Introduction to Quantum Key Distribution.

BB84 and B92 protocols.

In these notes we introduce one of the first applications of QM for quantum communication namely the generation of a common secret key between two distant parties. We specifically concentrate here first on the Bennet-Brassard in 1984 and then we briefly discuss a variant called the Bennet 1992 protocol.

We suppose that Alice (A) and Bob (B) are two distant parties which want to generate a one-time pad or in other words a common secret string of bits while being distant. The one-time pad should not be communicated from A to B or from B to A.

A "one-time pad" is a sequence $x_1 \dots x_N$ of secret bits shared by A and B. When A wants to encrypt a message $m_1 m_2 \dots m_N$ (with $m_i \in \{0, 1\}$) she does $m_i \to \tilde{m}_i = m_i \oplus x_i$ modulo 2. The encrypted message $\tilde{m}_i$ is sent to Bob who decrypts it by $\tilde{m}_i \to \tilde{m}_i \oplus x_i = m_i$. An eavesdropper (Eve) cannot decrypt $\tilde{m}_i$ as long as the one-time pad has never been revealed or intercepted.

Note: sometimes one talks about quantum cryptography but there is an abuse of language and it is more correct to talk about Quantum Key Distribution.

BB84 protocol.

Phase 1 **Encoding in A lab:** "A" generates random bits $c_1 c_2 \cdots c_N \in \{0,1\}^N$. These are kept secret for the moment. For $c_i = 0$ she generates a qubit in the state $|x_i\rangle \in \{|0\rangle, |1\rangle\}$ where x_i is random. (She can for example randomly orient a polarizer in the horizontal/vertical direction to generate a polarization state of a photon.). For $c_i = 1$ she generates a qubit in the state $\frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$ where the choice of $\pm$ is random. (She can do this by orienting a polarizer at $45^\circ / 135^\circ$).

In summary Alice has generated a

random sequence $e_1 \dots e_N \in \{0,1\}^N$ and qubits in the states $H^{e_i}|x_i\rangle$.

We recall that $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ the Hadamard matrix operates as

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad ; \quad H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Alice sends at each instant $i = 1 \dots n$ the qubit $H^{e_i}|x_i\rangle$ to Bob while keeping e_i still secret.

Phase 2 **Bob's decoding procedure in B-B84:**

Bob generates a sequence $d_1 \dots d_N \in \{0,1\}^N$ which he keeps secret.

For $d_i = 0$ he measures the received

qubit in the computational basis $\{|0\rangle, |1\rangle\}$.

For $d_i = 1$ he measures the received qubit in the Hadamard basis $\left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$.

So for $d_i = 0$ he gets meas outcome of the qubit $|0\rangle$ or $|1\rangle$. He records a classical bit y_i as follows $|0\rangle \rightarrow \underbrace{0}_{y_i}$; $|1\rangle \rightarrow \underbrace{1}_{y_i}$.

And for $d_i = 1$ he gets the measurement outcome $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ or $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. He records y_i as follows $\frac{|0\rangle + |1\rangle}{\sqrt{2}} \rightarrow y_i = 0$; $\frac{|0\rangle - |1\rangle}{\sqrt{2}} \rightarrow y_i = 1$.

[For example these measurements can be done with analysers and photodetectors.]

Phase 3 Public communication phase

A and B exchange their bits $e_1 \dots e_N$ and $d_1 \dots d_N$ on a (public) classical communication channel. It is important that they do so <u>after</u> they collected their measurement results which are kept secret.

- If $e_i = d_i$ they keep x_i and y_i. They also know (as shown below) that $x_i = y_i$ and this constitutes a common secret bit for the one-time pad.

- If $e_i \neq d_i$ they discard x_i and y_i. In fact as shown below we have

$$\text{prob}(x_i = y_i) = \text{prob}(x_i \neq y_i) = 1/2$$

At this point A & B have managed to generate $\frac{N}{2}$ common secret bits since $\text{Prob}(e_i = d_i) = \frac{1}{2}$. These are the bits used in the final one-time pad but there is first a security check :

Phase 4 **Final security check**

A & B exchange a fraction $\epsilon \frac{N}{2}$ of their "supposedly" common bits ($0 < \epsilon << 1$) over the public classical channel and check if

$$\#(\text{bits s.t } x_i = y_i) \approx \epsilon \frac{N}{2} .$$

If the test passes to "sufficiently good precision" they declare the one-time pads secure. Otherwise they stop the communication process.

In theory the test should pass exactly meaning

that $\#(\text{bits s.t } x_i = y_i) = \epsilon \frac{N}{2}$ exactly.

But in practice there will always be a small amount of noise in the channels and maybe also measurement errors. This noise should be characterized and low enough so that one may be certain that the errors come from noise and not from the interference of an eavesdropper.

Analysis of BB84.

We first show that

$$\begin{cases} \text{Prob}(x_i = y_i \mid e_i = d_i) = 1 \\ \text{Prob}(x_i \neq y_i \mid e_i = d_i) = 0 \end{cases}$$

and

$$\begin{cases} \text{Prob}(x_i = y_i \mid e_i \neq d_i) = 1/2 \\ \text{Prob}(x_i \neq y_i \mid e_i \neq d_i) = 1/2 \end{cases}$$

Proof: Alice sends $H^{e_i}|x_i\rangle$ and Bob thus receives this state. He measures in the basis $\{H^{d_i}|0\rangle, H^{d_i}|1\rangle\}$ so he gets the measurement outcome

- $H^{d_i}|0\rangle$ (so he records $y_i = 0$) with probability $|\langle 0|H^{d_i}H^{e_i}|x_i\rangle|^2$
- $H^{d_i}|1\rangle$ (so he records $y_i = 1$) with probability $|\langle 1|H^{d_i}H^{e_i}|x_i\rangle|^2$

$$\text{Prob}(x_i = y_i \mid e_i = d_i) = \text{Prob}(y_i = 0, x_i = 0 \mid e_i = d_i) + \text{Prob}(y_i = 1, x_i = 1 \mid e_i = d_i)$$

$$= \text{Prob}(y_i = 0 \mid x_i = 0, e_i = d_i)\,\text{Prob}(x_i = 0 \mid e_i = d_i) + \text{Prob}(y_i = 1 \mid x_i = 1, e_i = d_i)\,\text{Prob}(x_i = 1 \mid e_i = d_i)$$

$$= \text{Prob}(y_i = 0 \mid x_i = 0, e_i = d_i)\ \text{Prob}(x_i = 0)$$

$$+ \text{Prob}(y_i = 1 \mid x_i = 1, e_i = d_i)\ \text{Prob}(x_i = 1)$$

- For $e_i = d_i$ we have $H^{e_i} H^{d_i} = \mathbb{1}$. Thus

$$\begin{cases} \text{Prob}(y_i = 0 \mid x_i = 0, e_i = d_i) = |\langle 0 \mid 0 \rangle|^2 = 1 \\ \text{Prob}(y_i = 1 \mid x_i = 1, e_i = d_i) = |\langle 1 \mid 1 \rangle|^2 = 1 \end{cases}$$

Also in an ideal situation $\text{Prob}(x_i = 0) = \text{Prob}(x_i = 1) = \frac{1}{2}$.

$$\Rightarrow \boxed{\text{Prob}(x_i = y_i \mid e_i = d_i) = 1}$$

- For $e_i \neq d_i$ we have $H^{e_i} H^{d_i} = H$. Thus

$$\begin{cases} \text{Prob}(y_i = 0 \mid x_i = 0, e_i \neq d_i) = |\langle 0 | H | 0 \rangle|^2 = \frac{1}{2} \\ \text{Prob}(y_i = 1 \mid x_i = 1, e_i \neq d_i) = |\langle 1 | H | 1 \rangle|^2 = \frac{1}{2} \end{cases}$$

Therefore a similar calculation shows

$$\boxed{\text{Prob}(x_i = y_i \mid e_i \neq d_i) = \frac{1}{2} \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{2}}.$$

■

Attacks from Eve.

The general idea is that if Eve intercepts a qubit in the state $H^{c_i}|x_i\rangle$ (sent by A) she must measure it to extract some information. However she does not know which is the correct basis: she does not know c_i!

So she will choose a random basis (say) $E_i \in \{0, 1\}$: for $E_i = 0 \rightarrow$ computational basis, for $E_i = 1 \rightarrow$ Hadamard basis.

Once measured the photon is left in state $H^{E_i}|0\rangle$ or $H^{E_i}|1\rangle$ and sent to Bob. This state is the same undisturbed state $H^{c_i}|x_i\rangle$ when $E_i = c_i$. Otherwise if $E_i \neq c_i$ it is the same state only with probability $1/2$.

Bob will thus receive the correct state $H^{e_i}|x_i\rangle$ when $E_i' = e_i$ which happens with prob $1/2$.

And he will receive the wrong state when $E_i' \neq e_i$ which also happens with prob $1/2$.

Let us compute the prob of $x_i' = y_i'$ given $e_i' = d_i'$:

$$\text{Prob}(x_i' = y_i' / e_i' = d_i')$$

$$= \text{Prob}(x_i' = y_i' / e_i' = d_i', E_i' = e_i') \, \text{Prob}(E_i' = e_i')$$

$$+ \text{Prob}(x_i' = y_i' / e_i' = d_i', E_i' \neq e_i') \, \text{Prob}(E_i' \neq e_i')$$

For $(e_i' = d_i', E_i' = e_i')$ we have $d_i' = E_i'$ thus as before $\text{Prob}(x_i' = y_i' / e_i' = d_i', E_i' = e_i') = 1$.

For $(e_i' = d_i', E_i' \neq e_i')$ we have $d_i' \neq E_i'$ thus as before we will have $\text{Prob}(x_i' = y_i' / e_i' = d_i', E_i' \neq e_i') = \frac{1}{2}$

$$\Rightarrow \text{Prob}(x_i' = y_i' / e_i' = d_i') = 1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4} = 75\%.$$

Thus during the security check of the noise level is low enough A & B will notice the presence of Eve.

Remark: Another attack of Eve would be to intercept the qubit in state $H^{e_i}|x_i\rangle$ and attempt to create a copy $H^{e_i}|x_i\rangle \otimes H^{e_i}|x_i\rangle$; keep the copy till the encoding e_i and measurement bases d_i are revealed, and do the measurements in the correct basis later on. However by the no-cloning theorem it is impossible to copy all four possible states $|0\rangle$, $|1\rangle$, $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ with the same unitary transformation. So Eve has only a $1/2$ chance to get the correct "copy".

BB 84 protocol:

We notice that in BB 84 A use two encoding basis $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. This is sometimes called "conjugate coding".

In fact one can devise a simpler protocol where she uses only two non-orthogonal states

$$|0\rangle \quad \text{and} \quad |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

- So A generates $c_i \in \{0,1\}$ at random for $i = 1 \dots N$ and sends $|0\rangle$ if $c_i = 0$ and $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ if $c_i = 1$.
- Bob generates $d_i \in \{0,1\}$ at random and measure in the comp basis if $d_i = 0$ & in the Hadamard basis if $d_i = 1$. His possible outcomes are $|0\rangle$, $|1\rangle$, $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$, $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

When he gets $|0\rangle$ or $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ he records $y_i = 0$

When he gets $|1\rangle$ or $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ he records $y_i = +1$.

- We show below that:

$$\text{Prob}\left(e_i = 1 - d_i \mid y_i = 1\right) = 1 .$$

Thus the idea this time is that B reveals y_i on a public communication channel.

If $y_i = 1$:
they know that $e_i = 1 - d_i$ which thus form their one-time pad (Bob say has to take

$$d_i \to \tilde{d}_i = 1 - d_i$$

to match the e_i of Alice)

If on the other hand $y_i = 0$ then they discard e_i & d_i,

Remark: In this protocol the one-time pad is formed by the encoding/decoding basis bits.

- finally they sacrifice a small fraction of bits for a security check.

Analysis of BB92:

We prove that $\text{Prob}(e_i = 1-d_i \,/\, y_i = 1) = 1$.

By Bayes law this probability is

$$\frac{\text{Prob}(y_i = 1 \,/\, e_i = 1-d_i)\,\text{Prob}(e_i = 1-d_i)}{\text{Prob}(y_i = 1)}$$

Now $\boxed{\text{Prob}(e_i = 1-d_i) = \frac{1}{2}}$. When $e_i = 1-d_i$, for example $e_i = 1$, $d_i = 0$ the transmitted bit is $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and the measurement is done in the $\{|0\rangle, |1\rangle\}$ basis. The result is $|0\rangle$ with prob $1/2$ and $|1\rangle$ with prob $1/2$. So Bob records $y_i = 1$ with prob $1/2$. For $e_i = 0$, $d_i = 1$ the situation is similar.

Thus $\boxed{\text{Prob}(y_i = 1 \,/\, e_i = 1-d_i) = 1/2}$.

Finally for the denominator

$$\text{Prob}(y_i = 1) = \text{Prob}(y_i = 1 / c_i = 1 - d_i)\ \text{Prob}(c_i = 1 - d_i)$$

$$+ \underbrace{\text{Prob}(y_i = 1 / c_i = d_i)}_{0 \leftarrow \text{"exercise"}}\ \text{Prob}(c_i = d_i)$$

$$= \frac{1}{2} \cdot \frac{1}{2} + 0 \cdot \frac{1}{2} = \frac{1}{4} .$$

Putting everything together:

$$\text{Prob}(c_i = 1 - d_i / y_i = \pm 1) = \frac{1/2 \cdot 1/2}{1/4} = 1 .$$

■