protocol that can only achieve cheating probability 3/4 for both Alice and Bob.

Our next step is to make these two cheating probabilities equal. For this, we will use an unbalanced WCF with parameter z and optimize z and p in order to get the optimal bound of $1/\sqrt{2}$.

We can now describe our final protocol that uses a $WCF(z, \varepsilon)$ protocol Q as a subroutine.

Strong Coin Flipping protocol S

1. Alice chooses $a \in_R \{0, 1\}$ and sends a to Bob.
2. Alice and Bob perform the $WCF(z, \varepsilon)$ protocol Q
   - If Alice wins Q then honest players output $c_A = c_B = a$
   - If Bob wins Q then he flips a coin b such that $b = a$ with probability p and $b = \overline{a}$ with probability $(1 - p)$. He sends b to Alice. In this case, honest players output $c_A = c_B = b$.
   - If Q outputs Abort then Abort

4 Analysis of the strong coin flipping protocol S

We first describe the construction of the unbalanced $WCF(z, \varepsilon)$ protocol and then show how to optimize the parameters z and p in order to achieve the optimal bias.

4.1 An unbalanced weak coin flipping protocol

Our goal is to prove the following proposition

Proposition 2 *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.*
- *$|x - z| \leq 2^{-k}$.*
- *$\varepsilon_0 \leq 2\varepsilon$.*

The protocol Q is a sequential composition of the $WCF(1/2, \varepsilon)$ protocol P. In high level, we use P in order to combine two weak coin flipping protocols with parameters z_1 and z_2 into a new protocol with parameter $\frac{z_1+z_2}{2}$. Then, by recursion, for any given z we can create a protocol Q with parameter x that rapidly converges to z. We also prove that the bias of Q is at most 2ε.

Assume we have a $WCF(z_1, \varepsilon_0)$ protocol P_1 and a $WCF(z_2, \varepsilon_0)$ protocol P_2 each with at most M rounds of communication and $z_2 \geq z_1$. We combine them in the following way.

$$\mathbf{Comb(P_1, P_2)}$$

- Alice and Bob run P.
- If Alice wins, run P_2. If Bob wins, run P_1. If P Aborts then Abort.

Note that this protocol uses at most $N + M$ rounds. We have

Lemma 1 *$Comb(P_1, P_2)$ is a $WCF(\frac{z_1+z_2}{2}, \varepsilon_0 + \varepsilon(z_2 - z_1))$ protocol.*

Proof:
Alice and Bob are honest If Alice and Bob are honest then the protocol never aborts. We have Pr[Alice wins] $= \frac{z_1+z_2}{2}$ and Pr[Bob wins] $= 1 - \frac{z_1+z_2}{2}$.

Alice cheats and Bob is honest Let $x =$ Pr[Alice wins P] ; $y =$ Pr[Bob wins P]; $u =$ Pr[Alice wins P_2 | Alice wins P]; $v =$ Pr[Alice wins P_1 | Bob wins P]. We know the following inequalities concerning these probabilities:

$$x + y \leq 1 \quad x \leq 1/2 + \varepsilon \quad u \leq z_2 + \varepsilon_0 \quad v \leq z_1 + \varepsilon_0$$

Note that the last two inequalities hold, since the biases for the protocols P_1 and P_2 do not increase depending on the outcome of P. We have

$$\begin{aligned}
&\Pr[\text{ Alice wins } Comb(P_1, P_2)] \\
&= \quad x \cdot u + y \cdot v \quad \leq \quad x(z_2 + \varepsilon_0) + (1 - x)(z_1 + \varepsilon_0) \quad = \quad (z_1 + \varepsilon_0) + x(z_2 - z_1) \\
&\leq \quad (z_1 + \varepsilon_0) + (1/2 + \varepsilon)(z_2 - z_1) \qquad \text{since } z_2 \geq z_1 \\
&\leq \quad \frac{z_1 + z_2}{2} + \varepsilon_0 + \varepsilon(z_2 - z_1)
\end{aligned}$$

Bob cheats and Alice is honest Using a similar calculation as in the previous case, we have Pr[Bob wins $Comb(P_1, P_2)$] $\leq \frac{(1-z_2)+(1-z_1)}{2} + \varepsilon_0 + \varepsilon(z_2 - z_1) = 1 - \frac{z_1+z_2}{2} + \varepsilon_0 + \varepsilon(z_2 - z_1)$. ■

We now show the following inductive Lemma

Lemma 2 *Suppose we have a $WCF(1/2, \varepsilon)$ protocol P that uses N rounds of communication. Then $\forall z \in [0, 1]$ and $\forall k \in \mathbb{N}$, we can construct a $WCF(x_1, \varepsilon_0)$ protocol P_1 and a $WCF(x_2, \varepsilon_0)$ protocol P_2 such that*

- *P_1, P_2 each use at most $k \cdot N$ rounds.*
- *$x_1 \leq z \leq x_2$ and $x_2 - x_1 = 2^{-k}$.*
- *$\varepsilon_0 \leq (2 - 2(x_2 - x_1))\varepsilon$.*

Proof: Fix $z \in [0,1]$. We show this result by induction on k. For $k = 0$, we clearly have a $WCF(0,0)$ protocol (a protocol where Bob always wins) and a $WCF(1,0)$ (a protocol where Alice always wins) that use no rounds of communication. We suppose the Lemma is true for k and we show it for $k+1$.

Let $x_1, x_2, P_1, P_2, \varepsilon_0$ that satisfy the above properties for k. Let P' be the $Comb(P_1, P_2)$ protocol and $u = \frac{x_1+x_2}{2}$. P' uses at most $(k+1)N$ rounds and from Lemma 1, we know that P' is a $WCF(u, \varepsilon'_0 = \varepsilon_0 + (x_2 - x_1)\varepsilon)$ protocol. From the induction step we have that $\varepsilon'_0 \leq (2 - 2(x_2 - x_1))\varepsilon + (x_2 - x_1)\varepsilon \leq (2 - (x_2 - x_1))\varepsilon$. We now distinguish two cases

- If $z \leq u$, consider the protocols P_1 and P'. Each one uses at most $(k+1)N$ rounds. Also, $x_1 \leq z \leq u$ and $u - x_1 = \frac{x_2 - x_1}{2} = 2^{-(k+1)}$. Finally, $\varepsilon'_0 \leq (2 - (x_2 - x_1))\varepsilon = (2 - 2(u - x_1))\varepsilon$ which concludes the proof.
- If $z > u$, consider the protocols P' and P_2. Each one uses at most $(k+1)N$ rounds. Also, $u \leq z \leq x_2$ and $x_2 - u = \frac{x_2 - x_1}{2} = 2^{-(k+1)}$. Finally, $\varepsilon'_0 \leq (2 - (x_2 - x_1))\varepsilon = (2 - 2(x_2 - u))\varepsilon$ which concludes the proof.

■

In Lemma 2, we have $|x_1 - z| \leq (x_2 - x_1) \leq 2^{-k}$ and $\varepsilon_0 \leq 2\varepsilon$. Hence this Lemma directly implies Proposition 2 by considering $Q = P_1$.

4.2 Strong coin flipping from unbalanced weak coin flipping

We calculate the cheating probability of our protocol S that uses a $WCF(z, \varepsilon)$ protocol Q.

Proposition 3 *The protocol S is a strong coin flipping protocol with $N+2$ rounds of communication and cheating probabilities $P_A^* \leq \frac{1}{2-z-\varepsilon}$ and $P_B^* \leq \frac{2-z+\varepsilon}{2}$.*

Proof:
Alice and Bob are honest If both players are honest then they never abort. Moreover, since the protocol is symmetric in 0 and 1, we have $\Pr[c=0] = \Pr[c=1] = 1/2$.
Alice cheats and Bob is honest We prove that $\Pr[c=0] \leq \frac{1}{2-z-\varepsilon}$. By symmetry, the same holds for $\Pr[c=1]$. Since Alice cheats, she can choose arbitrarily between $a=0$ and $a=1$ instead of picking a uniformly at random. Hence, $Pr[c=0] \leq \max\{\Pr[c=0|a=0], \Pr[c=0|a=1]\}$.

- We first calculate $\Pr[c=0|a=0]$.
  Let $x = \Pr[\text{Alice wins } Q|a=0]$ and $y = \Pr[\text{Bob wins } Q|a=0]$. We have $\Pr[c=0|a=0] = x \cdot 1 + y \cdot p$. Note that $x + y \leq 1$ and also $x \leq z + \varepsilon$, since the maximum bias with which Alice can win Q is independent of the value of a. We have

$$\begin{aligned} \Pr[c=0|a=0] &= x \cdot 1 + y \cdot p \leq x + (1-x)p = p + x(1-p) \\ &\leq p + (z+\varepsilon)(1-p) \end{aligned}$$

- We now calculate $\Pr[c=0|a=1]$.
  Let $x = \Pr[\text{Alice wins } Q|a=1]$ and $y = \Pr[\text{Bob wins } Q|a=1]$. We have

$$\Pr[c=0|a=1] = x \cdot 0 + y(1-p) \leq y(1-p) \leq 1 - p$$

  which is achievable since Alice could always let Bob win Q.

Since $\Pr[c=0] \leq \max\{\Pr[c=0|a=0], \Pr[c=0|a=1]\}$, we choose p such that the upper bounds for $\Pr[c=0|a=0]$ and $\Pr[c=0|a=1]$ are equal.

$$\begin{aligned} p + (z+\varepsilon)(1-p) &= 1-p \\ p &= \frac{1-z-\varepsilon}{2-z-\varepsilon} \end{aligned}$$

With this value of p, we have

$$Pr[c=0] \leq \max\{\Pr[c=0|a=0], \Pr[c=0|a=1]\} = 1-p \leq \frac{1}{2-z-\varepsilon}$$

Since the protocol is symmetric in 0 and 1, we also have $\Pr[c=1] \leq \frac{1}{2-z-\varepsilon}$ and hence $P_A^* \leq \frac{1}{2-z-\varepsilon}$.

Bob cheats and Alice is honest We prove that $\Pr[c=0] \leq \frac{2-z+\varepsilon}{2}$. By symmetry, the same holds for $\Pr[c=1]$. Alice is honest and picks a uniformly at random. We first have $\Pr[c=0|a=0] \leq 1$. We now upper bound $\Pr[c=0|a=1]$. Let $x = \Pr[\text{Bob wins } Q|a=1]$ and $y = \Pr[\text{Alice wins } Q|a=1]$. We have

$$\Pr[c=0|a=1] \leq x \cdot 1 + y \cdot 0 \leq x \leq 1 - z + \varepsilon$$

Since Alice is honest, we have $\Pr[a=0] = \Pr[a=1] = 1/2$ and hence:

$$\begin{aligned} \Pr[c=0] &= \Pr[c=0|a=0] \cdot \Pr[a=0] + \Pr[c=0|a=1] \cdot \Pr[a=1] \\ &= \frac{1}{2}\left(\Pr[c=0|a=0] + \Pr[c=0|a=1]\right) \\ &\leq \frac{1}{2} + \frac{1-z+\varepsilon}{2} \\ &= \frac{2-z+\varepsilon}{2} \end{aligned}$$

Since the protocol is symmetric in 0 and 1, we also have $\Pr[c=1] \leq \frac{2-z+\varepsilon}{2}$ and hence $P_B^* \leq \frac{2-z+\varepsilon}{2}$.

■

4.3 Putting it all together

To conclude, we have to optimize z. In the case where there exists an ideal weak coin flipping protocol $WCF(1/2, 0)$, it is easy to see that in order to equalize the cheating probabilities P_A^* and P_B^*, we need to take $z = 2 - \sqrt{2}$. If also our Proposition 2 was ideal, *i.e.* if from P we could create perfectly a $WCF(2-\sqrt{2}, 0)$ protocol Q, then S would have cheating probability exactly $\frac{1}{\sqrt{2}}$.

In general, we need to take care of the small bias ε of the initial $WCF(1/2, \varepsilon)$ protocol P and the error of our Proposition 2. However, we will see that the overall increase in the cheating probability of our protocol S is only $O(\varepsilon)$.

Theorem 1 *If there exists a $WCF(1/2, \varepsilon)$ protocol P that uses N rounds of communication then there exists a strong coin flipping protocol S that uses $2\lceil \log(\frac{1}{\varepsilon}) \rceil \cdot N + 2$ rounds with cheating probability at most $\frac{1}{\sqrt{2}} + \sqrt{2}\varepsilon + o(\varepsilon)$.*

Proof: Starting from the $WCF(1/2, \varepsilon)$ weak coin flipping protocol P with N rounds, we can use Proposition 2 with $k = 2\lceil \log(\frac{1}{\varepsilon}) \rceil$ and construct a $WCF(x, \varepsilon')$ protocol Q with the following properties

- Q uses $2\lceil \log(\frac{1}{\varepsilon}) \rceil \cdot N$ rounds.
- $|x - (2 - \sqrt{2})| \leq \varepsilon^2$.
- $\varepsilon' \leq 2\varepsilon$.

Then, we use the protocol Q in the strong coin flipping protocol S we described in Section 3 and by Proposition 3 we have that S has $2\lceil \log(\frac{1}{\varepsilon}) \rceil \cdot N + 2$ rounds and

$$\begin{aligned} P_A^* &= \frac{1}{2 - x - \varepsilon'} \leq \frac{1}{\sqrt{2} - 2\varepsilon - \varepsilon^2} \leq \frac{1}{\sqrt{2}} + \sqrt{2}\varepsilon + o(\varepsilon) \\ P_B^* &= \frac{2 - x + \varepsilon'}{2} \leq \frac{\sqrt{2} + 2\varepsilon + \varepsilon^2}{2} = \frac{1}{\sqrt{2}} + \varepsilon + o(\varepsilon) \end{aligned}$$

■

Using Theorem 1 and Mochon's weak coin flipping protocol (Proposition 1) we conclude that

Corollary 1 *For any $\varepsilon > 0$, there exists a strong coin flipping protocol with cheating probability $\frac{1}{\sqrt{2}} + \varepsilon$.*

Last, note that our strong coin flipping protocol uses $O(N \cdot \log(\frac{1}{\varepsilon}))$ rounds, where N is the number of rounds of Mochon's weak coin flipping protocol.

5 Conclusion

In this paper, we presented the first quantum strong coin flipping protocol with a cheating probability arbitrarily close to the optimal value $\frac{1}{\sqrt{2}}$. Our protocol uses as a subroutine the quantum weak coin flipping protocol designed by Mochon which is arbitrarily close to optimal. Note that except when using this quantum weak coin flipping protocol, our entire protocol is classical.

We would like to note that Mochon's protocol is still not very well understood (protocol's unitary description, number of rounds). It is important to get a better understanding of that protocol and/or find a simpler construction of an optimal quantum weak coin flipping protocol. Moreover, it would be interesting to study what other cryptographic primitives can be derived from weak or strong coin flipping.

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.

[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. 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.