Quantum Cyber Security
Lecture 10: Other QKD and similar protocols

Mina Doosti
In this lecture…

We learn about:

- Coin flipping task and motivation
- Classical coin flipping
- Quantum coin flipping
- Simple quantum protocols for coin flipping
- Quantum coin flipping with qutrits
- Bounds on strong coin flipping
- Weak quantum coin flipping
- Implementations of quantum coin flipping
Coin flipping task and motivation

This is the task of a coin flipping protocol!
Coin flipping was introduced by Blum in 1983

Who gets to pick the music?

They need a protocol to agree on a random bit
But they don’t trust each other!
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 $b$ is uniformly distributed: $p(c = 0) = p(c = 1) = 1/2$.

2. **$\epsilon$-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 $\epsilon$ for which a protocol is $\epsilon$-secure is called the **bias**.

Note: Coin flipping is a completely randomized primitive. There is no fixed function that determines the outputs of the players.

**Question**: Is unconditionally secure coin flipping possible?
Unconditionally secure coin flipping?

Impossibility of classical unconditionally secure coin flipping [Blum83]:
No classical coin flipping protocol is secure, i.e. no value of $\varepsilon < 1/2$ can be achieved for security!

If Alice cannot completely bias the output of the protocol, Bob can (and vice versa)
A classical coin flipping protocol

1. Alice flips a random bit $a \in \{0, 1\}$ and sends it to Bob.

2. Bob flips a random bit $b \in \{0, 1\}$ and sends it to Alice.

3. Both return $c = a \oplus b$.

The protocol is correct

But not at all secure!

**Question:**
Why this protocol is not secure?

Bob sees Alice’s message before sending his message, so he can always force his favorite bit value.
Some intuition about the impossibility

There is some sort of asymmetry between Alice and Bob in any coin flipping protocol...

The order matters!

The outcome $c$ (regardless of the value) has to be determined after certain number of rounds in the protocol consisting of sending some messages. One can always find a message such that, before the message is sent, the outcome is not yet determined, but once the message has been sent it is.

That is why, the player who sends that message (or in other words, knows more) has the ability to bias the outcome to any possibility.
There exists a coin flipping protocol, assuming perfectly secure One Way Function (OWF) exists [Blum83]

**Blum’s coin flipping protocol based on OWF:**

Alice and Bob agree on some perfectly secure 1-1 OWF $f$, before the protocol

- Alice selects $x$, sends $f(x)$ to Bob
- Bob needs to guess some non-trivial property of $x$ from $f(x)$ (for instance if $x$ is even or odd) – which he can’t better than random because of the properties of OWF, so Bob has to also flip a coin, which will be a random bit
- Then Alice will convince Bob by revealing $x$

Cleve [Cleve 89,93] showed that for any two-party $r$-round coin-flipping protocol there exists an efficient adversary that can bias the output of the honest party by $\Omega(1/r)$
How about quantum coin flipping?
Now let Alice and Bob be **quantum** players!

**Question:** Why going to quantum regime might help?

The notion of **transcript** in the quantum case is less clear, because quantum states have interesting properties. One cannot easily determine a quantum message.

To determine the outcome of a quantum message you need measurements!
Aharonov’s quantum coin flipping protocols

Introduced by Aharonov’s (2000)

\[
|\phi_{x,a}\rangle = \begin{cases} 
|\phi_{x,0}\rangle = \cos \phi |0\rangle + (-1)^x \sin \phi |1\rangle \\
|\phi_{x,1}\rangle = \sin \phi |0\rangle + (-1)^{x\oplus 1} \cos \phi |1\rangle 
\end{cases}
\]

1. Alice selects two random bits \(x\) and \(a\) (\(a\) is Alice’s main bit)
2. Alice prepares a state \(|\phi_{x,a}\rangle\) based on her choice and sends to Bob
3. Bob also selects his random bit \(b\) and sends to Alice
4.a. Alice sends the random bits to Bob and Bob measures the qubit in the suitable basis
4.b. Bob sends back the qubit and Alice measures and verifies

\[c = a \oplus b\]
Security of Aharonov’s coin flipping protocol

**Cheating strategies for Alice:**
Preparing the wrong states (not according to uniform distribution) to bias the bit, or giving wrong information about \((x,a)\) to Bob

**Cheating strategies for Bob:**
Try to determine \(x, a\) (learn Alice’s bit) before she reveals them classically

**Theorem (Aharonov’s protocol security):**
The protocol is \(\varepsilon\)-secure with \(\varepsilon\) bias at most 0.42

\[
\Pr[\text{Alice win}] \leq 0.914 \\
\Pr[\text{Bob win}] \leq 0.86
\]

For optimal \(\phi = \frac{\pi}{8}\)
Why it is secure? Let’s say Bob is cheating…

 Compared to the classical protocol, Alice does not **fully** reveal her bit, before Bob sends his bit.

 To bound Bob’s success probability, we need to look at the mixture of the state Alice prepares.

\[
\rho_{a=0} = \frac{1}{2}(|\phi_{0,0}\rangle\langle\phi_{0,0}| + |\phi_{1,0}\rangle\langle\phi_{1,0}|)
\]

\[
\rho_{a=1} = \frac{1}{2}(|\phi_{0,1}\rangle\langle\phi_{0,1}| + |\phi_{1,1}\rangle\langle\phi_{1,1}|)
\]

This is a “State discrimination problem” between two density matrices (ensembles).

To do this, one needs to find the **best POVM**, that has the least error to distinguish between the two states.

**Holevo-Helstrom bound**: The optimal probability of distinguishing between two density matrices which have been picked with equal probability, is given by this bound:

\[
P_{\text{disc}}^{\text{opt}} = \frac{1}{2} + \frac{1}{4} \|\rho_1 - \rho_2\|_{\text{tr}}
\]
Let's calculate the Holevo bound!

\[ \Phi_{00} = \cos \psi |00\rangle + \sin \psi |11\rangle \]
\[ \Phi_{10} = \cos \psi |10\rangle - \sin \psi |11\rangle \]
\[ \Phi_{01} = \sin \psi |00\rangle - \cos \psi |11\rangle \]
\[ \Phi_{11} = \sin \psi |00\rangle + \cos \psi |11\rangle \]

\[ \rho_0 = \frac{1}{2} (\Phi_{00} \times \Phi_{00} + \Phi_{10} \times \Phi_{10}) \]
\[ = \frac{1}{2} (\cos^2 \psi |00\rangle \langle 00| + \sin^2 \psi |11\rangle \langle 11| + \sin \psi \cos \psi (|00\rangle \langle 01| + |11\rangle \langle 10|) + \cos^2 \psi |00\rangle \langle 00| + \sin^2 \psi |11\rangle \langle 11| - \sin \psi \cos \psi (|00\rangle \langle 11| + |11\rangle \langle 00|)) \]
\[ = \cos^2 \psi |00\rangle \langle 00| + \sin^2 \psi |11\rangle \langle 11| \]

Similarly, \[ \rho_1 = \sin^2 \psi |00\rangle \langle 00| + \cos^2 \psi |11\rangle \langle 11| \]

\[ \rho_0 - \rho_1 = (\cos^2 \psi - \sin^2 \psi) |00\rangle \langle 00| + (\sin^2 \psi - \cos^2 \psi) |11\rangle \langle 11| = \begin{pmatrix} \cos 2\psi & 0 \\ 0 & -\cos 2\psi \end{pmatrix} \]

\[ \lambda_1 = \cos 2\psi \quad \lambda_2 = -\cos 2\psi \]

\[ \| \rho_0 - \rho_1 \|_tr = \sum_i |\lambda_i| = 2 \cos 2\psi \]

\[ \| \rho_{a=0} - \rho_{a=1} \| = 2 \cos 2\psi \]

Optimal \( \psi = \frac{\pi}{8} \)

\[ Pr[\text{Bob cheat}] \leq \frac{1}{2} + \frac{\cos 2\phi}{2} \approx 0.853 \]
Another similar protocol was introduced by Ambainis (2004) with a better bias:

\[
|\phi_{a,x}\rangle = \begin{cases} 
\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & a = 0, x = 0 \\
\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & a = 0, x = 1 \\
\frac{1}{\sqrt{2}}(|0\rangle + |2\rangle) & a = 1, x = 0 \\
\frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) & a = 1, x = 1 
\end{cases}
\]

\[|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad |2\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}\]

**Ambainis’s coin flipping protocol:**
1. Alice selects \(x \in \{0, 1\}\) and \(a \in \{0, 1\}\) uniformly at random and sends \(|\phi_{a,x}\rangle\) to Bob.
2. Bob selects \(b \in \{0, 1\}\) uniformly at random and sends \(b\) to Alice.
3. Alice sends \(a\) and \(x\) to Bob.
4. Bob verifies the state he received from Alice in step 1. is \(|\phi_{a,x}\rangle\), if it is not the case then he declares that Alice has been cheating and aborts the protocol.
5. Both players return the outcome \(c = a \oplus b\)
Security of Ambainis coin flipping protocol

**Theorem (Security of Ambainis protocol):**
The protocol is $\varepsilon$-secure with $\varepsilon$ bias 0.25

As an exercise, compute the mixed state $\rho_0$ and $\rho_1$ for this protocol similar to the previous case (They are 3x3 density matrices).

Holevo bound $\rightarrow$ $P_r[\text{Bob cheating}] = \frac{1}{2} + \frac{1}{4} \times 1 = \frac{3}{4}$

How about Alice cheating?

Bounding success probability of Alice is harder because she can prepare arbitrary states (for instance entangled with other information), which she can use later to cheat, after Bob reveals.

To bound Alice’s success probability, we need to “symmetrize” Alice’s strategy. There is a strategy for dishonest Alice, leading to a density matrix of certain form for which Alice achieves $a=b$ with the same probability.

But again, it can be shown that for that symmetric density matrix Alice can at most cheat with probability $\frac{3}{4}$
Can we do much better? Can we design a quantum protocol that achieves arbitrary small bias using quantum information?

No!
perfectly secure strong coin-flipping is also impossible for quantum protocols.

**Kitaev’s bound for strong coin flipping:**
The smallest bias any strong coin flipping protocol can achieve is

\[ \varepsilon = \frac{\sqrt{2} - 1}{2} \approx 0.207. \]

The proof is not easy... It relies on Linear Programing (LP) and Semidefinite Programming (SDP).
If the choice of Alice and Bob is pre-determined, we can relax the security requirement:

**Weak coin flipping:**

Weak coin flipping is similar to strong coin flipping except that we only require that malicious Alice cannot force \( p(c = 0) \geq 1/2 + \varepsilon \), and malicious Bob cannot force \( p(c = 1) \geq 1/2 + \varepsilon \)

It has been shown that weak quantum coin flipping, with arbitrarily small (but non-zero) bias \( \varepsilon \), is possible (by Mochon in 2007)

But the protocol that achieves this arbitrary small bias is complicated and requires multiple rounds that scales exponentially with \( \frac{1}{\varepsilon} \). Designing concrete protocols with arbitrary small bias is still open research problem (Almost solved by Arora et al. (2019) for protocols with bias around 1/10)
Can we implement these protocols?

Just to satisfy your curiosity ;)

Implementation of Ambainis’ protocol:

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

Implementation of a practical coin flipping protocol by Pappa & Chailloux:
1. Introduction to Quantum Cryptography by *Thomas Vidick and Stephanie Wehner*: chapter 10, 10.1

**Extra materials:**