Introduction to Quantum Information Processing

QIC 710 / CS 768 / PH 767 / CO 681 / AM 871

Lecture 18 (2017)

Jon Yard

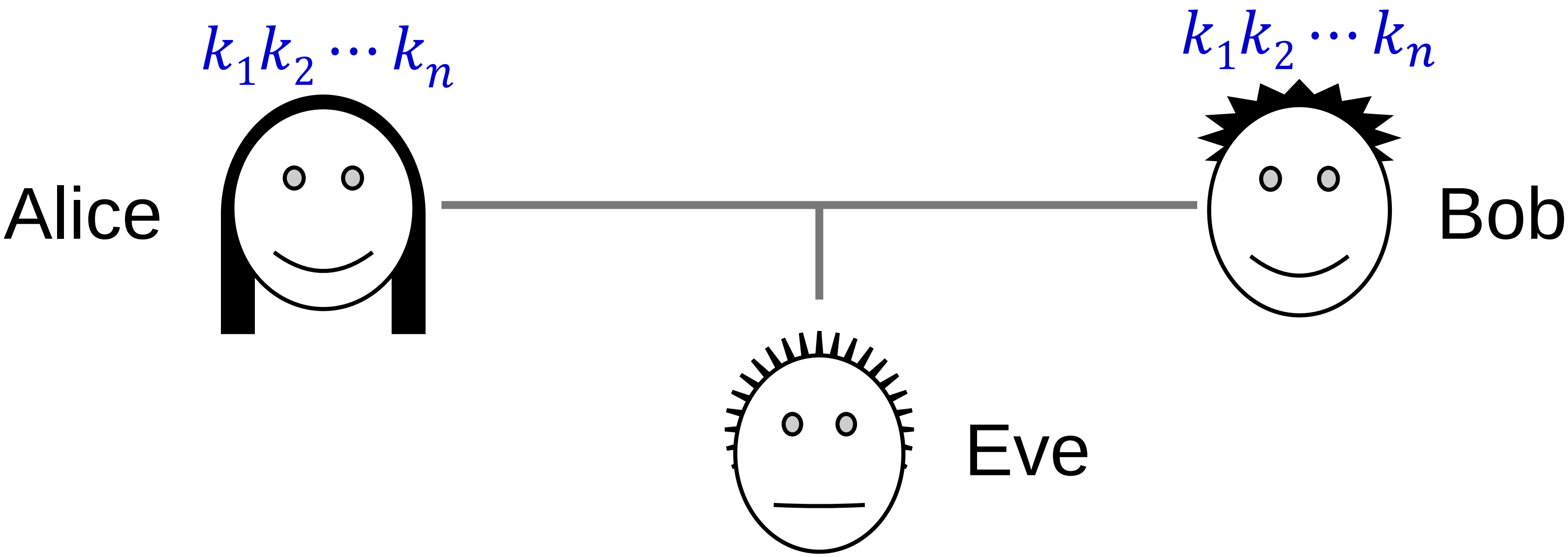
QNC 3126

jyard@uwaterloo.ca

http://math.uwaterloo.ca/~jyard/qic710

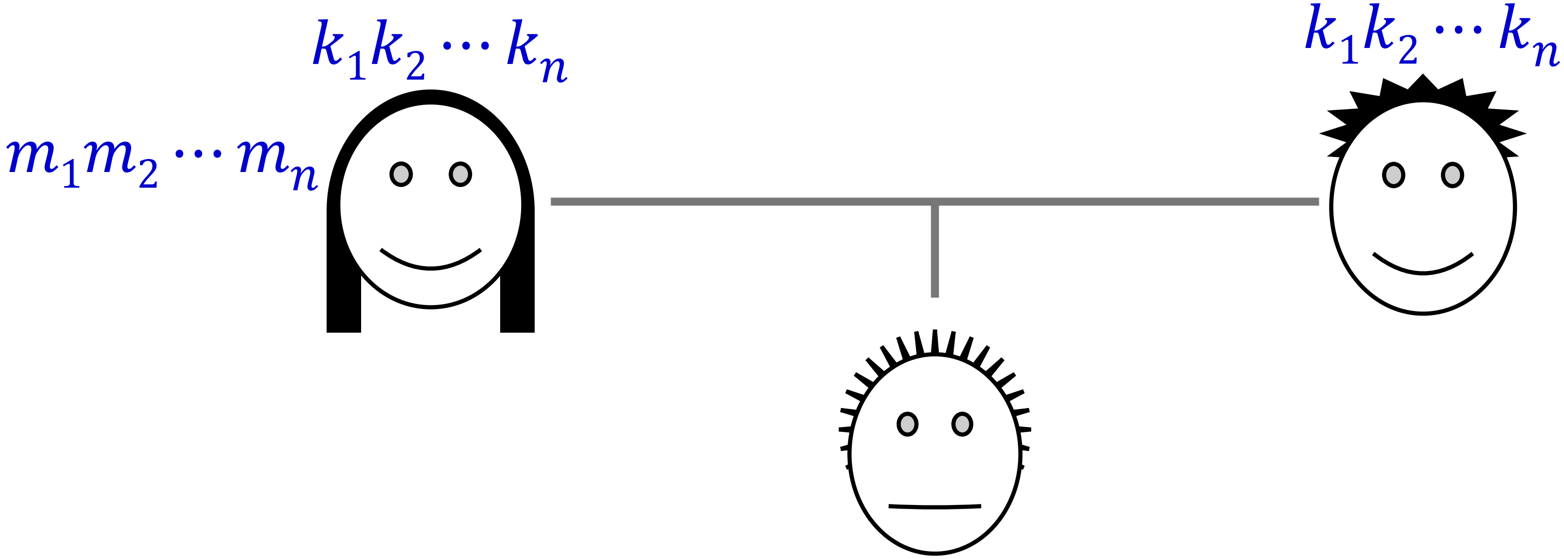
Quantum key distribution

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 $\{0,1\}^n$, uniformly distributed (secret from Eve).

Private communication



One-time pad protocol:

- Alice sends bitwise xor $c = m \oplus k$ 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 secret key bits?
  - 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

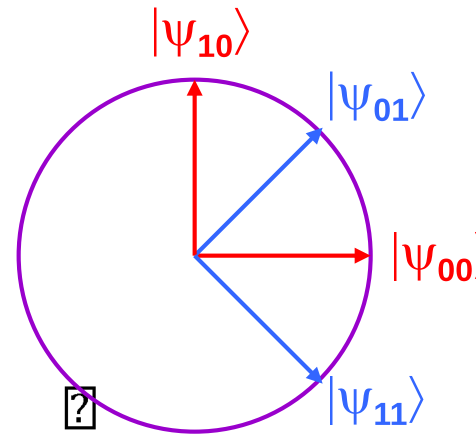
- The **RSA** protocol (say) can be used for key distribution:
  - Alice chooses a random key, encrypts it using Bob's ***public key***, and sends it to Bob
  - Bob decrypts Alice's message using his ***secret (private) key***
- The security of **RSA** is based on the presumed computational difficulty of factoring integers.
- More abstractly, a key distribution protocol can be based on any ***trapdoor one-way function***.
- Many such schemes are breakable by quantum computers (e.g., elliptic curve cryptography schemes).

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

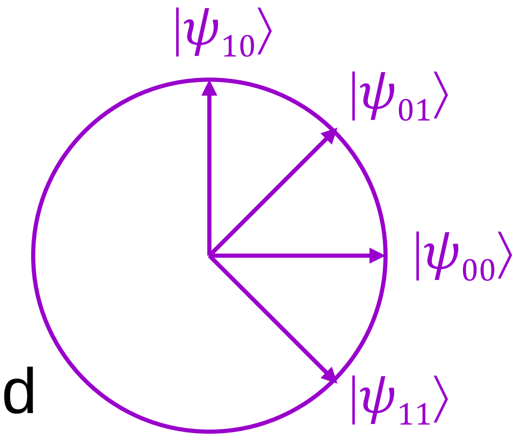
* **Information-theoretic security**

BB84



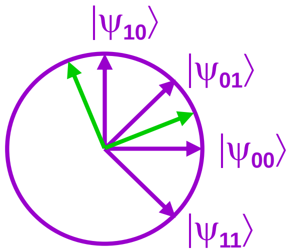
- First, define: $|\psi_{00}\rangle = |0\rangle$
  $|\psi_{10}\rangle = |1\rangle$
  $|\psi_{11}\rangle = |-\rangle = |0\rangle - |1\rangle$
  $|\psi_{01}\rangle = |+\rangle = |0\rangle + |1\rangle$
- Alice begins with two random n-bit strings a, b $\{0,1\}^n$
- Alice sends the state $|\psi\rangle = |\psi_{a_1 b_1}\rangle|\psi_{a_2 b_2}\rangle \ldots |\psi_{a_n b_n}\rangle$ to Bob
- **Note:** Eve may see these qubits (and tamper with them)
- After receiving $|\psi\rangle$, Bob randomly chooses b' $\{0,1\}^n$ 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 $\Pr[a'_i = a_i] = \frac{1}{2}$
  - 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's and Bob's remaining bits, a and a' (where the positions i s.t. $b_i \neq b_i$ 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

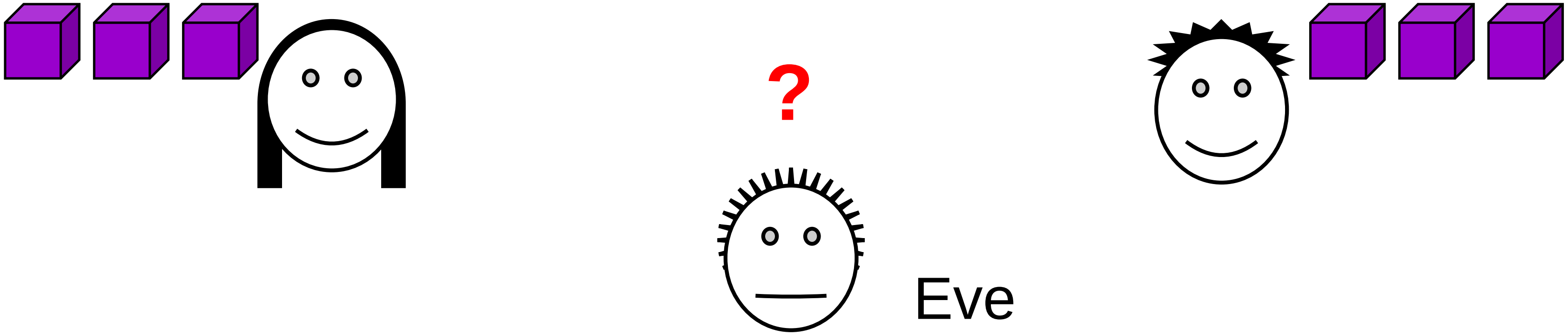
- If the error rate between a and a' is below some threshold (around 11%) then Alice and Bob can produce a good key using techniques from classical cryptography:
  - **Information reconciliation** ("distributed error correction")**:** to produce shorter a and a' such that (i) $a = a'$, and (ii) Eve doesn't 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 $|\phi^+\rangle|\phi^+\rangle \cdots |\phi^+\rangle$, (where $|\phi^+\rangle = |00\rangle + |11\rangle$) 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 $|\phi^+\rangle = |00\rangle + |11\rangle$ 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 they had the state $|\phi^+\rangle|\phi^+\rangle\cdots|\phi^+\rangle$ then they could simply measure each qubit pair (say, in the computational basis) to obtain a shared private key

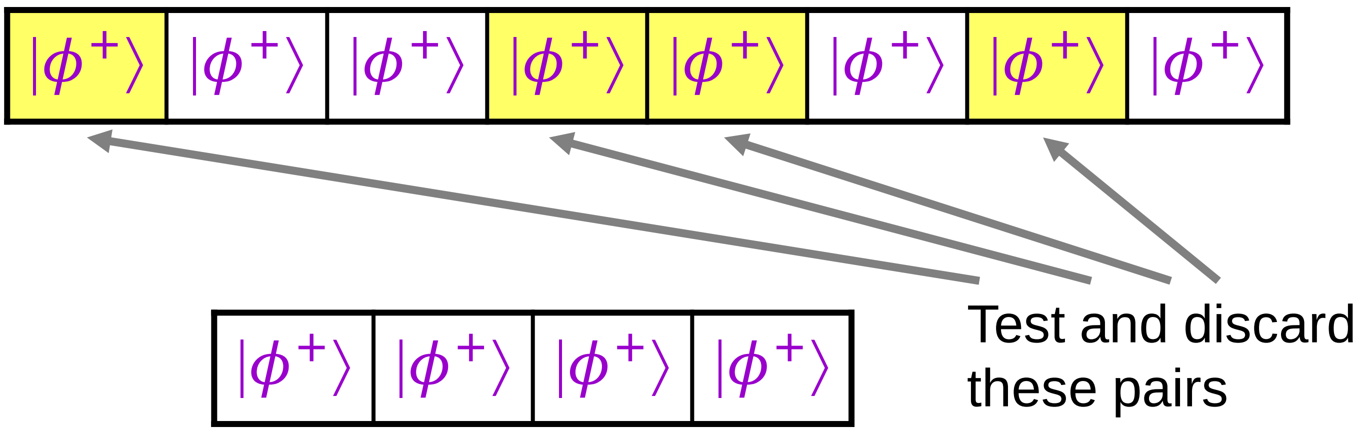
Since Eve can access the qubit channel, she can measure, or otherwise disturb the state in transit (e.g., replace by $|00\rangle$)

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 (1)

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 cannot 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 (2)

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 both properties **(a)** ***and*** **(c)**

Question: Why?

Testing $|00\rangle + |11\rangle$ states (3)

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

Solution: they pick the basis uniformly at random 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 is 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

If Eve slips in $|\mu\rangle$ in place of $|\phi^+\rangle$ then the probability it ***fails*** the test (and thus Eve's tampering is detected) is

$$\frac{1}{2}|\langle\mu|\phi^-\rangle|^2 + \frac{1}{2}|\langle\mu|\psi^+\rangle|^2 + |\langle\mu|\psi^-\rangle|^2$$

$$\geq \frac{|\langle\mu|\phi^-\rangle|^2 + \left|\langle\mu|\psi^+\rangle\right|^2 + |\langle\mu|\psi^-\rangle|^2}{2} = \frac{1 - \left|\langle\mu|\phi^+\rangle\right|^2}{2}$$

For $|00\rangle = \frac{1}{\sqrt{2}}|\phi^+\rangle + \frac{1}{\sqrt{2}}|\phi^-\rangle$ this is $\frac{1}{4}$.

Testing $|00\rangle + |11\rangle$ states (4)

Say there are n supposed $|\phi^+\rangle$ states and Alice and Bob test m of them (and are left with $n - m$ key bits).

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

Then the probability of this causing the test to fail (thereby ***detecting*** Eve) is only $\frac{m}{4n}$.

Even in the extreme case, where Alice and Bob set $m = n - 1$, the detection probability is $\frac{n-1}{4n} = \frac{1-\frac{1}{n}}{4} \leq \frac{1}{4}$.

So in this extreme case, Eve can control the value of one key bit (without her being detected) with probability at least $3/4$.

There is a much better approach…

Better testing (1)

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 $r \cdot x = 0$

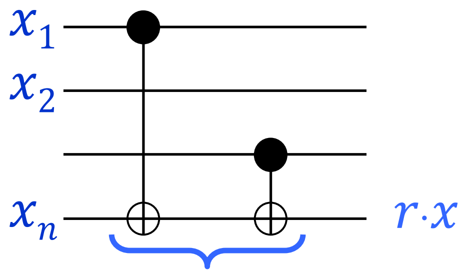
If $x \neq 00 \cdots 0$ then this test detects this with probability $1/2$.

Testing k such parities detects with probability $1 - \frac{1}{2^k}$

Better testing (2)

Another way of interpreting this idea is to allow CNOT gates to be applied before a bit position is checked/discarded

Construct a circuit of CNOT gates in the following way: choose a random $r \in \{0,1\}^n$ and compute $r \cdot x$ in some bit position using CNOT gates



example of circuit for $r = 1011$

Detects $x \neq 00 \cdots 0$ with probability $1/2$ by only discarding one bit.
By repeating this k times, detects with probability $1 - \frac{1}{2^k}$ by only discarding k bits.

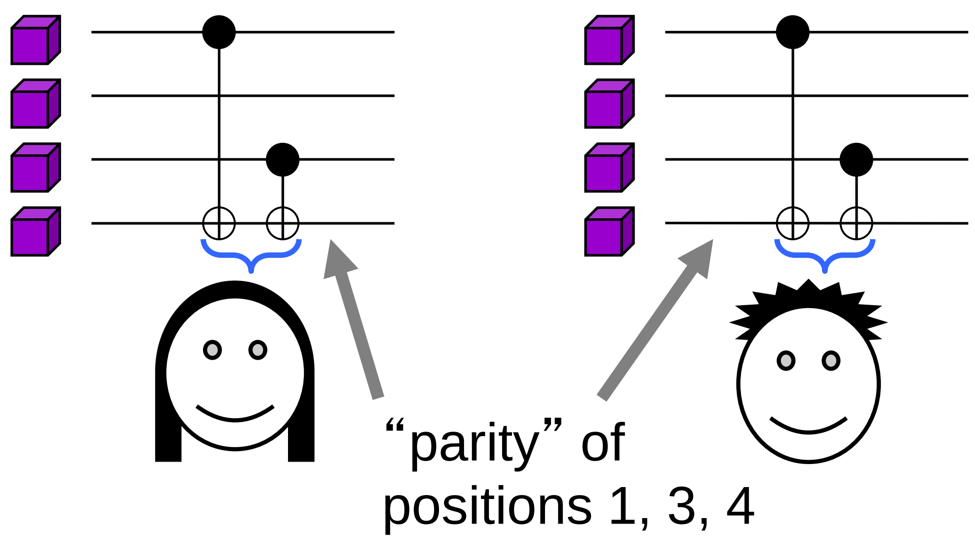
Better testing (3)

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 $r = 1011$

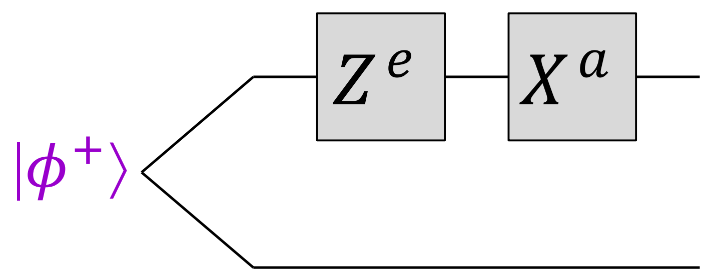


Methodology of bilateral CNOTS (1)

Since

$$(X^a Z^e \otimes I)|\phi^+\rangle = \begin{cases} |\phi^+\rangle = |00\rangle + |11\rangle & \text{if } ae = 00 \\ |\phi^-\rangle = |00\rangle - |11\rangle & \text{if } ae = 01 \\ |\psi^+\rangle = |10\rangle + |01\rangle & \text{if } ae = 10 \\ |\psi^-\rangle = |10\rangle - |01\rangle & \text{if } ae = 11 \end{cases}$$

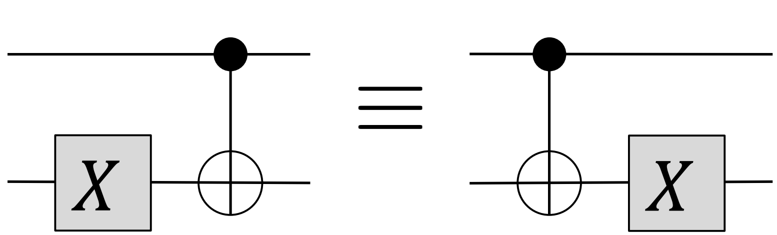
we can think of each supposed $|\phi^+\rangle$ state as:
(where $a, e \in \{0,1\}^n$)



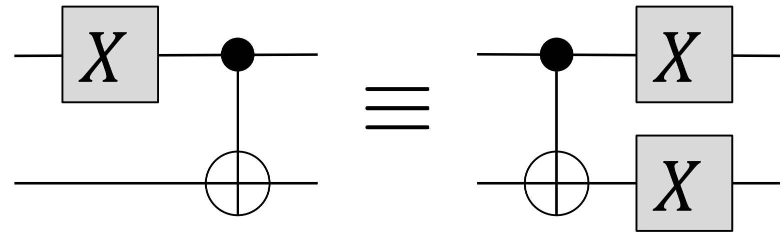
(We will consider ***general*** states—that are superpositions of states of the above form—later on)

Methodology of bilateral CNOTS (2)

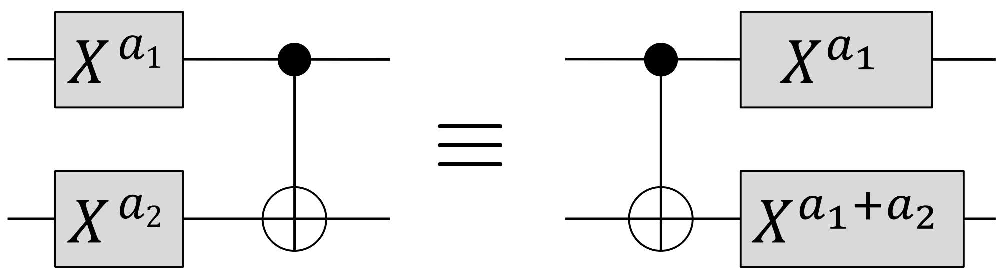
Note that:



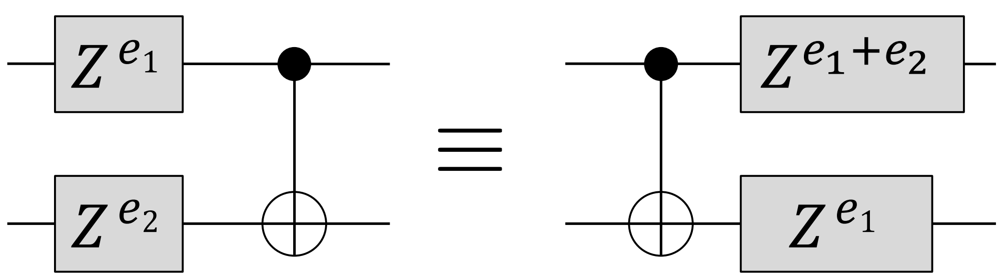
and



More generally:

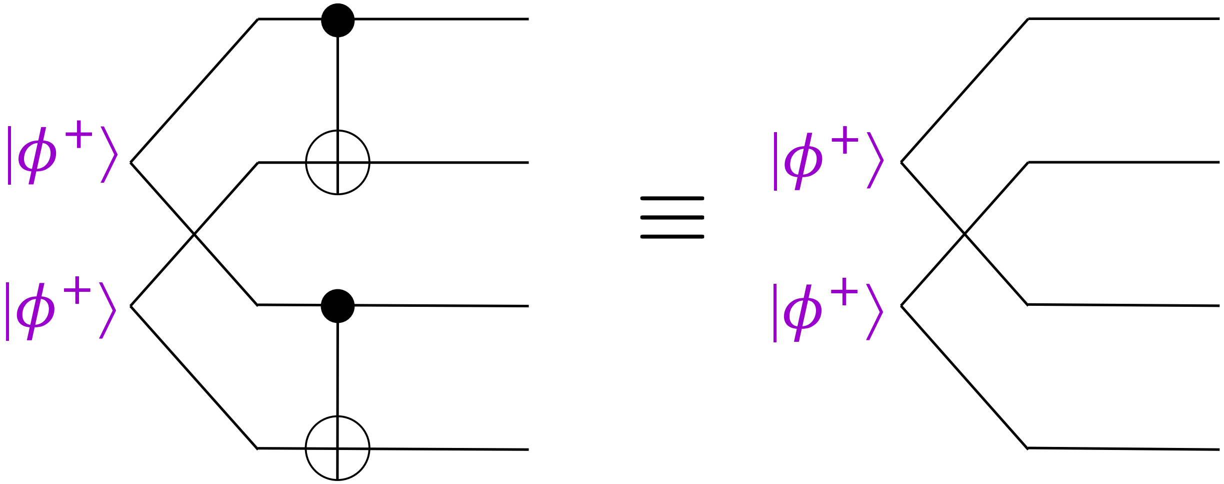


Similarly:

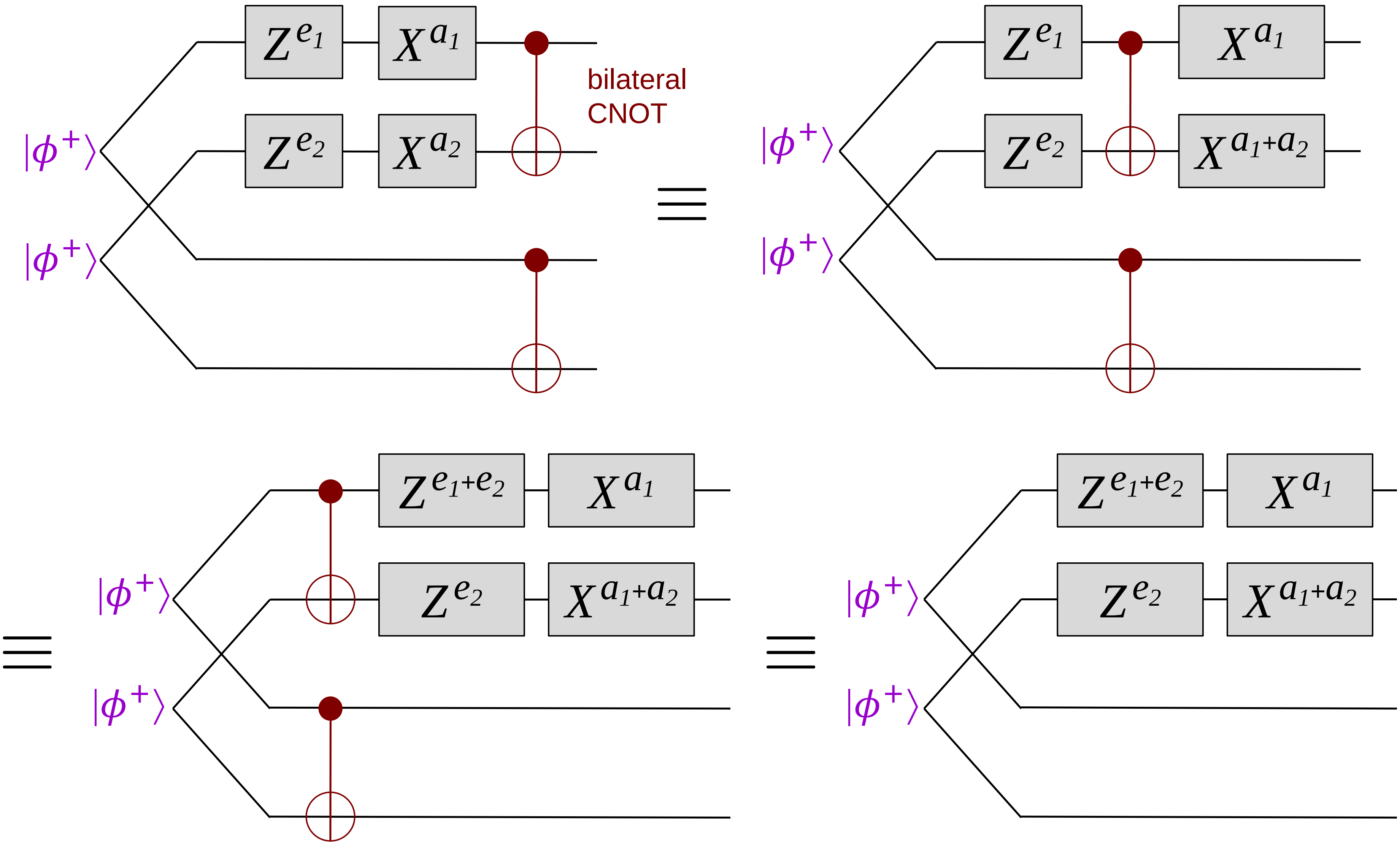


Methodology of bilateral CNOTS (3)

Also, it is straightforward to check that two $|\phi^+\rangle$ states remain unchanged when two CNOT gates are applied bilaterally across them as follows:

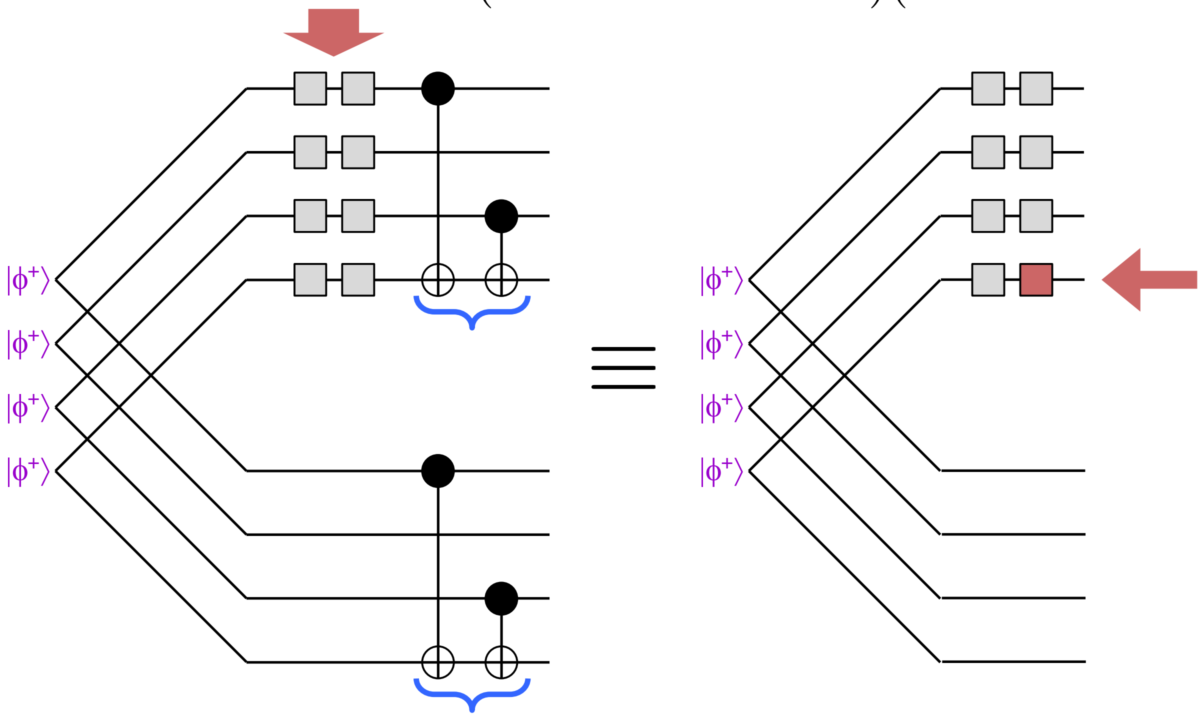


Methodology of bilateral CNOTS (4)



Methodology of bilateral CNOTS (5)

$$X^a Z^e = (X^{a_1} \otimes \cdots \otimes X^{a_n})(Z^{e_1} \otimes \cdots \otimes Z^{e_n})$$



$$X^{r \cdot a} = X^{r_1 a_1 + \cdots + r_n a_n}$$

This detects $a \neq 00\cdots0$ with probability ½

This test in Hadamard basis detects $e \neq 00\cdots0$ with probability ½

By randomly selecting which one of these two tests to perform, can detect **(**$a \neq 00\cdots0$ ***or*** $e \neq 00\cdots0$ **)** with probability ¼.

Conclusion of Lo-Chau scheme

What if Eve provides a states that is not of the form
$X^a Z^e|\Phi^+\rangle = (X^{a_1} \otimes \cdots \otimes X^{a_n})(Z^{e_1} \otimes \cdots \otimes Z^{e_n})|\phi^+\rangle \otimes \cdots \otimes |\phi^+\rangle$?

Rough idea: every $2n$-qubit state is a superposition of the form

$|\mu\rangle = \sum_{a,e\in\{0,1\}^n} \alpha_{a,e} X^a Z^e |\Phi^+\rangle$ and it fails test with prob. $\geq \frac{1-|\langle\mu|\Phi^+\rangle|^2}{2}$

If $|\langle\mu|\Phi^+\rangle|^2$ is not close to 1 then it is likely to fail the test;
if $|\langle\mu|\Phi^+\rangle|^2$ is close to 1 then Alice and Bob can safely use it in place of $|\Phi^+\rangle$ to generate their secret key.

Sacrificing say half the qubit pairs, Alice and Bob can establish a key that Eve has exponentially small information about.

Unlike BB84, this protocol requires Alice and Bob to have quantum computers—to store and perform nontrivial operations on states of several qubits. Shor-Preskill adapts this proof to BB84.