QUANTUM KEY DISTRIBUTION.

This lecture is about the QKD protocol of Bennett and Brassard 1984 (BB84) for the generation of a common one-time pad shared by two distant parties Alice & Bob.

One-time pads: this is a sequence of secret bits $z_1 z_2 \dots z_M$; $z_i \in \{0,1\}$ shared by A & B (which are supposed to be at two distant locations). It is used as follows. If A has a message $m_1 m_2 \dots m_M$ to communicate she encodes it as: $z_1 \oplus m_1 \; z_2 \oplus m_2 \dots z_M \oplus m_M$ and sends the sequence to B. Then B can decode it as

$$(z_i \oplus m_i) \oplus z_i = m_i \quad (\text{mod } 2)$$

Information theoretically this is a secure scheme if the one-time pad i.i.d uniformly random and is used only once.

The trouble is how to distribute it to A & B and make sure it is not intercepted.

The point of the QKD is that we do not distribute the one-time pad but generate it directly in the labs of A & B.

BB 84 protocol for QKD.

We will review the main phases;

1) Encoding phase of A.
2) Decoding phase of B.
3) Public communication phase of A & B.
4) Generation of common secret bit sequence and the "security check".

Finally we will review some possible attacks from Eavesdroppers and argue the protocol is secure.

1) Encoding in A-lab.

- A generates a unif random iid sequences of classical bits

$$x_1 \; x_2 \; \dots \; x_N \; \in \{0,1\} \quad \text{(secret always)}$$

$$e_1 \; e_2 \; \dots \; e_N \; \in \{0,1\} \quad \text{(secret for the moment)}$$

- For $e_i = 0$ A prepares a qubit $|x_i\rangle \in \{|0\rangle, |1\rangle\}$

(in the computational basis)

- For $e_i = 1$ A prepares a qubit

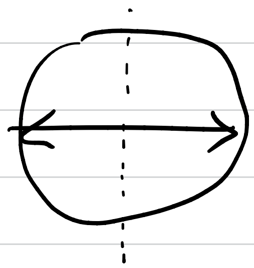
$$H|x_i\rangle \in \left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$$

(in Hadamard basis)

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

Remark: physically you can think about polarized states of photons for the qubits.

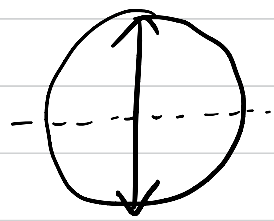
- A uses polarizers oriented as



to produce $|0\rangle$ horizontal pol

if $e_i = 0$
$x_i = 0$

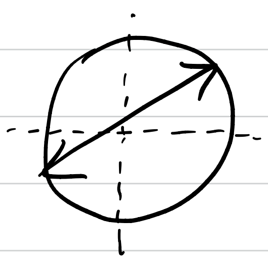
&



to produce $|1\rangle$ vertical pol.

if $e_i = 0$
$x_i = 1$.

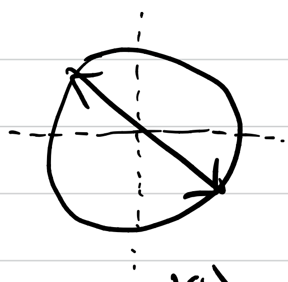
- A uses polarizers oriented as



to produce $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$

if $e_i = 1$
$x_i = 0$

&



to produce $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

if $e_i = 1$
$x_i = 1$.

<u>To summarize</u>: at each instant $i = 1 \dots N$

A has prepared a qubit (polarization state say)

in state $H^{e_i} |x_i\rangle$.

$$\in$$

$$\left\{ |0\rangle, |1\rangle, \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$$

- A sends this qubit (photon) to B through a quantum channel (optic fiber, free space comm)

2) Decoding in B - lab.

Bob receives the qubit (photon polarization) for each $i = 1 \dots N$. He has no idea of the state.

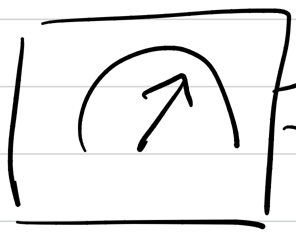
He does a measurement at each instant.

- Bob generates an iid unif random sequence $d_1 d_2 \ldots d_N \in \{0,1\}$.

- For $d_i = 0$ he chooses the measurement basis $\{|0\rangle, |1\rangle\}$ to do his measurement.

His output is

incoming state at time i $\rightarrow$



$\rightarrow |0\rangle$ registers $y_i = 0$

$\rightarrow |1\rangle$ registers $y_i = 1$

- For $d_i = 1$ he chooses the measurement basis $\left\{ \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$. His output is

incoming state at time i $\rightarrow$

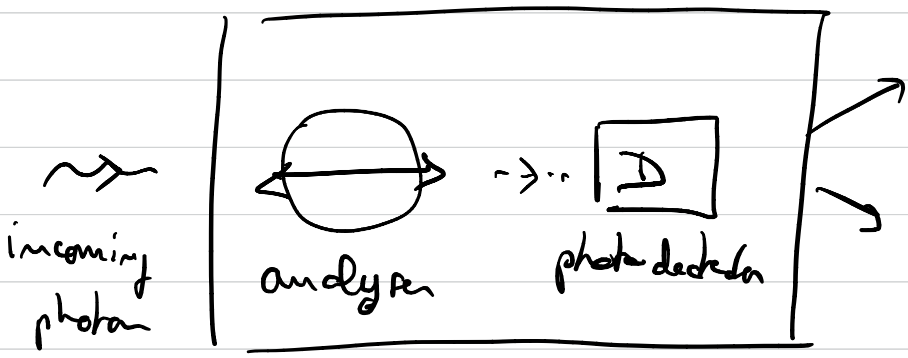
$\rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ registers $y_i = 0$

$\rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ registers $y_i = 1$

$\boxed{\text{In summary his output state is } H^{d_i} |y_i\rangle}$

Remark: physically you can think of the following measurement process in Bob's lab

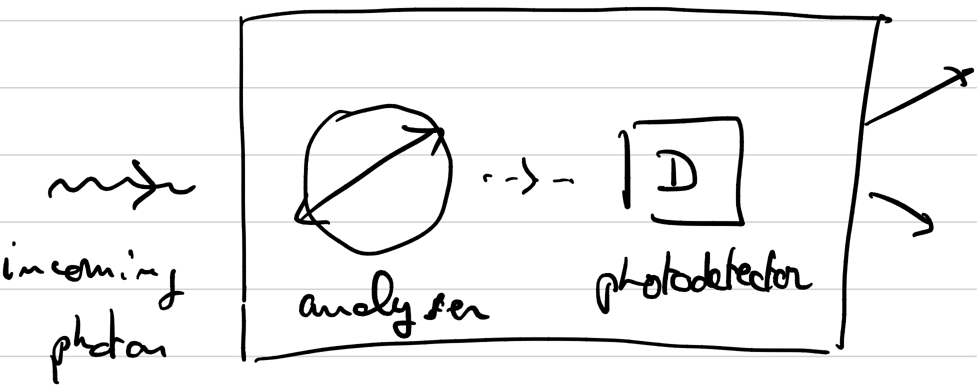
- for $d_i = 0$



clic $y_i = 0$; $|0\rangle$

no clic $y_i = 1$; $|1\rangle$

- for $d_i = 1$



clic $y_i = 0$; $\frac{|0\rangle + |1\rangle}{\sqrt{2}}$

no clic $y_i = 1$; $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$

- In summary Bob's measurement leaves the photon in state $H^{d_i}|y_i\rangle$ where $y_1 y_2 \cdots y_N \in \{0,1\}$ is a random binary sequence.

According to the Measurement Principle we have

Prob[to get $H^{d_i}|y_i\rangle$ given that incoming state is $H^{e_i}|x_i\rangle$]

$$= \left| \langle y_i | H^{d_i} H^{e_i} | x_i \rangle \right|^2$$

We will use this later on

3) Public communication phase.

Now (and not before!) A & B reveal over a public classical communication line their encoding and decoding sequences $e_1 \dots e_N$ & $d_1 \dots d_N$.
Anybody may know these sequences. However note that $x_1 \dots x_N$ & $y_1 \dots y_N$ are NOT revealed,

4) Generation of one-time pad.

- If $e_i = d_i$ A & B keeps the bits x_i and y_i. It turns out that $x_i = y_i$ (as proved later) and will go in the one-time pad.

- If $e_i \neq d_i$ A & B discard the bits x_i and y_i. It turns out that these may be different or equal (with prob 1/2 typically) and are useless,

- Security check:

→ out of $i = 1, \dots, N$ such that $e_i = d_i$ (for which $x_i = y_i$)

A and B select $\frac{\varepsilon N}{2}$ such instants $(0 < \varepsilon \ll 1)$ and sacrifice (burn) the (x_i, y_i) by exchanging them over the public channel. Thus they check if indeed $x_i = y_i$. If this test passes they conclude that the protocol has worked well and nobody has been eavesdropping.

→ Essentially the security check tests if

$$\frac{1}{(\varepsilon N/2)} \# \left\{ i \in \left[\varepsilon \tfrac{N}{2}\right] \subset \{1, \dots N\} \text{ s.t } e_i = d_i \,\middle|\, x_i = y_i \right\}$$

$\simeq 1$ with "sufficient accuracy".

Remark: Noise of channel should be specified and low enough so that the test distinguishes Noise from Eavesdropper.

This whole protocol (phases 1-2-3-4) is justified by the following Lemma:

Lemma

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

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

Proof

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

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

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

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

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

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

Now $\text{Prob}(x_i=0) = \text{Prob}(x_i=1) = 1/2$, and

by the meas principle:

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

$$= |\langle 0| \underbrace{H^{d_i} H^{e_i}}_{\mathbb{1} \text{ for } e_i=d_i} |0\rangle|^2 = |\langle 0|0\rangle|^2 = 1.$$

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

$$= |\langle 1| \underbrace{H^{d_i} H^{e_i}}_{\mathbb{1} \text{ for } e_i=d_i} |1\rangle|^2 = |\langle 1|1\rangle|^2 = 1.$$

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

For the second case $e_i \neq d_i$ we proceed in the same way:

$$\mathbb{P}(x_i = y_i \mid e_i \neq d_i) = \mathbb{P}(y_i = 0 \mid x_i = 0, e_i \neq d_i)\, \mathrm{Prob}(x_i = 0) + \mathbb{P}(y_i = 1 \mid x_i = 1, e_i \neq d_i)\, \mathrm{Prob}(x_i = 1)$$

and by the meas principle:

$$\mathbb{P}(y_i = 0 \mid x_i = 0, e_i \neq d_i) = |\langle 0| \underbrace{H^{d_i} H^{e_i}}_{e_i \neq d_i \Rightarrow H^{d_i} H^{e_i} = H} |0\rangle|^2$$

$$= |\langle 0 | H | 0\rangle|^2$$

$$= \left(\frac{1}{\sqrt{2}}\right)^2 |\underbrace{\langle 0 | 0\rangle}_{1} + \underbrace{\langle 0 | 1\rangle}_{0}|^2$$

$$= \frac{1}{2}$$

$$\mathbb{P}(y_i = 1 \mid x_i = 1, e_i \neq d_i) = |\langle 1 | H^{d_i} H^{e_i} | 1\rangle|^2$$

$$= |\langle 1 | H | 1\rangle|^2$$

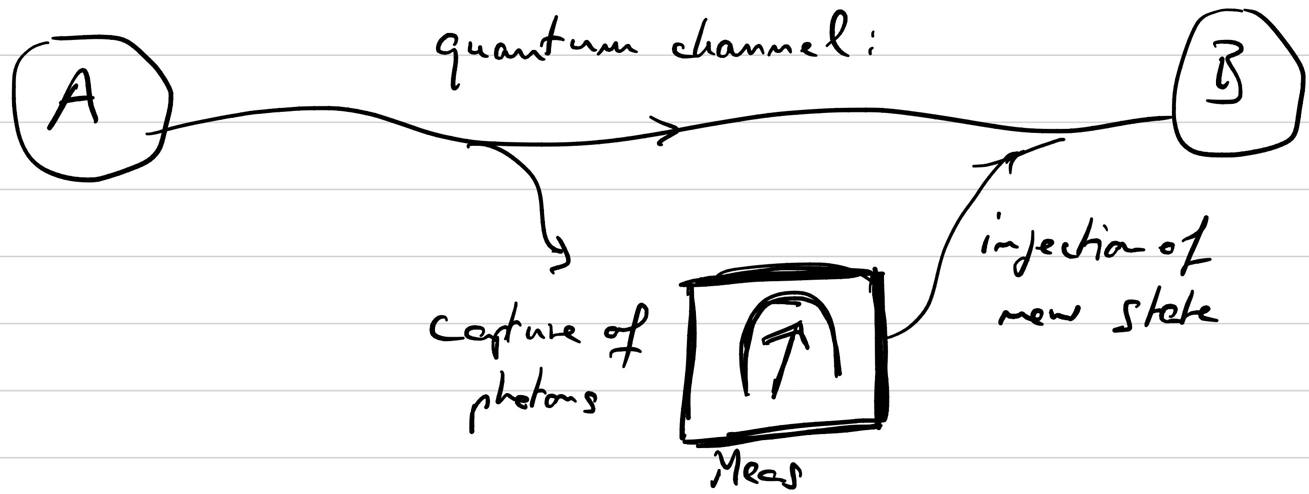
$$= \left(\frac{1}{\sqrt{2}}\right)^2 |\underbrace{\langle 1 | 0\rangle}_{0} + \underbrace{\langle 1 | 1\rangle}_{1}|^2$$

$$= 1/2$$

Attack from an Eavesdropper.

A complete discussion of security of the scheme goes well beyond these notes. One must imagine that an eavesdropper captures photons on the quantum channel, processes them (with unitary evolutions & measurements), sends them back to Bob etc... The space of possible attacks is huge and here we just scratch the surface of this subject by analyzing a very simple type of attack.

"Measurement attack":



- Eve captures photons in state : $H^{e_i} |x_i\rangle$
- Measures in computational or Hadamard basis according to a random sequence she generates

$$E_1 E_2 \dots E_N \in \{0, 1\}$$

[Note: she has no idea of e_i, d_i before public communication phase].

The measurement leaves the photon in state:

$$H^{E_i} |y_i^{Eve}\rangle \quad ; \quad y_i^{Eve} \in \{0, 1\}.$$

[Again, this can be done with an analyser + photodetector system and $y_i^{Eve} = 0$ if D clicks, $y_i^{Eve} = 1$ if D does not click],

- State $H^{E_i} |y_i^{Eve}\rangle$ is forwarded to Bob.

- Bob Measures as usual [he does not know what happens on the quantum channel] and he gets a state $H^{d_i}|y_i\rangle$ as before

but this time with probability:

$$|\langle y_i| H^{d_i} H^{E_i} |y_i^{Eve}\rangle|^2 .$$

<u>**Lemma**</u>

$$\begin{cases} \mathbb{P}_{Eve}(x_i = y_i \mid e_i = d_i) = \frac{3}{4} \\ \mathbb{P}_{Eve}(x_i \neq y_i \mid e_i = d_i) = \frac{1}{4} \end{cases}.$$

where $\mathbb{P}_{Eve}$ means the probability calculated in presence of Eve.

This lemma implies that the security protocol is not passed <u>after</u> the public communication phase since 1/4 of potential one-time-pad is corrupted:

$$\frac{1}{\varepsilon N/2} \# \{ i \in [\tfrac{\varepsilon N}{2}] \subset \{1 - - N\} \text{ s.t } e_i = d_i \mid x_i = y_i \}$$

$$\approx \frac{3}{4} \quad < 1 .$$

$\uparrow$

large gap detectable gap.

$\Rightarrow$ [A & B just abort protocol.].

$\#$.

Proof of Lemma (in presence of Eve):

$$\mathbb{P}_{Eve}(x_i = y_i \mid e_i = d_i)$$

$$= \mathbb{P}(x_i = y_i \mid e_i = d_i, \varepsilon_i = e_i) \underbrace{\mathbb{P}(\varepsilon_i = e_i)}_{1/2} + \mathbb{P}(x_i = y_i \mid e_i = d_i, \varepsilon_i \neq e_i) \cdot \underbrace{\mathbb{P}(\varepsilon_i \neq e_i)}_{1/2}$$

Given $\varepsilon_i = e_i$ we have $y_i^{Eve} = x_i$ (because photon is not perturbed). Thus

$$\mathbb{P}(x_i = y_i \mid e_i = d_i, \varepsilon_i = e_i) = \mathbb{P}(y_i^{\text{Eve}} = y_i \mid \varepsilon_i = d_i)$$

$$= |\langle y_i | \underbrace{H^{d_i} H^{\varepsilon_i}}_{\mathbb{1}} | y_i^{\text{Eve}} \rangle|^2$$

$$= |\langle y_i | y_i^{\text{Eve}} \rangle|^2 = 1.$$

Given $\varepsilon_i \neq e_i$ we have $y_i^{\text{Eve}} = x_i$ with Prob $1/2$.

Thus

$$\mathbb{P}(x_i = y_i \mid e_i = d_i, \varepsilon_i \neq e_i)$$

$$= \underbrace{\mathbb{P}(y_i^{\text{Eve}} = y_i \mid \varepsilon_i \neq d_i)}_{1/2} \cdot \frac{1}{2} + \underbrace{\mathbb{P}(y_i^{\text{Eve}} \neq y_i \mid \varepsilon_i \neq d_i)}_{1/2} \cdot \frac{1}{2}$$

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

Finally: $\mathbb{P}_{\text{Eve}}(x_i = y_i \mid e_i = d_i) = 1 \cdot \frac{1}{2} + \frac{1}{2} \cdot \frac{1}{2}$

$$= \frac{3}{4} \qquad \blacksquare$$

Impossibility of "copy photon" & resend attack.

If we where in a classical world we could imagine that Eve captures the photon sent by Alice, copies it perfectly, and sends the original to Bob. She would then wait the public communication phase to then make measurement in the "correct basis" $e_i = d_i$ (always) and get the same information as Bob!

(see hmw 3)

However in a quantum world the NO CLONING THEOREM tells us that it is impossible to copy a photon in one of the four states $\left\{ |0\rangle, |1\rangle, \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$ with the same ("universal") unitary machine. The reason is that these states are not all mutually orthogonal.