

# Quantum Cryptography

Slides based in part on "A talk on quantum cryptography or how Alice outwits Eve," by Samuel Lomonaco Jr. and "Quantum Computing" by André Bertiaume.

## The Classical World

- Bits either 0 or 1.
- Bits can be copied.
- Bits can be observed without changing them. (So, eavesdropping cannot be detected in classical cryptosystems.)

## Quantum Bits

- A quantum bit (**qubit**) can be 0 or 1 at the same time.
- It can not be copied (no cloning theorem).
- Its state will collapse if it is observed (measured).

If a qubit can be 0 or 1 at the same time, how many values can  $n$  qubits have at the same time?  $2^n$

# Physical Qubits

In classical physics, a thing is described by its state.

In quantum physics, a thing is described by the probabilities that the thing is in a certain state.

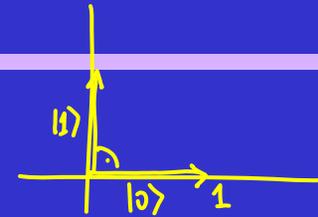
For qubits, we need a two-state system. In principle, any property in the microscopical world that has two possible states may serve as a qubit. Some examples that have been proposed to be used in the actual construction are

1. Photon polarization (horizontal versus vertical polarization).
2. Energy states of electrons (ground state or excited state).
3. Nuclear spin (clockwise or counter clockwise).

# Mathematical Qubits

Mathematical modelling of a qubit:

$|0\rangle$   
 $|1\rangle$



- A qubit is a unit-vector in a 2D complex vector space.

- Let  $|0\rangle$  and  $|1\rangle$  be two orthonormal vectors, then we can write each qubit as

*length 1, perpendicular (right angle)*

$$a|0\rangle + b|1\rangle$$



*qubit can be viewed as a vector of length 1*

where  $a$  and  $b$  are complex numbers such that  $|a|^2 + |b|^2 = 1$  where  $|a|$  is the modulus of  $a$ .

*the Pythagorean Thm*

- A qubit is said to be in superposition of states  $|0\rangle$  and  $|1\rangle$ .

- If the qubit is observed (measured) with respect to basis  $B = \{|0\rangle, |1\rangle\}$ , it immediately "makes a decision." It decides to be 0 with probability  $|a|^2$  and 1 with probability  $|b|^2$ .

What happens if you measure the same qubit twice with respect to the same basis?

*get the same measurement*

*if before  $|1\rangle$ , now also  $|1\rangle$*

# Orthonormal Bases

There are orthonormal bases other than  $B$ .

For example, let:

$$|0'\rangle = 1/\sqrt{2} (|0\rangle + |1\rangle)$$

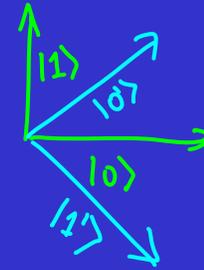
$$|1'\rangle = 1/\sqrt{2} (|0\rangle - |1\rangle)$$

Let  $O = \{ |0'\rangle, |1'\rangle \}$ , this is another orthonormal basis.

Note that

$$|0\rangle = 1/\sqrt{2} (|0'\rangle + |1'\rangle)$$

$$|1\rangle = 1/\sqrt{2} (|0'\rangle - |1'\rangle)$$



# Quantum Key Distribution

Alice and Bob need a one-way (public) quantum channel (through which they can exchange qubits) and a public (classical) channel (to send normal bits).

Alice and Bob will use the quantum channel and the classical channel to establish the key using two-stage protocol, called the BB84 protocol.

# BB84: Stage 1 protocol

## Communication over a quantum channel

1. Alice flips a fair coin to generate a random sequence of zeros and ones (normal bits). This random sequence will be used to construct the secret key, shared only by Alice and Bob.
2. For each bit in the random sequence, Alice flips a fair coin. If heads, she sends bit  $b$  as  $|b\rangle$ . If tails, she sends bit  $b$  as  $|b'\rangle$ .
3. Each time that Bob receives a qubit, he has no way of knowing which basis was used. He flips a fair coin to select one of the two bases, and he measures the qubit using that basis. We will see that if he guesses correctly, the measurement will correspond to the bit sent by Alice. If he guessed incorrectly, the measurement will agree with Alice in 50% of the cases.

## BB84: Stage 1 - Case analysis

If Alice sends  $|0\rangle$ , and Bob measures using basis B, the measurement will be 0 with probability 1.

If Alice sends  $|0\rangle$ , and Bob measures using basis O, the measurement will be 0 with probability  $1/2$ , since:

$$|0\rangle = 1/\sqrt{2} (|0'\rangle + |1'\rangle)$$

Do the other cases.

# BB84: Stage 2 protocol

## Communication over a public channel

### Phase 1: raw key extraction

1. Bob communicates to Alice which bases he used for each of his measurements.
2. Alice communicates to Bob which of his measurements were made using the correct basis.
3. Both Alice and Bob discard the bits for which they used incompatible bases. The resulting bitstrings are the **raw keys**. If Eve has not eavesdropped, the raw keys are the same.

# BB84: Evil Eavesdropping Eve

What happens if Eve eavesdrops on the quantum channel? For now, let's examine **opaque eavesdropping**: Eve intercepts the qubit, measures it, and sends the qubit on to Bob.

Like Bob, Eve does not know which basis Alice is using. That means that with probability  $1/2$  she uses the wrong basis when eavesdropping.

For example, if Alice sends  $|0\rangle$ , and Eve eavesdrops using basis  $O$ , what is the probability that Eve measures  $0$ ?

If Eve's measurement is  $0$ , the qubit after measurement will be  $|0'\rangle$ . Suppose Bob measures using the same basis as Alice, i.e., with basis  $B$ . Then Bob's measurement will be  $0$  with probability  $1/2$ . Since Bob uses the same basis as Alice, this bit will not be discarded, but it is wrong with probability  $1/2$ .

# BB84: Stage 2 protocol

## Communication over a public channel

### Phase 2: error estimation

Over the public channel, Alice and Bob compare small portions of their raw keys to determine the error rate. If the error rate is greater than 0, they know that Eve has been eavesdropping. They discard the keys and start from scratch.

If the error rate is 0, they will both delete the disclosed bits from their raw keys, obtaining the final key.

# More about quantum cryptography

- BB84 with noise
- other quantum cryptography protocols (E91, S09, ...)
- quantum key distribution commercially available
- the longest distance over which quantum key distribution was used (as of early 2007), is 148.7 km, using optic fiber (by Los Alamos National Laboratory / NSIT)
- attacks include implementation weaknesses, e.g. it is hard to guarantee that a source emits exactly one quantum
- other quantum computing results:
  - Shor's factoring algorithm (polytime, with high prob.)
  - discrete logarithm in polytime