A New Protocol and Lower Bounds for Quantum Coin Flipping

Andris Ambainis*
School of Mathematics
Institute for Advanced Study
Princeton, NJ 08540
e-mail: ambainis@ias.edu

Abstract

We present a new protocol and two lower bounds for quantum coin flipping. In our protocol, no dishonest party can achieve one outcome with probability more than 0.75. Then, we show that our protocol is optimal among 3-round protocols of a certain form.

For arbitrary quantum protocols, we show that if a protocol achieves a bias of at most ϵ, it must use at least $\Omega(\log\log\frac{1}{\epsilon})$ rounds of communication. This implies that the parallel repetition fails for quantum coin flipping. (The bias of a protocol cannot be arbitrarily decreased by running several copies of it in parallel.)

1 Introduction

In many cryptographic protocols, there is a need for random bits that are common to both parties. However, if one of parties is allowed to generate these random bits, this party may have a chance to influence the outcome of the protocol by appropriately picking the random bits. This problem can be solved by using a cryptographic primitive called *coin flipping*.

Definition 1 *A coin flipping protocol with ϵ bias is one where Alice and Bob communicate and finally decide on a value $c \in \{0,1\}$ such that*

- *If both Alice and Bob are honest, then $Prob(c=0) = Prob(c=1) = 1/2$.*
- *If one of them is honest (follow the protocol), then, for any strategy of the dishonest player, $Prob(c=0) \leq 1/2+\epsilon$, $Prob(c=1) \leq 1/2+\epsilon$.*

*Supported by NSF Grant CCR-9987845 and the State of New Jersey. Part of this work done while at University of California, Berkeley (supported by Microsoft Research Graduate Fellowship and NSF grant CCR-9800024) and IBM Almaden.

Classically, coin flipping was introduced by Blum[6]. Classical coin flipping protocols are based on computational assumptions such as one-way functions.

However, classical one-way functions may not be hard against quantum adversaries. (For example, factoring and discrete log are not hard in the quantum case[30].) Finding a good candidate for a one-way function secure against quantum adversaries is an important open problem.

On the other hand, the unique properties of quantum mechanics allow the implementation of certain cryptographic tasks without any computational assumptions. (The security proof is based only on the validity of quantum mechanics.) The most famous example is the quantum key distribution[4, 5, 23, 25, 31]. The question is: can we replace the computational assumptions of the classical case by information-theoretic security in the quantum case for the coin flipping?

There are several cryptographic primitives for which this is impossible. In any information-theoretic quantum protocol for bit commitment, one party can successfully cheat with a constant probability of success [21, 22, 24][1]. Similar results are also known for oblivious transfer and some other cryptographic primitives [20].

A protocol for bit commitment can be used to build a protocol for coin flipping [6]. The impossibility of quantum bit commitment means that one cannot build a protocol for quantum coin flipping with arbitrarily small $\epsilon > 0$ in this way. However, it does not mean that quantum coin flipping cannot be achieved using different methods. After the fall of quantum bit commitment, the interest in this direction grew.

The best impossibility result for coin flipping is that there is no quantum protocol for perfect quantum coin flipping (quantum coin flipping with bias 0) [22, 26]. This still leaves the possibility that there might be quantum protocols with an arbitrarily small $\epsilon > 0$.

The first positive result was by Aharonov et.al.[2] who gave a protocol for quantum coin flipping in which a dishonest party cannot force a given outcome with probability more than 0.9143...

There has been some effort to construct more complicated protocols which would achieve arbitrarily small $\epsilon > 0$. At least two protocols have been proposed: by Mayers et.al.[26] and by Zhang et.al.[36]. None of them had provable security guarantees but both were conjectured to achieve an arbitrarily small $\epsilon > 0$ for an appropriate choice of parameters. Both of them were eventually broken: the protocol of [26] was broken by [13, 19, 34][2] and the protocol of [36] is insecure because of our Theorem 5.

In this paper, we give a simple protocol in which a dishonest party cannot achieve one outcome with probability more than 0.75.

Then, we show that our protocol is optimum among 3-round protocols of certain structure. This includes our protocol, the protocol of [2] and other

[1]It is possible, however, to have quantum protocols for bit commitment under quantum complexity assumptions (existence of quantum 1-way functions). See Dumais et.al.[9] and Crepeau et.al.[8]

[2]The paper [34] claims to break any protocol for coin flipping but this claim is incorrect. It does break a class of protocols which includes the one of [26], though.

similar protocols.

Our third result (Theorem 5) shows that, if there is a protocol with an arbitrarily small bias $\epsilon > 0$, it must use a non-constant number of rounds of communication (*not just communicate many qubits in a constant number of rounds*). Namely, a coin flipping algorithm with a bias ϵ needs to have at least $\Omega(\log\log\frac{1}{\epsilon})$ rounds. In particular, this means that the parallel repetition fails for quantum coin flipping. (One cannot decrease the bias arbitrarily by repeating the protocol in parallel many times.)

Recent developments. We have recently learned that two of results in this paper (the 0.75 protocol and the matching lower bound for a class of protocols) have been independently discovered by Spekkens and Rudolph [32]. Also, Kitaev [18] has very recently shown that, in any protocol, at least one party can achieve one outcome with probability at least $1/\sqrt{2} = 0.71....$ Thus, our 0.75 protocol is close to being optimal.

Curiously, Kitaev's lower bound does not apply to a weaker version of coin flipping. In *weak coin flipping*, it is known in advance that Alice wants to bias the coin to 0 and Bob wants to bias it to 1. Then, it is enough to give guarantees about $Pr[c = 0]$ if Bob is honest but Alice cheats and $Pr[c = 1]$ if Alice is honest but Bob cheats. Protocols for weak coin flipping have been studied by Goldenberg [11], Spekkens and Rudolph [33] and Ambainis[3]. The best protocol [33] achieves a maximum bias of $1/\sqrt{2}$. We note that the best lower bound for weak coin flipping is Theorem 5 of this paper.

The role of rounds in quantum communication has been studied in a different context (quantum communication complexity of pointer jumping) by Klauck et. al. [27]. There is a popular survey of quantum cryptography by Gottesman and Lo[12].

2 Preliminaries

2.1 Quantum states

We briefly introduce the notions used in this paper. For more detailed explanations and examples, see [29].

Pure states: An n-dimensional pure quantum state is a vector $|\psi\rangle \in \mathbb{C}^n$ of norm 1. Let $|0\rangle$, $|1\rangle$, ..., $|n-1\rangle$ be an orthonormal basis for $\mathbb{C}^n$. Then, any pure state can be expressed as $|\psi\rangle = \sum_{i=0}^{n-1} a_i|i\rangle$ for some $a_0 \in \mathbb{C}$, $a_1 \in \mathbb{C}$, ..., $a_{n-1} \in \mathbb{C}$. Since the norm of $|\psi\rangle$ is 1, $|a_i|^2 = 1$.

The simplest special case is $n = 2$. Then, the basis for $\mathbb{C}^2$ consists of two vectors $|0\rangle$ and $|1\rangle$ and any pure state is of form $a|0\rangle + b|1\rangle$, $a \in \mathbb{C}$, $b \in \mathbb{C}$, $|a|^2 + |b|^2 = 1$. Such quantum system is called a *quantum bit (qubit).*

We often look at $|\psi\rangle$ as a column vector consisting of coefficients a_i. Then, we use $\langle\psi|$ to denote the conjugate transpose of $|\psi\rangle$. $\langle\psi|$ is a row vector consisting of a_i^* (complex conjugates of a_i). In this notation, $\langle\psi|\phi\rangle$ denotes the inner product of ψ and ϕ. (If $|\psi\rangle = \sum a_i|i\rangle$, $|\phi\rangle = \sum b_i|i\rangle$, then

$\langle\psi|\phi\rangle = \sum a_i^* b_i$.) $|\psi\rangle\langle\phi|$ denotes the outer product of ψ and ϕ (an $n \times n$ matrix with entries $a_i b_j^*$).

Mixed states: A mixed state is a classical probability distribution $(p_i, |\psi_i\rangle)$, $0 \le p_i \le 1$, $\sum_i p_i = 1$ over pure states $|\psi_i\rangle$. The quantum system described by a mixed state is in the pure state $|\psi_i\rangle$ with probability p_i.

A mixed state can be also described by its density matrix $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$. It can be shown that any density matrix has trace 1. (*A trace* of a matrix is the sum of its diagonal entries.)

A quantum system can undergo two basic operations: a unitary evolution and a measurement.

Unitary evolution : A *unitary transformation* U is a linear transformation on $\mathbb{C}^k$ that preserves the l_2 norm (i.e., maps vectors of unit norm to vectors of unit norm).

If, before applying U, the system was in a pure state $|\psi\rangle$, then the state after the transformation is $U|\psi\rangle$.

If, before U, the system was in a mixed state with a density matrix ρ, the state after the transformation is the mixed state with the density matrix $U\rho U^\dagger$.

Projective measurements : An observable is a decomposition of $\mathbb{C}^k$ into orthogonal subspaces $\mathcal{H}_1, \ldots, \mathcal{H}_l$: $\mathbb{C}^n = \mathcal{H}_1 \oplus \mathcal{H}_2 \oplus \ldots \oplus \mathcal{H}_l$. A measurement of a pure state $|\psi\rangle$ with respect to this observable gives the result i with probability $\|P_i|\psi\rangle\|^2$ where $P_i|\psi\rangle$ denotes the projection of $|\psi\rangle$ to the subspace $\mathcal{H}_i$. After the measurement, the state of the system becomes $\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|}$.

A more general class of measurements are POVM measurements (see [29]). In most of this paper, it will be sufficient to consider projective measurements.

2.2 Bipartite states

Bipartite states: In the analysis of quantum coin flipping protocols, we often have a quantum state part of which is held by Alice and the other part by Bob. For example, we can have the EPR state (the state of two qubits $\frac{1}{\sqrt{2}}|0\rangle|0\rangle + \frac{1}{\sqrt{2}}|1\rangle|1\rangle$), with the first qubit held by Alice and the second qubit held by Bob. Such states are called *bipartite* states.

Tracing out: If Alice measures her part, Bob's part becomes a mixed state. For example, if Alice measures the first qubit of the EPR state in the basis consisting of $|0\rangle$ and $|1\rangle$, Bob's state becomes $|0\rangle$ with probability 1/2 and $|1\rangle$ with probability 1/2. Let ρ be the density matrix of the mixed state that Bob gets if Alice measures her part of a bipartite state $|\psi\rangle$. Then, we say that ρ is obtained by *tracing out* the Alice's part of $|\psi\rangle$.

There are many different ways how Alice can measure (trace out) her part. However, they all give the same density matrix ρ for Bob's part.

Purification: Let ρ be a mixed state. Then, any pure state $|\psi\rangle$ of a larger system that gives ρ if a part of the system is traced out is called a *purification* of ρ.

2.3 Distance measures between quantum states

We use two measures of distance between quantum states (represented by density matrices): trace distance and fidelity. For more information on these (and other) measures of distance between density matrices, see [10, 29].

Trace distance: Let $p = (p_1, \ldots, p_k)$ and $q = (q_1, \ldots, q_k)$ be two classical probability distributions. Then, the *variational distance* between p and q is

$$|p - q| = \sum_{i=1}^{k} |p_i - q_i|.$$

The variational distance characterizes how well one can distinguish the distributions p and q.

In the quantum case, the counterpart of a probability distribution is a mixed state. The counterpart of the variational distance is the trace distance. It is defined as follows.

The trace norm of a matrix A is the trace of $|A|$ where $|A| = \sqrt{A^\dagger A}$ is the positive square root of $A^\dagger A$. We denote the trace norm of A by $\|A\|_t$. The following lemma relates the trace norm of $\rho_1 - \rho_2$ (which we also call trace distance between ρ_1 and ρ_2) with the variational distance between distributions obtained by measuring ρ_1 and ρ_2.

Lemma 1 *[1] Let $p^M_{\rho_1}$, $p^M_{\rho_2}$ be the probability distributions generated by applying a measurement $\mathcal{M}$ to mixed states ρ_1 and ρ_2. Then, for any (projective or POVM) measurement $\mathcal{M}$, $|p^M_{\rho_1} - p^M_{\rho_2}| \leq \|\rho_1 - \rho_2\|_t$ and there exists a measurement $\mathcal{M}$ that achieves the variational distance $\|\rho_1 - \rho_2\|_t$.*

We can always choose the measurement $\mathcal{M}$ that achieves the variational distance $\|\rho_1 - \rho_2\|_t$ so that $\mathcal{M}$ is a projective measurement and it has just two outcomes: 0 and 1.

Fidelity: Let $|\psi_1\rangle$ and $|\psi_2\rangle$ be two bipartite states. Let ρ_1 and ρ_2 be the mixed states obtained from $|\psi_1\rangle$ and $|\psi_2\rangle$ by tracing out (measuring) Alice's part.

Lemma 2 *[22, 24] If $\rho_1 = \rho_2$, then Alice can transform $|\psi_1\rangle$ into $|\psi_2\rangle$ by a transformation on her part of the state.*

For example, consider the bipartite states

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle),$$

$$|\psi_2\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle),$$

with the first qubit held by Alice and the second qubit held by Bob. If Alice measures her qubit of $|\psi_1\rangle$, Bob is left with $|0\rangle$ with a probability 1/2 and $|1\rangle$ with a probability 1/2. If Alice measures her qubit of $|\psi_2\rangle$, Bob is left with $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ with a probability 1/2 and $\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$ with a probability 1/2. Both of those states have the same density matrix

$$\begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}.$$

By lemma 2, this means that Alice can transform $|\psi_1\rangle$ into $|\psi_2\rangle$. Indeed, she can do that by applying the Hadamard transform H to her qubit.

A generalization of lemma 2 is: if the two density matrices ρ_1 and ρ_2 are close, then Alice can transform $|\psi_1\rangle$ into a state $|\psi_1'\rangle$ that is close to $|\psi_2\rangle$.

In this case, the distance between the two density matrices is measured by the fidelity $F(\rho_1, \rho_2)$. The fidelity is defined as

$$F(\rho_1, \rho_2) = \max_{|\psi_1\rangle, |\psi_2\rangle} |\langle\psi_1|\psi_2\rangle|^2,$$

over all choices of $|\psi_1\rangle$ and $|\psi_2\rangle$ that give density matrices ρ_1 and ρ_2 when a part of system is traced out.

Lemma 3 *[16] Let ρ_1, ρ_2 be two mixed states with support in a Hilbert space $\mathcal{H}$, $\mathcal{K}$ any Hilbert space of dimension at least $\dim(\mathcal{H})$, and $|\phi_i\rangle$ any purifications of ρ_i in $\mathcal{H}\otimes\mathcal{K}$. Then, there is a local unitary transformation U on $\mathcal{K}$ that maps $|\phi_2\rangle$ to $|\phi_2'\rangle = I \otimes U|\phi_2\rangle$ such that*

$$|\langle\phi_1|\phi_2'\rangle|^2 = F(\rho_1, \rho_2).$$

Lemma 4 *[35]*

$$F(\rho_1, \rho_2) = \left[Tr\left(\sqrt{\sqrt{\rho_1}\rho_2\sqrt{\rho_1}}\right)\right]^2.$$

Relation between trace distance and fidelity: The trace distance and the fidelity are closely related. If ρ_1 and ρ_2 are hard to distinguish for Bob, then Alice can transform $|\psi_1\rangle$ into a state close to $|\psi_2\rangle$ and vica versa. Quantitatively, this relation is given by

Lemma 5 *[10] For any two mixed states ρ_1 and ρ_2,*

$$1 - \sqrt{F(\rho_1, \rho_2)} \leq \frac{1}{2}\|\rho_1 - \rho_2\|_t \leq \sqrt{1 - F(\rho_1, \rho_2)}.$$

In particular, $F(\rho_1, \rho_2) = 0$ if and only if $\|\rho_1 - \rho_2\|_t = 2$.

3 A protocol with bias 0.25

Protocol: Define

$$|\phi_{b,x}\rangle = \begin{cases} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle & \text{if } b=0,\ x=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle & \text{if } b=0,\ x=1 \\ \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|2\rangle & \text{if } b=1,\ x=0 \\ \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|2\rangle & \text{if } b=1,\ x=1 \end{cases}$$

1. Alice picks a uniformly random $b \in \{0,1\}$ and $x \in \{0,1\}$ and sends $|\phi_{b,x}\rangle$ to Bob.
2. Bob picks a uniformly random $b' \in \{0,1\}$, sends b' to Alice.
3. Alice sends b and x to Bob, he checks if the state that he received from Alice in the 1st step is $|\phi_{b,x}\rangle$ (by measuring it in with respect to in a basis consisting of $|\phi_{b,x}\rangle$ and two vectors orthogonal to it)[3]. If the outcome of the measurement is not $|\phi_{b,x}\rangle$, he has caught Alice cheating and he stops the protocol.
4. Otherwise, the result of the coin flip is $b \oplus b'$.

Theorem 1 *The bias of this protocol is* 0.25.

Proof: We bound the probability of dishonest Alice (or dishonest Bob) achieving $b \oplus b' = 0$. The maximum probability of achieving $b \oplus b' = 1$ is the same because the protocol is symmetric.

Case 1: Alice is honest, Bob cheats. If $b = 0$, Alice sends a mixed state that is equal to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ with probability 1/2 and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ with probability 1/2. If $b = 1$, she sends a mixed state that is equal to $\frac{1}{\sqrt{2}}(|0\rangle + |2\rangle)$ with probability 1/2 and $\frac{1}{\sqrt{2}}(|0\rangle - |2\rangle)$ with probability 1/2. The density matrices of these two mixed states are

$$\rho_0 = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 \end{pmatrix} \rho_1 = \begin{pmatrix} \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & \frac{1}{2} \end{pmatrix}$$

and $\|\rho_0 - \rho_1\|_t = 1$. To achieve $b \oplus b' = 0$, Bob has to guess b from ρ_b, if he is given ρ_0 with probability 1/2 and ρ_1 with probability 1/2. This is a problem which was first studied by Helstrom [15, pp. 106-108]. As shown in [15, 10], the probability with which Bob can guess b is at most $\frac{1}{2} + \frac{\|\rho_0 - \rho_1\|_t}{4} = \frac{3}{4}$.

Case 2: Bob honest, Alice cheats.

Let ρ be the density matrix of the state sent by Alice in the 1st step. The first step of the proof is to "symmetrize" Alice's strategy so that it becomes easier to bound her success probability.

[3]For example, if $b = x = 0$, then Bob could measure in the basis $|\phi_{00}\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, $|2\rangle$.

Lemma 6 *There is a strategy for dishonest Alice where the state sent by Alice in the* 1^{st} *round has the density matrix of the form*

$$\rho' = \begin{pmatrix} 1-\delta_1-\delta_2 & 0 & 0 \\ 0 & \delta_1 & 0 \\ 0 & 0 & \delta_2 \end{pmatrix} \tag{1}$$

for some δ_1 *and* δ_2 *and Alice achieves* $b = b'$ *with the same probability.*

Proof: Let $U_0 = I$,

$$U_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad U_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

$$U_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Assume that Alice, before sending the state $|\psi\rangle$ to Bob in the 1^{st} round, applies U_i to it and, then, in the 3^{rd} round, replaces each description of $|\phi_{b,x}\rangle$ by a description of $U_i|\phi_{b,x}\rangle$. Then, Alice achieves the outcomes 0 and 1 and gets caught with the same probabilities as before because

(a) For all $i \in \{0,1,2,3\}$, $b \in \{0,1\}$, $x \in \{0,1\}$, $U_i|\phi_{b,x}\rangle$ is either $|\phi_{b,0}\rangle$ or $|\phi_{b,1}\rangle$, and

(b) For any $|\psi\rangle$, the inner product between $U_i|\psi\rangle$ and $U_i|\phi_{b,x}\rangle$ is the same as the inner product between $|\psi\rangle$ and $|\phi_{b,x}\rangle$.

Probabilities of obtaining 0, 1 and getting caught also stay the same if Alice picks a uniformly random $i \in \{0,1,2,3\}$ and then applies U_i to both the state sent in the 1^{st} round and the description sent in the 3^{rd} round. In this case, the density matrix of the state sent by Alice in the 1^{st} round is $\rho' = \frac{1}{4}(U_0\rho U_0^\dagger + U_1\rho U_1^\dagger + U_2\rho U_2^\dagger + U_3\rho U_3^\dagger)$. For every $j,k \in \{1,2,3\}$, $j \neq k$, $(U_i\rho U_i^\dagger)_{jk}$ is equal to ρ_{jk} for two $i \in \{0,1,2,3\}$ and to $-\rho_{jk}$ for the two other i. Therefore, $\rho'_{jk} = 0$ for all $j \neq k$, i.e. ρ' is of the form (1). □

Lemma 7 *For "symmetrized" Alice's strategy, the probability that Alice convinces Bob that* $b = 0$ *is at most* $F(\rho', \rho_0)$.

Proof: Let

$$|\psi\rangle = \sum_i a_i |i\rangle|\psi_i\rangle \tag{2}$$

be the purification of ρ' chosen by Alice if she want to convince Bob that $b = 0$. For every $|\psi_i\rangle$, Alice sends to Bob a description of a state $|\psi'_i\rangle$ which is one of $|\phi_{b,x}\rangle$, $b \in \{0,1\}$, $x \in \{0,1\}$.

Alice is trying to convince Bob that $b = 0$. Therefore, we can assume that she always sends to Bob a description of $|\phi_{0,0}\rangle$ or $|\phi_{0,1}\rangle$. (Replacing a description of $|\phi_{1,x}\rangle$ by a description of $|\phi_{0,x}\rangle$ can only increase the probability of Bob accepting $b = 0$, although it may simultaneously increase the probability of Alice caught cheating.)

We pair up each state $|\psi_i\rangle$ with the state $|\psi_j\rangle = U_1|\psi_i\rangle$ and each state $U_2|\psi_i\rangle$ with $U_3|\psi_i\rangle = U_2U_1|\psi_i\rangle$. Our "symmetrization" guarantees that

- if $|\psi_i\rangle$ and $|\psi_j\rangle$ are the two states in one pair, then $a_i = a_j$,
- if one of states in a pair has $|\psi'_i\rangle = |\phi_{0,0}\rangle$, the other has $|\psi'_j\rangle = U_1|\phi_{0,0}\rangle = |\phi_{0,1}\rangle$, and conversely,
- $\langle\psi_i|\psi'_i\rangle = \langle\psi_j|\psi'_j\rangle$ (because performing U_1 maps $|\psi_i\rangle$ and $|\psi_j\rangle$ to $|\psi'_i\rangle$ and $|\psi'_j\rangle$, respectively).

Therefore, we can write the equation (2) as

$$|\psi\rangle = \sum_i a_i \left(\frac{1}{\sqrt{2}}|i,0\rangle|\psi_{i,0}\rangle + \frac{1}{\sqrt{2}}|i,1\rangle|\psi_{i,1}\rangle\right) \tag{3}$$

with $|\psi'_{i,0}\rangle = |\phi_{0,0}\rangle$ and $|\psi'_{i,1}\rangle = |\phi_{0,1}\rangle$.

The probability that Bob accepts $|\psi_{i,x}\rangle$ as $|\psi'_{i,x}\rangle$ is $|\langle\psi_{i,x}|\psi'_{i,x}\rangle|^2$. The total probability of Bob accepting is

$$\sum_i \frac{1}{2}|a_i|^2(|\langle\psi_{i,0}|\psi'_{i,0}\rangle|^2 + |\langle\psi_{i,1}|\psi'_{i,1}\rangle|^2). \tag{4}$$

Notice that, because of "symmetrization", $\langle\psi_{i,0}|\psi'_{i,0}\rangle = \langle\psi_{i,1}|\psi'_{i,1}\rangle$. Therefore, if we define $|\varphi_i\rangle = \frac{1}{\sqrt{2}}|i,0\rangle|\psi_{i,0}\rangle + \frac{1}{\sqrt{2}}|i,1\rangle|\psi_{i,1}\rangle$ and $|\varphi'_i\rangle = \frac{1}{\sqrt{2}}|i,0\rangle|\psi'_{i,0}\rangle + \frac{1}{\sqrt{2}}|i,1\rangle|\psi'_{i,1}\rangle$, we have $\langle\varphi_i|\varphi'_i\rangle = \langle\psi_{i,0}|\psi'_{i,0}\rangle = \langle\psi_{i,1}|\psi'_{i,1}\rangle$. This means that (4) is equal to

$$\sum_i |a_i|^2|\langle\varphi_i|\varphi'_i\rangle|^2.$$

Let ρ_i be a mixed state which is $|\psi_{i,0}\rangle$ with probability 1/2 and $|\psi_{i,1}\rangle$ with probability 1/2. Then, $\rho' = \sum_i |a_i|^2\rho_i$. Since $|\varphi_i\rangle$ and $|\varphi'_i\rangle$ are purifications of ρ_i and ρ_0, we have $|\langle\varphi_i|\varphi'_i\rangle|^2 \leq F(\rho_i, \rho_0)$ and

$$\sum_i |a_i|^2|\langle\varphi_i|\varphi'_i\rangle|^2 \leq \sum_i |a_i|^2 F(\rho_i, \rho).$$

By concavity of fidelity [29],

$$\sum_i |a_i|^2 F(\rho_i, \rho_0) \leq F(\sum_i |a_i|^2\rho_i, \rho_0) = F(\rho, \rho_0).$$

□

Lemma 8 *For "symmetrized" Alice's strategy, the probability that Alice achieves $b \oplus b' = 0$ (or, equivalently, $b \oplus b' = 1$) is at most $\frac{1}{2}(F(\rho', \rho_0) + F(\rho', \rho_1))$.*

Proof: With probability 1/2, Bob's bit is $b' = 0$. Then, to achieve $b \oplus b' = 0$, Alice needs to convince him that $b = 0$. By Lemma 7, she succeeds with probability at most $F(\rho', \rho_0)$.

With probability 1/2, Bob's bit is $b' = 1$. Then, Alice needs to convince Bob that $b = 1$ and she can do that with probability $F(\rho', \rho_1)$. The overall probability that Alice succeeds is $\frac{1}{2}(F(\rho', \rho_0) + F(\rho', \rho_1))$. $\square$

By Lemma 4,

$$F(\rho', \rho_0) = [Tr(\sqrt{\sqrt{\rho'}\rho_0\sqrt{\rho'}})]^2 = \left(\frac{1}{\sqrt{2}}\sqrt{1-\delta_1-\delta_2} + \frac{1}{\sqrt{2}}\sqrt{\delta_1}\right)^2.$$

Similarly, $F(\rho', \rho_1) = (\frac{1}{\sqrt{2}}\sqrt{1-\delta_1-\delta_2} + \frac{1}{\sqrt{2}}\sqrt{\delta_2})^2$. Therefore,

$$\frac{1}{2}(F(\rho', \rho_0) + F(\rho', \rho_1))$$

$$= (\frac{1}{\sqrt{2}}\sqrt{1-\delta_1-\delta_2} + \frac{1}{\sqrt{2}}\sqrt{\delta_1})^2 + (\frac{1}{\sqrt{2}}\sqrt{1-\delta_1-\delta_2} + \frac{1}{\sqrt{2}}\sqrt{\delta_2})^2$$

$$= \frac{1}{2}\left((1-\delta_1-\delta_2) + \frac{\delta_1}{2} + \frac{\delta_2}{2} + \sqrt{1-\delta_1-\delta_2}(\sqrt{\delta_1}+\sqrt{\delta_2})\right). \quad (5)$$

Let $\delta = \frac{\delta_1+\delta_2}{2}$. The convexity of the square root implies that $\sqrt{\delta_1}+\sqrt{\delta_2} \leq 2\sqrt{\delta}$ and (5) is at most

$$\frac{1}{2}\left(1-\delta+2\sqrt{\delta(1-2\delta)}\right).$$

Taking the derivative of this expression shows that it is maximized by $\delta = \frac{1}{6}$. Then, it is equal to $\frac{1}{2}(1-\frac{1}{6}+\frac{4}{6}) = \frac{3}{4}$. $\square$

4 Lower bound for subclass of 3 round protocols

We show a lower bound for a class of 3 round protocols which includes the protocol of section 3 and the protocol of [2]. This class is defined by fixing the structure of the protocol and varying the choice of states $|\phi_{b,x}\rangle$.

Let X_0 and X_1 be two sets and π_0 and π_1 be probability distributions over X_0 and X_1, respectively. Assume that, for every $b \in \{0,1\}$ and $x \in X_b$ we have a state $|\phi_{b,x}\rangle$.

1. Alice picks a uniformly random $b \in \{0,1\}$. Then, she picks $x \in X_b$ according to the distribution π_b and sends $|\phi_{b,x}\rangle$ to Bob.

2. Bob picks a random $b' \in \{0,1\}$, sends b' to Alice.

3. Alice sends b and x to Bob. Bob checks if the state that he received in the 1^{st} step is $|\phi_{b,x}\rangle$.

4. The result of the coin flip is $b \oplus b'$.

Theorem 2 *Any protocol of this type has a bias at least 0.25.*

Proof: Let ρ_0 and ρ_1 be the density matrices sent by an honest Alice if $b = 0$ and $b = 1$, respectively. (These density matrices are mixtures of $|\phi_{b,x}\rangle$ over $x \in X_i$.)

Lemma 9 *Bob can achieve 0 with probability* $\frac{1}{2} + \frac{\|\rho_0 - \rho_1\|_t}{4}$.

Proof: By Lemma 1, there is a measurement $\mathcal{M}$ that, applied to ρ_0 and ρ_1, produces two probability distributions with the variational distance between them equal to $\|\rho_0 - \rho_1\|_t$ and it can be chosen so that there are just two outcomes: 0 and 1.

Let p_0 and $1 - p_0$ be the probabilities of outcomes 0 and 1 when the measurement $\mathcal{M}$ is applied to ρ_0. For the variational distance to be $\|\rho_0 - \rho_1\|_t$, the probabilities of outcomes 0 and 1 when the measurement $\mathcal{M}$ is applied to ρ_1 have to be $p_0 - \frac{\|\rho_0 - \rho_1\|_t}{2}$ and $1 - p_0 + \frac{\|\rho_0 - \rho_1\|_t}{2}$.

Bob applies the measurement $\mathcal{M}$ to the state that he receives from Alice and sends $b = 0$ if the measurement gives 0 and $b = 1$ if the measurement gives 1. Since an honest Alice chooses $a = 0$ with probability 1/2 and $a = 1$ with probability 1/2, Bob achieves $a = b$ (and $a \oplus b = 0$) with probability

$$\frac{1}{2}p_0 + \frac{1}{2}\left(1 - p_0 + \frac{\|\rho_0 - \rho_1\|_t}{2}\right) = \frac{1}{2} + \frac{\|\rho_0 - \rho_1\|_t}{4}.$$

□

Lemma 10 *Alice can achieve 0 with probability*

$$\frac{1}{2} + \frac{\sqrt{F(\rho_0, \rho_1)}}{2}.$$

Proof: First, we consider an honest Alice which does the protocol on a quantum level. That means that she flips a classical coin to determine $a \in \{0, 1\}$ and then prepares the superposition

$$|\psi_a\rangle = \sum_{i \in X_a} \sqrt{\pi_a(i)} |i\rangle |\phi_{a,i}\rangle$$

and sends the second part of the superposition to Bob. After receiving b from Bob, she measures i and sends a and i to Bob.

The pure states $|\psi_0\rangle$ and $|\psi_1\rangle$ are purifications of the density matrices ρ_0 and ρ_1. By Lemma 3, there is a unitary transformation U on the Alice's part of ψ_1 such that $|\langle \psi_0 | U(\psi_1) \rangle^2 = F(\rho_0, \rho_1)$.

Let α be such that $F(\rho_0, \rho_1) = \cos^2 \alpha$. Then, $\langle \psi_0 | U(\psi_1) \rangle = \cos \alpha$. This means that

$$\begin{cases} |\psi_0\rangle = \cos\frac{\alpha}{2}|\varphi_0\rangle + \sin\frac{\alpha}{2}|\varphi_1\rangle \\ U|\psi_1\rangle = \cos\frac{\alpha}{2}|\varphi_0\rangle - \sin\frac{\alpha}{2}|\varphi_1\rangle \end{cases}$$

for some states $|\varphi_0\rangle$, $|\varphi_1\rangle$.

A dishonest Alice prepares $|\varphi_0\rangle$ and sends the 2^{nd} part to Bob. If she receives $b' = 0$ from Bob, she acts as an honest quantum Alice who has prepared $|\psi_0\rangle$ and sent the 2^{nd} part to Bob. (That is, she measures her part $|i\rangle$ and sends 0 and i to Bob.) Bob accepts $b = 0$ with probability at least[4] $|\langle\psi_0|\varphi_0\rangle|^2 = \cos^2\frac{\alpha}{2}$.

If she receives $b' = 1$, Alice performs U^{-1} on her part of $|\varphi_0\rangle$ and continues as an honest quantum Alice who has prepared $|\psi_1\rangle$ (measures $|i\rangle$ and sends to 1 and i to Bob). Bob accepts $b = 1$ with probability

$$|\langle U^{-1}(\varphi_0)|\psi_1\rangle|^2 = |\langle\varphi_0|U(\psi_1)\rangle|^2 = \cos^2\frac{\alpha}{2}.$$

In both cases, the probability of Bob accepting $b\oplus b' = 0$ is $\cos^2\frac{\alpha}{2}$. Therefore, the overall probability of $b \oplus b' = 0$ is $\cos^2\frac{\alpha}{2}$ as well and we have

$$\cos^2\frac{\alpha}{2} = \frac{1+\cos\alpha}{2} = \frac{1+\sqrt{F(\rho_0,\rho_1)}}{2}.$$

□

If $F(\rho_0,\rho_1) \geq \frac{1}{4}$, then, by Lemma 10, Alice can achieve a bias of $\frac{\sqrt{F(\rho_0,\rho_1)}}{2} \geq \frac{1}{4}$.

If $F(\rho_0,\rho_1) \leq \frac{1}{4}$, then, by Lemma 9, Bob can achieve a bias of $\frac{1}{4}\|\rho_0-\rho_1\|_t$ and, by Lemma 5,

$$\frac{1}{4}\|\rho_0,\rho_1\|_t \geq \frac{1}{2}(1-\sqrt{F(\rho_0,\rho_1)}) \geq \frac{1}{4}.$$

□

5 Two standard forms for quantum protocols

We use the following "standard form" for quantum protocols.

Theorem 3 *[24] If there is a protocol for quantum coin flipping with a bias at most ϵ, there is also a protocol with bias at most ϵ in which no party makes measurements until all communication is complete.*

The main idea of the proof of Theorem 3 is that all measurements can be delayed till the end of protocol. This idea is known as the "principle of safe storage" in the context of quantum computing and quantum cryptography [7, 24] and as the "Church of the Larger Hilbert space" in quantum physics. (The name "church of the Larger Hilbert space" is due to John Smolin.) It has been useful for many purposes (for example, the impossibility of quantum bit commitment [22, 24] or results about entanglement manipulations).

A different "standard form" has been pointed out to us by Kitaev [17].

[4] For a formal proof of this, define $\mathcal{H}$ to be the space of all bipartite states $|\psi\rangle$ such that Bob accepts with probability 1, if Alice acts in this way. Then, $|\psi_0\rangle \in \mathcal{H}$ and, since the angle between $|\varphi_0\rangle$ and $|\psi_0\rangle$ is $\frac{\alpha}{2}$, the squared projection of $|\varphi_0\rangle$ on $\mathcal{H}$ is at least $\cos^2\frac{\alpha}{2}$, implying that Bob accepts with probability at least $\cos^2\frac{\alpha}{2}$ if Alice starts with $|\varphi_0\rangle$.

Theorem 4 *[17] If there is a protocol for quantum coin flipping with a bias ϵ, there is another protocol with bias ϵ in which only the first message from Alice to Bob is quantum and all the other messages are classical.*

The proof idea is that Alice transmits a lot of EPR pairs in the first round and, after that, Alice and Bob can replace all quantum communication by classical communication using teleportation.

We do not use this result in our paper but we decided to mention it because it might be useful for other purposes. The protocols of the form of Theorem 4 have a fairly simple structure. In the first step Alice creates an entangled state with Bob and then they both do operations on their qubits and communicate classical information. Because of this simple structure, they might be easier to analyze than general protocols. We note that this structure of a protocol somewhat resembles the well-known LOCC (local operations and classical communication) paradigm in the study of entanglement [28, 29].

6 The lower bound on the number of rounds

Theorem 5 *Any protocol for quantum coin flipping that achieves a bias ϵ must use $\Omega(\log\log \frac{1}{\epsilon})$ rounds.*

Note. One could also consider a type of protocols in which honest Alice and honest Bob may end up disagreeing about the outcome of the coin flip with some small probability $\delta > 0$. Our proof can be extended to this case, showing that any protocol in which both probability of honest players disagreeing about the outcome and maximum bias achieved by a cheater are at most ϵ must use $\Omega(\log\log \frac{1}{\epsilon})$ rounds. The proof is mostly similar to Theorem 5.
Proof : If $\epsilon \geq \frac{1}{4}$, then $\log\log\epsilon \leq \log\log 4 = 1$ and any nontrivial protocol clearly needs at least 1 round. Therefore, it suffices to consider $\epsilon < 1/4$.

Assume we have a protocol for quantum coin flipping with k rounds and a bias ϵ. By Theorem 3, we can assume that this protocol does not make any measurements till the end of communication.

The protocol starts with a fixed starting state $|\psi^0\rangle$. Then (if both players are honest), Alice applies a unitary transformation U_1, sends some qubits to Bob, he applies U_2, sends some qubits to Alice and so on. After U_k, both Alice and Bob perform measurements on their parts. Since there is no measurements till the communication is finished, the joint state of Alice and Bob after i steps is a pure state $|\psi^i\rangle$.

At the end of protocol, Alice and Bob measure the final state to determine the outcome of the coin flip. If both Alice and Bob follow the protocol, the two measurements give the same result and this result is 0 with probability 1/2 and 1 with probability 1/2.

For our analysis, we decompose each of intermediate states $|\psi^i\rangle$ as $|\psi^i_0\rangle+|\psi^i_1\rangle$, where $|\psi^i_0\rangle$ is the state which leads to the outcome 0 if the rest of protocol is applied and $|\psi^i_1\rangle$ is the state which leads to the outcome 1 if the rest of protocol is applied. This is done as follows.

First, we decompose the final state $|\psi^k\rangle$. Let $|\psi_0^k\rangle$ and $|\psi_1^k\rangle$ be the (unnormalized) states after the final measurement if the measurement gives 0 (1). Then, $|\psi_0^k\rangle \perp |\psi_1^k\rangle$ and $|\psi^k\rangle = |\psi_0^k\rangle + |\psi_1^k\rangle$. Also, $\|\psi_0^k\|^2 = \|\psi_1^k\|^2 = \frac{1}{2}$ (since a protocol must give 0 with probability 1/2 and 1 with probability 1/2).

Next, we define $|\psi_0^i\rangle = (U_{i+1}U_{i+2}\dots U_k)^{-1}|\psi_0^k\rangle$ and $|\psi_1^i\rangle = (U_{i+1}U_{i+2}\dots U_k)^{-1}|\psi_1^k\rangle$. Then, $|\psi^k\rangle = |\psi_0^k\rangle + |\psi_1^k\rangle$ implies $|\psi^i\rangle = |\psi_0^i\rangle + |\psi_1^i\rangle$.

Let $\rho_{A,j}^i$ ($\rho_{B,j}^i$) be the density matrix of Alice's (Bob's) part of the (normalized) bipartite state $\sqrt{2}|\psi_j^i\rangle$. Let F_A^i (F_B^i) be the fidelity between $\rho_{A,0}^i$ and $\rho_{A,1}^i$ ($\rho_{B,0}^i$ and $\rho_{B,1}^i$).

Our proof is based on analyzing how F_A^i and F_B^i change during the protocol. We show that they must be large at the beginning, 0 at the end and, if they decrease too fast, this creates an opportunity for cheating. This implies the lower bound on the number of rounds.

We start with the simplest part of the proof: F_A^i and F_B^i must be small at the end ($i = k$).

Lemma 11 *$F_A^k = F_B^k = 0$.*

Proof: At the end, both Alice and Bob know the outcome of the protocol with certainty. That means that there is a measurement of Alice's qubits that perfectly distinguishes $|\psi_0^k\rangle$ and $|\psi_1^k\rangle$ (i.e., this measurement gives 0 with probability 1 on $|\psi_0^k\rangle$ and 1 with probability $|\psi_1^k\rangle$). By Lemma 1, $\|\rho_{A,0}^k - \rho_{A,1}^k\|_t = 2$. By Lemma 5, $F(\rho_{A,0}^k, \rho_{A,1}^k)$ must be 0.

Similarly, $F_B^k = 0$. $\square$

Note: If we consider the version of coin flipping in which honest Alice and Bob may disagree with probability ϵ, we have $F_A^k = F_B^k = O(\epsilon)$ instead of $F_A^k = F_B^k = 0$ but this is sufficient for the rest of proof.

Second, we show that, if F_A^0 or F_B^0 is too small, one of sides can cheat.

Lemma 12 *Alice can achieve one of outcomes 0 and 1 with probability at least $1 - \sqrt{F_A^0}$.*

Proof: Since there is no communication before the start of the protocol, the starting superposition $|\psi^0\rangle$ is a tensor product $|\psi_A\rangle \otimes |\psi_B\rangle$, with Alice having $|\psi_A\rangle$ and Bob having $|\psi_B\rangle$.

Consider the best measurement $\mathcal{M}$ (for Alice) that distinguishes $\rho_{A,0}^0$ and $\rho_{A,1}^0$ (Lemma 1). Then, $|\psi_0^0\rangle = |\psi_{00}\rangle + |\psi_{01}\rangle$, where $|\psi_{00}\rangle$ is the remaining state if the measurement $\mathcal{M}$ on $|\psi_0^0\rangle$ gives the outcome 0 and $|\psi_{01}\rangle$ is the remaining state if $\mathcal{M}$ gives the outcome 1. Let $|\psi_1^0\rangle = |\psi_{10}\rangle + |\psi_{11}\rangle$, with $|\psi_{10}\rangle$ and $|\psi_{11}\rangle$ defined similarly.

If Alice applies $\mathcal{M}$ to $|\psi^0\rangle = |\psi_0^0\rangle + |\psi_1^0\rangle$, she either gets the outcome 0 and the remaining state $|\psi_0'\rangle = |\psi_{00}\rangle + |\psi_{10}\rangle$ or 1 and the remaining state $|\psi_1'\rangle = |\psi_{01}\rangle + |\psi_{11}\rangle$. $|\psi^0\rangle$ is a product state and the measurement $\mathcal{M}$ is applied to Alice's side only. Therefore, $|\psi_0'\rangle$ and $|\psi_1'\rangle$ (the remaining states when $\mathcal{M}$ gives 0 and 1) are product states as well.

Since $|\psi^0\rangle = |\psi'_0\rangle + |\psi'_1\rangle$, either $\|\psi'_0\|^2 \geq \frac{1}{2}$ or $\|\psi'_1\|^2 \geq \frac{1}{2}$. For simplicity, we assume that $\|\psi'_0\|^2 \geq \frac{1}{2}$ and Alice is trying to achieve the outcome 0. (The outcome 1 can be achieved similarly with a slightly smaller probability.)

Let $|\psi'_A\rangle \otimes |\psi_B\rangle$ be the normalized state $\frac{|\psi'_0\rangle}{\|\psi'_0\|}$. To bias the coin towards 0, Alice just runs the honest protocol with her starting state being $|\psi'_A\rangle$ instead of $|\psi_A\rangle$.

Let $\|\psi_{01}\|^2 + \|\psi_{10}\|^2 \leq \epsilon$. We show that this implies that $|\psi'_A\rangle \otimes |\psi_B\rangle$ is close to the normalized state $\sqrt{2}|\psi^0_0\rangle$ (which gives the outcome 0 with probability 1). We have

$$\frac{|\psi'_0\rangle}{\|\psi'_0\|} = \frac{|\psi_{00}\rangle + |\psi_{10}\rangle}{\|\psi'_0\|} = \frac{|\psi_{00}\rangle + |\psi_{01}\rangle}{\|\psi'_0\|} + \frac{|\psi_{10}\rangle - |\psi_{01}\rangle}{\|\psi'_0\|}.$$

$|\psi_{00}\rangle + |\psi_{01}\rangle = |\psi^0_0\rangle$ leads to the outcome 0 with certainty. Therefore, the probability of a different outcome (1 or Alice caught cheating) is at most

$$\frac{\|\psi_{10} - \psi_{01}\|^2}{\|\psi'_0\|^2} \leq \frac{\|\psi_{10}\|^2 + \|\psi_{01}\|^2}{\|\psi'_0\|^2} \leq \frac{\epsilon}{1/2} = 2\epsilon.$$

Therefore, the described strategy for dishonest Alice gives 0 with probability at least $1 - 2\epsilon$.

Next, we bound $\|\psi_{01}\|^2 + \|\psi_{10}\|^2$.

Let $1 - p_0$ and p_0 be the probabilities of outcomes 0 and 1 when measuring $\sqrt{2}|\psi^i_0\rangle$. Let p_1 and $1-p_1$ be the probabilities of 0 and 1 when measuring $\sqrt{2}|\psi^i_1\rangle$. Then, the variational distance between these two probability distributions is $2(1 - p_0 - p_1)$. Since we are using the best measurement for distinguishing $\rho^0_{A,0}$ and $\rho^0_{A,1}$, $2(1 - p_0 - p_1)$ is equal to $\|\rho^0_{A,0} - \rho^0_{A,1}\|_t$. By Lemma 5, this implies

$$1 - \sqrt{F^0_A} = 1 - \sqrt{F(\rho^0_{A,0}, \rho^0_{A,1})} \leq \|\rho^0_{A,0} - \rho^0_{A,1}\|_t = (1 - p_0 - p_1)$$

and this is equivalent to $p_0 + p_1 \leq \sqrt{F^0_A}$.

Notice that $p_0 = 2\|\psi_{01}\|^2$ because $\rho^0_{A,0}$ is the density matrix of Alice's side of $\sqrt{2}|\psi^0_{A,0}\rangle$ and $|\psi_{01}\rangle$ is the remaining state if the measurement of $|\psi^0_{A,0}\rangle$ gives 1. Similarly, $p_1 = 2\|\psi_{10}\|^2$. Therefore, we have $\|\psi_{01}\|^2 + \|\psi_{10}\|^2 \leq \frac{1}{2}\sqrt{F^0_A}$ and Alice can bias the coin to 0 with probability at least $1 - \sqrt{F^0_A}$. $\square$

Hence, if the bias of a protocol is ϵ, then, by Definition 1, we must have $1 - \sqrt{F^0_A} \leq \frac{1}{2} + \epsilon$. This implies $\sqrt{F^0_A} \geq \frac{1}{2} - \epsilon$ and $F^0_A \geq (\frac{1}{2} - \epsilon)^2$. Since we are considering the $\epsilon < 1/4$ case (see beginning of the proof of Theorem 5), we must have $F^0_A \geq \frac{1}{16}$.

Third, we show that, if after any round, one of F^i_A and F^i_B is much larger than the other, this also creates a possibility for cheating.

Lemma 13 *Let $i \in \{1, \ldots, k-1\}$. Then, there is a strategy for dishonest Alice which achieves the result 0 with probability at least*

$$\left(\frac{1}{\sqrt{2}} - \sqrt[4]{F^i_A}\right)^2 + \left(\frac{\sqrt{F^i_B}}{\sqrt{2}} - \sqrt[4]{F^i_A}\right)^2. \tag{6}$$

Proof: For brevity, we denote F_A^i and F_B^i by F_A and F_B (omitting the index i which is the same throughout the proof).

We first prove the $F_A = 0$ case. This case was previously considered by Mayers et.al.[26]. They showed that, if $F_A = 0$ and $F_B > 0$, then Alice can successfully cheat. Below, we show how to formalize their argument so that it shows the probability of cheating Alice making the result 0.

$F_A = 0$ *case.* Then, (6) is just $\frac{1}{2} + \frac{F_B}{2}$.

By Lemma 5, $F(\rho^i_{A,0}, \rho^i_{A,1}) = F_A = 0$ implies $\|\rho^i_{A,0} - \rho^i_{A,1}\|_t = 2$. By Lemma 1, there is a measurement for Alice that perfectly distinguishes $\rho^i_{A,0}$ and $\rho^i_{A,1}$. With probability 1/2, the outcome of the measurement is 0 and the joint state of Alice and Bob after the measurement is $|\psi^i_0\rangle$. With probability 1/2, the outcome is 1 and the joint state of Alice and Bob becomes $|\psi^i_1\rangle$. In the first case, she just continues as in the honest protocol. This gives the answer 0 with probability 1/2.

If she gets $|\psi^i_1\rangle$, by Lemma 3, there is a unitary transformation U that can be performed by Alice such that

$$|\langle\psi^i_0|U(\psi^i_1)\rangle|^2 = F(\rho^i_{B,0}, \rho^i_{B,1})\|\psi^i_0\|^2 = \frac{F(\rho^i_{B,0}, \rho^i_{B,1})}{2} = \frac{F_B}{2}. \tag{7}$$

Alice performs U and then continues as in the honest protocol. This gives the answer 0 with probability at least $F_B/2$.

Together, the probability of answer 0 is at least $\frac{1}{2}(1 + F_B)$.

$F_A \geq 0$ *case.* By Lemma 5, there is a measurement $\mathcal{M}$ for Alice that, applied to $\rho^i_{A,0}$ and $\rho^i_{A,1}$, produces two probability distributions with the variational distance between them at least $2(1 - \sqrt{F_A})$. Without the loss of generality, we can assume that this is a measurement with two outcomes 0 and 1 and the probability of 0 is higher for $\rho^i_{A,0}$ and the probability of 1 is higher for $\rho^i_{A,1}$.

The strategy for cheating Alice is the same as in the $F_A = 0$ case. She applies the measurement $\mathcal{M}$ and, then, if she gets 0, continues as in the honest protocol. If she gets 1, she applies the transformation U and then continues as in the honest protocol.

Next, we show that this strategy achieves the result 0 with the probability given by the formula (6).

Let $|\psi'_0\rangle$ and $|\psi'_1\rangle$ denote the (unnormalized) remaining states when the outcome of the measurement $\mathcal{M}$ is 0 and 1, respectively.

Also, let $|\psi_{ab}\rangle$ (for $a, b \in \{0, 1\}$) denote the (unnormalized) remaining states when $|\psi^i_a\rangle$ is measured and the outcome of the measurement is b. Since $|\psi^i\rangle = |\psi^i_0\rangle + |\psi^i_1\rangle$, we have $|\psi'_0\rangle = |\psi_{00}\rangle + |\psi_{10}\rangle$ and $|\psi'_1\rangle = |\psi_{01}\rangle + |\psi_{11}\rangle$.

On the other hand, $|\psi^i_0\rangle = |\psi_{00}\rangle + |\psi_{01}\rangle$ and $|\psi^i_1\rangle = |\psi_{10}\rangle + |\psi_{11}\rangle$. Therefore,

$$\|\psi'_0 - \psi^i_0\| = \|\psi_{10} - \psi_{01}\| \leq \|\psi_{10}\| + \|\psi_{01}\| \leq \sqrt{2(\|\psi_{10}\|^2 + \|\psi_{01}\|^2)}. \tag{8}$$

Similarly to the proof of Lemma 12, $\|\psi_{10}\|^2 + \|\psi_{01}\|^2 \leq \frac{1}{2}\sqrt{F_A}$. Therefore, (8) is at most $\sqrt[4]{F_A}$. We also have $\|\psi'_1 - \psi^i_1\| \leq \sqrt[4]{F_A}$ with the same proof.

Let $\mathcal{H}_0^i$ be the set of bipartite states such that applying the rest of the protocol ($U_k U_{k-1} \ldots U_{i+1}$) and the final measurement at the end of the protocol gives the outcome 0 with probability 1. Then, $|\psi_0^i\rangle \in \mathcal{H}_0^i$. Also, the norm of the projection of $U(|\psi_1^i\rangle)$ on $\mathcal{H}_0^i$ is at least $\sqrt{F_B/2}$ (by (7)).

Consider the norms of the projections of $|\psi_0'\rangle$ and $|\psi_1'\rangle$ on $\mathcal{H}_0^i$. They differ from the norms of $|\psi_0^i\rangle$ and $|\psi_1^i\rangle$ by at most $\|\psi_0' - \psi_0^i\| \leq \sqrt[4]{F_A}$ and $\|\psi_1' - \psi_1^i\| \leq \sqrt[4]{F_A}$. Therefore, the projection of $|\psi_0'\rangle$ on $\mathcal{H}_0^i$ is of norm at least $\frac{1}{\sqrt{2}} - \sqrt[4]{F_A}$ and the projection of $U|\psi_1'\rangle$ is of norm at least $\frac{\sqrt{F_B}}{\sqrt{2}} - \sqrt[4]{F_A}$. This means that the probability of outcome 0 is at least

$$\left(\frac{1}{\sqrt{2}} - \sqrt[4]{F_A}\right)^2 + \left(\frac{\sqrt{F_B}}{\sqrt{2}} - \sqrt[4]{F_A}\right)^2.$$

□

For the purposes of this paper, a weaker form of lemma 13 is sufficient.

Corollary 1 *Let $i \in \{1, \ldots, k-1\}$. Then, there is a strategy for dishonest Alice which achieves the result 0 with probability at least $\frac{1}{2} + \frac{F_B}{2} - 2\sqrt{2}\sqrt[4]{F_A}$.*

Proof: We have

$$\begin{aligned}
&\left(\frac{1}{\sqrt{2}} - \sqrt[4]{F_A}\right)^2 + \left(\frac{\sqrt{F_B}}{\sqrt{2}} - \sqrt[4]{F_A}\right)^2 \\
&= \left(\frac{1}{2} - \sqrt{2}\sqrt[4]{F_A} + \sqrt{F_A}\right) + \left(\frac{F_B}{2} - \sqrt{2}\sqrt{F_B}\sqrt[4]{F_A} + \sqrt{F_A}\right) \\
&\geq \left(\frac{1}{2} - \sqrt{2}\sqrt[4]{F_A}\right) + \left(\frac{F_B}{2} - \sqrt{2}\sqrt[4]{F_A}\right) \\
&= \frac{1}{2} + \frac{F_B}{2} - 2\sqrt{2}\sqrt[4]{F_A}.
\end{aligned}$$

□

Corollary 2 *Assume that the bias of a protocol is at most ϵ. Then, after every round, $F_B \leq 2\epsilon + 6\sqrt[4]{F_A}$ and $F_A \leq 2\epsilon + 6\sqrt[4]{F_B}$.*

Proof: By Lemma 13, Alice can achieve $Pr[0] = \frac{1}{2} + \frac{F_B}{2} - 2\sqrt{2}\sqrt[4]{F_A}$. Because the bias of the protocol is at most ϵ, we must have $\frac{F_B}{2} - 2\sqrt{2}\sqrt[4]{F_A} \leq \epsilon$ and $F_B \leq 2\epsilon + 4\sqrt{2}\sqrt[4]{F_A} \leq 2\epsilon + 6\sqrt[4]{F_A}$.

$F_A \leq 2\epsilon + 6\sqrt[4]{F_B}$ follows similarly. □

Next, we use Corollary 2 to show that the fidelities F_A^i and F_B^i cannot decrease too fast.

Lemma 14 *Assume that a k-round protocol has the bias at most ϵ. Then, for any $i < k$, $F_A^i \leq 14\epsilon^{1/4^{k-i-1}}$ and $F_B^i \leq 14\epsilon^{1/4^{k-i-1}}$.*

Proof: By induction on $k-i$.

Base case. $i=k-1$.

First, remember that $F_A^k = F_B^k = 0$. Let $X \in \{A,B\}$ be the person who sends the message in the k^{th} round and Y be the person who receives the message. Sending away a part of the state can only increase the fidelity. Therefore, $F_X^{k-1} \leq F_X^k = 0$, i.e. $F_X^{k-1} = 0$.

By Corollary 2, $F_Y^{k-1} \leq 2\epsilon + 6\sqrt[4]{F_X^{k-1}} = 2\epsilon < 14\epsilon$.

Inductive case.

We assume that the lemma is true for i and show that it is also true for $i-1$. Similarly to the previous case, let X be the person who sends the message in the i^{th} round and Y be the other person. Then,

$$F_X^{i-1} \leq F_X^i \leq 14\epsilon^{1/4^{k-i-1}}.$$

By Corollary 2,

$$F_Y^{i-1} \leq 2\epsilon + 6\sqrt[4]{14\epsilon^{1/4^{k-i-1}}} \leq (2+6\sqrt[4]{14})\epsilon^{1/4^{k-i}} < 14\epsilon^{1/4^{k-i}}.$$

□

In particular, Lemma 14 implies that $F_A^0 \leq 14\epsilon^{1/4^{k-1}}$. We also have $F_A^0 \geq \frac{1}{16}$ (Lemma 12 and the first paragraph after its proof). Therefore, $14\epsilon^{1/4^{k-1}} \geq \frac{1}{16}$. Taking log of both sides twice gives $k = \Omega(\log\log\frac{1}{\epsilon})$.

7 Conclusion

We have constructed a protocol for quantum coin flipping with bias 0.25 and shown that it is optimal for a restricted class of protocols. We also gave a general lower bound on the number of rounds needed to achieve a bias ϵ. A stronger lower bound has been later shown by Kitaev [18] but our bound also applies to weak coin flipping. The table below summarizes the known results for both strong and weak coin flipping.

	Best protocol	Best lower bound
Strong	0.25 (this paper)	$\frac{1}{\sqrt{2}} - \frac{1}{2} = 0.21...$ [18]
Weak	$\frac{1}{\sqrt{2}} - \frac{1}{2} = 0.21...$ [33]	$\epsilon > 0$, $\Omega(\log\log\frac{1}{\epsilon})$ rounds required (this paper)

The bounds for strong coin flipping are quite close but weak coin flipping is still wide open.

Another interesting question about coin flipping protocols is "cheat-sensitivity" studied by [2, 14, 33]. A protocol is for coin flipping or other cryptographic tasks is cheat-sensitive if a dishonest party cannot increase the probability of one outcome without being detected with some probability. Many quantum protocols display some cheat-sensitivity but it remains to be seen what degree of cheat-sensitivity can be achieved.

8 Acknowledgments

Thanks to Dorit Aharonov, Daniel Gottesman, Alexei Kitaev, Boaz Leslau, Hoi-Kwong Lo, Rashindra Manniesing, Moni Naor, Ashwin Nayak, Louis Salvail, Yaoyun Shi, Rob Spekkens, Amnon Ta-Shma, Umesh Vazirani and Xinlan Zhou for useful comments, discussions and information about related work.

References

[1] D. Aharonov, A. Kitaev, N. Nisan. Quantum circuits with mixed states. *Proceedings of STOC'97*, pp. 20-30.

[2] D. Aharonov, A. Ta-Shma, U. Vazirani, A. Yao. Quantum bit escrow. *Proceedings of STOC'00*, pp. 705-714.

[3] A. Ambainis. A lower bound for a class of weak quantum coin flipping protocols, quant-ph/0204063.

[4] C. Bennett, G. Brassard. Quantum cryptography: public-key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pp. 175-179, Bangalore, India, 1984.

[5] E. Biham, M. Boyer, P. Boykin, T. Mor, V. Roychowdhury. A proof of the security of quantum key distribution. *Proceedings of STOC'00*, pp. 715-724.

[6] M. Blum. Coin flipping by telephone: A protocol for solving impossible problems. *Advances in Cryptology: Report on CRYPTO'81*, pp. 11-15.

[7] E. Bernstein, U. Vazirani. Quantum complexity theory. *SIAM Journal on Computing*, 26:1411-1473, 1997.

[8] C. Crepeau, F. Legare, L. Salvail. How to convert the flavour of a quantum bit commitment. *Proceedings of EUROCRYPT'01*, Lecture Notes in Computer Science, 2045:60-77, Springer, Berlin, 2001.

[9] P. Dumais, D. Mayers, L. Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. *Advances in Cryptology: EUROCRYPT 2000: Proceedings*, Lecture Notes in Computer Science, 1807:300-315, Springer, Berlin, 2000.

[10] C. Fuchs, J. van der Graaf. Cryptographic distinguishability measures for quantum mechanical states. *IEEE Transactions on Information Theory*, 45:1216-1227, 1999.

[11] L. Goldenberg, L. Vaidman, S. Wiesner. Quantum gambling. *Physical Review Letters*, 82:3356-3359, 1999.

[12] D. Gottesman and H.-K. Lo. From quantum cheating to quantum security. *Physics Today*, 53, no. 11, pp. 22-27.

[13] D. Gottesman, D. Simon. Personal communication, January 2001.

[14] L. Hardy, A. Kent. Cheat-sensitive quantum bit commitment, quant-ph/9911043[5].

[15] C. Helstrom. *Quantum Detection and Estimation Theory.* Academic Press, 1976.

[16] R. Jozsa. Fidelity for mixed quantum states. *Journal of Modern Optics*, 41:2315-2323, 1994.

[17] A. Kitaev, personal communication, 2000.

[18] A. Kitaev, personal communication, November 2001.

[19] B. Leslau. Attacks on symmetric quantum coin-tossing protocols, quant-ph/0104075.

[20] H. Lo. Insecurity of quantum secure computations. *Physical Review A*, 56:1154-1162, 1997.

[21] H. Lo, H. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410-3413, 1997.

[22] H. Lo, H. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D*, 120:177-187, 1998.

[23] H. Lo, H. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050-2056, 1999.

[24] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414-3417, 1997.

[25] D. Mayers. Unconditional security in quantum cryptography. *Journal of ACM*, to appear. Also quant-ph/9802025.

[26] D. Mayers, L. Salvail, Y. Chiba-Kohno. Unconditionally secure quantum coin-tossing. quant-ph/9904078.

[27] H. Klauck, A. Nayak, A. Ta-Shma, D. Zuckerman. Interaction in quantum communication complexity and the complexity of set disjointness. *Proceedings of STOC'01*, pp. 124-133.

[28] M. Nielsen. Conditions for a class of entanglement transformations. *Physical Review Letters*, 83:436-439, 1999.

[29] M. Nielsen, I. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2000.

[5]quant-ph preprints are available at `http://www.arxiv.org/archive/quant-ph`

[30] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Computing*, 26:1484-1509, 1997. Also *FOCS'94*.

[31] P. Shor, J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters*, 85:441-444, 2000.

[32] R. Spekkens, T. Rudolph. Degrees of concealment and bindingness in quantum bit commitment protocols. *Physical Review A*, 65:012310, 2002.

[33] R. Spekkens, T. Rudolph. A quantum protocol for cheat-sensitive weak coin flipping. quant-ph/0202118.

[34] Y. Tokunaga, Quantum coin flipping with arbitrary small bias is impossible. quant-ph/0108026.

[35] A. Uhlmann. The 'transition probability' in the state space of *-algebra. *Reports on Mathematical Physics*, 9:273-279, 1976.

[36] Y. Zhang, C. Li, G. Guo. Unconditionally secure quantum coin tossing via entanglement swapping, quant-ph/0012139.