Quantum Cryptography beyond Key distribution

Quantum key distribution (QKD) - importance

There are others

Alice and Bob - no Eve

How an honest Alice (or Bob) will protect against a dishonest Bob (or Alice)?

Coin Flipping

Blum 1980

Alice (Europe) Bob (America)

Tossing a coin $c \in \{0, 1\}$

they need to exchange the information by classical (or quantum) communication.

Can we find a good protocol?

- To ensure neither can bias the coin too much

$$p(c=0) \approx p(c=1) \approx \frac{1}{2}$$

(strong coin flipping)

Strong coin flipping is a two party task between Alice and Bob. The goal is for both parties to output the same value $c \in \{0,1\}$ such that the following properties hold.

- Correctness: If both Alice and Bob are honest, then c is uniformly distributed:
$$p(c=0) = p(c=1) = \frac{1}{2}.$$
- ε-secure: If Alice (or Bob) is honest, then Bob (or Alice) cannot bias the coin by more than ε:
$$\frac{1}{2} - \varepsilon \leq p(c=0), \quad p(c=1) < \frac{1}{2} + \varepsilon$$
where $p(c)$ is the probability that the honest party outputs the value c.

The smallest ε for which a protocol is ε-secure is called the strong coin flipping bias.

- We are overshooting the goal a little:
- Both Alice and Bob wants to win.
  Let's say, $c=0$ Alice wins
  $c=1$ Bob wins
  A protocol would need to assure
  Alice cannot force $p(c=0) > 1/2 + \varepsilon$
  Bob cannot force $p(c=1) > \frac{1}{2} + \varepsilon$
  } → leads to a weaker protocol.

Weak coin flipping is a two-party task between Alice and Bob. Neither party has an input. The goal is for both parties to output the same value $c \in \{0,1\}$ such that the following properties hold:

- Correctness: If both Alice and Bob are honest, then c is uniformly distributed:

$$\Pr(c=0) = \Pr(c=1) = 1/2.$$

- ε-secure: If Alice is honest, then $\Pr(c=0) \leq \frac{1}{2} + \varepsilon$.
If Bob is honest, then $\Pr(c=1) \leq \frac{1}{2} + \varepsilon$.

As before, the smallest ε for which a protocol is ε-secure is called the weak coin flipping bias of the protocol.

While the second definition is clearly less demanding than the first, it is not immediately clear that either definition can be satisfied at all.

Is secure coin flipping possible?

Exercise: A modification is made to the coin flipping protocol such that whoever wins the weak coin flip gets to flip their own 50 - 50 coin (if acting honestly) and announce the final outcome of the protocol. What is the bias of this strong coin flipping protocol, if the weak coin flipping protocol had a bias of ε?

Classical coin flipping

Alice and Bob have access to classical communication channel.

Instead of just one party flipping a coin, both of them do it simultaneously and then announce the result,

A more sophisticated protocol.

Blum 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 parties output the coin flip $c = a \oplus b$.

Check! Correct - Yes. If both are honest then c is uniformly distributed. (In fact, it is enough for one party to be honest).

Secure - Alice sends a to Bob. Bob can cheat and force any outcome $c = b'$ of his choice by selecting $b = b' \oplus a$.

Doesn't fulfill security.

- No classical coin flipping is secured.
- Additional assumptions needed.

For example, Alice and Bob both send a and b simultaneously. Impose some time synchronization or limit.

- Quantum protocols?

Quantum strong coin flipping

- can overcome the disadvantage of classical
- The outcome being 'determined' are not well defined

Reason? Everything can happen in superposition.

For describing the protocol, we introduce the term 'qutrit' which is used to refer to a quantum state in $\mathbb{C}^3$, i.e. $\alpha_0|0\rangle + \alpha_1|1\rangle + \alpha_2|2\rangle$.

Quantum strong coin flipping: For $a, x \in \{0,1\}$ define $|\phi_{a,x}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x|a+1\rangle)$.

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 that the state he received from Alice in step 1 is $|\phi_{a,x}\rangle$ (e.g. by measuring in any orthonormal basis containing $|\phi_{a,x}\rangle$). If it is not the case then he declares Alice has cheated and aborts.
5. Both return the outcome $c = a \oplus b$.

- Similarity with Blum protocol.
- Four states are not orthogonal, so Bob can't discover the value of a, without first learning x.

Quantum weak coin flipping?

Relax requirements – quantum protocols with arbitrarily small (but nonzero) bias ε possible!

Exercice

Consider the quantum strong coin flipping protocol. Compute the reduced density matrices $\rho^B_{|a=0}$ and $\rho^B_{|a=1}$ associated with the Bob's view of the protocol after Alice's first message has been sent, for a uniformly random choice of $x \in \{0,1\}$ and $a=0$ or $a=1$ respectively. Find the trace distance between the two matrices.