

Quantum Key Distribution

100% provably secure encryption

One-time pad

m = message, n bits

r = n random bits

$C = m \oplus r$ encoded message

never reuse r

[Careful $m_0 \oplus r = C_0$ $m_1 \oplus r = C_1$

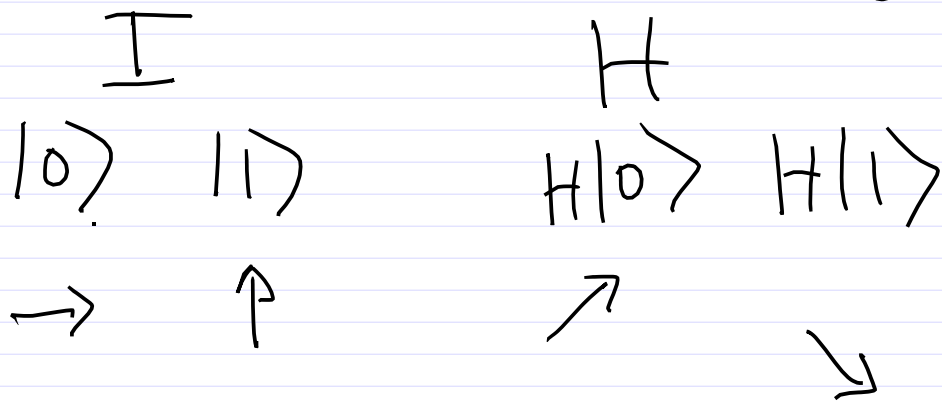
Then $C_0 \oplus C_1 = m_0 \oplus m_1$

has direct info on m_0, m_1

(r cancels if reused)]

QKD is a secure way of transmitting a one-time pad

Alice & Bob can agree on a one-time pad and they know if intercepted by Eve



Alice sends photons to Bob and each chooses independently H, I. If they choose same + measure then get same result.

But if e.g. Alice $H|0\rangle$ and Bob measures -- only 50% agreement w/o H

Alice prepares	I	H	H	H	I	I	H	I	H
Bob measures	H	H	H	I	I	H	I	I	I
	0	1	0	1	1	0	1	0	0
	1	1	0	0	1	1	1	0	0

By classical channel,
communicate sequence of H, I,
identify the roughly 50% same choice.

Discard the rest!

How do they know if intercepted by
Eve? she has to guess I, H
and measure. But if she guesses
wrong, e.g., doesn't apply H, measures,

$H|0\rangle \xrightarrow{E} |0\rangle$ then forwards to
 \searrow Bob, he applies H
 $E \rightarrow |1\rangle$ and half the time
his measurement will disagree with Alice.

Alice and Bob sacrifice some of their good bits and exchange via public channel.

Eve guesses H, I correctly

50% of time. If guesses wrong, then Bob's measurement corrupted half of those times.

so $\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4}$ of the sacrificed bits will disagree if eavesdrop:

$$P_{\text{detect Eve}} = 1 - \left(\frac{3}{4}\right)^n \quad \text{For } n=72 \text{ sacrificed,}$$

(all agree)

$$\approx .999999999 \approx 1 - 10^{-9}$$

Can Eve do anything more?

$$|\varphi_m\rangle = |0\rangle_0 |1\rangle_1 |H0\rangle_2 |H1\rangle_3$$

$$U|\varphi_m\rangle|\varphi\rangle_n = |\varphi_m\rangle|\varphi_m\rangle_n$$

U preserves inner product

$$\langle\varphi_\nu|\varphi_m\rangle\langle\varphi|\varphi\rangle = \langle\varphi_\nu|\varphi_m\rangle\langle\varphi_\nu|\varphi_m\rangle$$

$$\langle\varphi_\nu|\varphi_m\rangle \neq 0 \quad \text{for } \nu, m = \begin{matrix} 0 & 2 \\ 0 & 3 \\ 1 & 2 \\ 1 & 3 \end{matrix} \quad |\varphi_0\rangle = |\varphi_2\rangle \\ = |\varphi_1\rangle \\ = |\varphi_3\rangle$$

so can't obtain distinguishing info
and leave state $|\varphi_m\rangle$ uncorrupted

What if Alice, Bob share an entangled $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$?

Still need random choice of H

$$(H \otimes H) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

doesn't buy an advantage:

Once measured, equivalent to earlier protocol.

Only difference: QM makes choice of $|0\rangle, |1\rangle$ (or $H|0\rangle, H|1\rangle$)
(BB84) see also Eq 1



Vienna

