

Tight Bounds for Classical and Quantum Coin Flipping

Esther Hänggi¹ and Jürg Wullschleger²

¹ *ETH Zurich, Switzerland.* esther.haenggi@inf.ethz.ch

² *University of Bristol, UK.* j.wullschleger@bristol.ac.uk

September 27, 2010

Abstract

Coin flipping is a cryptographic primitive for which strictly better protocols exist if the players are not only allowed to exchange classical, but also quantum messages. During the past few years, several results have appeared which give a tight bound on the range of implementable unconditionally secure coin flips, both in the classical as well as in the quantum setting and for both weak as well as strong coin flipping. However, all these results consider only protocols with *perfect correctness*, i.e., where two honest players must *always* output the same value and *never* abort. We remove this restriction by giving a more general definition of coin flipping which unifies the notion of strong and weak coin flipping (it contains both of them as special cases) and allows the honest players to abort with a certain probability. We give tight bounds on the achievable range of parameters both in the classical and in the quantum setting.

1 Introduction

Coin flipping (or coin tossing) as a cryptographic primitive has been introduced by Blum [Blu83] and is one of the basic building blocks of *secure two-party computation* [Yao82].

Coin flipping can be defined in several ways. The most common definition, sometimes called *strong coin flipping*, allows two honest players to receive a uniform random bit $c \in \{0, 1\}$, such that a dishonest player cannot *increase* the probability of any output. A dishonest player may, however, abort the protocol, in which case the honest player gets the erasure symbol Δ as output¹. A weaker definition, called *weak coin flipping*, only requires that each party cannot increase the probability of their preferred value.

Without any additional assumptions, unconditionally secure weak coin flipping (and therefore also strong coin flipping) is impossible to implement by a classical protocol. This follows from a result by Hofheinz, Müller-Quade and Unruh [HMQU06], which implies that if two honest players always receive the same uniform bit, then there always exists one player that can force the bit to be his preferred value with certainty.

If the players can communicate using a quantum channel, unconditionally secure coin flipping is possible to some extent. The bounds of the possibilities in the quantum setting have been investigated by a long line of research. Aharonov *et al.* [ATSVY00] presented a strong coin flipping protocol where no quantum adversary can force the outcome to a certain value with probability larger than 0.914. This bound has been improved by Ambainis [Amb01] and independently by Spekkens and Rudolph [SR01] to 0.75 (see also [Col07] for a different protocol). For weak coin flipping, Spekkens and Rudolph [SR02] presented a protocol where the dishonest player cannot force the outcome to its preferred value with probability larger than $1/\sqrt{2} \approx 0.707$. (Independently, Kerenidis and Nayak [KN04] showed a slightly weaker bound of 0.739.) This bound has further been improved by Mochon, first to 0.692 [Moc04a] and finally to $1/2 + \varepsilon$ for any constant $\varepsilon > 0$ [Moc07],

¹ The dishonest player may abort after receiving the output bit, but before the honest player gets the output bit. This allows cases where the honest player gets, for example, 0 with probability 1/2 and Δ otherwise. There exists also a definition of coin flipping where a dishonest player does not have this unfair advantage, and the honest player must always get a uniformly random bit, no matter what the other player does. See [Cle86, LC98, MNS09].

therefore getting arbitrarily close to the optimum. For strong coin flipping, on the other hand, this is not possible, since it has been shown by Kitaev [Kit02] (see [ABDR04] for a proof) that for any quantum protocol there is always a player able to force an outcome with probability at least $1/\sqrt{2}$. Chailloux and Kerenidis [CK09] showed that a bound of $1/\sqrt{2} + \varepsilon$ for any constant $\varepsilon > 0$ can be achieved, by combining two classical protocols with Mochon’s result: They first showed that an *unbalanced* weak coin flip can be implemented using many instances of weak coin flips, and then that one instance of an unbalanced weak coin flip suffices to implement a strong coin flip with optimal bias.

1.1 Limits of previous Results

In all previous work on quantum coin flipping, honest players are required to output a *perfect* coin flip, i.e., the probability of both values has to be exactly $1/2$, and the players must never disagree on the output or abort. However, the players may very well be willing to allow a small probability of error even if both of them are honest. Furthermore, a (quantum) physical implementation of any protocol will always contain some noise and, therefore, also some probability to disagree or abort. This requirement is, therefore, overly strict and raises the question how much the cheating probability can be improved by allowing some error.

Indeed, there exist examples of different cryptographic primitives where allowing an (arbitrarily small) error can greatly improve the performance of the protocol. For example, as shown in [BM04], the amount of secure AND gates (or, alternatively, oblivious transfers) needed between two parties to test equality of two strings is only $O(\log 1/\varepsilon)$ for any small error $\varepsilon > 0$, while it is exponential in the length of the inputs in the perfect case. Considering reductions from oblivious transfer to different variants of oblivious transfer where the players can use quantum communication, it has recently been shown in [WW10] that introducing a small error can reduce the amount of oblivious transfer needed by an arbitrarily large factor.

That *some* improvement on the achievable parameters must be possible also in the case of coin flipping can be seen easily: In any protocol, the honest players can simply flip the output bit with some (small) probability. This increases the error, but decreases the bias. In the extreme case, the two players simply flip two independent coins and output this value. This prohibits any bias from the adversary, at the cost of making the players disagree with probability $1/2$.

The only bound on coin flipping we are aware of allowing for an error of the honest players has been given in [HMQU06], for weak coin flipping in the classical setting.

1.2 Contribution

We introduce a general definition of coin flipping, characterized by 6 parameters, which we denote by

$$\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1}) .$$

The value p_{ii} (where $i \in \{0, 1\}$) is the probability that two honest players output i and the value p_{*i} (p_{i*}) is the maximal probability that the first (second) player can force the honest player to output i . With probability $1 - p_{00} - p_{11}$, two honest players will abort the protocol and output a dummy symbol.² This new definition has two main advantages:

- It generalizes both weak and strong coin flipping, but also allows for additional types of coin flips which are unbalanced or lay somewhere between weak and strong.
- It allows two honest players to abort with some probability.

We will first consider classical protocols (Section 3), and give tight bounds for all parameters. The impossibility result (Lemma 5) uses a similar proof technique as Theorem 7 in [HMQU06]. In

²Similar to [HMQU06], we can require two honest players to always output the same values. This is not a big restriction, since the players can always add a final round to check if they have the same value and abort if the values differ.

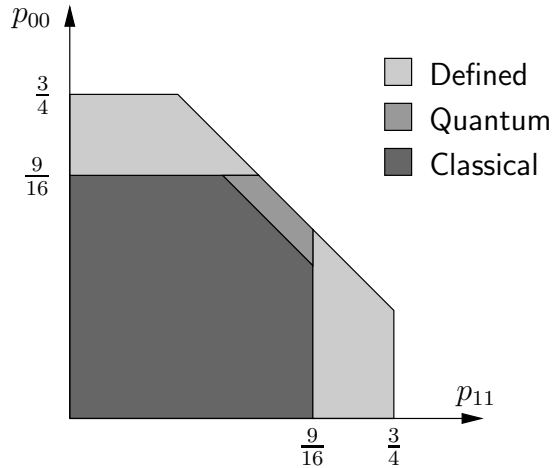


Figure 1: For values $p_{0*} = p_{*0} = p_{1*} = p_{*1} = \frac{3}{4}$, this figure shows the achievable values of p_{00} and p_{11} in the classical and the quantum setting. The light gray area is the set of all coin flips that can be defined.

combination with two protocols showing that this bound can be reached (Lemma 4), we obtain the following theorem.

Theorem 1. *Let $p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$. There exists a classical protocol that implements an unconditionally secure $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$ if and only if*

$$\begin{aligned} p_{00} &\leq p_{0*}p_{*0} \\ p_{11} &\leq p_{1*}p_{*1} \\ p_{00} + p_{11} &\leq p_{0*}p_{*0} + p_{1*}p_{*1} - \max(0, p_{0*} + p_{1*} - 1) \max(0, p_{*0} + p_{*1} - 1). \end{aligned}$$

For weak coin flipping, i.e., $p_{*1} = 1$ and $p_{0*} = 1$, the bound of Theorem 1 simplifies to

$$1 - p_{00} - p_{11} \geq (1 - p_{*0})(1 - p_{1*}),$$

which is the bound that is also implied by Theorem 7 in [HMQU06].

In Section 4, we consider the quantum case, and give tight bounds for all parameters. The quantum protocol (Lemma 10) bases on one of the protocols presented in [CK09], and is a classical protocol that uses an unbalanced quantum weak coin flip as a resource. The impossibility result follows from the proof of Kitaev's bound on quantum strong coin flipping (Lemma 11).

Theorem 2. *Let $p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$. There exists a quantum protocol that implements an unconditionally secure $\text{CF}(p_{00}, p_{11}, p_{0*} + \varepsilon, p_{1*} + \varepsilon, p_{*0} + \varepsilon, p_{*1} + \varepsilon)$ for any $\varepsilon > 0$, if*

$$\begin{aligned} p_{00} &\leq p_{0*}p_{*0} \\ p_{11} &\leq p_{1*}p_{*1} \\ p_{00} + p_{11} &\leq 1. \end{aligned}$$

If these bounds are not satisfied, there does not exist a quantum protocol for $\varepsilon = 0$.

Our results, therefore, give the exact trade-off between weak vs. strong coin flipping, between bias vs. abort-probability, and between classical vs. quantum coin flipping. (Some of these trade-offs are shown in Figures 1 and 2.) They imply, in particular, that quantum protocols give strictly better bounds if $p_{0*} + p_{1*} > 1$ and $p_{*0} + p_{*1} > 1$. Outside that range classical protocols can achieve the same bounds as quantum protocols.

Since the optimal quantum protocol is a classical protocol using quantum weak coin flips as a resource, the possibility to do weak coin flipping, as shown by Mochon [Moc07], can be seen as the crucial difference between the classical and the quantum case.

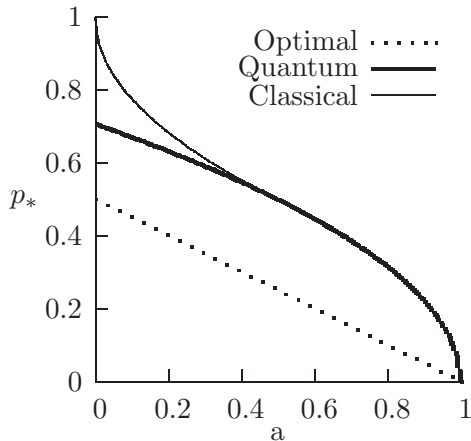


Figure 2: This graph shows the bounds for symmetric coin flipping of the form $\text{CF}(\frac{1-a}{2}, \frac{1-a}{2}, p_*, p_*, p_*, p_*)$. The value p_* is the maximal probability that any player can force the coin to be a certain value, and a is the abort probability. Therefore, the smaller p_* for a fixed value of a , the better is the protocol. The optimal bound is $p_* = \frac{1-a}{2}$. In the quantum case, the achievable bound is $p_* = \sqrt{(1-a)/2}$, and in the classical case the achievable bound is equal to the quantum bound for $a \geq \frac{1}{2}$, but $p_* = 1 - \sqrt{a/2}$ for $a < \frac{1}{2}$.

2 Preliminaries

In a classical protocol, the two players (Alice and Bob) are restricted to classical communication. Both players are given unlimited computing power and memory, and are able to locally sample random variables from any distribution. In a quantum protocol, the two players may exchange quantum messages. They have unlimited quantum memory and can perform any unitary transformation on it. All operations are noiseless. At the beginning of the protocol, the players do not share any randomness or entanglement. While honest players have to follow the protocol, we do not make any assumption about the behavior of the malicious players. We assume that the adversary is static, i.e., any malicious player is malicious from the beginning.

Definition 1. Let $p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$, such that $p_{00} + p_{11} \leq 1$, $p_{00} \leq \min\{p_{0*}, p_{*0}\}$ and $p_{11} \leq \min\{p_{1*}, p_{*1}\}$ holds. A protocol implements a $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$, if the following conditions are satisfied:

- If both players are honest, then they output value $i \in \{0, 1\}$ with probability p_{ii} and Δ with probability $1 - p_{00} - p_{11}$.
- For any dishonest Alice, the probability that Bob outputs 0 is at most p_{*0} , and the probability that he outputs 1 is at most p_{*1} .
- For any dishonest Bob, the probability that Alice outputs 0 is at most p_{0*} , and the probability that she outputs 1 is at most p_{1*} .

Definition 1 generalizes the notion of both weak and strong coin flips and encompasses, in fact, the different definitions given in the literature.

- A perfect weak coin flip is a $\text{CF}(\frac{1}{2}, \frac{1}{2}, 1, \frac{1}{2}, \frac{1}{2}, 1)$.
- A perfect strong coin flip is a $\text{CF}(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2})$.
- The weak coin flip with error $\varepsilon > 0$ of [Moc07] is a $\text{CF}(\frac{1}{2}, \frac{1}{2}, 1, \frac{1}{2} + \varepsilon, \frac{1}{2} + \varepsilon, 1)$.
- The unbalanced weak coin flip WCF(z, ε) of [CK09] is a $\text{CF}(z, 1 - z, 1, 1 - z + \varepsilon, z + \varepsilon, 1)$.
- The strong coin flip of [CK09] is a $\text{CF}(\frac{1}{2}, \frac{1}{2}, \frac{1}{\sqrt{2}} + \varepsilon, \frac{1}{\sqrt{2}} + \varepsilon, \frac{1}{\sqrt{2}} + \varepsilon, \frac{1}{\sqrt{2}} + \varepsilon)$.

Note that $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$ can also be defined as an ideal functionality that is equivalent to the above definition. Such a functionality would look like this: If there is any corrupted player, then the functionality first asks him to send a bit $b \in \{0, 1\}$ that indicates which value he prefers. The functionality then flips a coin $c \in \{0, 1, \Delta\}$, where the probabilities depend on b and on which player is corrupted. For example, if the first player is corrupted and $b = 0$, then $c = 0$ will be chosen with probability p_{*0} , $c = 1$ with probability $\min(p_{*1}, 1 - p_{*0})$ and Δ otherwise. The functionality then sends c to the adversary, and the adversary chooses whether he wants to abort the protocol or not. If he does not abort, the honest player receives c , and Δ otherwise. If none of the players are corrupted, the functionality chooses a value $c \in \{0, 1, \Delta\}$ which takes on $i \in \{0, 1\}$ with probability p_{ii} and sends c to the two players.

3 Classical Coin Flipping

3.1 Protocols

Protocol **CoinFlip1**:

Parameters: $p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$, $p_{0*} + p_{1*} \leq 1$.

1. Alice flips a three-valued coin a such that the probability that $a = i$ is p_{i*} for $i = \{0, 1\}$, and $a = \Delta$ otherwise. She sends a to Bob.
2. If $a = \Delta$, Bob outputs $b = \Delta$. If $a \neq \Delta$, Bob flips a coin b such that $b = a$ with probability p_{*a} and $b = \Delta$ otherwise. Bob sends b to Alice and outputs b .
3. If $b = a$ Alice outputs b , otherwise Δ .

Lemma 1. *If either $p_{0*} + p_{1*} \leq 1$ or $p_{*0} + p_{*1} \leq 1$, then there exists a classical coin flipping protocol with $p_{00} = p_{0*}p_{*0}$ and $p_{11} = p_{1*}p_{*1}$.*

Proof. If $p_{0*} + p_{1*} \leq 1$, they use Protocol **CoinFlip1**. (If $p_{*0} + p_{*1} \leq 1$, they exchange the role of Alice and Bob.) By construction, a malicious Bob cannot bias Alice's output by more than p_{i*} , and a malicious Alice cannot bias Bob's output by more than p_{*i} . Honest players output the value 0 with probability $p_{0*}p_{*0}$ and 1 with probability $p_{1*}p_{*1}$. \square

Protocol **CoinFlip2**:

Parameters: $p, x_0, x_1, y_0, y_1 \in [0, 1]$.

1. Alice flips a coin $a \in \{0, 1\}$ such that $a = 0$ with probability p and sends it to Bob.
2. Bob receives the coin a and flips a coin $b \in \{0, 1\}$ such that the probability that $b = a$ is x_a . He sends b to Alice. If $b = a$ he outputs b .
3. If $b = a$, then Alice outputs b . If $a \neq b$, then Alice flips a coin c , such that with probability y_b , $c = b$ and else $c = \Delta$. She sends c to Bob and outputs it.
4. If $c = b$ Bob outputs c , else Δ .

Lemma 2. *If $p_{0*} + p_{1*} > 1$, $p_{*0} + p_{*1} > 1$, $p_{00} \leq p_{0*}p_{*0}$ and $p_{11} \leq p_{1*}p_{*1}$, then there exists a protocol that achieves a coin flip with*

$$p_{00} + p_{11} = p_{0*}p_{*0} + p_{1*}p_{*1} - (p_{0*} + p_{1*} - 1)(p_{*0} + p_{*1} - 1). \quad (1)$$

Proof. We use Protocol `CoinFlip2` and choose the parameters

$$x_i := p_{*i}, \quad y_0 := \frac{p_{0*} - p}{1 - p}, \quad y_1 := \frac{p_{1*} + p - 1}{p}, \quad p := \frac{p_{00} - p_{0*} + p_{0*}p_{*1}}{p_{*0} + p_{*1} - 1}.$$

These parameters need to be between 0 and 1. We have $y_0, y_1 \in [0, 1]$, if $p \in [1 - p_{1*}, p_{0*}]$. To see that p lies indeed in this interval, note that the upper bound follows from

$$p = \frac{p_{00} - p_{0*} + p_{0*}p_{*1}}{p_{*0} + p_{*1} - 1} \leq \frac{p_{0*}p_{*0} - p_{0*} + p_{0*}p_{*1}}{p_{*0} + p_{*1} - 1} = \frac{p_{0*}(p_{*0} + p_{*1} - 1)}{p_{*0} + p_{*1} - 1} = p_{0*}.$$

For the lower bound, note that

$$\begin{aligned} 1 - p &= \frac{p_{*0} + p_{*1} - 1}{p_{*0} + p_{*1} - 1} - \frac{p_{00} - p_{0*} + p_{0*}p_{*1}}{p_{*0} + p_{*1} - 1} \\ &= \frac{p_{*0} + p_{*1} - 1 - p_{00} + p_{0*} - p_{0*}p_{*1}}{p_{*0} + p_{*1} - 1} \\ &= \frac{p_{1*}p_{*0} - p_{1*} + p_{11}}{p_{*0} + p_{*1} - 1}, \end{aligned}$$

where we have used that

$$\begin{aligned} &p_{*0} + p_{*1} - 1 - p_{00} + p_{0*} - p_{0*}p_{*1} \\ &= p_{*0} + p_{*1} - 1 - (p_{0*}p_{*0} + p_{1*}p_{*1} - (p_{0*} + p_{1*} - 1)(p_{*0} + p_{*1} - 1) - p_{11}) + p_{0*} - p_{0*}p_{*1} \\ &= p_{*0} + p_{*1} - 1 - p_{0*}p_{*0} - p_{1*}p_{*1} + p_{0*}p_{*0} + p_{0*}p_{*1} - p_{0*} + p_{1*}p_{*0} + p_{1*}p_{*1} - p_{1*} - p_{*0} - p_{*1} + 1 \\ &\quad + p_{11} + p_{0*} - p_{0*}p_{*1} \\ &= p_{1*}p_{*0} - p_{1*} + p_{11}. \end{aligned}$$

Therefore

$$p = 1 - \frac{p_{11} - p_{1*} + p_{1*}p_{*0}}{p_{*0} + p_{*1} - 1} \geq 1 - \frac{p_{*1}p_{1*} - p_{1*} + p_{1*}p_{*0}}{p_{*0} + p_{*1} - 1} = 1 - p_{1*}.$$

It follows that $p, x_0, x_1, y_0, y_1 \in [0, 1]$.

If both players are honest, then the probability that they both output 0 is

$$\begin{aligned} px_0 + (1 - p)(1 - x_1)y_0 &= px_0 + (1 - p)(1 - x_1)\frac{p_{0*} - p}{1 - p} \\ &= pp_{*0} + (1 - p_{*1})(p_{0*} - p) \\ &= pp_{*0} - p(1 - p_{*1}) + p_{0*}(1 - p_{*1}) \\ &= \frac{p_{00} - p_{0*} + p_{0*}p_{*1}}{p_{*0} + p_{*1} - 1}(p_{*0} + p_{*1} - 1) + p_{0*}(1 - p_{*1}) \\ &= p_{00}. \end{aligned}$$

That they both output 1 is

$$\begin{aligned} p(1 - x_0)y_1 + (1 - p)x_1 &= p(1 - p_{*0})\frac{p_{1*} + p - 1}{p} + (1 - p)p_{*1} \\ &= (1 - p_{*0})(p_{1*} + p - 1) + (1 - p)p_{*1} \\ &= p_{1*}(1 - p_{*0}) - (1 - p)(1 - p_{*0}) + (1 - p)p_{*1} \\ &= p_{1*}(1 - p_{*0}) + (1 - p)(p_{*1} + p_{*0} - 1) \\ &= p_{1*}(1 - p_{*0}) + \frac{p_{1*}p_{*0} - p_{1*} + p_{11}}{p_{*0} + p_{*1} - 1}(p_{*1} + p_{*0} - 1) \\ &= p_{11}. \end{aligned}$$

If Alice is malicious, she can bias Bob to output value i either by sending i as first message hoping that Bob does not change the value, which has probability $x_i = p_{*i}$; or by sending the value

$1 - i$ hoping that Bob changes the value, which occurs with probability $1 - x_{1-i} = 1 - p_{*1-i} \leq p_{*i}$. Hence, she succeeds with probability p_{*i} .

Bob can bias Alice to output value i by sending $b = i$ independently of what Alice had sent as first message. For $i = 0$, Alice will accept this value with probability

$$p + (1 - p)y_0 = p + (1 - p)\frac{p_{0*} - p}{1 - p} = p_{0*}$$

and for $i = 1$ with probability

$$1 - p + py_1 = 1 - p + p\frac{p_{1*} + p - 1}{p} = p_{1*} .$$

□

In order to show that all values below the bound can be reached, we will need additionally the following lemma.

Lemma 3. *If there exists a protocol P that implements $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$, then there exists a protocol P' that implements $\text{CF}(p'_{00}, p'_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$, for any $p'_{00} \leq p_{00}$ and $p'_{11} \leq p_{11}$.*

Proof. P' is defined as follows: The players execute protocol P . If the output is $i \in \{0, 1\}$, then Alice changes to Δ with probability $1 - p'_{ii}/p_{ii}$. Obviously, the cheating probabilities are still bounded by $p_{0*}, p_{1*}, p_{*0}, p_{*1}$, which implies that that protocol P' implements a $\text{CF}(p'_{00}, p'_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$. □

Combining Lemma 1, 2 and 3, we get

Lemma 4. *Let $p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$. There exists a classical protocol that implements $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$ if*

$$\begin{aligned} p_{00} &\leq p_{0*}p_{*0} \\ p_{11} &\leq p_{1*}p_{*1} \\ p_{00} + p_{11} &\leq p_{0*}p_{*0} + p_{1*}p_{*1} - \max(0, p_{0*} + p_{1*} - 1) \max(0, p_{*0} + p_{*1} - 1) . \end{aligned}$$

Proof. If $p_{0*} + p_{1*} \geq 1$ and $p_{*0} + p_{*1} \geq 1$, then Lemmas 2 and 3 imply the bound. Otherwise, i.e., if either $p_{0*} + p_{1*} < 1$ or $p_{*0} + p_{*1} < 1$, then $\max(0, p_{0*} + p_{1*} - 1) \max(0, p_{*0} + p_{*1} - 1) = 0$. Therefore, the bound is implied by Lemmas 1 and 3. □

3.2 Impossibilities

The following lemma shows that the bounds obtained in Lemma 4 are optimal. The proof uses the same idea as the proof of Theorem 7 in [HMQU06].

Lemma 5. *Let $p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$. A $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$ can only be implemented by a classical protocol if*

$$\begin{aligned} p_{00} &\leq p_{0*}p_{*0} \\ p_{11} &\leq p_{1*}p_{*1} \\ p_{00} + p_{11} &\leq p_{0*}p_{*0} + p_{1*}p_{*1} - \max(0, p_{0*} + p_{1*} - 1) \max(0, p_{*0} + p_{*1} - 1) . \end{aligned}$$

Proof. We can assume that the output is a deterministic function of the transcript of the protocol. This can be enforced by adding an additional round at the end of the protocol where the two players tell each other what they are going to output. Since we do not require the protocol to be efficient, Lemma 7 in [HMQU06] implies that we can also assume that the honest parties maintain no internal state except for the list of previous messages.

For any partial transcript t of a protocol, we define p_{0*}^t as the maximum over all transcripts starting with t , i.e., the maximum probability with which Bob can force Alice to output 0, given

the previous interaction has given t . In the same way, we define $p_{1*}^t, p_{*0}^t, p_{*1}^t$. We define p_{00}^t and p_{11}^t as the probabilities that the output of the honest players will be 00 and 11, respectively, given the previous interaction has given t . We will now do an induction over all transcripts, showing that for all t , we have

$$\begin{aligned} p_{00}^t &\leq p_{0*}^t p_{*0}^t \\ p_{11}^t &\leq p_{1*}^t p_{*1}^t \\ p_{00}^t + p_{11}^t &\leq p_{0*}^t p_{*0}^t + p_{1*}^t p_{*1}^t - \max(0, p_{0*}^t + p_{1*}^t - 1) \max(0, p_{*0}^t + p_{*1}^t - 1). \end{aligned}$$

For complete transcripts t , each honest player will output either 0, 1 or Δ with probability 1. We always have $p_{0*}^t + p_{1*}^t - 1 = 0$ and $p_{*0}^t + p_{*1}^t - 1 = 0$. Therefore, we only need to check that $p_{00}^t \leq p_{0*}^t p_{*0}^t$ and $p_{11}^t \leq p_{1*}^t p_{*1}^t$. For $j \in \{0, 1\}$, if $p_{jj}^t = 1$, then $p_{j*}^t = p_{*j}^t = 1$, so the condition is satisfied. In all the other cases we have $p_{jj}^t = 0$, in which case the condition is satisfied as well.

Let t now be a partial transcript, and let Alice be the next to send a message. Let M be the set of all possible transcripts after Alice has sent her message. For the induction step, we now assume that the statement holds for all transcript in M , and show that then it must also hold for t . Let r_i be the probability that an honest Alice will choose message $i \in M$. By definition, we have

$$\begin{aligned} p_{00}^t &= \sum_{i \in M} r_i p_{00}^i, & p_{11}^t &= \sum_{i \in M} r_i p_{11}^i, & p_{0*}^t &= \sum_{i \in M} r_i p_{0*}^i, & p_{1*}^t &= \sum_{i \in M} r_i p_{1*}^i, \\ p_{*0}^t &= \max_{i \in M} p_{*0}^i, & p_{*1}^t &= \max_{i \in M} p_{*1}^i. \end{aligned}$$

For $j \in \{0, 1\}$ it holds that

$$p_{jj}^t = \sum_{i \in M} r_i p_{jj}^i \leq \sum_{i \in M} r_i p_{j*}^i p_{*j}^i \leq \sum_{i \in M} r_i p_{j*}^i p_{*j}^t = p_{j*}^t p_{*j}^t,$$

which shows the induction step for the first two inequalities. For the last, let

$$f(a, b, c, d) := ac + bd - \max(0, a + b - 1) \max(0, c + d - 1),$$

where $a, b, c, d \in [0, 1]$. If we fix the values c and d , we get the function $f_{c,d}(a, b) := f(a, b, c, d)$. It consists of two linear functions: If $a + b \leq 1$, we have

$$f_{c,d}(a, b) = ac + bd,$$

and if $a + b \geq 1$ we have

$$f_{c,d}(a, b) = ac + bd - (a + b - 1) \max(0, c + d - 1).$$

Note that these two linear functions are equal if $a + b = 1$, and we have $(a + b - 1) \max(0, c + d - 1) \geq 0$ if $a + b \geq 1$. It follows that $f_{c,d}(a, b)$ is concave, meaning that for all $\alpha, a, b, a', b' \in [0, 1]$, we have

$$\alpha f_{c,d}(a, b) + (1 - \alpha) f_{c,d}(a', b') \leq f_{c,d}(\alpha a + (1 - \alpha) a', \alpha b + (1 - \alpha) b'). \quad (2)$$

Using

$$\frac{\partial}{\partial c} f(a, b, c, d) \geq 0 \quad \text{and} \quad \frac{\partial}{\partial d} f(a, b, c, d) \geq 0, \quad (3)$$

we obtain

$$\begin{aligned} p_{00}^t + p_{11}^t &= \sum_{i \in M} r_i (p_{00}^i + p_{11}^i) \\ &\leq \sum_{i \in M} r_i (p_{0*}^i p_{*0}^i + p_{1*}^i p_{*1}^i - \max(0, p_{0*}^i + p_{1*}^i - 1) \max(0, p_{*0}^i + p_{*1}^i - 1)) \\ &\stackrel{(3)}{\leq} \sum_{i \in M} r_i (p_{0*}^i p_{*0}^t + p_{1*}^i p_{*1}^t - \max(0, p_{0*}^i + p_{1*}^i - 1) \max(0, p_{*0}^t + p_{*1}^t - 1)) \\ &\stackrel{(2)}{\leq} p_{0*}^t p_{*0}^t + p_{1*}^t p_{*1}^t - \max(0, p_{0*}^t + p_{1*}^t - 1) \max(0, p_{*0}^t + p_{*1}^t - 1). \end{aligned}$$

Hence, the inequalities also hold for t . The statement follows by induction. \square

4 Quantum Coin Flipping

4.1 Protocols

An *unbalanced weak coin with error ε* $\text{WCF}(z, \varepsilon)$ is a $\text{CF}(z, 1 - z, 1, 1 - z + \varepsilon, z + \varepsilon, 1)$, i.e., a coin flip where Alice wins with probability z , Bob with probability $1 - z$ and both cannot increase their probability to win by more than ε . (They may, however, decrease the probability to 0.). Let $\text{WCF}(z) := \text{WCF}(z, 0)$.

It has been shown by Mochon [Moc07] that weak coin flipping can be implemented with an arbitrarily small error.

Theorem 3 ([Moc07]). *For any constant $\varepsilon > 0$, there exists a quantum protocol that implements $\text{WCF}(1/2, \varepsilon)$.*

In [Moc04b], Mochon showed that quantum coin flipping protocols compose sequentially. Implicitly using this result, Chailloux and Kerenidis showed that an unbalanced weak coin flip can be implemented from many instances of (balanced) weak coin flips.

Proposition 1 ([CK09]). *For all $z \in [0, 1]$, there exists a classical protocol that uses k instances of $\text{WCF}(1/2, \varepsilon)$ and implements $\text{WCF}(x, 2\varepsilon)$, for a value $x \in [0, 1]$ with $|x - z| \leq 2^{-k}$.*

The following lemma shows that parameter z can be slightly changed without increasing the error to much.

Lemma 6. *For any $1 > z' > z > 0$, there exists a classical protocol that uses 1 instance of $\text{WCF}(z', \varepsilon)$ and implements $\text{WCF}(z, \varepsilon + z' - z)$.*

Proof. The protocol first calls $\text{WCF}(z', \varepsilon)$. If Alice wins, i.e., if the output is 0, then she changes the output bit to 1 with probability $1 - z/z'$, and sends the bit to Bob. Bob only accepts changes from 0 to 1, but not from 1 to 0. Alice can force the coin to be 0 with probability at most $z' + \varepsilon = z + (\varepsilon + z' - z)$. Let $x \in [0, 1 - z' + \varepsilon]$ be the probability that a corrupted Bob chooses $\text{WCF}(z', \varepsilon)$ to output 1. Alice will output 1 with probability

$$x + (1 - x) \left(1 - \frac{z}{z'}\right) = 1 - \frac{z}{z'} + x \cdot \frac{z}{z'} \leq 1 - \frac{z}{z'} + (1 - z' + \varepsilon) \cdot \frac{z}{z'} = 1 - z + \varepsilon \cdot \frac{z}{z'} \leq 1 - z + \varepsilon.$$

□

Theorem 3 together with Proposition 1 and Lemma 6 implies that $\text{WCF}(z, \varepsilon)$ can be implemented for any $z \in [0, 1]$ with an arbitrarily small error ε . To simplify the analysis of our protocols, we will assume that we have access to $\text{WCF}(z)$ for any $z \in [0, 1]$. The following lemma shows that when $\text{WCF}(z)$ is replaced by $\text{WCF}(z, \varepsilon)$, the bias of the output is increased by at most 2ε .

Lemma 7. *Let P be a protocol that implements $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$ using one instance of $\text{WCF}(z)$. If $\text{WCF}(z)$ is replaced by $\text{WCF}(z, \varepsilon)$, then P implements $\text{CF}(p_{00}, p_{11}, p_{0*} + 2\varepsilon, p_{1*} + 2\varepsilon, p_{*0} + 2\varepsilon, p_{*1} + 2\varepsilon)$.*

Proof. Let us compare two settings: one where the players execute P using one instance of $\text{WCF}(z, \varepsilon)$, and the other where they use one instance of $\text{WCF}(z)$. When both players are honest, the two settings are obviously identical. Let Alice be honest and Bob malicious. For each setting, we can define an event that occurs with probability at most ε , such that conditioned that the two events do not occur, $\text{WCF}(z)$ and $\text{WCF}(z, \varepsilon)$ and hence the whole protocol are identical. The probability that the two events do not occur is at least $1 - 2\varepsilon$ by the union bound. Therefore, the probabilities that the honest player outputs 0 (or 1) differ by at most 2ε . The statement follows. □

The following protocol is a generalization of the strong coin flipping protocol S from [CK09]. It gives optimal bounds for the case where the honest players never abort, i.e., $p_{00} + p_{11} = 1$.

Protocol **QCoinFlip1**:

Parameters: $x, z_0, z_1, p_0, p_1 \in [0, 1]$.

- Alice flips a coin $a \in \{0, 1\}$ such that the probability that $a = 0$ is x and sends a to Bob.
- Alice and Bob execute $\text{WCF}(z_a)$.
- If Alice wins, then both output a .
- If Bob wins, then he flips a coin b such that $b = a$ with probability p_a . Both output b .

Lemma 8. *Let $p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$ where $p_{*0} + p_{*1} > 1$, $p_{0*} + p_{1*} > 1$ and $p_{*0}p_{0*} + p_{*1}p_{1*} = 1$. Given access to one instance of $\text{WCF}(z)$, we can implement a $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$ where $p_{00} = p_{0*}p_{*0}$ and $p_{11} = p_{1*}p_{*1}$.*

Proof. We execute Protocol **QCoinFlip1**, choosing the parameters

$$p_i := 1 - p_{*1-i}, \quad z_0 := \frac{p_{*0} + p_{*1} - 1}{p_{*1}}, \quad z_1 := \frac{p_{*0} + p_{*1} - 1}{p_{*0}} \quad \text{and} \quad x := \frac{p_{0*}p_{*0} + p_{*1} - 1}{p_{*0} + p_{*1} - 1}.$$

Note that

$$1 - z_0 = \frac{1 - p_{*0}}{p_{*1}} \quad \text{and} \quad 1 - z_1 = \frac{1 - p_{*1}}{p_{*0}}.$$

Since $1 - p_{*0} < p_{*1}$ and $1 - p_{*1} < p_{*0}$, these values are between 0 and 1, and hence also z_0 and z_1 are between 0 and 1. From $p_{0*} \leq 1$ follows that $x \leq 1$, and from $p_{*0}p_{0*} + p_{*1} \geq p_{*0}p_{0*} + p_{*1}p_{1*} = 1$ that $x \geq 0$. Furthermore, we have

$$z_0 + (1 - z_0)p_0 = \frac{p_{*0} + p_{*1} - 1}{p_{*1}} + \frac{(1 - p_{*1})(1 - p_{*0})}{p_{*1}} = p_{*0}$$

and

$$z_1 + (1 - z_1)p_1 = \frac{p_{*0} + p_{*1} - 1}{p_{*0}} + \frac{(1 - p_{*1})(1 - p_{*0})}{p_{*0}} = p_{*1}.$$

Alice can bias Bob's coin to 0 with probability

$$\max\{z_0 + (1 - z_0)p_0; (1 - p_1)\} = p_{*0}$$

and to 1 with probability

$$\max\{z_1 + (1 - z_1)p_1; (1 - p_0)\} = p_{*1}.$$

The probability that Bob can bias Alice's coin to 0 is

$$\begin{aligned} x + (1 - x)(1 - z_1) &= (1 - z_1) + xz_1 \\ &= \frac{1 - p_{*1}}{p_{*0}} + \frac{p_{0*}p_{*0} + p_{*1} - 1}{p_{*0} + p_{*1} - 1} \cdot \frac{p_{*0} + p_{*1} - 1}{p_{*0}} \\ &= p_{0*} \end{aligned}$$

and the probability that he can bias it to 1 is

$$\begin{aligned} (1 - x) + x(1 - z_0) &= 1 - xz_0 \\ &= 1 - \frac{p_{0*}p_{*0} + p_{*1} - 1}{p_{*0} + p_{*1} - 1} \cdot \frac{p_{*0} + p_{*1} - 1}{p_{*1}} \\ &= 1 - \frac{p_{0*}p_{*0} + p_{*1} - 1}{p_{*1}} \\ &= \frac{1 - p_{0*}p_{*0}}{p_{*1}} \\ &= \frac{p_{1*}p_{*1}}{p_{*1}} = p_{1*}. \end{aligned}$$

Furthermore, two honest players output 0 with probability

$$\begin{aligned}
xz_0 + x(1 - z_0)p_0 + (1 - x)(1 - z_1)(1 - p_1) &= x(z_0 + (1 - z_0)p_0) + (1 - x)\frac{1 - p_{*1}}{p_{*0}}p_{*0} \\
&= xp_{*0} + (1 - x)(1 - p_{*1}) \\
&= 1 - p_{*1} + x(p_{*0} + p_{*1} - 1) \\
&= p_{0*}p_{*0} \\
&= p_{00}
\end{aligned}$$

and 1 with probability $1 - p_{00} = 1 - p_{0*}p_{*0} = p_{1*}p_{*1} = p_{11}$. \square

The following protocol gives optimal bounds for the general case. It uses one instance of the above protocol, and lets Alice and Bob abort in some situations.

Protocol **QCoinFlip2**:

Parameters: Protocol P , $\varepsilon_0, \varepsilon_1 \in [0, \frac{1}{2}]$.

- Alice and Bob execute the coin flipping protocol P .
- If Alice obtains 0, she changes to Δ with probability ε_0 . If Bob obtains 1, he changes to Δ with probability ε_1 . If either Alice or Bob has changed to Δ , they both output Δ , otherwise they output the value obtained from P .

Lemma 9. *Let $p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$ where $p_{*0} + p_{*1} > 1$, $p_{0*} + p_{1*} > 1$ and $p_{0*}p_{*0} + p_{*1}p_{1*} \leq 1$. Given access to $\text{WCF}(z)$ for any $z \in [0, 1]$, we can implement a $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$ where $p_{00} = p_{0*}p_{*0}$ and $p_{11} = p_{1*}p_{*1}$.*

Proof. From $p_{*0} + p_{*1} > 1$ and $p_{0*} + p_{1*} > 1$ follows that either $p_{*0} + p_{1*} > 1$ or $p_{0*} + p_{*1} > 1$. Without loss of generality, let us assume that $p_{*0} + p_{1*} > 1$.

Let

$$p'_{0*} := \min\left(1, \frac{1 - p_{1*}p_{*1}}{p_{*0}}\right) \quad p'_{*1} := \frac{1 - p'_{0*}p_{*0}}{p_{1*}}.$$

First, note that since $p_{0*} \leq \frac{1 - p_{1*}p_{*1}}{p_{*0}}$ we have $p'_{0*} \geq p_{0*}$. Obviously, we also have $p'_{0*} \leq 1$. Since $p'_{0*} \leq \frac{1 - p_{1*}p_{*1}}{p_{*0}}$, we have

$$p'_{*1} = \frac{1 - p'_{0*}p_{*0}}{p_{1*}} \geq \frac{1 - \frac{1 - p_{1*}p_{*1}}{p_{*0}}p_{*0}}{p_{1*}} = \frac{p_{1*}p_{*1}}{p_{1*}} = p_{*1},$$

and since $p'_{0*} \leq 1$, we have

$$p'_{*1} = \frac{1 - p'_{0*}p_{*0}}{p_{1*}} \leq \frac{1 - p_{*0}}{p_{1*}} < \frac{p_{1*}}{p_{1*}} \leq 1.$$

Since $p'_{0*}p_{*0} + p_{1*}p'_{*1} = 1$, according to Lemma 8, we can use protocol **QCoinFlip1** to implement a $\text{CF}(p'_{00}, p'_{11}, p'_{0*}, p_{1*}, p_{*0}, p'_{*1})$, where $p'_{00} = p'_{0*}p_{*0}$ and $p'_{11} = p_{1*}p'_{*1}$. Using that protocol as protocol P , let Alice and Bob execute protocol **QCoinFlip2** with $\varepsilon_0 := 1 - p_{0*}/p'_{0*}$, and $\varepsilon_1 := 1 - p_{*1}/p'_{*1}$.

The probability that Bob can bias Alice to 0 is now $(1 - \varepsilon_0)p'_{0*} = p_{0*}$, and the probability that Alice can bias Bob to 1 is now $(1 - \varepsilon_1)p'_{*1} = p_{*1}$. Furthermore, the probability that two honest players output both 0 is $(1 - \varepsilon_0)p'_{00} = (1 - \varepsilon_0)p'_{0*}p_{*0} = p_{0*}p_{*0}$ and the probability that they both output 1 is $(1 - \varepsilon_1)p'_{11} = (1 - \varepsilon_1)p_{1*}p'_{*1} = p_{1*}p_{*1}$. \square

Lemma 10. Let $p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1} \in [0, 1]$ with

$$\begin{aligned} p_{00} &\leq p_{0*}p_{*0} \\ p_{11} &\leq p_{1*}p_{*1} \\ p_{00} + p_{11} &\leq 1. \end{aligned}$$

there exists a quantum protocol that implements $\text{CF}(p_{00}, p_{11}, p_{0*} + \varepsilon, p_{1*} + \varepsilon, p_{*0} + \varepsilon, p_{*1} + \varepsilon)$, for any constant $\varepsilon > 0$.

Proof. Let us first assume that $p_{*0} + p_{*1} > 1$ and $p_{0*} + p_{1*} > 1$. We reduce the value of p_{0*} to p_{00}/p_{*0} and the value of p_{1*} to p_{11}/p_{*1} , which ensures that $p_{0*}p_{*0} + p_{1*}p_{*1} \leq 1$. Now we can apply Lemma 9, together Theorem 3, Proposition 1 and Lemmas 6, 7 and 3.

If the assumption does not hold then either $p_{*0} + p_{*1} \leq 1$ or $p_{0*} + p_{1*} \leq 1$. In this case, we can apply Lemmas 1 and 3. \square

In order to see that this bound is tight, we can use the proof of Kitaev [Kit02] (printed in [ABDR04]) showing that an adversary can always bias the outcome of a strong quantum coin flipping protocol. In fact, Equations (36) - (38) in [ABDR04] imply that for any quantum coin flipping protocol, it must hold that $p_{11} \leq p_{1*}p_{*1}$. In the same way, it can be proven that $p_{00} \leq p_{0*}p_{*0}$. We obtain the following lemma.

Lemma 11. A $\text{CF}(p_{00}, p_{11}, p_{0*}, p_{1*}, p_{*0}, p_{*1})$ can only be implemented by a quantum protocol if $p_{00} \leq p_{0*}p_{*0}$, $p_{11} \leq p_{1*}p_{*1}$ and $p_{00} + p_{11} \leq 1$.

Lemma 10 and 11 imply together Theorem 2.

5 Conclusions

We have shown tight bounds for a general definition of coin flipping, which give trade-offs between weak vs. strong coin flip, between bias vs. abort-probability, and between classical vs. quantum.

Our results extends the work of [CK09], and shows that the whole advantage of the quantum setting lies in the ability to do weak coin flips (as shown by Mochon [Moc07]). If weak coin flips are available in the classical setting, classical protocols can achieve the same bounds as quantum protocols.

For future work, it would be interesting to see if similar bounds holds for the definition of coin flipping without the possibility for the malicious player to abort.

Acknowledgements: We thank Thomas Holenstein, Stephanie Wehner and Severin Winkler for helpful discussions. This work was funded by the Swiss National Science Foundation (SNSF), an ETHIRA grant of ETH's research commission, and the U.K. EPSRC, grant EP/E04297X/1. Part of this work was done while JW was visiting McGill University in Montréal and ETH in Zürich.

References

- [ABDR04] Andris Ambainis, Harry Buhrman, Yevgeniy Dodis, and Hein Röhrig. Multiparty quantum coin flipping. In *CCC '04: Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 250–259. IEEE Computer Society, 2004.
- [Amb01] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. In *STOC '01: Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 134–142. ACM, 2001.
- [ATSVY00] 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. ACM, 2000.

- [Blu83] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *SIGACT News*, 15(1):23–27, 1983.
- [BM04] Amos Beimel and Tal Malkin. A quantitative approach to reductions in secure computation. In *Theory of Cryptography Conference — TCC '04*, pages 238–257, 2004.
- [CK09] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *FOCS '09: Proceedings of the 2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 527–533. IEEE Computer Society, 2009.
- [Cle86] Richard Cleve. Limits on the security of coin flips when half the processors are faulty. In *STOC '86: Proceedings of the eighteenth annual ACM symposium on Theory of computing*, pages 364–369. ACM, 1986.
- [Col07] Roger Colbeck. An entanglement-based protocol for strong coin tossing with bias $1/4$. *Physics Letters A*, 362(5-6):390 – 392, 2007.
- [HMQU06] Dennis Hofheinz, Jörn Müller-Quade, and Dominique Unruh. On the (im-)possibility of extending coin toss. In *Advances in Cryptology, Proceedings of EUROCRYPT '06*, Lecture Notes in Computer Science, pages 504–521. Springer, 2006. Preprint on IACR ePrint 2006/177.
- [Kit02] Alexei Kitaev. Quantum coin-flipping. QIP'03, 2002. slides available at <http://www.msri.org/publications/ln/msri/2002/qip/kitaev/1/index.html>.
- [KN04] Iordanis Kerenidis and Ashwin Nayak. Weak coin flipping with small bias. *Inf. Process. Lett.*, 89(3):131–135, 2004.
- [LC98] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica*, D120:177–187, 1998.
- [MNS09] Tal Moran, Moni Naor, and Gil Segev. An optimally fair coin toss. In *TCC '09: Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography*, pages 1–18. Springer-Verlag, 2009.
- [Moc04a] 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. IEEE Computer Society, 2004.
- [Moc04b] Carlos Mochon. Serial composition of quantum coin flipping and bounds on cheat detection for bit commitment. *Phys. Rev. A*, 70(3):032312, Sep 2004.
- [Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. arXiv:0711.4114v1, 2007.
- [SR01] Robert W. Spekkens and Terry Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65, 2001.
- [SR02] Robert W. Spekkens and Terry Rudolph. A quantum protocol for cheat-sensitive weak coin flipping. *Physical Review Letter*, 89, 2002.
- [WW10] Severin Winkler and Jürg Wullschleger. On the efficiency of classical and quantum oblivious transfer reductions. In *Advances in Cryptology — CRYPTO '10*, Lecture Notes in Computer Science. Springer-Verlag, 2010.
- [Yao82] Andrew C. Yao. Protocols for secure computations. In *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science (FOCS '82)*, pages 160–164, 1982.