

Pr 1 BB84 (Bennett - Brassard) ; quantum key distribution

Alice wants to send a "secret key" to Bob

Alice will

- choose $x, y \in \{0, 1\}^n$
- encode x into a qubit state $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$ using y : if $y_i = 0$ use $|0\rangle, |1\rangle$ basis to repr $x_i = 0, 1$; if $y_i = 1$ use $|+\rangle, |-\rangle$ basis $\sim |\psi_i\rangle \in \mathbb{C}^2$, $|\psi\rangle = |\psi_0\rangle \otimes \dots \otimes |\psi_{n-1}\rangle$
- send $|\psi\rangle$ to Bob.

Bob will

- choose $y' \in \{0, 1\}^n$
- measure each qubit of $|\psi\rangle$ according to y'_i (same rule as Alice) $\sim x' \in \{0, 1\}^n$

Then they can exchange y & y' , get
keep x_i (for Alice), x'_i (for Bob)

i s.t. $y_i = y'_i$ as their secret.

- such i happens about $\frac{n}{2}$ under uniform rand choice
- for such i , $x_i = x'_i$ is guaranteed

Ex. $x = 0101$, $y = 0110$, $y' = 1010$

$$|\psi\rangle = |0\rangle \otimes |-\rangle \otimes |+\rangle \otimes |1\rangle = |0-+1\rangle$$

Bob's meas: 0-th in $|+\rangle, |-\rangle$

$$\leadsto x'_0 = 0, 1 \text{ with prob } \frac{1}{2}$$

$$1\text{-st in } |0\rangle, |1\rangle \leadsto x'_1 = 0, 1 \text{ with prob } \frac{1}{2}$$

$$2\text{-nd in } |+\rangle, |-\rangle \leadsto x'_2 = 0$$

$$3\text{-rd in } |0\rangle, |1\rangle \leadsto x'_3 = 1$$

So "01" will be the shared sec.

What if $| \psi \rangle$ is "eavesdropped" by a third actor, Eve?

for each i s.t. $y_i = y'_i =$

Eve could use a wrong basis to meas. $| \psi_i \rangle$
with prob $\frac{1}{2}$

$\rightarrow$ Bob could get an inconsistent meas. with
prob $\frac{1}{4}$

$\rightarrow$ A & B can test if $| \psi \rangle$ was eavesdropped
by comparing small portions of secret x_i 's
What they need: authenticated classical
comm. (senders are guaranteed)

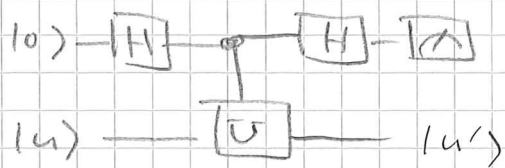
Prob. 3 Kitaev's also

U : unitary gate

$| u \rangle$: eigenstate of U

Prob. decide the eigenval $e^{2\pi i \theta}$ of $| u \rangle$

Circuit



$| 0 \rangle$ is measured with prob. $\cos^2(\pi \theta)$

after H : $\frac{1}{\sqrt{2}}(| 0 u \rangle + | 1 u \rangle)$

after $\text{Cont-}U$: $\frac{1}{\sqrt{2}}(| 0 u \rangle + e^{2\pi i \theta} | 1 u \rangle)$

after H : $\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ e^{2\pi i \theta} \end{bmatrix} \rightarrow \frac{1}{2} \begin{bmatrix} 1 + e^{2\pi i \theta} \\ 1 - e^{2\pi i \theta} \end{bmatrix}$

$| 0 \rangle$ obs. w. $\left| \frac{1}{2} (1 + e^{2\pi i \theta}) \right|^2$