Quantum Cyber Security
Lecture 12: Quantum Coin Flipping

Petros Wallden

University of Edinburgh

6th March 2025

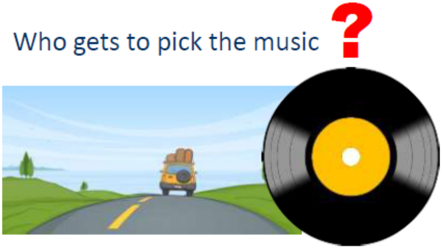
This Lecture: Quantum Coin-flipping

1. Motivation and Definition
2. Classical Coin-Flipping (impossibility)
3. Quantum Coin-Flipping
4. Protocols
5. Weak Coin-Flipping
6. Implementations

Motivation

Coin Flipping

Two distant people, need to decide e.g. who will pick the music!



- Cryptographic task (people have incentive to cheat)
- Introduced formally by Blum 1983

Definition

(Strong) Coin Flipping

The task of coin flipping consists of two mutually distrustful players, Alice and Bob, and the goal is for both players to output the same random bit $c \in \{0, 1\}$ such that the following properties hold

1. **Correctness:** if both Alice and Bob are honest then c is uniformly distributed: $p(c = 0) = p(c = 1) = 1/2$.
2. ϵ**-secure:** neither player can force $p(c = 0) \geq 1/2 + \epsilon$ or $p(c = 1) \geq 1/2 + \epsilon$, where $p(c)$ is the probability that the honest player outputs a value c.

   The smallest ϵ a protocol is ϵ-secure is called the **bias**.

Q: Is Information Theoretic Secure coin flipping possible?

An (insecure) classical coin flipping protocol

- Alice picks a random bit $a \leftarrow \{0, 1\}$
- Alice send a to Bob
- Bob picks a random bit $b \leftarrow \{0, 1\}$
- Bob sends b to Alice

An (insecure) classical coin flipping protocol

- Alice picks a random bit $a \leftarrow \{0, 1\}$
- Alice send a to Bob
- Bob picks a random bit $b \leftarrow \{0, 1\}$
- Bob sends b to Alice
- Both return $c := a \oplus b$

An (insecure) classical coin flipping protocol

- Alice picks a random bit $a \leftarrow \{0,1\}$
- Alice send a to Bob
- Bob picks a random bit $b \leftarrow \{0,1\}$
- Bob sends b to Alice
- Both return $c := a \oplus b$

  The protocol is **correct**, bit is **NOT secure** (at all)

An (insecure) classical coin flipping protocol

- Alice picks a random bit $a \leftarrow \{0, 1\}$
- Alice send a to Bob
- Bob picks a random bit $b \leftarrow \{0, 1\}$
- Bob sends b to Alice
- Both return $c := a \oplus b$

  The protocol is **correct**, bit is **NOT secure** (at all)

- Why is this protocol insecure?

An (insecure) classical coin flipping protocol

- Alice picks a random bit $a \leftarrow \{0, 1\}$
- Alice send a to Bob
- Bob picks a random bit $b \leftarrow \{0, 1\}$
- Bob sends b to Alice
- Both return $c := a \oplus b$

  The protocol is **correct**, bit is **NOT secure** (at all)

- Why is this protocol insecure?
- Bob can select his bit after seeing Alice's and can bias the coin as he desires!

Impossibility of classical coin flipping

Impossibility of classical info theoretic secure coin flipping [Blum83]

No classical coin flipping protocol is secure, i.e. no value of $\epsilon < 1/2$ can be achieved for security!

- If Alice can't bias then Bob can completely bias the coin

Impossibility of classical coin flipping

Impossibility of classical info theoretic secure coin flipping [Blum83]

No classical coin flipping protocol is secure, i.e. no value of $\epsilon < 1/2$ can be achieved for security!

- If Alice can't bias then Bob can completely bias the coin
- Assume a protocol of n-rounds of interaction
- Let k be the last round that the value of c is not fixed
- The party that runs round k can fully bias the outcome

Classical Coin Flipping under Assumptions

- Coin Flipping is possible with computational assumptions
- An example is assuming the existence of secure one-way functions (OWF), [Blum 83]
- **OWF**: A function f that can be computed efficiently but cannot be inverted efficiently

  (efficiently is understood as "in poly-time")

Classical Coin Flipping under Assumptions

- Coin Flipping is possible with computational assumptions
- An example is assuming the existence of secure one-way functions (OWF), [Blum 83]
- **OWF**: A function f that can be computed efficiently but cannot be inverted efficiently

  (efficiently is understood as "in poly-time")
- Alice chooses bit a and string r randomly
- Alice sends to Bob $f(a, r) = d$ (commits a)
- Bob chooses bit b and sends it to Alice
- Alice announces a, r to Bob
- Bob checks that $f(a, r) = d$ and if yes they proceed
- They both return $c = a \oplus b$

General Idea

- Alice 'commits' to a bit a sending $\mathrm{commit}(a) = d$ to Bob
- Bob sends his bit b to Alice
- Alice reveals her commitment $\mathrm{reveal}(d) = a$
- Bob (if reveal is compatible with the commitment) accepts to proceed (otherwise aborts)
- Both output $c = a \oplus b$

General Idea

- Alice 'commits' to a bit a sending $\mathrm{commit}(a) = d$ to Bob
- Bob sends his bit b to Alice
- Alice reveals her commitment $\mathrm{reveal}(d) = a$
- Bob (if reveal is compatible with the commitment) accepts to proceed (otherwise aborts)
- Both output $c = a \oplus b$

\- Commitment is impossible (classically or quantumly) with ITS, but quantumly can achieve protocol with non-trivial bias ϵ using this idea

Quantum Coin Flipping

- Quantum transcript of a round contains information that may not be "extractible"
- Can (partly) evade the problem that there is a round that after that round (and not earlier) the output bit is determined
- Alice attempts to (partially) commit to message by encoding to a quantum state
- Cannot achieve zero bias, but can achieve $\epsilon < 1/2$
- Recall, bias $\epsilon < 1/2$ is defined as the largest probability that any of the two players can bias the coin towards one outcome.

Qubit QCF protocol (Aharanov 2000)

- Family of protocols, one for each choice ϕ
- Define the states $|\phi_{x,a}\rangle$ (note x is the basis bit, a the 'outcome' bit, check orthogonality!):

$$|\phi_{0,0}\rangle = \cos\phi\,|0\rangle + \sin\phi\,|1\rangle \;\; ; \;\; |\phi_{0,1}\rangle = \sin\phi\,|0\rangle - \cos\phi\,|1\rangle$$

$$|\phi_{1,0}\rangle = \cos\phi\,|0\rangle - \sin\phi\,|1\rangle \;\; ; \;\; |\phi_{1,1}\rangle = \sin\phi\,|0\rangle + \cos\phi\,|1\rangle$$

Qubit QCF protocol (Aharanov 2000)

- Family of protocols, one for each choice ϕ
- Define the states $|\phi_{x,a}\rangle$ (note x is the basis bit, a the 'outcome' bit, check orthogonality!):

$$|\phi_{0,0}\rangle = \cos\phi\,|0\rangle + \sin\phi\,|1\rangle \;\; ; \;\; |\phi_{0,1}\rangle = \sin\phi\,|0\rangle - \cos\phi\,|1\rangle$$

$$|\phi_{1,0}\rangle = \cos\phi\,|0\rangle - \sin\phi\,|1\rangle \;\; ; \;\; |\phi_{1,1}\rangle = \sin\phi\,|0\rangle + \cos\phi\,|1\rangle$$

- Alice chooses two bit $a, x \leftarrow \{0, 1\}$
- Alice prepares the state $|\phi_{x,a}\rangle$
- Bob sends his bit b
- Alice reveals x, a, Bob meas. in x-basis, checks if he gets a
- They return $c = a \oplus b$

Cheating probabilities and ϵ-bias

- ϵ-bias: $\epsilon + 1/2 = \max\{Pr(\text{Alice win}), Pr(\text{Bob win})\}$
- **Alice to cheat:** Preparing the wrong states (different, non-uniform random); giving wrong information about (x, a)
- **Bob to cheat:** Try to determine (x, a) from Alice's states, and reveal some info on Alice's choice before he gives his bit b

Cheating probabilities and ϵ-bias

- ϵ-bias: $\epsilon + 1/2 = \max\{Pr(\text{Alice win}), Pr(\text{Bob win})\}$
- **Alice to cheat:** Preparing the wrong states (different, non-uniform random); giving wrong information about (x, a)
- **Bob to cheat:** Try to determine (x, a) from Alice's states, and reveal some info on Alice's choice before he gives his bit b

Aharanov's Protocol Security

The protocol is ϵ-secure with bias at most 0.42

Cheating probabilities and ϵ-bias

- ϵ-bias: $\epsilon + 1/2 = \max\{Pr(\text{Alice win}), Pr(\text{Bob win})\}$
- **Alice to cheat:** Preparing the wrong states (different, non-uniform random); giving wrong information about (x, a)
- **Bob to cheat:** Try to determine (x, a) from Alice's states, and reveal some info on Alice's choice before he gives his bit b

Aharanov's Protocol Security

The protocol is ϵ-secure with bias at most 0.42

- For different ϕ's the two probabilities scale inversely
- For $\phi = \frac{\pi}{8}$, we have the best bias that leads to $Pr(\text{Alice win}) \leq 0.914$ and $Pr(\text{Bob win}) \leq 0.86$

Bob's optimal cheating probabilities

- Bob want to distinguish two cases: $a = 0$ and $a = 1$, without any information on x.
- $\rho_{a=0} = \frac{1}{2}(|\phi_{0,0}\rangle \langle\phi_{0,0}| + |\phi_{1,0}\rangle \langle\phi_{1,0}|)$
- $\rho_{a=1} = \frac{1}{2}(|\phi_{0,1}\rangle \langle\phi_{0,1}| + |\phi_{1,1}\rangle \langle\phi_{1,1}|)$

Bob's optimal cheating probabilities

- Bob want to distinguish two cases: $a = 0$ and $a = 1$, without any information on x.
- $\rho_{a=0} = \frac{1}{2}(|\phi_{0,0}\rangle \langle\phi_{0,0}| + |\phi_{1,0}\rangle \langle\phi_{1,0}|)$
- $\rho_{a=1} = \frac{1}{2}(|\phi_{0,1}\rangle \langle\phi_{0,1}| + |\phi_{1,1}\rangle \langle\phi_{1,1}|)$
- Maximum distinguishing probability:

$$p_{dist}^{opt} = \frac{1}{2} + \frac{1}{2} T(\rho_{a=0}, \rho_{a=1}) = \frac{1}{2} + \frac{1}{4} \|\rho_{a=0} - \rho_{a=1}\|$$

Bob's optimal cheating probabilities

- Bob want to distinguish two cases: $a = 0$ and $a = 1$, without any information on x.
- $\rho_{a=0} = \frac{1}{2}(|\phi_{0,0}\rangle\langle\phi_{0,0}| + |\phi_{1,0}\rangle\langle\phi_{1,0}|)$
- $\rho_{a=1} = \frac{1}{2}(|\phi_{0,1}\rangle\langle\phi_{0,1}| + |\phi_{1,1}\rangle\langle\phi_{1,1}|)$
- Maximum distinguishing probability:

  $p_{dist}^{opt} = \frac{1}{2} + \frac{1}{2}T(\rho_{a=0}, \rho_{a=1}) = \frac{1}{2} + \frac{1}{4}\|\rho_{a=0} - \rho_{a=1}\|$

  $\rho_0 = \cos^2\phi\,|0\rangle\langle 0| + \sin^2\phi\,|1\rangle\langle 1|\ ;\ \rho_1 = \sin^2\phi\,|0\rangle\langle 0| + \cos^2\phi\,|1\rangle\langle 1|$
- $\|\rho_0 - \rho_1\| = 2\cos 2\phi$
- $Prob(\mathrm{Bob\ win}) \leq \frac{1}{2} + \frac{\cos 2\phi}{2}$
- Choosing $\phi = \pi/8$ (optimal to minimise Alice's probability): $Prob(\mathrm{Bob\ win}) \approx 0.853$

Qutrit QCF protocol (Ambainis 2004)

- We consider qutrits (dim 3): $\{|0\rangle, |1\rangle, |2\rangle\}$
- Consider the four states (two pairs of orthogonal) $|\phi_{x,a}\rangle$:

$$|\phi_{0,0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \; ; \; |\phi_{0,1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\phi_{1,0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle) \; ; \; |\phi_{1,1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle)$$

Qutrit QCF protocol (Ambainis 2004)

- We consider qutrits (dim 3): $\{|0\rangle, |1\rangle, |2\rangle\}$
- Consider the four states (two pairs of orthogonal) $|\phi_{x,a}\rangle$:

$$|\phi_{0,0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \;;\; |\phi_{0,1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|\phi_{1,0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |2\rangle) \;;\; |\phi_{1,1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle)$$

- Alice chooses two bit $a, x \leftarrow \{0, 1\}$
- Alice prepares the state $|\phi_{x,a}\rangle$
- Bob sends his bit b
- Alice reveals x, a, Bob meas. in x-basis, checks if he gets a
- Note: $\{|\phi_{0,a}\rangle, |2\rangle\}$ and $\{|\phi_{1,a}\rangle, |1\rangle\}$ are bases
- They return $c = a \oplus b$

Optimal biases for QCF

- Ambainis protocol is secure with $\epsilon = 0.25$
- (Both Alice and Bob can cheat with at most prob 0.75)
- Aharanov protocol had bias $\epsilon = 0.42$

Optimal biases for QCF

- Ambainis protocol is secure with $\epsilon = 0.25$
- (Both Alice and Bob can cheat with at most prob 0.75)
- Aharanov protocol had bias $\epsilon = 0.42$

Impossibility of Strong Quantum Coin Flipping

Perfect ($\epsilon \approx 0$) strong coin flipping is impossible for quantum protocols

Optimal biases for QCF

- Ambainis protocol is secure with $\epsilon = 0.25$
- (Both Alice and Bob can cheat with at most prob 0.75)
- Aharanov protocol had bias $\epsilon = 0.42$

Impossibility of Strong Quantum Coin Flipping

Perfect ($\epsilon \approx 0$) strong coin flipping is impossible for quantum protocols

- Kitaev proved that QCF need to have at least $\epsilon = \frac{\sqrt{2}-1}{2} \approx 0.207$ bias

Weak (quantum) coin flipping

Definition: Weak Coin Flipping

Same as strong CF, except the security where: **Alice** cannot force $p(c = 0) \geq 1/2 + \epsilon$, and **Bob** cannot force $p(c = 1) \geq 1/2 + \epsilon$.

- In other words, Alice/Bob cannot bias the coin in their favour (but could bias it in the other person's favour)

Weak (quantum) coin flipping

Definition: Weak Coin Flipping

Same as strong CF, except the security where: **Alice** cannot force $p(c=0) \geq 1/2 + \epsilon$, and **Bob** cannot force $p(c=1) \geq 1/2 + \epsilon$.

- In other words, Alice/Bob cannot bias the coin in their favour (but could bias it in the other person's favour)
- Weak Coin Flipping with arbitrarily small (non-zero) bias ϵ is:
  - Impossible Classically
  - Possible Quantumly

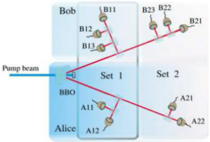
Weak (quantum) coin flipping

Definition: Weak Coin Flipping

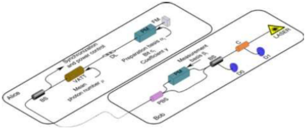
Same as strong CF, except the security where: **Alice** cannot force $p(c = 0) \geq 1/2 + \epsilon$, and **Bob** cannot force $p(c = 1) \geq 1/2 + \epsilon$.

- In other words, Alice/Bob cannot bias the coin in their favour (but could bias it in the other person's favour)
- Weak Coin Flipping with arbitrarily small (non-zero) bias ϵ is:
  - Impossible Classically
  - Possible Quantumly
- Rounds of interaction required scale as $N \sim 1/\epsilon$ at best
- Practical protocol with $\epsilon = 1/10$ exists, but open question to design protocol for arbitrarily small bias

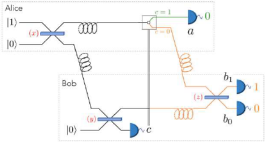
Experimental Implementations



Implementation of Ambainis' protocol:
Molina-Terriza, G., Vaziri, A., Ursin, R., & Zeilinger, A. (2005). Experimental quantum coin tossing. *PRL*



Implementation of a practical coin flipping protocol by Pappa & Chailloux:
Pappa, A., Jouguet, P., Lawson, T., Chailloux, A., Legré, M., Trinkler & Diamanti, E. (2014). Experimental plug and play quantum coin flipping. *Nature communications*



Implementation of weak coin flipping:
Bozzio, M., Chabaud, U., Kerenidis, I., & Diamanti, E. (2020). Quantum weak coin flipping with a single photon. *PRA*

Some references and further reading

- Introduction to Quantum Cryptography by Thomas Vidick and Stephanie Wehner: chapter 10, 10.1

Blu83 Manuel Blum. "Coin flipping by telephone a protocol for solving impossible prob- lems". In: ACM SIGACT News 15.1 (1983), pages 23–27.

Cle+86 R. Cleve. Limits on the security of coin flips when half the processors are faulty. In Proceedings of the 18th Annual ACM Symposium on Theory of Computing, pages 364–369, 1986.

Cle+93 Cleve R, Impagliazzo R. Martingales, collective coin flipping and discrete control processes. other words. 1993 Nov;1(5):8.

Aha+00 Dorit Aharonov et al. "Quantum bit escrow". In: Proceedings of the thirty-second annual ACM symposium on Theory of computing. ACM. 2000, pages 705–714

Amb01 Andris Ambainis. "A new protocol and lower bounds for quantum coin flipping". In: Proceedings of the thirty-third annual ACM symposium on Theory of computing. ACM. 2001, pages 134–142.

GW07 Gus Gutoski and John Watrous. "Toward a general theory of quantum games". In: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing. ACM. 2007, pages 565–574

Moc07 Carlos Mochon. "Quantum weak coin flipping with arbitrarily small bias". In: arXiv preprint arXiv:0711.4114 (2007)

Aha+16 Dorit Aharonov et al. "A Simpler Proof of the Existence of Quantum Weak Coin Flipping with Arbitrarily Small Bias". In: SIAM Journal on Computing 45.3 (2016), pages 633–679.

CK09 André Chailloux and Iordanis Kerenidis. "Optimal quantum strong coin flipping". In: Foundations of Computer Science, 2009. FOCS'09. 50th Annual IEEE Symposium on. IEEE. 2009, pages 527–533.

Aro+19 Arora AS, Roland J, Weis S. Quantum weak coin flipping. InProceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing 2019 (pp. 205-216).