Quantum Information Processing

Lecture 6

Dr. Ahmad Khonsari

Uiversity of Tehran

Fall 2022

December 16, 2022

Slides Prepared by Mahdi Dolati

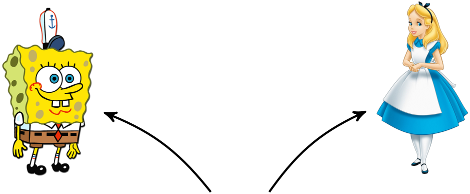
Why look at "some applications of quantum information"?

Before getting into the details of quantum computing proper, we will look at some other aspects of quantum information processing, which have remarkable results that cannot be achieved classically, even in principle. Specifically, we will look at:

- Using entanglement as a resource, in teleportation and superdense coding.
- Using quantum phenomena to achieve information theoretically (rather than computationally) secure communications.

Alice and Bob revisited

Alice and Bob once again share an entangled pair $((1/\sqrt{2})(|00\rangle + |11\rangle))$. Previously we saw that they couldnt use this alone for signalling, so we will also give them a communication channel.

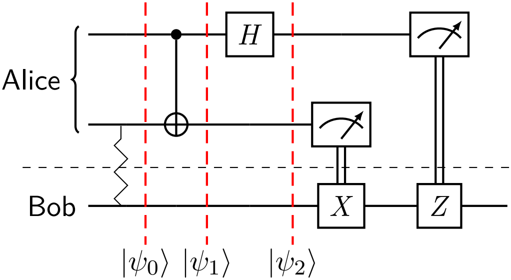


$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

We will now see how they can:

1. Use the shared entanglement and two bits of classical information to transfer one qubit (teleportation).
2. Use the shared entanglement and one qubit of quantum information to transfer two classical bits (superdense coding).

Teleportation



$$
\begin{aligned}
|\psi_0\rangle &= \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle)(|00\rangle + |11\rangle) \\
&= \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)) \\
|\psi_1\rangle &= \frac{1}{\sqrt{2}}(\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)) \\
|\psi_2\rangle &= \frac{1}{2}(\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle))
\end{aligned}
$$

Teleportation (cont.)

$$|\psi_2\rangle = \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle))$$

Alice now measures her two qubits, and sends the results to Bob, who uses this classical information to apply a correction to his qubit (qubit 3):

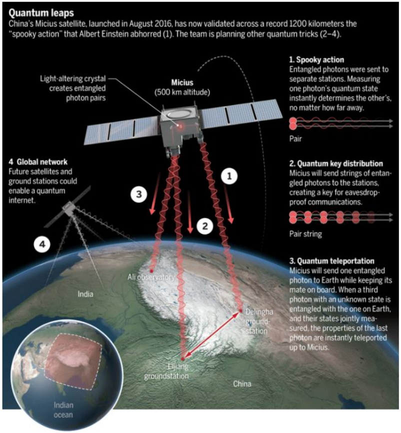
Measurement	Qubit 3 before	Correction	Qubit 3 after
00	$\alpha|0\rangle + \beta|1\rangle$	I	$\alpha|0\rangle + \beta|1\rangle$
01	$\alpha|1\rangle + \beta|0\rangle$	X	$\alpha|0\rangle + \beta|1\rangle$
10	$\alpha|0\rangle - \beta|1\rangle$	Z	$\alpha|0\rangle + \beta|1\rangle$
11	$\alpha|1\rangle - \beta|0\rangle$	ZX	$\alpha|0\rangle + \beta|1\rangle$

So we can see that, regardless of the measurement outcomes, Alices qubit state has now been realised on qubit 3 (i.e., in Bobs possession).

Note that teleportation does not violate the no-cloning principle, as Alices original qubit has been destroyed in the process.

History of quantum teleportation

- Discovered in 1993
- Experimentally realised in 1997
- The latest reported record distance for quantum teleportation is 1,400 km (870 miles) using the Micius satellite for space-based quantum teleportation



Micius Satellite

Superdense coding

Alice's transmission

Superdense coding was discovered in 1992, and experimentally realised in 1996, it goes as follows:
Alice and Bob share an entangled pair, Alice wants to send two bits, i.e., one of 00, 01, 10 or 11. To do so, she applies a single-qubit unitary to her qubit:

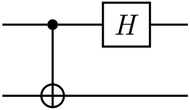
Initial state	Alice's bitstring	Operation	Final state
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	00	I	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	01	X	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	10	Z	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	11	XZ	$\frac{1}{\sqrt{2}}(\|10\rangle - \|01\rangle)$

Alice then sends her qubit to Bob.

Superdense coding

Bob's correction

Bob then receives Alice's qubit, so now has both qubits, and applies the following circuit to the two:



Which yields:

Initial state	After CNOT	After H
$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle) = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|0\rangle$	$\|00\rangle$
$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle) = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)\|1\rangle$	$\|01\rangle$
$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle) = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\|0\rangle$	$\|10\rangle$
$\frac{1}{\sqrt{2}}(\|10\rangle - \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle - \|01\rangle) = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)\|1\rangle$	$\|11\rangle$

The final step is for Bob to perform a computational basis measurements on the two qubits, which will give him Alice's bitstring.

Quantum key distribution

- Quantum key distribution (QKD) was discovered in 1984, and the original protocol (which we will study) is known as BB84 after its discoverers, Bennett and Brassard.
- It later turned out that QKD had previously been discovered, but not make public, by researchers at GCHQ.
- BB84 does not require entanglement (although some subsequent protocols do).

The headquarters of GCHQ

- The record bit rate (of exchange of secure keys) is 1 Mbit/s, in a collaboration between this university and Toshiba.

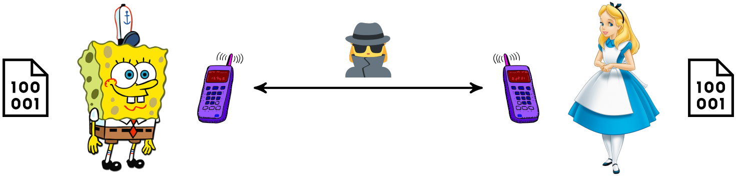
The one-time pad

These days, we are used to public-key cryptography, such as RSA which relies on the one-way nature of some mathematical function (i.e., factoring numbers is hard – or is it?!) to computationally guarantee security. A stronger requirement is to absolutely (information theoretically) guarantee security. Of which the simplest example is a one-time pad:

- At some date in the future Alice will send Bob an n bit message.
- Before that Alice and Bob meet-up and share a "one-time pad" (or key) – a list of n random bits r.
- When the time comes to send the message m, Alice encodes the message by using her copy of r to send $m \otimes r$.
- Bob receives the message and decodes it by using his copy of r: $(m \otimes r) \otimes r = m$

Alice and Bob then discard r.

Resources required to use a one-time pad



Lets take a more detailed look at the practicalities of using a one-time pad:

1. Alice and Bob must previously meet in person (or communicate at a distance via an absolutely secure channel).
2. Alice sends an encoded message $(m \otimes r)$ to Bob via a channel, which in general could be tapped...

...but without access to r, all that an eavesdropper (Eve) would get is a random string of bits.
So the problem here is item 1, that Alice and Bob must meet in advance (or that they must have an absolutely secure channel – in which case they may as well use that for the message transmission).

A one-time pad from quantum key distribution

QKD can be used to generate a one-time pad without Alice and Bob meeting, the resources required to achieve this are:

- An authenticated public classical channel.
- A quantum channel, which could possibly be eavesdropped.

Additionally,

- Alice has a private source of random classical bits.
- Alice can produce qubits in states $|0\rangle$, $|1\rangle = X|0\rangle$, $|+\rangle = H|0\rangle$ and $|-\rangle = H|1\rangle$.
- Bob can measure qubits in either the computational ($|0\rangle$, $|1\rangle$) basis, or the $|+\rangle$, $|-\rangle$ basis.

The BB84 protocol

1. Alice has a bitstring, and for each bit she either encodes $\{0, 1\}$ as $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ (chosen at random with equal probability). Alice then sends the qubit to Bob.
2. Bob receives the qubit and either measures in the $\{|0\rangle, |1\rangle\}$ basis or the $\{|+\rangle, |-\rangle\}$ basis.
3. Bob announces over a public channel in which basis he measured the qubit.
4. Alice replies over the public channel whether that was the basis in which the qubit was prepared.
5. If the same basis was indeed used for the preparation and the measurement then Bob's measurement outcome will equal Alice's bit, and they both append this bit to each of their copies of the key, otherwise they discard.

On average, Alice and Bob will discard half of their bits. In the following worked example we will see that this does indeed yield a shared key, and furthermore we will see that it is private in the sense that any attempt by a third-party to discover the key will lead to a detectable change.

A bit	A basis	Qubit	B basis	B bit
0	$\|0\rangle, \|1\rangle$	$\|0\rangle$	$\|0\rangle, \|1\rangle$	0
1	$\|+\rangle, \|-\rangle$	$\|-\rangle$	$\|+\rangle, \|-\rangle$	1
1	$\|0\rangle, \|1\rangle$	$\|1\rangle$	$\|+\rangle, \|-\rangle$	$\{0, 1\}$
0	$\|0\rangle, \|1\rangle$	$\|0\rangle$	$\|0\rangle, \|1\rangle$	0
1	$\|0\rangle, \|1\rangle$	$\|1\rangle$	$\|0\rangle, \|1\rangle$	1
0	$\|+\rangle, \|-\rangle$	$\|+\rangle$	$\|+\rangle, \|-\rangle$	0
1	$\|0\rangle, \|1\rangle$	$\|1\rangle$	$\|+\rangle, \|-\rangle$	$\{0, 1\}$
1	$\|+\rangle, \|-\rangle$	$\|-\rangle$	$\|0\rangle, \|1\rangle$	$\{0, 1\}$

BB84 attack

Intercept, measure and retransmit

Which of the bits Alice and Bob transmitted / measured in the same basis is a matter of public record. However, it is also possible that an eavesdropper could “tap” the quantum channel to try to discover the key. The first option is for Eve to intercept, measure and retransmit.

However, as Eve would have to decide a basis to measure in before it was made public in which basis Alice transmitted in, then she too would have to make a random decision. Moreover, the agreement about which qubits would be used in the key remains between Alice and Bob alone.

BB84

Worked example with eavesdropping

A bit	A basis	Qubit	E basis	E bit	Qubit	B basis	B bit
0	$\|0\rangle, \|1\rangle$	$\|0\rangle$	$\|0\rangle, \|1\rangle$	0	$\|0\rangle$	$\|0\rangle, \|1\rangle$	0
1	$\|+\rangle, \|-\rangle$	$\|-\rangle$	$\|0\rangle, \|1\rangle$	$\{0, 1\}$	$\{\|0\rangle, \|1\rangle\}$	$\|+\rangle, \|-\rangle$	$\{0, 1\}$
1	$\|0\rangle, \|1\rangle$	$\|1\rangle$	$\|+\rangle, \|-\rangle$	$\{0, 1\}$	$\{\|+\rangle, \|-\rangle\}$	$\|+\rangle, \|-\rangle$	$\{0, 1\}$
0	$\|0\rangle, \|1\rangle$	$\|0\rangle$	$\|+\rangle, \|-\rangle$	$\{0, 1\}$	$\{\|+\rangle, \|-\rangle\}$	$\|0\rangle, \|1\rangle$	$\{0, 1\}$
1	$\|0\rangle, \|1\rangle$	$\|1\rangle$	$\|0\rangle, \|1\rangle$	1	$\|1\rangle$	$\|0\rangle, \|1\rangle$	1
0	$\|+\rangle, \|-\rangle$	$\|+\rangle$	$\|+\rangle, \|-\rangle$	0	$\|+\rangle$	$\|+\rangle, \|-\rangle$	0
1	$\|0\rangle, \|1\rangle$	$\|1\rangle$	$\|0\rangle, \|1\rangle$	1	$\|1\rangle$	$\|+\rangle, \|-\rangle$	$\{0, 1\}$
1	$\|+\rangle, \|-\rangle$	$\|-\rangle$	$\|0\rangle, \|1\rangle$	$\{0, 1\}$	$\{\|0\rangle, \|1\rangle\}$	$\|0\rangle, \|1\rangle$	$\{0, 1\}$

Eavesdropping

Other factors

As seen in the worked example, eavesdropping disturbs the shared key – thus whilst Alice and Bob can rest assured that Eve hasn't discovered their key, they do need to set aside a subset of the bits to compare on the public channel, to check whether their key has been disturbed by eavesdropping.

Eve may try to avoid the problem by using a more sophisticated intercept, copy, retransmit attack, where she would keep a copy of the qubit, and only measure it once Alice and Bob had shared on the public channel the bases they agreed on – but this would violate the no-cloning principle.