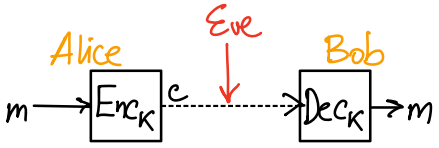
LECTURE 4.2

QUANTUM KEY DISTRIBUTION



Common 2-party crypto goals:
- secrecy (Eve cannot learn info about m from c)
- integrity (B knows that m was sent by A and not modified in transit) (authentication)

(Classical) Private/symmetric key cryptography relies on the two parties having a shared secret key $K \in \{0,1\}^n$.

How do they obtain this key K?

- Public-key encryption schemes (e.g. RSA, Diffie-Hellman)
  - broken by QC
  - offer computational security (i.e. secure against efficient adversaries only)

BB'84 Protocol

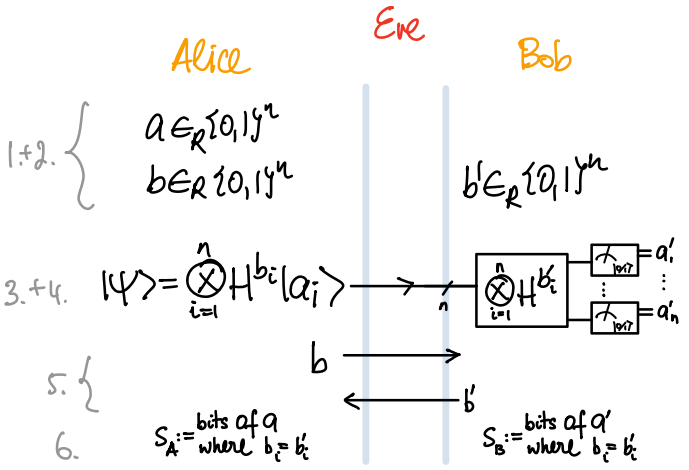
Key idea: measuring unknown state $|\psi\rangle$, disturbs it & the disturbance can be detected.
"info-gain ⇒ disturbance"

Result: shared key about which Eve has negligible information (if protocol hasn't aborted)

Security is information-theoretic.

Phase 1: Obtaining shared string

1. Alice chooses random n-bit strings $a = a_1 \cdots a_n \in \{0,1\}^n$ and $b = b_1 \cdots b_n \in \{0,1\}^n$
2. Bob chooses random string $b' = b'_1 \cdots b'_n \in \{0,1\}^n$
3. Alice prepares n-qubit state $\bigotimes_{i=1}^{n} H^{b_i} |a_i\rangle$ and sends it to Bob
4. Bob applies $\bigotimes_{i=1}^{n} H^{b'_i}$ and measures all n qubits in standard basis. He records the measurement outcome a'.
5. Alice sends Bob her string b. Bob sends Alice b'.
6. Alice and Bob keep the positions, i, of a and a', respectively, where $b_i = b'_i$. Call these, "shared strings", s_A and s_B.



Q. What is the probability that $b_1 = b'_1$?

Ans: $\Pr(b_1 = b'_1) = \Pr(b_1 = 0) \cdot \Pr(b'_1 = 0) + \Pr(b_1 = 1) \Pr(b'_1 = 1) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$

Q: Suppose $b_1 = b'_1$. What is the probability that $a'_1 = a_1$?

Ans: After step 3, Bob's first qubit is $H^{b_1} |a_1\rangle$.
He then applies $H^{b'_1}$, which leaves him with

$$H^{b'_1} H^{b_1} |a_1\rangle = H^{b'_1 + b_1} |a_1\rangle = \mathbb{1} |a_1\rangle = |a_1\rangle$$

Measuring this in standard basis yields outcome $a'_1 = a_1$ with probability one.

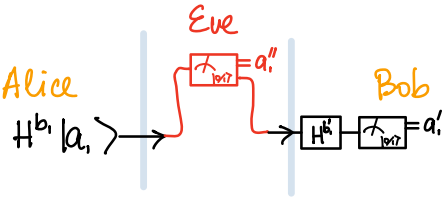
Q: What could be the reasons why $s_A \neq s_B$?

Tampering by Eve, noise on the quantum communication channel.

Q. Suppose $b_1 = b_1'$. (we know that also $a_1' = a_1$ in that case)

Suppose Eve intercepts the first qubit and measures it in standard basis.

What is the probability that $a_1' = a_1$?



Ans:

- If $b_1 = b_1' = 0$, then Eve's measurement will not disturb the state and Bob will get outcome $a_1' = a_1$ with certainty (also Eve will learn the bit a_1).
- If $b_1 = b_1' = 1$, Bob will measure state $|+\rangle$ or $|-\rangle$, each with probability $1/2$. In each of the cases, his measurement will yield 0 or 1 with probability $\frac{1}{2}$. So $Pr(a_1' = a_1) = \frac{1}{2}$.

Overall, we have

$$Pr(a_1' = a_1 \mid b_1' = b_1) = \sum_{i=0}^{1} Pr(b_1 = b_1' = i \mid b_1' = b_1) \cdot Pr(a_1 = a_0 \mid b_1 = b_1' = i)$$

$$= \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$$

Take-away: If Bob learns a_1, he can detect Eve's attack with prob. $\frac{1}{4}$.

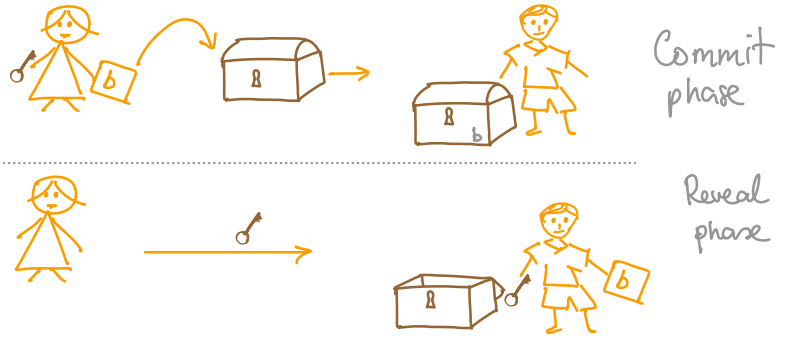
Phase 2: Guarranteeing secrecy.

1. Alice randomly selects half of the positions in s_A and sends them along with the corresponding bits of s_A to Bob. Bob checks these against s_B. if the discrepancy exceeds a certain treshold, they abort.
2. The remaining bits of shared strings, s_A and s_B, are classically post-procesed to improve security.

Note: the classical communication channel btw Alice and Bob needs to be authenticated (Eve can only listen).

Bit commitment

Two mistrusting parties, Alice and Bob.



Commit phase: Alice decides on a value, b, and passes commitment, commit(b) to Bob

Reveal phase: Alice reveals b, potentially along with extra data.

Desirata:

Concealing: Bob cannot learn any info about b, before the reveal phase.

Binding: Alice cannot change her mind about b after the end of commit phase

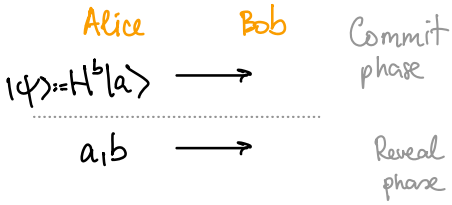
Protocol for committing to bit b

Commit phase:

Alice chooses a random bit $a \in \{0,1\}$ and sends $|\psi\rangle = H^b|a\rangle$ to Bob

Reveal phase:

Alice sends bits a, b to Bob



(Bob can check that $H^b|\psi\rangle$ gives outcome a when measured in standard basis.

Is our protocol concealing?

- if $b=0$, Bob's state is $\frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}\mathbb{1}$
- if $b=1$, Bob's state is $\frac{1}{2}|+\rangle\langle +| + \frac{1}{2}|-\rangle\langle -| = \frac{1}{2}\mathbb{1}$

same state, so Bob cannot tell apart $b=0$ from $b=1$.

Is our protocol binding?

No: there is actually a perfect cheating strategy for Alice.
In the commit phase, she prepares $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
and sends the second qubit to Bob.
(Note: she hasn't commited to any b)
In the reveal phase Alice can trick Bob into
accepting any b of her choice.
To reveal b, Alice applies H^b and measures her
qubit in standard basis to get outcome a.
After this measurement Bob's state is $H^b|a\rangle$
so he cannot tell apart cheating Alice from an
honest one.

In fact there is no quantum bit commitment protocol
(see [RdW] for impossibility proof).