Quantum Criptograhy

With a look at Quantum Key Distribution

Michele Beretta

UniBG
https://github.com/micheleberetta98/qkd-presentation

2021

Table of Contents

The Qubit

The *bit* is the fundamental concept of classical computation - it can be either 0 or 1.

In a quantum world, where *superposition of states* is a thing, we use an analogous concept - the *quantum bit*, or **qubit**.

A qubit can be in any *linear combination* of two base states.

The Qubit

A classical bit is like a coin - either *head* or *tail*.

A qubit can be both *head* or *tail* at the same time - until observed.

Observing a qubit makes it *decay* in one of the base states. Hence, measurement *changes* the real world.

Making a Quantum Computer

Making a qubit is hard - for example, nuclear spin can be mantained for long, but it's hard to measure.

A good quantum computer has to be *well isolated*, but its qubits have to be *accessible* in order to be manipulated.

A Mathematical Representation

Qubit

Given two states $|0\rangle$ and $|1\rangle$ a qubit is defined as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle \quad \alpha, \beta \in \mathbb{C}$$

For our purposes, it's safe to assume $\alpha, \beta \in \mathbb{R}$.

Some Linear Algebra

A qubit can be thought as a *vector* in a 2-dimensional vector space. The states $|0\rangle$ and $|1\rangle$ are the basis of this space.

One example could be

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \implies |\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

Some operations

- *Dot product*: $\langle\psi|\varphi\rangle$
- *Tensor product*: $|\psi\rangle \otimes |\varphi\rangle = |\psi\rangle\,|\varphi\rangle$

Note that $\langle\psi| = |\psi\rangle^{T}$.

Measuring

When measuring a qubit, we can get:

- A 0 with probability $|\alpha|^2$
- A 1 with probability $|\beta|^2$

Since they are probabilities, it has to be

$$|\alpha|^2 + |\beta|^2 = 1$$

Or, in other words, the qubit's state must be *normalized*.

Definition

Mathematical Representation of a Qubit

A qubit is a *unit vector* in a *two-dimensional complex vector field*.

For example

$$|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

is a qubit that, when measured, gives either 0 or 1 fifty-percent of the time.

Multiple qubits

We can combine multiple qubits. For example, a 2-qubit system has four *computational basis*

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

In this system, a qubit can be in a superposition on 4 states.

In general, if we have n qubits, then the system can be in a superposition of 2^n states.

Gates

How do we modify qubits? With *quantum gates*.

Quantum Gate

A quantum gate is a *complex matrix* which must be unitary.

For example, the **NOT** gate is defined as

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \implies X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}$$

It's called a **NOT** gate because it inverts the probabilities of measuring 0 and 1.

More gates

Other important gates are:

- The **Z** gate, which flips the sign of the $|1\rangle$ state

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- The **H** gate, or *Hadamard* gate, used to bring the qubit in a superposition

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Can we copy a qubit?

If we measure a qubit we destroy its superposition - but can we copy the qubit itself?

The answer is **no**. It is impossible to make a copy of an unknown quantum state.

Proof/1

It's a proof by absurd.

Suppose it exists a copying machine that copies a qubit $|\psi\rangle$ into another qubit $|s\rangle$. The initial state of this machine is

$$|\psi\rangle \otimes |s\rangle$$

So there is a unitary evolution U that actually does the copying procedure, ideally

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} |\psi\rangle \otimes |\psi\rangle$$

Now, given two particular states $|\psi\rangle$ and $|\varphi\rangle$, we have

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$
$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

Proof/2

Taking the inner product of these two equations gives us

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$$

But $x = x^2$ has only two solutions - 0 and 1, which means

$$\langle\psi|\varphi\rangle = 0 \vee \langle\psi|\varphi\rangle = 1$$

So $|\psi\rangle = |\varphi\rangle$ or $|\psi\rangle$ and $|\varphi\rangle$ are orthogonal.

Hence we can only clone orthogonal states, making general quantum cloning impossible.

Table of Contents

Why do we care about this?

Because quantum computers could be capable of a lot of things.

Namely, efficiently perform some tasks that *are not feasible on a classical computer*.

In particular, **public key cryptography** is based on the infeasibility of some problems, such as prime factorization or discrete logarithm.

Fast prime factorization

For example, finding the prime factorization of an *n*-bit integer requires

$$\exp \Theta \left(n^{\frac{1}{3}} \log^{\frac{2}{3}} n \right)$$

operations using the *number field sieve*.

A quantum algorithm can accomplish the same task using

$$O \left(n^2 \log n \log \log n \right)$$

operations - so it's *exponentially faster*.

The demonstration is quite lengthy, but can be found in [NC10] or in [DW99].

Private Key Cryptography

In a private key cryptosystem, if Alice and Bob wish to exchange information they both must have a *matching key*, used to encrypt and decrypt the message.

As long as the keys are truly secret, this method is provably secure.

The problem is the *secure distribution* of the keys.

Quantum Key Distribution (QKD)

It's a *provably secure* protocol by which *private keys* can be created between two parties over a *public channel*, exchanging qubits.

An external observer (Eve) cannot gain any information from the qubits transmitted without disturbing the state, because

1. Qubits cannot be copied (no-cloning theorem)
2. Measurement changes the data itself

Some algorithms

There are some algorithms for Quantum Key Distribution, such as:

1. BB84 protocol
2. B98 protocol
3. EPR protocol
4. Modified Lo-Chau protocol

The BB84 Protocol/1

Suppose Alice and Bob want to distill a shared secret key

Alice has two strings a and b of $(4+\delta)n$ bits. She encodes them as a block of $(4+\delta)n$ qubits

$$|\psi\rangle = \bigotimes_{k=1}^{(4+\delta)n} |\psi_{a_k b_k}\rangle$$

where a_k is the k^{th} bit of a (similarly for b).

The BB84 Protocol/2

So every qubit is one of these four states

$$|\psi_{00}\rangle = |0\rangle \qquad |\psi_{10}\rangle = |1\rangle$$

$$|\psi_{01}\rangle = |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad |\psi_{11}\rangle = |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

We can think of these as qubits encoded in one of two basis - X or Z - based on the value of the bit b_k:

- $b_k = 0 \implies 0 \to |0\rangle, 1 \to |1\rangle$
- $b_k = 1 \implies 0 \to |+\rangle, 1 \to |-\rangle$

The BB84 Protocol/3

If Eve is eavesdropping, then Bob receives a "disturbed" version of the qubits.

When Bob receives the qubits, he announces it and then measures each qubit in basis X or Z, based on a $(4 + \delta)n$ bits string b', created randomly. Let's call the measurement result a'.

The BB84 Protocol/4

Alice publicly transmits b, and Alice and Bob discard any bits where Bob measured a different basis than Alice prepared.

With high probability, there are at least $2n$ bit left (if not, abort). Let's keep only the first $2n$ bits.

Alice chooses a subset of n bits as a check, and tells Bob which bits she selected.

They both compare these, and if more than an acceptable number of bits disagree the protocol is aborted. Otherwise, they have the key!

The BB84 Protocol - summary

1. Alice prepares $(4+\delta)n$ random data bits - a
2. Alice randomly chooses $(4+\delta)n$ random base bits - b
3. She encodes each data bit a_i as $(\left|0\right\rangle, \left|1\right\rangle)$ if $b_i = 0$, or as $(\left|+\right\rangle, \left|-\right\rangle)$ if $b_i = 1$
4. She sends the qubits to Bob
5. Once received, Bob measures each qubit in a random base (X or Z)
6. Alice announces b
7. Alice and Bob keep only the bits measured in the same bases, and max $2n$ bits
8. Alice chooses n bits as a check and tells Bob which ones she selected
9. They both compare these bits, and if they match then the remaining bits are the key

But does any of this work?

Yes, Quantum Key Distribution has already been tested in real life. For example

- In 2015 the Unversity of Geneva and Corning Inc. achieved a secret key rate of $12.7\mathrm{kbit/s}$ over $307\mathrm{km}$ [K+15]
- In 2017 the Institute for Quantum Compuing and the University of Waterloo (Canada) achieved quantum key distribution between a ground transmitter and a moving aircraft [P+17]

Quick demo

```
→ qkdsim git:(master) iex -S mix
Erlang/OTP 23 [erts-11.2.2] [source] [64-bit] [smp:4:4] [ds:4:4:10] [async-threads:1] [hipe] [dtrace]

Interactive Elixir (1.11.4) - press Ctrl+C to exit (type h() ENTER for help)
iex(1)> Sim.start(100)
BOB :: Started
ALICE :: Started
:ok
ALICE :: Given n = 100, generated k = 500 random bits
ALICE :: Protocol finished, key of length 100 received
BOB   :: Protocol finished, key of length 100 received
ALICE :: 10111000000010001001000100010001001001010011111010000100110010110001110111011000100010101011010011010
BOB   :: 10111000000010001001000100010001001001010011111010000100110010110001110111011000100010101011010011010
iex(2)> Sim.start_with_eve(100)
BOB :: Started
ALICE :: Started
:ok
ALICE :: Given n = 100, generated k = 500 random bits
EVE :: Intercepting qubits...
EVE :: Measured the qubits
BOB   :: Protocol aborted
ALICE :: Protocol aborted
iex(3)>
```

Code available at `https://github.com/micheleberetta98/qkd-sim`

References and further reading

- Ronald De Wolf.
  Quantum computation and shor's factoring algorithm, 1999.
- Boris Korzh et al.
  Provably secure and practical quantum key distribution over 307 km of optical fiber, 2015.
- Michale Nielsen and Isaac Chuang.
  Quantum Computation and Quantum Information.
  Cambridge University Press, 2010.
- Cristopher Pugh et al.
  Airborne demonstration of a quantum key distribution receiver payload, 2017.