Introduction to Quantum Information Processing

Lecture 20

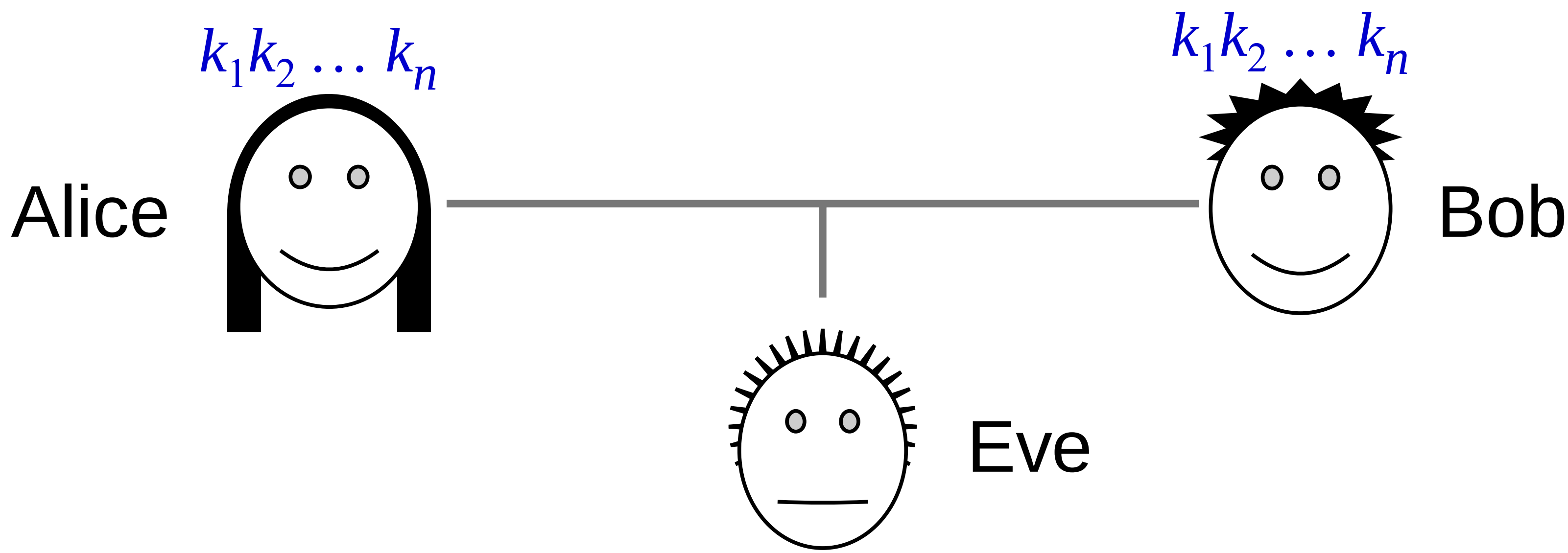
Richard Cleve

Overview of Lecture 20

- Cryptography: the key distribution problem
- The BB84 quantum key distribution protocol
- The bit commitment problem

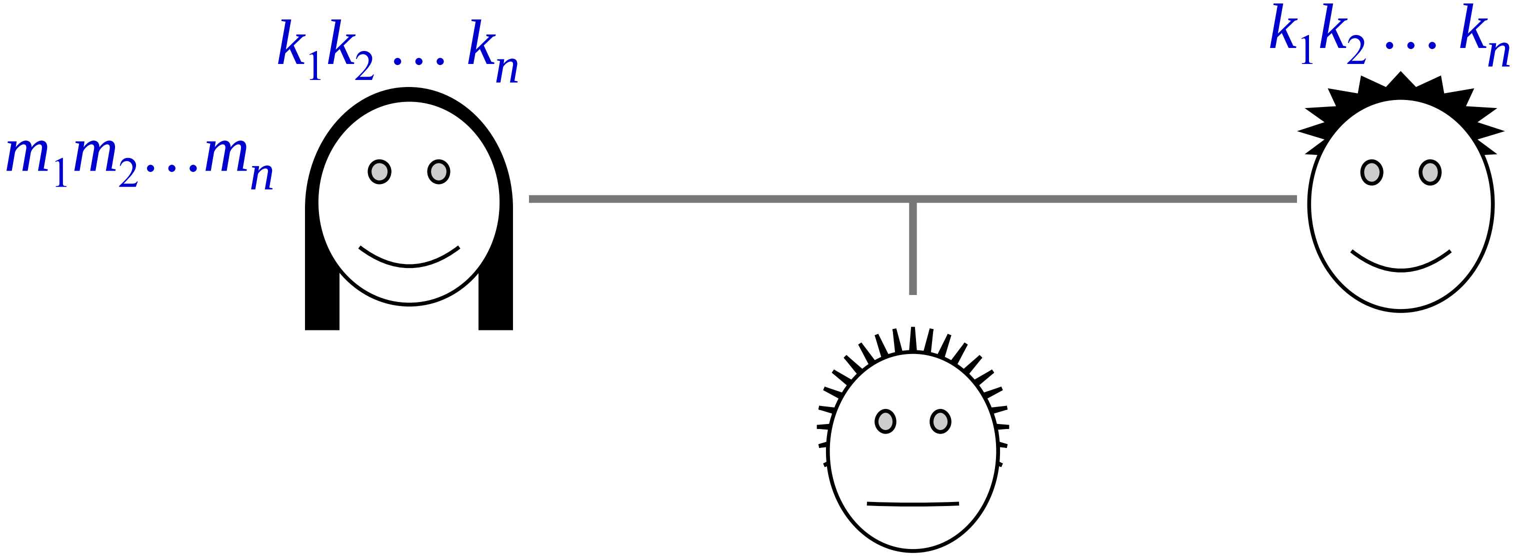
quantum key distribution

Private communication



- Suppose Alice and Bob would like to communicate privately in the presence of an eavesdropper Eve
- A provably secure (classical) scheme exists for this, called the ***one-time pad***
- The one-time pad requires Alice & Bob to share a ***secret key***: $k \in \{0,1\}^n$, uniformly distributed (secret from Eve)

Private communication



One-time pad protocol:

- Alice sends $c = m \oplus k$ to Bob
- Bob receives computes $c \oplus k$, which is $(m \oplus k) \oplus k = m$

This is secure because, what Eve sees is c, and c is uniformly distributed, regardless of what m is

Key distribution scenario

- For security, Alice and Bob must never reuse the key bits
  - E.g., if Alice encrypts both m and m' using the same key k then Eve can deduce $m \oplus m' = c \oplus c'$
- Problem: how do they distribute the secret key bits in the first place?
  - Presumably, there is some trusted preprocessing stage where this is set up (say, where Alice and Bob get together, or where they use a trusted third party)
- **Key distribution problem:** set up a large number of secret key bits

Key distribution based on computational hardness

- The **RSA** protocol can be used for key distribution:
  - Alice chooses a random key, encrypts it using Bob's ***public key***, and sends it to Bob
  - Bob decrypts Alice's message using his ***secret (private) key***

- The security of **RSA** is based on the presumed computational difficulty of factoring integers

- More abstractly, a key distribution protocol can be based on any ***trapdoor one-way function***

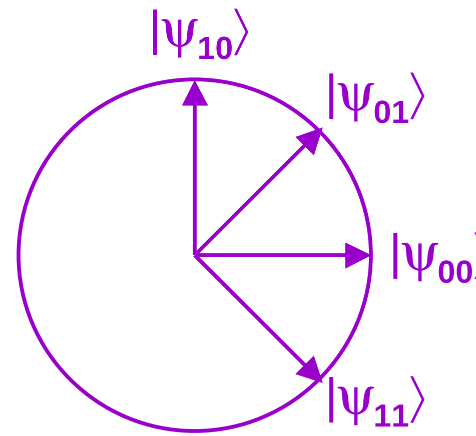
- Most such schemes are breakable by quantum computers

Quantum key distribution (QKD)

- A protocol that enables Alice and Bob to set up a secure***** secret key, provided that they have:
  - A ***quantum channel***, where Eve can read and modify messages
  - An ***authenticated classical channel***, where Eve can read messages, but cannot tamper with them (the authenticated classical channel can be simulated by Alice and Bob having a ***very short*** classical secret key)
- There are several protocols for QKD, and the first one proposed is called "**BB84**" [Bennett & Brassard, 1984]:
  - BB84 is "easy to implement" physically, but "difficult" to prove secure
  - [Mayers, 1996]: first true security proof (quite complicated)
  - [Shor & Preskill, 2000]: "simple" proof of security

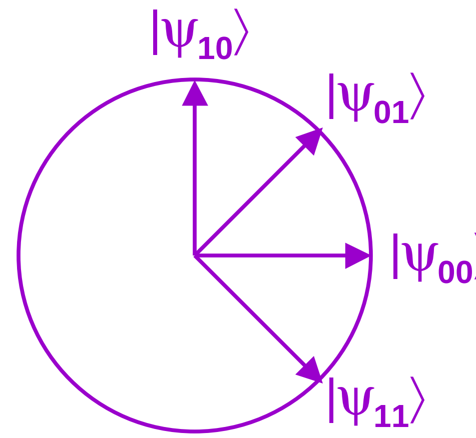
∗ Information-theoretic security

BB84



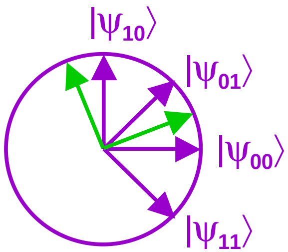
- First, define: $|\psi_{00}\rangle = |0\rangle$
  $|\psi_{10}\rangle = |1\rangle$
  $|\psi_{11}\rangle = |-\rangle = |0\rangle - |1\rangle$
  $|\psi_{01}\rangle = |+\rangle = |0\rangle + |1\rangle$
- Alice begins with two random n-bit strings $a, b \in \{0,1\}^n$
- Alice sends the state $|\psi\rangle = |\psi_{a_1 b_1}\rangle|\psi_{a_2 b_2}\rangle \ldots |\psi_{a_n b_n}\rangle$ to Bob
- **Note:** Eve may see these qubits (and tamper wth them)
- After receiving $|\psi\rangle$, Bob randomly chooses $b' \in \{0,1\}^n$ and measures each qubit as follows:
  - If $b'_i = 0$ then measure qubit in basis $\{|0\rangle, |1\rangle\}$, yielding outcome a'_i
  - If $b'_i = 1$ then measure qubit in basis $\{|+\rangle, |-\rangle\}$, yielding outcome a'_i

BB84



- **Note:**
  - If $b'_i = b_i$ then $a'_i = a_i$
  - If $b'_i \neq b_i$ then $\Pr[a'_i = a_i] = ½$
- Bob informs Alice when he has performed his measurements (using the public channel)
- Next, Alice reveals b and Bob reveals b' over the public channel
- They discard the cases where $b'_i \neq b_i$ and they will use the ***remaining bits*** of a and a' to produce the key
- **Note:**
  - If Eve did not disturb the qubits then the key can be just a (= a')
  - The ***interesting*** case is where Eve may tamper with $|\psi\rangle$ while it is sent from Alice to Bob

BB84



- **Intuition:**
  - Eve cannot acquire information about $|\psi\rangle$ without disturbing it, which will cause ***some*** of the bits of a and a' to disagree
  - It can be proven***** that: the more information Eve acquires about a, the more bit positions of a and a' will be different
- From Alice and Bob's remaining bits, a and a' (where the positions where $b'_i \neq b_i$ have already been discarded):
  - They take a random subset and reveal them in order to estimate the fraction of bits where a and a' disagree
  - If this fraction is not too high then they proceed to distill a key from the bits of a and a' that are left over (around $n/4$ bits)

$*$ To prove this rigorously is nontrivial

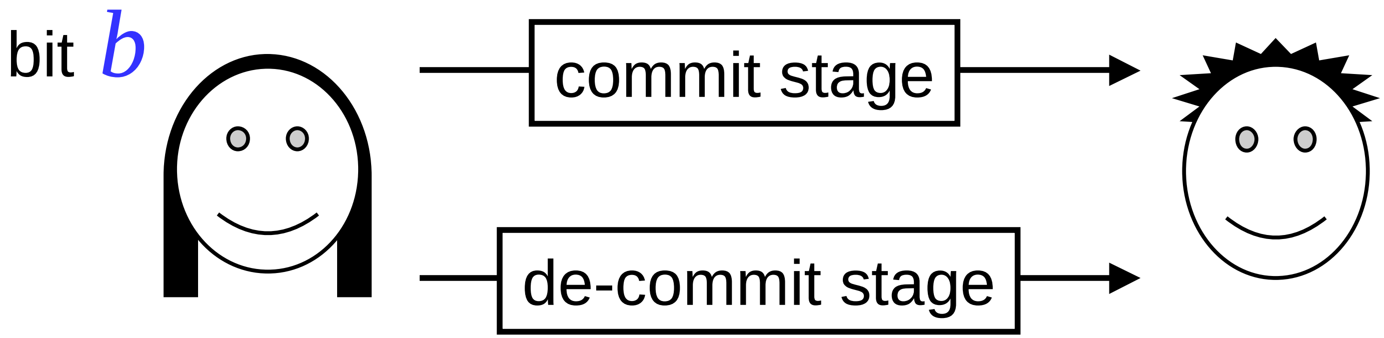
BB84

- If the error rate between a and a' is below some threshold (around 11%) then Alice and Bob can produce a good key using techniques from classical cryptography:
  - **Information reconciliation** (“distributed error correction”)**:** to produce shorter a and a' such that (i) $a = a'$, and (ii) Eve doesn’t acquire much information about a and a' in the process
  - **Privacy amplification:** to produce shorter a and a' such that Eve’s information about a and a' is very small

- There are already commercially available implementations of BB84, though assessing their true security is a subtle matter (since their physical mechanisms are not ideal)

the story of bit-commitment

Bit-commitment



- Alice has a bit b that she wants to ***commit*** to Bob:
- After the ***commit*** stage, Bob should know nothing about b, but Alice should not be able to change her mind
- After the ***de-commit*** stage, either:
  - Bob should learn b and accept its value, or
  - Bob should reject Alice’s de-commitment messages, if she deviates from the protocol

Simple physical implementation

- **Commit:** Alice writes b down on a piece of paper, locks it in a safe, sends the safe to Bob, but keeps the key
- **De-commit:** Alice sends the key to Bob, who then opens the safe
- Desireable properties:
  - **Binding:** Alice cannot change b after **commit**
  - **Concealing:** Bob learns nothing about b until **de-commit**

Question: why should anyone care about bit-commitment?

Answer: it is a useful primitive operation for other protocols, such as zero-knowledge proofs of language-membership

Complexity-theoretic implementation

Based on a ***one-way function*** $f : \{0,1\}^n \to \{0,1\}^n$ and a ***hard-predicate*** $h : \{0,1\}^n \to \{0,1\}$ for f

Commit: Alice picks a random $x \in \{0,1\}^n$, sets $y = f(x)$ and $c = b \oplus h(x)$ and then sends y and c to Bob

De-commit: Alice sends x to Bob, who verifies that $y = f(x)$ and then sets $b = c \oplus h(x)$

This is (i) perfectly binding and (ii) computationally concealing, based on the hardness of predicate h

Quantum implementation

- Inspired by the success of QKD, one can try to use the properties of quantum mechanical systems to design an information-theoretically secure bit-commitment scheme
- One simple idea:
  - To **commit** to **0**, Alice sends a random sequence from $\{|0\rangle, |1\rangle\}$
  - To **commit** to **1**, Alice sends a random sequence from $\{|+\rangle, |-\rangle\}$
  - Bob measures each qubit received in a random basis
  - To **de-commit**, Alice tells Bob exactly which states she sent in the commitment stage (by sending its index 00, 01, 10, or 11), and Bob checks for consistency with his measurement results
- A paper appeared in 1993 proposing a quantum bit-commitment scheme and a proof of security

Quantum implementation

- Not only was the 1993 scheme shown to be insecure, but it was later shown that no such scheme can exist
- To understand the impossibility proof, recall the ***Schmidt decomposition:***

Let $|\psi\rangle$ be ***any*** bipartite quantum state:

$$|\psi\rangle = \sum_{\substack{x\in X \\ y\in Y}} \alpha_{x,y}|x\rangle|y\rangle$$

Then there exist orthonormal states

$|\mu_1\rangle, |\mu_2\rangle, \ldots, |\mu_m\rangle$ and $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_m\rangle$ such that

$$|\psi\rangle = \sum_{z\in Z} \beta_z|\mu_z\rangle|\varphi_z\rangle$$

[Mayers '96][Lo & Chau '96]

Eigenvectors of $\mathrm{Tr}_1|\psi\rangle\langle\psi|$

Quantum implementation

- **Corollary:** if $|\psi_0\rangle$, $|\psi_1\rangle$ are such that $\mathrm{Tr}_1|\psi_0\rangle\langle\psi_0| = \mathrm{Tr}_1|\psi_1\rangle\langle\psi_1|$ then there exists a unitary U (acting on the first register) such that $(U\otimes I)|\psi_0\rangle = |\psi_1\rangle$
- **Proof:**

$$|\psi_0\rangle = \sum_{z\in Z}\beta_z|\mu_z\rangle|\varphi_z\rangle \quad \text{and} \quad |\psi_1\rangle = \sum_{z\in Z}\beta_z|\mu'_z\rangle|\varphi_z\rangle$$

  Let $U|\mu_z\rangle = |\mu'_z\rangle$ $\blacksquare$

- Protocol can be "purified" so that Alice's commit states are $|\psi_0\rangle$ & $|\psi_1\rangle$ (where she sends the second register to Bob)
- By applying U to her register, Alice can change her commitment from $b = 0$ to $b = 1$ (by changing $|\psi_0\rangle$ to $|\psi_1\rangle$)

THE END