Introduction to Quantum Information Processing

CS 467 / CS 667
Phys 467 / Phys 767
C&O 481 / C&O 681

Lecture 19 (2005)

Richard Cleve
DC 3524
cleve@cs.uwaterloo.ca

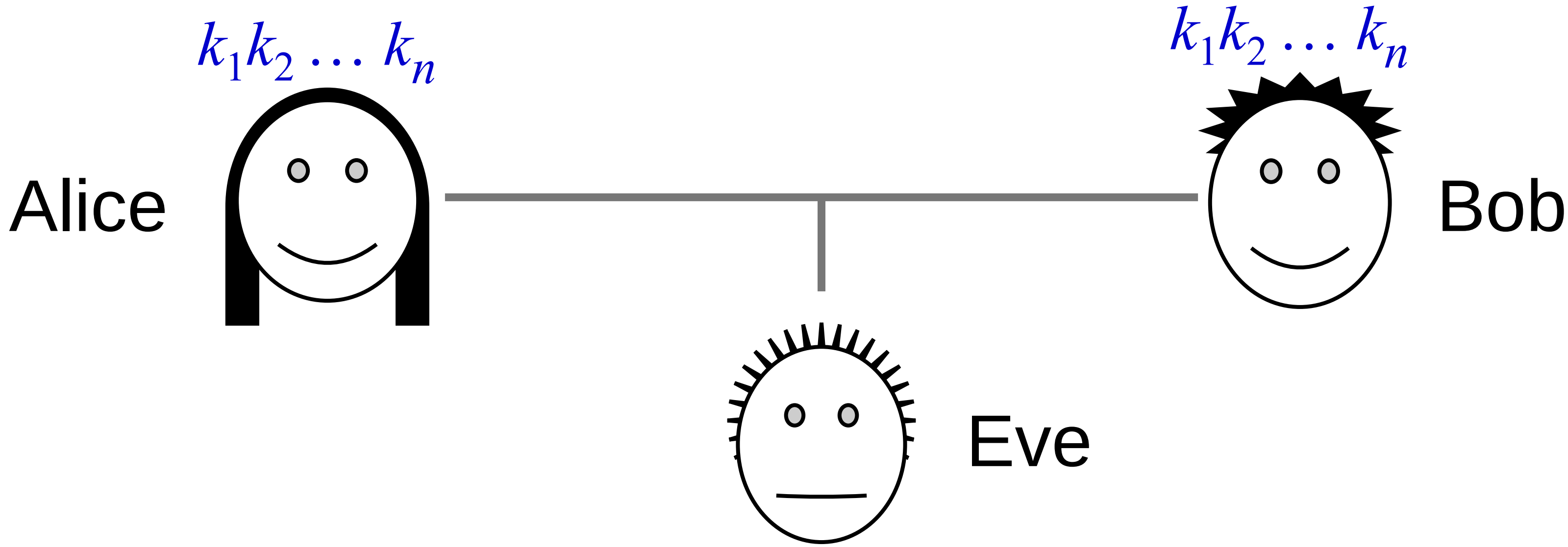
Course web site at:
http://www.cs.uwaterloo.ca/~cleve/courses/cs467

Contents

- Quantum key distribution
- Schmidt decomposition

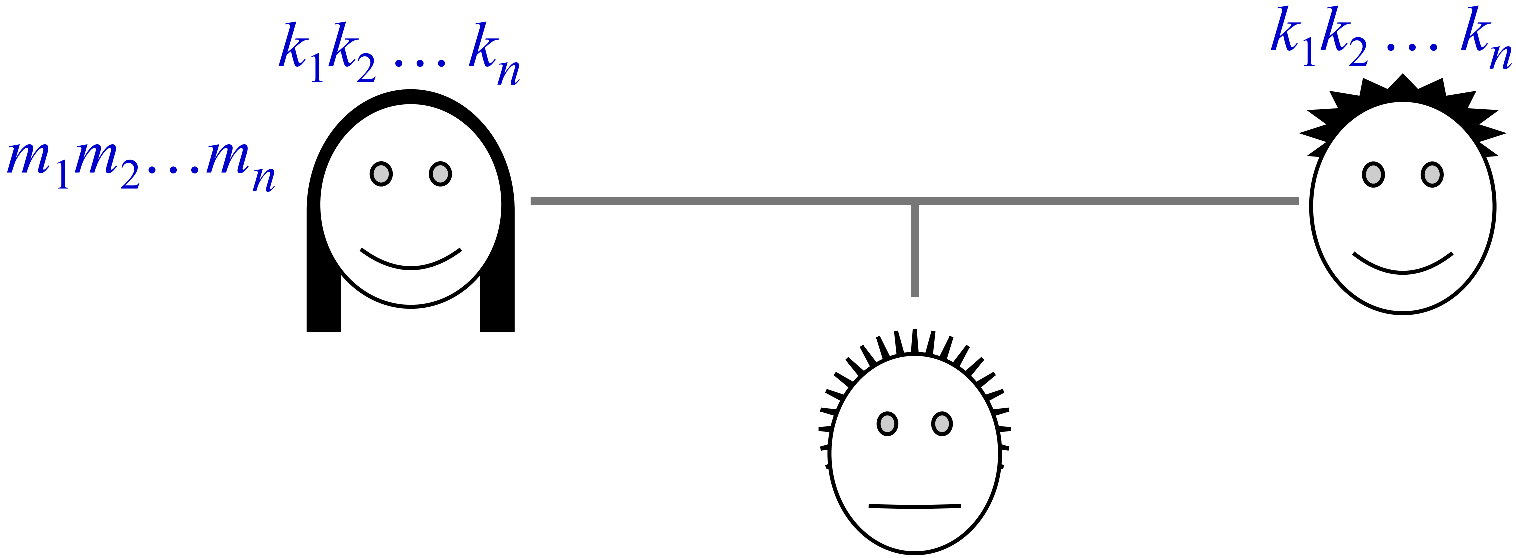
- Quantum key distribution
- Schmidt decomposition

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***

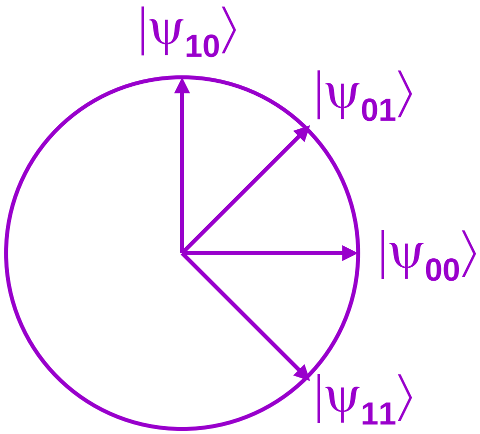
- Most such schemes are breakable by quantum computers

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

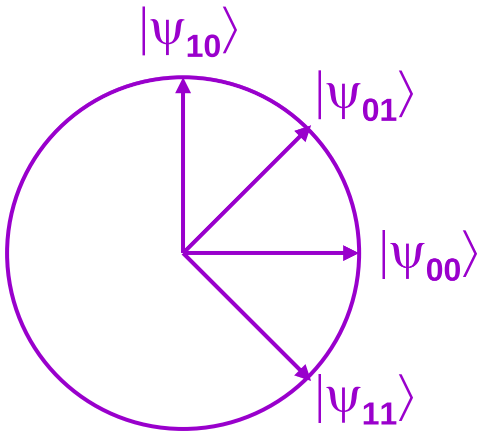
∗ Information-theoretic security

BB84



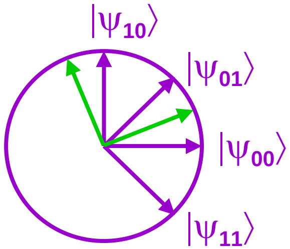
- First, define: $|\psi_{00}\rangle = |0\rangle$
  $|\psi_{10}\rangle = |1\rangle$
  $|\psi_{11}\rangle = |-\rangle = |0\rangle - |1\rangle$
  $|\psi_{01}\rangle = |+\rangle = |0\rangle + |1\rangle$
- Alice begins with two random n-bit strings $a, b \in \{0,1\}^n$
- Alice sends the state $|\psi\rangle = |\psi_{a_1 b_1}\rangle|\psi_{a_2 b_2}\rangle \ldots |\psi_{a_n b_n}\rangle$ 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)

- Quantum key distribution
- Schmidt decomposition

This will have some cryptographic applications for analyzing “bit-commitment” schemes

Schmidt decomposition

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

$|\psi\rangle = \sum_{a=1}^{n}\sum_{b=1}^{m}\alpha_{a,b}|a\rangle\otimes|b\rangle$ (where we can assume $n \le m$)

Then there exist orthonormal states

$|\mu_1\rangle, |\mu_2\rangle, \ldots, |\mu_n\rangle$ and $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ such that

$|\psi\rangle = \sum_{c=1}^{n}\sqrt{p_c}\,|\mu_c\rangle\otimes|\varphi_c\rangle$

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

Schmidt decomposition: proof (I)

The density matrix for state $|\psi\rangle$ is given by $|\psi\rangle\langle\psi|$

Tracing out the first system, we obtain the density matrix of the second system, $\rho = \mathrm{Tr}_1|\psi\rangle\langle\psi|$

Since ρ is a density matrix, we can express $\rho = \sum_{c=1}^{m} p_c|\varphi_c\rangle\langle\varphi_c|$,

where $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_m\rangle$ are orthonormal eigenvectors of ρ

Now, returning to $|\psi\rangle$, we can express $|\psi\rangle = \sum_{c=1}^{m}|\nu_c\rangle\otimes|\varphi_c\rangle$, where $|\nu_1\rangle, |\nu_2\rangle, \ldots, |\nu_m\rangle$ are ***just some arbitrary vectors*** (not necessarily valid quantum states; for example, they might not have unit length, and we cannot presume they're orthogonal)

We will next show that $\langle\nu_c|\nu_{c'}\rangle = \begin{cases} p_c & \text{if } c = c' \\ 0 & \text{if } c \neq c' \end{cases}$

Schmidt decomposition: proof (II)

To show that $\langle \nu_c | \nu_{c'} \rangle = \begin{cases} p_c & \text{if } c = c' \\ 0 & \text{if } c \neq c', \end{cases}$ (where $p_c = 0$ for $c > n$)

we compute the partial trace Tr_1 of $|\psi\rangle\langle\psi|$ in terms of

$$|\psi\rangle\langle\psi| = \left(\sum_{c=1}^{m} |\nu_c\rangle \otimes |\varphi_c\rangle \right) \left(\sum_{c'=1}^{m} \langle \nu_{c'}| \otimes \langle \varphi_{c'}| \right) = \sum_{c=1}^{m} \sum_{c'=1}^{m} |\nu_c\rangle\langle \nu_{c'}| \otimes |\varphi_c\rangle\langle\varphi_{c'}|$$

A careful calculation (shown later) of this partial trace yields

$$\sum_{c=1}^{m} \sum_{c'=1}^{m} \langle \nu_{c'} | \nu_c \rangle \otimes |\varphi_c\rangle\langle\varphi_{c'}| \quad \text{which must equal} \quad \sum_{c=1}^{m} p_c |\varphi_c\rangle\langle\varphi_c|$$

The claimed result about $\langle \nu_c | \nu_{c'} \rangle$ now follows

Next, setting $|\mu_c\rangle = \frac{1}{\sqrt{p_c}} |\nu_c\rangle$ completes the construction

Schmidt decomposition: proof (III)

For completeness, we now give the "careful calculation" of

$$\mathrm{Tr}_1\left(\sum_{c=1}^{m}\sum_{c'=1}^{m}|v_c\rangle\langle v_{c'}|\otimes|\varphi_c\rangle\langle\varphi_{c'}|\right)$$

$$=\sum_{a=1}^{n}\left(\langle a|\otimes I\right)\left(\sum_{c=1}^{m}\sum_{c'=1}^{m}|v_c\rangle\langle v_{c'}|\otimes|\varphi_c\rangle\langle\varphi_{c'}|\right)\left(|a\rangle\otimes I\right)$$ (by definition of Tr_1)

$$=\sum_{c=1}^{m}\sum_{c'=1}^{m}\left(\sum_{a=1}^{n}\langle a|v_c\rangle\langle v_{c'}|a\rangle\right)\otimes|\varphi_c\rangle\langle\varphi_{c'}|$$ (linearity, and properties of $\otimes$)

$$=\sum_{c=1}^{m}\sum_{c'=1}^{m}\left(\sum_{a=1}^{n}\langle v_{c'}|a\rangle\langle a|v_c\rangle\right)\otimes|\varphi_c\rangle\langle\varphi_{c'}|$$ ($\langle v|w\rangle = \mathrm{Tr}(\langle v|w\rangle) = \mathrm{Tr}(|w\rangle\langle v|)$)

$$=\sum_{c=1}^{m}\sum_{c'=1}^{m}\left(\langle v_{c'}|\left(\sum_{a=1}^{n}|a\rangle\langle a|\right)|v_c\rangle\right)\otimes|\varphi_c\rangle\langle\varphi_{c'}|$$ (linearity)

$$=\sum_{c=1}^{m}\sum_{c'=1}^{m}\langle v_{c'}|v_c\rangle\otimes|\varphi_c\rangle\langle\varphi_{c'}|$$ ($\sum_{a=1}^{n}|a\rangle\langle a| = I$)

THE END