Introduction to Quantum Information Processing

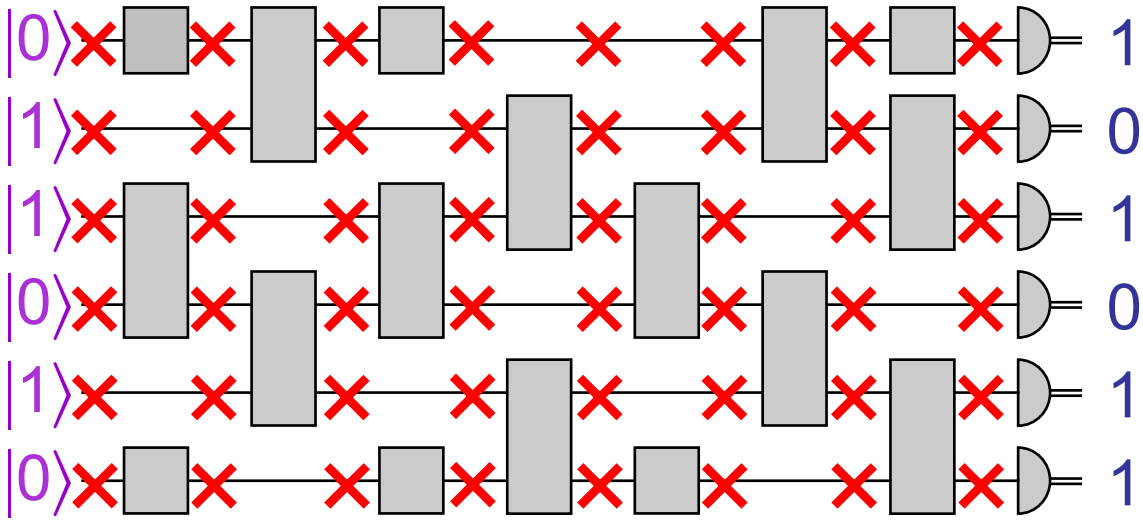
QIC 710 / CS 667 / PH 767 / CO 681 / AM 871

Lecture 23 (2012)

Richard Cleve
DC 2117 / RAC 2211
cleve@cs.uwaterloo.ca

Brief remarks about fault-tolerant computing

A simple error model



At each qubit there is an ✕ error per unit of time, that denotes the following noise:

$$\begin{cases} I & \text{with probability } 1\text{-}\varepsilon \\ X & \text{with probability } \varepsilon/3 \\ Y & \text{with probability } \varepsilon/3 \\ Z & \text{with probability } \varepsilon/3 \end{cases}$$

Threshold theorem

If ε is very small then this is okay — a computation of size* less than $1/(10\varepsilon)$ will still succeed most of the time

But, for every constant value of ε, the size of the maximum computation possible is constant

Threshold theorem: There is a fixed constant $\varepsilon_0 > 0$ such that any computation of size T can be translated into one of size $O(T \log^c(T))$ that is robust against the error model with parameter ε_0

(The proof is omitted here)

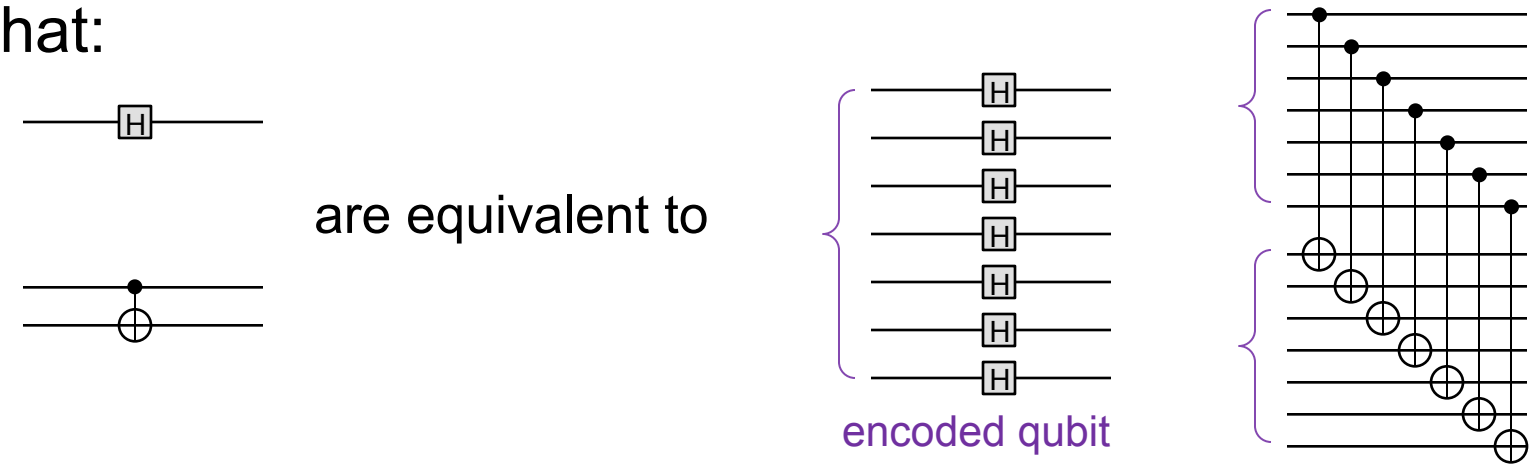
* where size = (# qubits)x(# time steps)

Comments about the threshold theorem

Idea is to use a quantum error-correcting code at the start and then perform all the gates ***on the encoded data***

At regular intervals, an error-correction procedure is performed, very carefully, since these operations are also subject to errors!

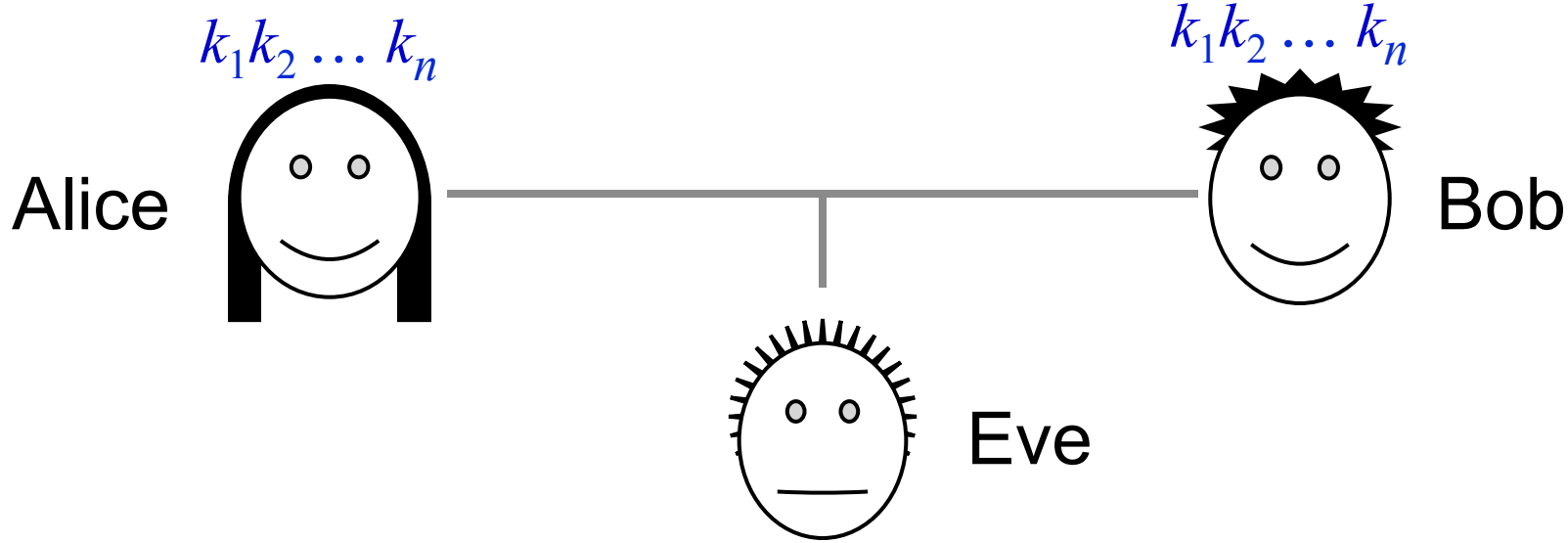
The 7-qubit CSS code has some nice properties that enable some (not all) gates to be directly peformed on the encoded data: H and $CNOT$ gates act "transversally" in the sense that:



Also, codes applied recursively become stronger

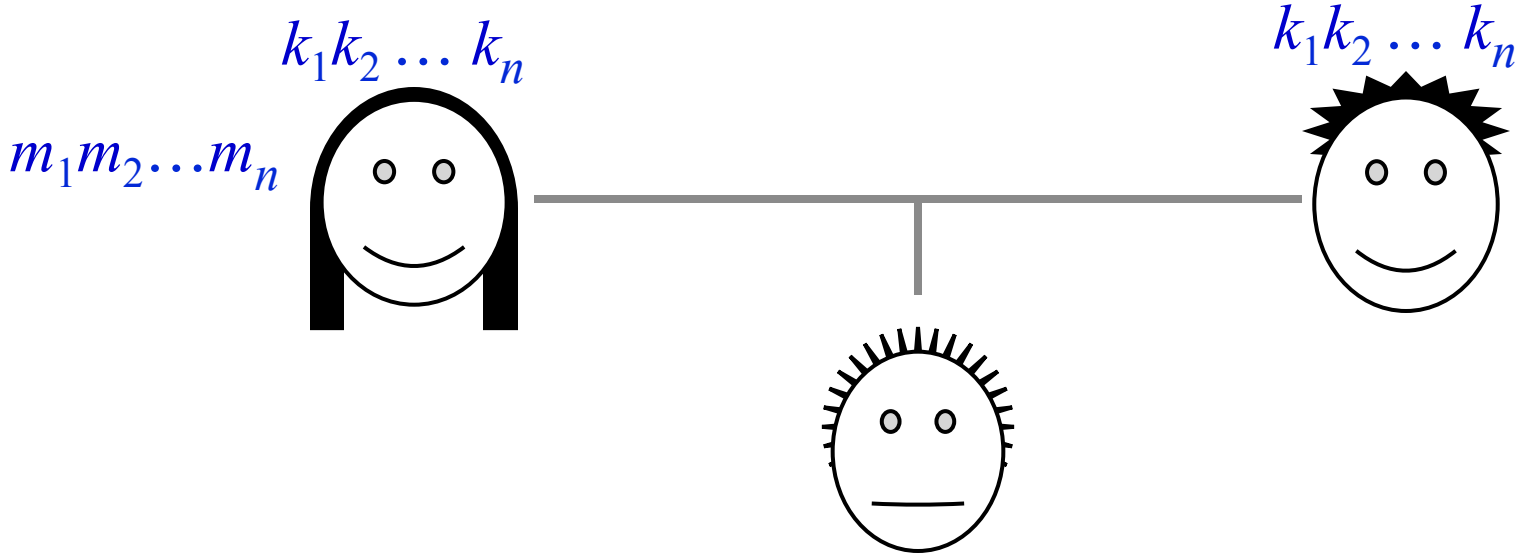
Quantum key distribution

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***

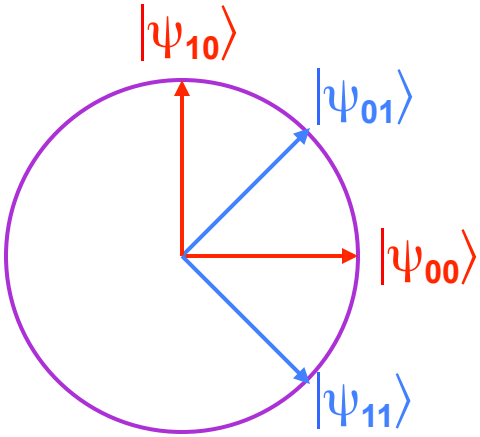
- Most such schemes are breakable by quantum computers

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

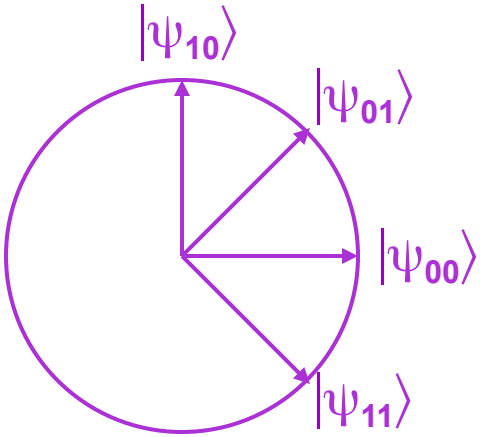
* Information-theoretic security

BB84



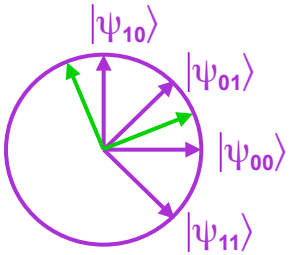
- First, define: $|\psi_{00}\rangle = |0\rangle$
  $|\psi_{10}\rangle = |1\rangle$
  $|\psi_{11}\rangle = |-\rangle = |0\rangle - |1\rangle$
  $|\psi_{01}\rangle = |+\rangle = |0\rangle + |1\rangle$
- Alice begins with two random n-bit strings $a,\ b \in \{0,1\}^n$
- Alice sends the state $|\psi\rangle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

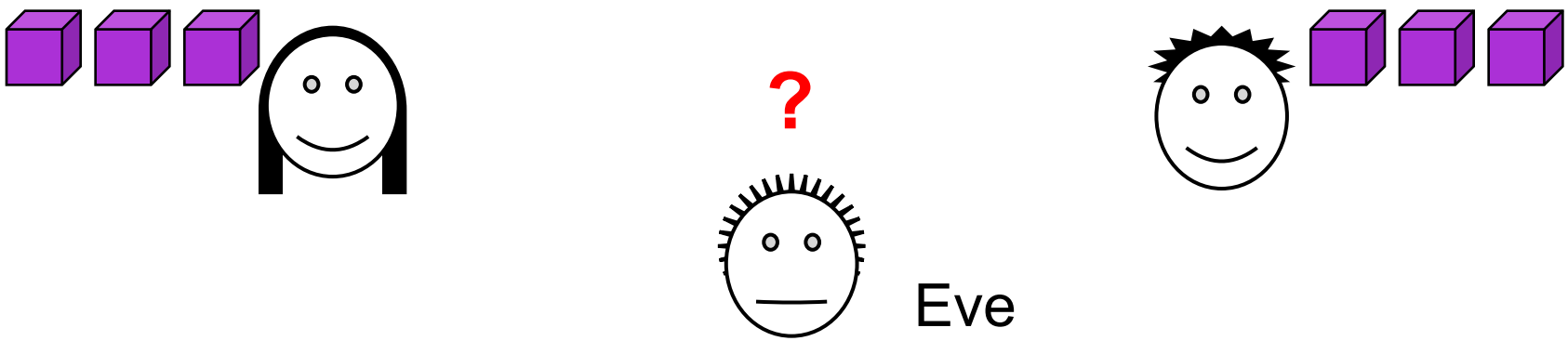
- If the error rate between a and a' is below some threshold (around 11%) then Alice and Bob can produce a good key using techniques from classical cryptography:
  - **Information reconciliation** ("distributed error correction"): to produce shorter a and a' such that (i) $a = a'$, and (ii) Eve doesn't 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 Lo-Chau key exchange protocol: easier to analyze, though harder to implement

Sufficiency of Bell states

If Alice and Bob can somehow generate a series of Bell states between them, such as $|\phi^+\rangle|\phi^+\rangle...|\phi^+\rangle$, then it suffices for them to measure these states to obtain a secret key



Intuitively, this is because there is nothing that Eve can "know" about $|\phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$ that will permit her to predict a future measurement that she has no access to

Key distribution protocol based on $|\phi^+\rangle$

Preliminary idea: Alice creates several $|\phi^+\rangle$ states and sends the second qubit of each one to Bob

If they knew that that they possessed state $|\phi^+\rangle|\phi^+\rangle \ldots |\phi^+\rangle$ then they could simply measure each qubit pair (say, in the computational basis) to obtain a shared private key

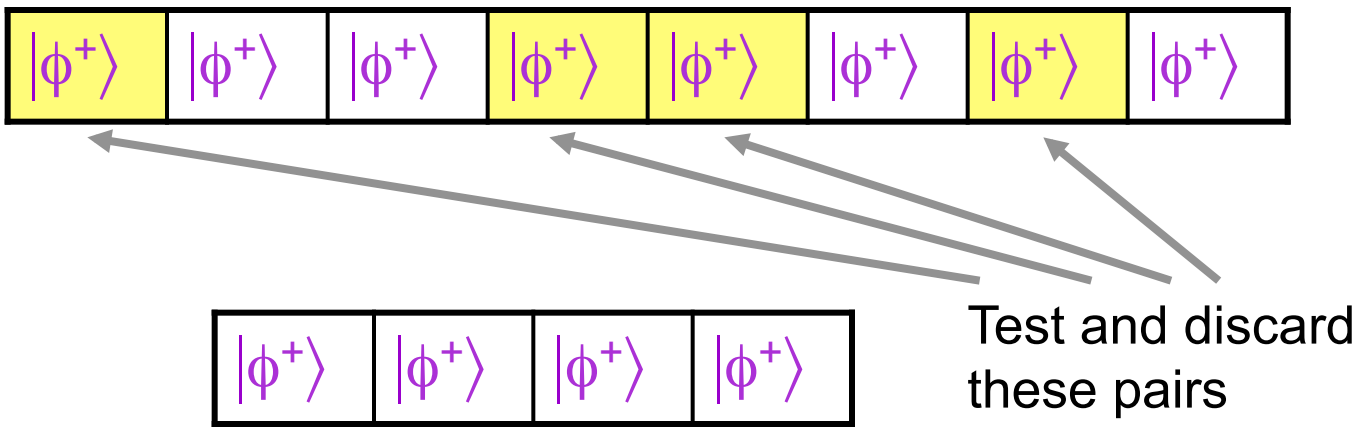
Since Eve can access the qubit channel, she can measure, or otherwise disturb the state in transit (e.g., replace by $|00\rangle$)

We might as well assume that Eve is supplying the qubits to Alice and Bob, who somehow test whether they're $|\phi^+\rangle$

Question: how can Alice and Bob test the validity of their states?

Testing $|00\rangle + |11\rangle$ states I

Alice and Bob can pick a ***random subset*** of their $|\phi^+\rangle$ states (say half of them) to test, and then forfeit those



How do Alice and Bob "test" the pairs in this subset?

Due to Eve, they can't use the quantum channel to actually measure them in the Bell basis ... but they can do individual measurements and compare results via the classical channel

Testing $|00\rangle + |11\rangle$ states II

The Bell state $|\phi^+\rangle = |00\rangle + |11\rangle$ has the following properties:

(a) if both qubits are measured in the ***computational basis*** the resulting bits will be the same (i.e., 00 or 11)

(b) it does not change if $H \otimes H$ is applied to it

Therefore,

(c) if both qubits are measured in the ***Hadamard basis*** the resulting bits will still be the same

Moreover, $|\phi^+\rangle$ is the ***only*** two-qubit state that satisfies properties **(a)** ***and*** **(c)**

Question: Why?

Testing $|00\rangle + |11\rangle$ states III

Problem: they can only measure in ***one*** of these two bases

Solution: they pick the basis randomly among the two types (Alice decides by flipping a coin and announcing the result to Bob on the read-only classical channel)

For example, if Eve slips in a state $|00\rangle$ and then Alice & Bob measure this pair in the Hadamard basis, result is the ***same*** bit with probability only ½ (so it's detected with probability ¼)

Basis:	computational	Hadamard
	$a \oplus b$	$a \oplus b$
$\lvert\phi^+\rangle$	0	0
$\lvert\phi^-\rangle$	0	1
$\lvert\psi^+\rangle$	1	0
$\lvert\psi^-\rangle$	1	1

$$|00\rangle = \tfrac{1}{\sqrt{2}}|\phi^+\rangle + \tfrac{1}{\sqrt{2}}|\phi^-\rangle$$

In general, undetected with probability

$$\frac{1 + \text{fidelity}^2}{2}$$

Testing $|00\rangle + |11\rangle$ states IV

Suppose there are n purported $|\phi^+\rangle$ states and Alice and Bob test m of them

Suppose Eve slips in just one $|00\rangle$ state

Then the probability of Eve

- succeeding in corrupting the key is $(n-m)/n$
- being undetected is $(n-m)/4n$

Setting $m = n-1$, reduces Eve's is success/undetected probability to $\leq 1/4n$

This permits at least one secure key to be created (already something that cannot be done with classical information)

Better testing I

Think of a related (simpler) classical problem: detect if a binary array contains at least one 1

0	0	0	0	1	0	0	0

If one is confined to examining ***individual bits***, this is difficult to do with very high probability making few tests

If one can test ***parities of subsets of bits*** then the following procedure exposes a 1 with probability ½:

pick a random $r \in \{0,1\}^n$ and test if $r \cdot x = 0$

If $x \neq 00...0$ then this test detects this with probability ½

Testing k such parities detects with probability $1 - (½)^k$

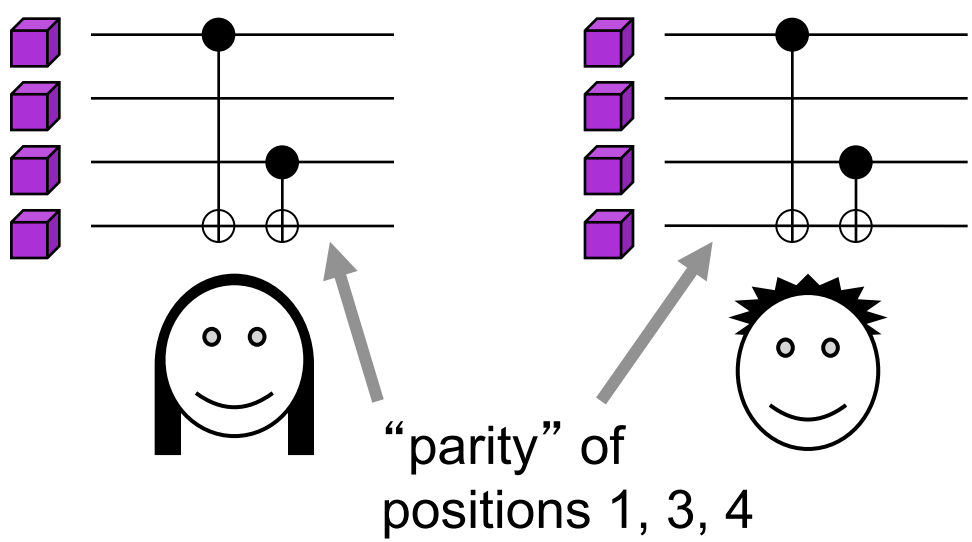
Better testing II

The previous idea can be translated into the context of testing whether pairs Bell states are all $|\phi^+\rangle$ or not

$\lvert\phi^+\rangle$	$\lvert\phi^+\rangle$	$\lvert\phi^+\rangle$	$\lvert\phi^+\rangle$	$\lvert\phi^+\rangle$	$\lvert\phi^+\rangle$	$\lvert\phi^+\rangle$	$\lvert\phi^+\rangle$

1. Alice picks a random $r \in \{0,1\}^n$ and sends it to Bob
2. Alice and Bob perform various bilateral CNOT operations on their qubits

For $r = 1011$

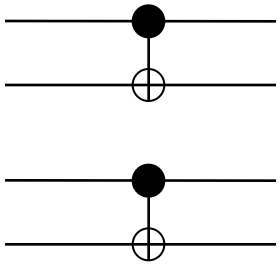


Better testing III

Call:

$|\phi^+\rangle = |\tilde{o},\tilde{o}\rangle$
$|\phi^-\rangle = |\tilde{o},\tilde{\imath}\rangle$
$|\psi^+\rangle = |\tilde{\imath},\tilde{o}\rangle$
$|\psi^-\rangle = |\tilde{\imath},\tilde{\imath}\rangle$

Then bilateral CNOT gates cause $|\tilde{a}_1,\tilde{e}_1\rangle|\tilde{a}_2,\tilde{e}_2\rangle$ to become $|\tilde{a}_1\oplus\tilde{a}_2,\tilde{e}_1\rangle|\tilde{a}_1,\tilde{e}_1\oplus\tilde{e}_2\rangle$



(Example: $|\tilde{o},\tilde{o}\rangle|\tilde{\imath},\tilde{o}\rangle$ becomes $|\tilde{\imath},\tilde{o}\rangle|\tilde{\imath},\tilde{o}\rangle$)

If the states are not all $|\phi^+\rangle = |\tilde{o},\tilde{o}\rangle$ then there is either: a $\tilde{\imath}$ in the first slot or a $\tilde{\imath}$ in the second slot

A measurement of bit parities will detect the former, and this measurement in the Hadamard basis will detect the latter—in either case a series of bilateral CNOTs will cause this parity information to appear in a single pair of qubits that can be measured

Net result

By sacrificing say half the qubit pairs, Alice and Bob can establish with probability exponentially close to 1 that all remaining qubit pairs are in state $|\phi^+\rangle$ from which a secret key can be directly obtained

Note 1: unlike BB84, this protocol requires Alice and Bob to have quantum computers—to perform nontrivial operations on several qubits

Note 2: the Shor-Preskill [2000] security proof for BB84 is shown by ***reducing*** BB84 security to Lo-Chau security (and uses CSS codes to establish the reduction)

Schmidt decomposition

Schmidt decomposition

<u>Theorem:</u>

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

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

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

- $|\psi\rangle = \sum_{c=1}^{n}\sqrt{p_c}|\mu_c\rangle\otimes|\varphi_c\rangle$
- $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ are the 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 $\rho = \sum_{c=1}^{n} p_c|\varphi_c\rangle\langle\varphi_c|$,
where $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ are orthonormal eigenvectors of ρ

Now, returning to $|\psi\rangle$, we can express $|\psi\rangle = \sum_{c=1}^{n} |\nu_c\rangle \otimes |\varphi_c\rangle$,
where $|\nu_1\rangle, |\nu_2\rangle, \ldots, |\nu_n\rangle$ 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)

Schmidt decomposition: proof (II)

Claim: $\langle \nu_c | \nu_{c'} \rangle = \begin{cases} p_c & \text{if } c = c' \\ 0 & \text{if } c \neq c' \end{cases}$

Proof of Claim: Compute the partial trace Tr_1 of $|\psi\rangle\langle\psi|$ from

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

Note that: $\mathrm{Tr}_1(A \otimes B) = \mathrm{Tr}(A) \cdot B$ Example: $\mathrm{Tr}_1(\rho \otimes \sigma) = \sigma$

$$\mathrm{Tr}_1\left(\sum_{c=1}^{n}\sum_{c'=1}^{n} |\nu_c\rangle\langle\nu_{c'}| \otimes |\varphi_c\rangle\langle\varphi_{c'}|\right) = \sum_{c=1}^{n}\sum_{c'=1}^{n} \mathrm{Tr}\left(|\nu_c\rangle\langle\nu_{c'}|\right)|\varphi_c\rangle\langle\varphi_{c'}| \quad \text{(linearity)}$$

$$= \sum_{c=1}^{n}\sum_{c'=1}^{n} \langle \nu_{c'}|\nu_c\rangle |\varphi_c\rangle\langle\varphi_{c'}|$$

Since $\sum_{c=1}^{n}\sum_{c'=1}^{n} \langle \nu_{c'}|\nu_c\rangle \otimes |\varphi_c\rangle\langle\varphi_{c'}| = \sum_{c=1}^{n} p_c |\varphi_c\rangle\langle\varphi_c|$ the claim follows

Schmidt decomposition: proof (III)

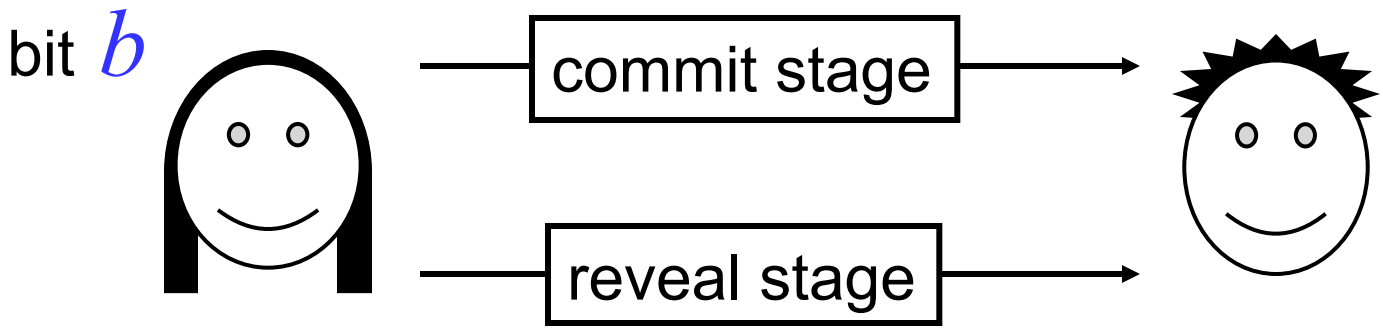
Normalize the $|\nu_c\rangle$ by setting $|\mu_c\rangle = \frac{1}{\sqrt{p_c}}|\nu_c\rangle$

Then $\langle\mu_c|\mu_{c'}\rangle = \begin{cases} 1 & \text{if } c = c' \\ 0 & \text{if } c \neq c' \end{cases}$

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

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 ***reveal*** stage, either:
  - Bob should learn b and accept its value, or
  - Bob should reject Alice's reveal message, 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
- **Reveal:** Alice sends the key to Bob, who then opens the safe
- Desirable properties:
  - **Binding:** Alice cannot change b after **commit**
  - **Concealing:** Bob learns nothing about b until **reveal**

Question: why should anyone care about bit-commitment?

Answer: it is a useful primitive operation for other protocols, such as coin-flipping, and "zero-knowledge proof systems"

Complexity-theoretic implementation

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

Reveal: 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

* should be one-to-one

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 **reveal**, 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

Impossibility proof (I)

- 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:

$$|\psi\rangle = \sum_{a=1}^{n}\sum_{b=1}^{n} \alpha_{a,b}|a\rangle|b\rangle$$

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

$$|\psi\rangle = \sum_{c=1}^{n} \beta_c|\mu_c\rangle|\phi_c\rangle$$

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

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

Impossibility proof (II)

- **Corollary:** if $|\psi_0\rangle$, $|\psi_1\rangle$ are two bipartite states 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:**

$$|\psi_0\rangle = \sum_{c=1}^{n} \beta_c |\mu_c\rangle|\phi_c\rangle \quad \text{and} \quad |\psi_1\rangle = \sum_{c=1}^{n} \beta_c |\mu'_c\rangle|\phi_c\rangle$$

We can define U so that $U|\mu_c\rangle = |\mu'_c\rangle$ for $c = 1,2,\ldots,n$ ∎

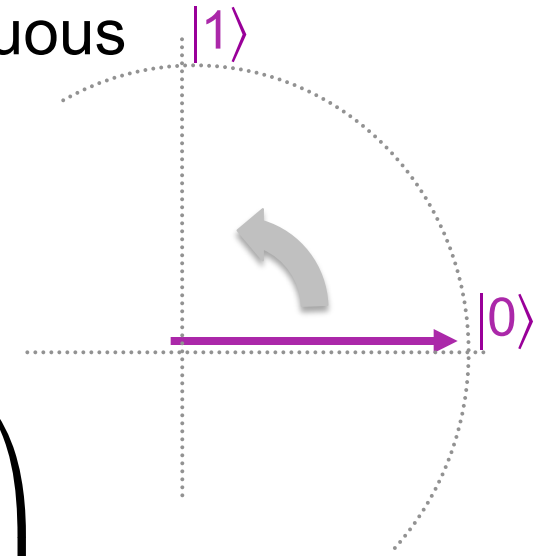
- Protocol can be "purified" so that Alice's commit states are $|\psi_0\rangle$ & $|\psi_1\rangle$ (where she sends the second register to Bob)
- By applying U to her register, Alice can change her commitment from $b = 0$ to $b = 1$ (by changing $|\psi_0\rangle$ to $|\psi_1\rangle$)

Continuous-time evolution

(very briefly)

Continuous-time evolution

Although we've expressed quantum operations in discrete terms, in real physical systems, the evolution is continuous



Let H be any ***Hermitian*** matrix and $t \in \mathbf{R}$

Then e^{iHt} is ***unitary*** — why?

H is called a ***Hamiltonian***

$$H = U^\dagger D U, \text{ where } D = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_d \end{pmatrix}$$

$$e^{iHt} = U^\dagger e^{iDt} U = U^\dagger \begin{pmatrix} e^{i\lambda_1 t} & & \\ & \ddots & \\ & & e^{i\lambda_d t} \end{pmatrix} U \quad \text{(unitary)}$$