12.6.3 Quantum key distribution

Quantum key distribution (QKD) is a protocol which is *provably* secure, by which private key bits can be created between two parties over a *public* channel. The key bits can then be used to implement a classical private key cryptosystem, to enable the parties to communicate securely. The only requirement for the QKD protocol is that qubits can be communicated over the public channel with an error rate lower than a certain threshold. The security of the resulting key is guaranteed by the properties of quantum information, and thus is conditioned only on fundamental laws of physics being correct!

Basic idea behind QKD $\Longrightarrow$ Eve cannot gain any information from the qubits transmitted from Alice to Bob without disturbing their state.

1st : Eve cannot clone Alice's qubit, by no-cloning theorem

2nd :

Proposition 12.18: **(Information gain implies disturbance)** In any attempt to distinguish between two non-orthogonal quantum states, information gain is only possible at the expense of introducing disturbance to the signal.

Proof

Let $|\psi\rangle$ and $|\varphi\rangle$ be the non-orthogonal quantum states Eve is trying to obtain information about. By the results of Section 8.2, we may assume without loss of generality that the process she uses to obtain information is to unitarily interact the state ($|\psi\rangle$ or $|\varphi\rangle$) with an ancilla prepared in a standard state $|u\rangle$. Assuming that this process does not disturb the states, in the two cases one obtains

$$|\psi\rangle|u\rangle \rightarrow |\psi\rangle|v\rangle \tag{12.175}$$

$$|\varphi\rangle|u\rangle \rightarrow |\varphi\rangle|v'\rangle\,. \tag{12.176}$$

Eve would like $|v\rangle$ and $|v'\rangle$ to be different so that she can acquire information about

the identity of the state. However, since inner products are preserved under unitary transformations, it must be that

$$\langle v|v'\rangle \langle \psi|\varphi\rangle = \langle u|u\rangle \langle \psi|\varphi\rangle \tag{12.177}$$

$$\langle v|v'\rangle = \langle u|u\rangle = 1\,, \tag{12.178}$$

which implies that $|v\rangle$ and $|v'\rangle$ must be identical. Thus, distinguishing between $|\psi\rangle$ and $|\varphi\rangle$ must inevitably disturb at least one of these states. □

We make use of this idea by transmitting non-orthogonal qubit states between Alice and Bob. By checking for disturbance in their transmitted states, they establish an upper bound on any noise or eavesdropping occurring in their communication channel. These 'check' qubits are interspersed randomly among data qubits (from which key bits are later extracted), so that the upper bound applies to the data qubits as well. Alice and Bob then

The BB84 protocol

Alice begins with 2 bits strings, a and b, each of $(4+\delta)n$ random classical bits.

She then encodes these bit strings as a block of $(4+\delta)n$ qubits.

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

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

and each qubit is one of the four states:

$$|\psi_{00}\rangle = |0\rangle$$

$$|\psi_{10}\rangle = |1\rangle$$

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

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

The effect of this procedure is to encode a in the basis X or Z, as determined by b.

ie.,

If $b_k = 1$ then $|\psi_{a_k 1}\rangle = \begin{cases} |+\rangle & \text{for } a_k = 0 \\ |-\rangle & \text{for } a_k = 1 \end{cases}$

The 4 states are not all mutually orthogonal, and therefore no measurement can distinguish b/w all of them with certainty.

Alice then sends $|\psi\rangle$ to Bob, over their public quantum communication channel. Bob receives $\mathcal{E}(|\psi\rangle\langle\psi|)$, where $\mathcal{E}$ describes the quantum operation due to the combined effect of the channel and Eve's actions. At this point, Alice, Bob and Eve each have their own states described by separate density matrices.

Since Alice hasn't revealed b, Eve has no knowledge of what basis she should have measured in to eavesdrop on the communication. At best she can only guess, and if her guess was wrong, then she would have disturbed the state received by Bob.

Moreover, whereas in reality the noise $\mathcal{E}$ may be partially due to the environment (a poor channel) in addition to Eve's eavesdropping, it doesn't help Eve to have complete control over the channel, so that she is entirely responsible for $\mathcal{E}$.

Bob also finds $\mathcal{E}(|\psi\rangle\langle\psi|)$ uninformative at this point, because he does not know anything about b.
Nevertheless, he goes ahead & measure each qubit in basis $\times$ or $+$, as determined by a random $(4+\delta)n$ bit string b', which he creates on his own.

Let Bob's measurement result be a'. After this Alice publicly announces b, & by discussion over a public channel, Bob and Alice discard all bits in $\{a', a\}$ except those for which corresponding bits of b' & b are equal. Their remaining bits satisfy $a' = a$, since for these bits Bob measured in the same basis Alice prepared in.

Note that b reveals nothing about either a, or the bits a' resulting from Bob's measurement, but it is important that Alice not publish b until after Bob announces reception of Alice's qubits.

For simplicity, let Alice & Bob keep just an bits of their result. δ can be chosen sufficiently large so that this can be done with exponentially high probability.

Now, Alice & Bob perform some tests to determine how much noise or eavesdropping happened during their communication —

Alice selects n bits of their an bits at random, and publicly announce the selection. Bob & Alice then publish & compare the values of these check bits. If more than t bits disagree, then they abort & retry the protocol from the start.

t is selected such that if the test passes, then they can apply information reconciliation and privacy amplification algorithms to obtain m acceptably secret shared key bits from the remaining n bits.

The BB84 QKD protocol

1: Alice chooses $(4 + \delta)n$ random data bits.
2: Alice chooses a random $(4 + \delta)n$-bit string b. She encodes each data bit as $\{|0\rangle, |1\rangle\}$ if the corresponding bit of b is 0 or $\{|+\rangle, |-\rangle\}$ if b is 1.
3: Alice sends the resulting state to Bob.
4: Bob receives the $(4 + \delta)n$ qubits, announces this fact, and measures each qubit in the X or Z basis at random.
5: Alice announces b.
6: Alice and Bob discard any bits where Bob measured a different basis than Alice prepared. With high probability, there are at least $2n$ bits left (if not, abort the protocol). They keep $2n$ bits.
7: Alice selects a subset of n bits that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
8: Alice and Bob announce and compare the values of the n check bits. If more than an acceptable number disagree, they abort the protocol.
9: Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

The B92 Protocol

The BB84 protocol can be generalized to use other states and bases, and similar conclusions hold. In fact, a particularly simple protocol exists in which only two states are used. For simplicity, it is sufficient to consider what happens to a single bit at a time; the description easily generalizes to block tests just as is done in BB84.

Suppose,

Alice prepares one random classical bit a, & depending on the result, sends Bob:

$$|\psi\rangle = \begin{cases} |0\rangle & \text{if } a=0 \\ \frac{|0\rangle+|1\rangle}{\sqrt{2}} & \text{if } a=1 \end{cases}$$

Depending on a random classical bit a' which he generates, Bob subsequently measures the qubit he receives from Alice in either the Z basis $|0\rangle, |1\rangle$ (if $a'=0$), or in the X basis $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ (if $a'=1$). From his measurement, Bob obtains the result b.

$$b = \begin{cases} 0 & \text{if Bob obtain } |0\rangle \text{ or } |+\rangle \\ 1 & \text{" } \quad |1\rangle \text{ or } |-\rangle \end{cases}$$

Bob then publicly announces b, but keeps a' secret.

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \quad \& \quad |1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

Case 1 $(b = 0)$:

Bob gets $|0\rangle$ or $|+\rangle$ upon measurement

$\Rightarrow a' = a$ (or) $a' = 1 - a$ (some times)
(for sure)

Case 2 $(b = 1)$:

Bob gets $|1\rangle$ or $|-\rangle$ upon measurement

$\Rightarrow$ happens iff $a' = 1 - a$

∴ Only if $a' = 1 - a$ will Bob obtain $b = 1$, and that occurs with probability $1/2$.

Alice & Bob conduct a public discussion keeping only those pairs $\{a, a'\}$ for which $b = 1$.

$\Rightarrow$ The final key is a for Alice & $1 - a'$ for Bob.

The EPR protocol

The key bits generated in the BB84 and B92 protocols may appear to have been originated by Alice. However, it turns out that the key can be seen to arise from a fundamentally random process involving the properties of entanglement.

Suppose,

Alice & Bob share a set of n entangled pairs of qubits in the state

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$ (EPR pair)

These states are known as EPR pairs. Obtaining these states could have come about in many different ways; for example, Alice could prepare the pairs and then send half of each to Bob, or vice versa. Alternatively, a third party could prepare the pairs and send halves to Alice and Bob. Or they could have met a long time ago and shared them, storing them until the present.

Alice and Bob then select a random subset of the EPR pairs, and test to see if they violate Bell's inequality (Equation (2.225), on page 115 in Section 2.6), or some other appropriate test of fidelity. Passing the test certifies that they continue to hold sufficiently pure, entangled quantum states, placing a lower bound on the fidelity of the remaining EPR pairs (and thus any noise or eavesdropping). And when they measure these in jointly determined random bases, Alice and Bob obtain correlated classical bit strings from which they can obtain secret key bits as in the B92 and BB84 protocols.

$$|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2}}\left[\left(\frac{|+\rangle + |-\rangle}{\sqrt{2}} \otimes \frac{|+\rangle + |-\rangle}{\sqrt{2}}\right) + \left(\frac{|+\rangle - |-\rangle}{\sqrt{2}} \otimes \frac{|+\rangle - |-\rangle}{\sqrt{2}}\right)\right]$$

$$= \frac{1}{2\sqrt{2}}\left[\left(|++\rangle + |+-\rangle + |-+\rangle + |--\rangle\right) + \left(|++\rangle - |+-\rangle - |-+\rangle + |--\rangle\right)\right]$$

$$= \frac{|++\rangle + |--\rangle}{\sqrt{2}}$$

Suppose that,

Alice prepares a random classical bit b, and according to it, measures her half of the EPR pair in either the $|0\rangle, |1\rangle$ basis or in the basis $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ obtaining a.

Let Bob do identically,

measuring in his randomly chosen basis b' and obtaining a'.

Now, they communicate b & b' over a public classical channel, and keep as their key only those $\{a, a'\}$ for which $b = b'$.

This key is undetermined until Alice or Bob performs a measurement on their EPR pair half.