Lower bound for a class of weak quantum coin flipping protocols

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

Abstract
We study the class of protocols for weak quantum coin flipping introduced by Spekkens and Rudolph (quant-ph/0202118). We show that, for any protocol in this class, one party can win the coin flip with probability at least $1/\sqrt{2}$.

1 Introduction
Coin flipping is a cryptographic primitive in which two parties (Alice and Bob) together generate a random bit so that the value of the random bit cannot be controlled by any one party. If both parties are honest, the random bit must be 0 with probability 1/2 and 1 with probability 1/2. If one party is honest but the other is not, the honest party is still guaranteed that the cheater cannot control the outcome.

There are two variants of this requirement. In strong coin flipping, we require that, no matter what a dishonest Alice (dishonest Bob) does, the probability of the result being $a$ is at most $P_A$ (at most $P_B$), for each of the two possible outcomes $a \in \{0, 1\}$. In weak coin flipping, we know in advance that one outcome (say, 0) benefits Alice and the other outcome (say, 1) benefits Bob. Therefore, we only require that dishonest Alice cannot make result 0 with probability more than $P_A$ and dishonest Bob cannot make the result 1 with probability more than $P_B$.

Coin flipping is possible classically with complexity assumptions such as the existence of one-way functions [3]. In an information-theoretic setting (parties with unlimited computational power), in any classical protocol there is a party

*Supported by NSF Grant CCR-9987845 and the State of New Jersey.
which can set the outcome to 0 with certainty and 1 with certainty. Thus, neither of the two variants is possible classically information-theoretically.

In the quantum model, strong coin flipping has been studied by [8, 9, 1, 2, 10, 7, 6]. The best protocol [2, 10] can achieve any combination of $P_A$ and $P_B$ such that $0 \leq P_A$, $0 \leq P_B$, $P_A + P_B = \frac{1}{2}$. In particular, if we want to have the same security guarantees for both parties, we can achieve $P_A = P_B = \frac{4}{7}$. The best known lower bound is that any protocol for strong coin flipping must have $\frac{1}{2} \leq P_A P_B$. If we want to have the same security guarantees for both parties, this gives $P_A = P_B = \frac{1}{\sqrt{2}}$. This is quite close to what is achieved by [2, 10].

Less is known about weak coin flipping. The lower bound of [6] does not apply to weak coin flipping. Thus, we might still have a protocol for weak coin flipping with $P_A = \frac{1}{2} + \epsilon$ and $P_B = \frac{1}{2} + \epsilon$ for an arbitrarily small $\epsilon > 0$. An “exact” protocol with $\epsilon = 0$ is impossible because the impossibility proof for exact protocols from [3] applies to weak coin flipping. Also, we know that if $\epsilon > 0$ is achievable, at least $\Omega(\log \log \frac{1}{\epsilon})$ rounds are needed [2].

Weak coin flipping has been studied by [4, 11]. The first protocol [4] achieved $P_A = P_B \approx 0.327$. [11] described a general class of protocols and showed that this class achieves any combination of $P_A$, $P_B$ such that $0 < P_A \leq 1$, $0 < P_B \leq 1$ and $P_A P_B = \frac{1}{2}$. (The protocol achieving $P_A P_B = \frac{1}{2}$ was also independently discovered by the author of this note.) [11] conjectured that this is the best possible for this class of protocols. In this note, we prove this conjecture.

## 2 A class of protocols

Rudolph and Spekkens [11] considered the following class of protocols for weak coin flipping:

1. Alice prepares a pair of systems in a state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ and sends the system $B$ to Bob.

2. Bob performs the POVM measurement $\{E_0, E_1\}$ on $\mathcal{H}_B$, sends a classical bit $b$ with the outcome of the measurement to Alice.

3. If $b = 0$, Bob sends the system $B$ back to Alice. If $b = 1$, Alice sends the system $A$ to Bob. The party that receives the system then checks whether the joint state of $A$ and $B$ is $|\psi_b\rangle = \frac{I \otimes \sqrt{E_b} |\psi\rangle}{\sqrt{\langle \psi | I \otimes E_b | \psi \rangle}}$ by measuring an observable consisting of $|\psi_b\rangle$ and its orthogonal complement. The possibilities are

   (a) $b = 0$, Alice finds $|\psi_0\rangle$. Bob wins.
   (b) $b = 0$, Alice does not find $|\psi_0\rangle$. Alice has caught Bob cheating.
   (c) $b = 1$, Bob finds $|\psi_1\rangle$. Alice wins.
   (d) $b = 1$, Bob does not find $|\psi_1\rangle$. Bob has caught Alice cheating.
Different choices of $|\psi\rangle$, $E_0$ and $E_1$ give different protocols. [11] showed how to achieve any combination of $0 < P_A \leq 1$, $0 < P_B \leq 1$ such that $P_A P_B = \frac{1}{2}$. They also showed that this is the best possible for this protocol using two-dimensional systems $\mathcal{H}_A$ and $\mathcal{H}_B$ and conjectured that this is the best for $\mathcal{H}_A$ and $\mathcal{H}_B$ of arbitrary dimension. Thus, using qubits would be optimal for this class of protocols, unlike in the known protocols for strong quantum coin flipping [2, 10] where qutrits are needed to achieve the best results.

3 The lower bound

We now prove this conjecture.

Let $P_{A_{\text{max}}}^{\max}(E_0, |\psi\rangle)$ and $P_{B_{\text{max}}}^{\max}(E_0, |\psi\rangle)$ be the maximum probabilities of winning for Alice and Bob, for the given choices of $E_0$ and $|\psi\rangle$. We use the expressions for $P_{A_{\text{max}}}^{\max}$ and $P_{B_{\text{max}}}^{\max}$ shown by [11]:

\[
P_{A_{\text{max}}}^{\max} = 2 Tr(\rho E_0^2), \quad P_{B_{\text{max}}}^{\max} = 2 Tr(\sqrt{\rho E_0 \rho})^2,
\]

where $\rho$ is the density matrix of Bob’s part of $|\psi\rangle$. We will show that the product of these expressions is at least $\frac{1}{2}$. The first step is to show that it is enough to consider the case when the Schmidt decomposition of $|\psi\rangle$ consists of eigenvectors of $E_0$.

Lemma 1 For any choice of $|\psi\rangle$ and $E_0$ in the protocol of [11], there exists $|\tilde{\psi}\rangle$ such that Bob’s part of Schmidt decomposition of $|\tilde{\psi}\rangle$ consists of eigenvectors of $E_0$ and $P_{A_{\text{max}}}^{\max}(E_0, |\psi\rangle) \leq P_{A_{\text{max}}}^{\max}(E_0, |\tilde{\psi}\rangle)$, $P_{B_{\text{max}}}^{\max}(E_0, |\tilde{\psi}\rangle) \leq P_{B_{\text{max}}}^{\max}(E_0, |\psi\rangle)$.

Proof: Let $|\phi_1\rangle, \ldots, |\phi_k\rangle$ be the eigenvectors of $E_0$. Since $E_1 = I - E_0$, they are also eigenvectors of $E_1$. We write the state $|\psi\rangle$ sent by Alice in round 1 as

\[
|\psi\rangle = \sum_{i=1}^{k} \lambda_i |\phi_i\rangle |\phi_i\rangle.
\]

Notice that this is not a Schmidt decomposition because $|\phi_i\rangle$ are not necessarily orthogonal. We consider a protocol in which Alice sends the state

\[
|\tilde{\psi}\rangle = \sum_{i=1}^{k} \lambda_i |i\rangle |\phi_i\rangle
\]

instead of $|\psi\rangle$. We claim that $P_{A_{\text{max}}}^{\max}$ and $P_{B_{\text{max}}}^{\max}$ in this protocol are less than or equal to $P_{A_{\text{max}}}^{\max}$ and $P_{B_{\text{max}}}^{\max}$ when Alice sends $|\psi\rangle$. This is shown by mapping Alice’s and Bob’s cheating strategies from the protocol with $|\tilde{\psi}\rangle$ to the protocol with $|\psi\rangle$. 

3
**Case 1: Alice.** The most general strategy of Alice is to prepare a state

$$|\psi'\rangle = \sum_{i=1}^{k} \mu_i |\varphi'_i\rangle |\phi_i\rangle.$$ 

Bob's measurement splits the state into two parts $|\psi'_0\rangle$ and $|\psi'_1\rangle$. Since $|\phi_i\rangle$ are eigenvectors of $E_0$ and $E_1$,

$$|\psi'_1\rangle = \sum_{i=1}^{k} \mu'_i |\varphi'_i\rangle |\phi_i\rangle.$$ 

After Alice sending her part to Bob, Bob tests the state $|\psi'_1\rangle$ against the state $|\tilde{\psi}_1\rangle$ which would have resulted if Alice had prepared the honest state $|\tilde{\psi}\rangle$. Since $|\tilde{\psi}\rangle$ is a superposition of $|i\rangle |\phi_i\rangle$ and $E_0$, $E_1$ are diagonal in the basis consisting of $|\phi_i\rangle$, $|\psi'_1\rangle$ is a superposition of $|i\rangle |\phi_i\rangle$ as well. Therefore, the inner product between $|\psi'_1\rangle$ and $|\psi_1\rangle$ is maximized if $|\varphi'_i\rangle = |i\rangle$ for all $i$ and, if Alice sends

$$|\psi''\rangle = \sum_{i=1}^{k} \mu_i |i\rangle |\phi_i\rangle$$

instead of $|\psi'\rangle$, this only increases her success probability. To finish the proof, notice that sending the state

$$|\psi'''\rangle = \sum_{i=1}^{k} \mu_i |\varphi_i\rangle |\phi_i\rangle$$

in the protocol for $|\psi\rangle$ achieves the same probability as sending $|\psi''\rangle$ in the protocol for $|\psi\rangle$.

**Case 2: Bob.** An honest Bob's measurement splits $|\tilde{\psi}\rangle$ into states $|\tilde{\psi}_0\rangle$ and $|\tilde{\psi}_1\rangle$. Since $E_0$ and $E_1$ are diagonal in the basis $|\phi_i\rangle$, the state $|\tilde{\psi}_0\rangle$ is of the form

$$|\tilde{\psi}_0\rangle = \sum_{i=1}^{k} a_i |i\rangle |\phi_i\rangle.$$ 

A dishonest Bob's most general strategy is to transform the state $|\tilde{\psi}\rangle$ into a state having maximum overlap with $|\tilde{\psi}_0\rangle$. Since he cannot access $|i\rangle$, the state having maximum overlap is just $|\tilde{\psi}\rangle$. Therefore, Bob's best strategy is just to leave $|\tilde{\psi}\rangle$ unchanged, claim $b = 0$ and send his part of the state back to Alice. The same success probability can be achieved by Bob in the protocol for $|\psi\rangle$ by a similar strategy (claim $b = 0$ and send the state back). □

Similarly to [11], let $\rho$ be the density matrix of Bob's side of $|\psi\rangle$. We write density matrices $\rho$ and $E_0$ in the basis consisting of $|\psi_i\rangle$. Both matrices are
diagonal in this basis. Let $a_i$ be the elements on the diagonal of $\rho$ and $b_i$ be the elements on the diagonal of $E_0$. Then,

$$P_A^{\max} = 2 \text{Tr}(\rho E_0^2) = 2 \sum_{i=1}^{k} a_i b_i^2,$$

$$P_B^{\max} = 2 \text{Tr}(\sqrt{\rho E_0} \rho) = 2 \sqrt{\sum_{i=1}^{2} a_i \sqrt{b_i}}^2$$

and we have the extra constraint that $\text{Tr}(\rho E_0) = \sum_i a_i b_i = \frac{1}{2}$ (because the outcome of an honest coin flip is 0 with probability $1/2$).

By Holder’s inequality, we have $\|x\|_3 \|y\|_3 \geq \langle x | y \rangle$ and $\|x\|_3 \|y\|_3 \geq \langle x | y \rangle^3$ for any vectors $x$, $y$. Applying this inequality to $x = (a_i^{1/3} b_i^{2/3})_{i=1}^{k}$ and $y = (a_i^{2/3} b_i^{1/3})_{i=1}^{k}$ gives us

$$P_A^{\max} P_B^{\max} = 4 \sum_{i=1}^{k} a_i b_i^2 \left( \sum_{i=1}^{k} a_i \sqrt{b_i} \right)^2 \geq 4 \left( \sum_{i=1}^{k} a_i b_i \right)^3 = 4 \left( \frac{1}{2} \right)^{3} = \frac{1}{2}.$$

4 Conclusion

We have shown that any choice of parameters in the protocol of [11] gives $P_A^{\max} P_B^{\max} \geq \frac{1}{2}$. Curiously, this is the same as the lower bound of [6] for arbitrary protocols for strong coin flipping. However, there does not seem to be any direct connection between the two results. It remains open whether a different protocol (not in the class described above) for weak coin flipping could achieve a better security.

Another interesting question about coin flipping protocols is “cheat-sensitivity” studied by [1, 5, 11]. A protocol 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.

Acknowledgment. Thanks to Terry Rudolph for useful comments.

References

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

[2] A. Ambainis. A new protocol and lower bounds for quantum coin flipping. Proceedings of STOC’01.
[3] M. Blum. Coin flipping by telephone: A protocol for solving impossible problems. *Advances in Cryptology: Report on CRYPTO’81*, pp. 11-15.

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

[5] L. Hardy, A. Kent. Cheat-sensitive quantum bit commitment, [quant-ph/9911043](https://arxiv.org/abs/quant-ph/9911043).

[6] A. Kitaev. Personal communication, November 2001.

[7] B. Leslau. Attacks on symmetric quantum coin-tossing protocols, [quant-ph/0104073](https://arxiv.org/abs/quant-ph/0104073).

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

[9] D. Mayers, L. Salvail, Y. Chiba-Kohno. Unconditionally secure quantum coin-tossing, [quant-ph/9904078](https://arxiv.org/abs/quant-ph/9904078).

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

[11] R. Spekkens, T. Rudolph. A quantum protocol for cheat-sensitive weak coin flipping, [quant-ph/0202118](https://arxiv.org/abs/quant-ph/0202118).