Introduction to Quantum Information Processing

CS 667 / PH 767 / CO 681 / AM 871

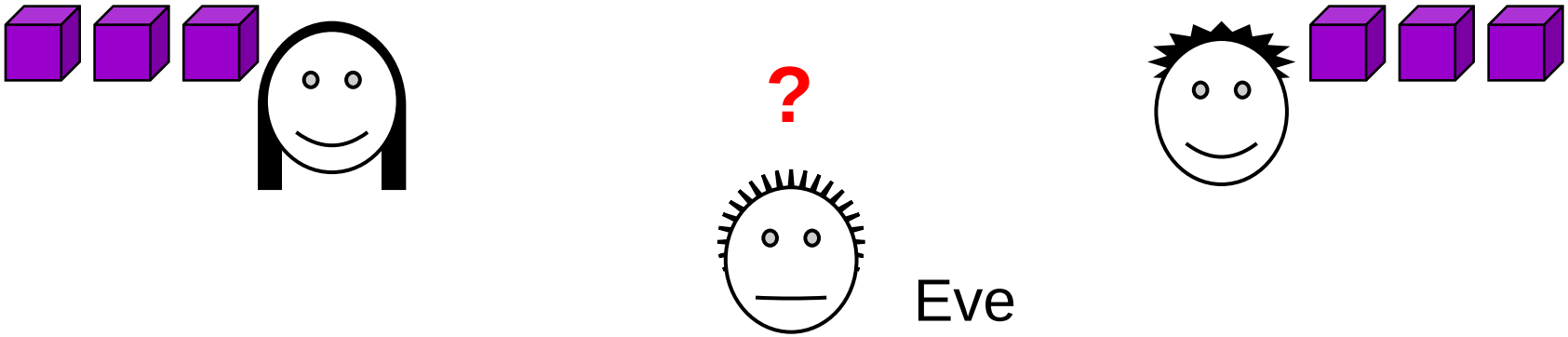
Lecture 24 (2009)

Richard Cleve
DC 2117
cleve@cs.uwaterloo.ca

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

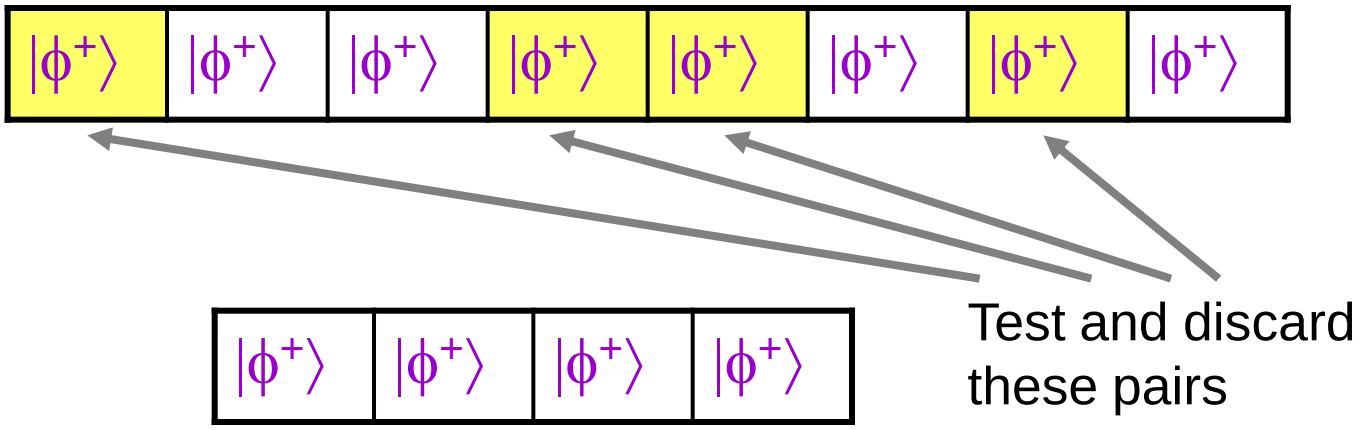
Since Eve can access the qubit channel, she can measure, or otherwise disturb the state in transit (e.g., replace by $|00\rangle$)

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**
	$a \oplus b$	$a \oplus b$
$\|\phi^+\rangle$	0	0
$\|\phi^-\rangle$	0	1
$\|\psi^+\rangle$	1	0
$\|\psi^-\rangle$	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 $1 - (½)^k$

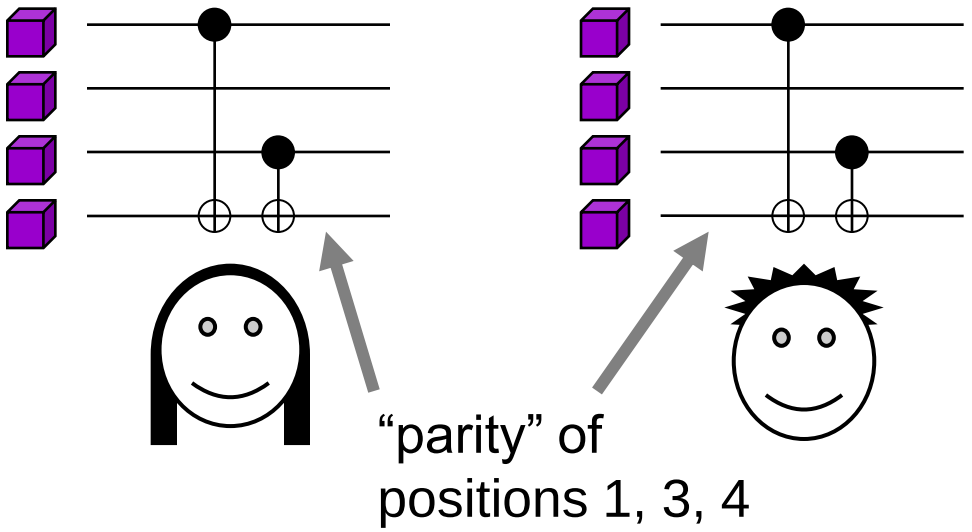
Better testing II

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

$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$	$\|\phi^+\rangle$

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 $r = 1011$



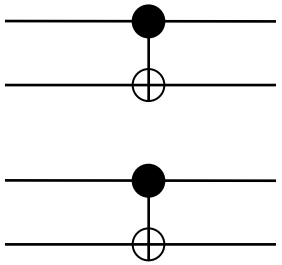
Better testing III

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)


THE END