Lecture 4: Entanglement based QKD

Today's lecture

- QKD with entangled States
  - Entangled states
  - Salient features of entanglement in QKD
  - Verifying entanglement
  - E-91 protocol
  - BBM92 protocol

Entanglement:

Maximally entangled Bell states:

$$|\varphi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left[|00\rangle_{AB} \pm |11\rangle_{AB}\right]. \quad \neq \psi_A \otimes \psi_B$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\left[|01\rangle_{AB} \pm |10\rangle_{AB}\right]$$

Measurement on $|\varphi^{+}\rangle_{AB}$ by A: if yields $|0\rangle \Rightarrow B$ is in $|0\rangle$
: if yields $|1\rangle \Rightarrow B$ is in $|1\rangle$.

All Bell states are mutually orthogonal

$$\langle\varphi^{+}|\varphi^{-}\rangle = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\langle 00| + \langle 11| \; |00\rangle - |11\rangle$$

$$= \langle 00|00\rangle + 0 + 0 - \langle 11|11\rangle$$

$$= 0$$

also $\langle\varphi^{\pm}|\psi^{\pm}\rangle = \langle\psi^{+}|\psi^{-}\rangle = 0$.

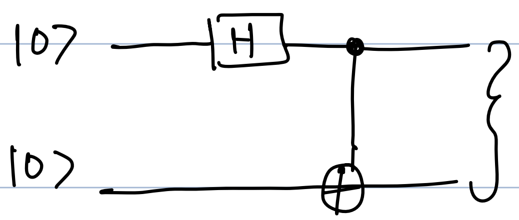
The four Bell states form a complete basis set in 4-d Hilbert space:

There is a complete basis set $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Another : $\{|++\rangle, |+-\rangle, |-+\rangle, |--\rangle\}$.

Another: $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$.

How to create these Bell states:



$$|\phi^+\rangle = \left(|00\rangle + |11\rangle\right)\frac{1}{\sqrt{2}}$$

$$|00\rangle_{AB} \xrightarrow{H_A} \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)|0\rangle$$

$$= \frac{1}{\sqrt{2}}\left(|00\rangle + |10\rangle\right).$$

$$\Big\downarrow \text{CNOT}$$

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

$$= |\phi^+\rangle.$$

Similarly other Bell states can be formed by the same circuit by just changing the initial state.

Converting from one Bell state to other:

by local operation on one of the qubit.

e.g. $|\varphi^+\rangle$ can be converted to $|\varphi^-\rangle$ by applying a Z gate on A alone.

$$|\varphi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left[|0_A 0_B\rangle + |1_A 1_B\rangle\right]$$

$$Z_A \otimes I_B |\varphi^+\rangle = \frac{1}{\sqrt{2}}\left[|0_A 0_B\rangle - |1_A 1_B\rangle\right].$$

$$= |\varphi^-\rangle.$$

Similarly:

$$X_A \otimes I_B |\varphi^+\rangle_{AB} = |\psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|10\rangle + |01\rangle\right)$$

$$Y_A \otimes I_B |\varphi^+\rangle = |\psi^-\rangle_{AB}.$$

Salient Features of Entanglement in QKD:

Intrinsic randomness of entangled states:

- Intrinsic Randomness

Classical Correlations

Earth | Moon

Randomness $\longrightarrow$ Ignorance

Quantum Entanglement

Randomness $\longrightarrow$ Intrinsic

$$|\psi^{+}\rangle = \frac{1}{\sqrt{2}}\left(\underset{0}{\updownarrow}\ \underset{1}{\nwarrow\!\!\searrow} \pm \underset{1}{\nwarrow\!\!\searrow}\ \underset{0}{\updownarrow}\right)$$

Measurement at Earth: $\updownarrow$ 0, $\nwarrow\!\!\searrow$ 1

At Moon: $\nwarrow\!\!\searrow$ 1, $\updownarrow$ 0.

Wole vs part of entangled states:

If you know the whole, you know the parts as well. Not for Bell states. Also if you look at one particle only, you cannot tell whether it's part of $|\varphi^+\rangle$, $|\varphi^-\rangle$, $|\psi^+\rangle$ or $|\psi^-\rangle$.

Looking a part means, taking a partial trace on other

For $|\varphi^+\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle_{AB} + |11\rangle_{AB}\right)$.

$$\rho_{AB} = |\varphi^+\rangle_{AB}\langle\varphi|_{AB} = \frac{1}{\sqrt{2}}\, |00\rangle + |11\rangle \,\langle 00| + \langle 11| \Big) \frac{1}{\sqrt{2}}$$

Taking a partial trace on B.

$$\rho_A = \mathrm{Tr}_B\, \rho_{AB} = \frac{1}{2}\left[\,|0\rangle\langle 0|_A + |1\rangle\langle 1|_B\,\right].$$

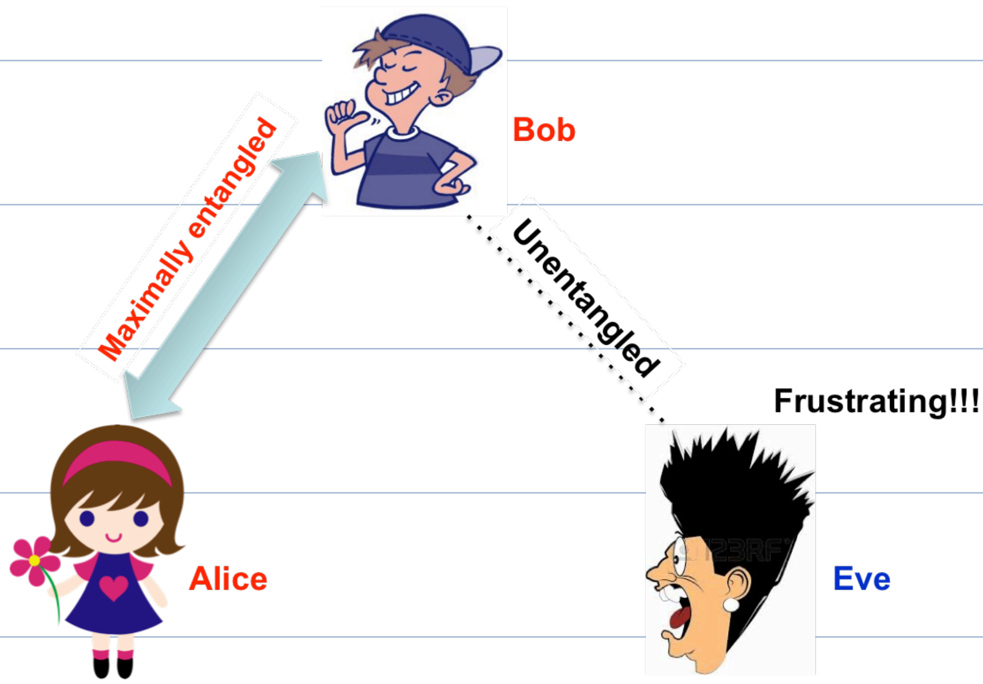
Also for $|\varphi^-\rangle$, $|\psi^+\rangle$ & $|\psi^-\rangle$.

$$\rho_A = \frac{1}{2}\left[\,|0\rangle\langle 0|_A + |1\rangle\langle 1|\,\right].$$

Monagomy of entanglement:

- Entanglement is Monogamous

  Unlike classical correlations



To ensure that two parties are unentangled with 3rd one.

Need to ensure that they are maximally entangled with each other.

Verifying Entaglement:

CHSH Inequality

variables X_1, Z_1, W_2, V_2.

values: $+1, -1$.

classically for such variables, a correlation:

$C = Z_1 W_2 + X_1 W_2 + Z_1 V_2 - X_1 V_2$.

$= (Z_1 + X_1) W_2 + (Z_1 - X_1) V_2$.

Z_1 & X_1	$Z_1 + X_1 = 2$	$Z_1 - X_1 = 0$.
$1, -1$	$Z_1 + X_1 = 0$	$Z_1 - X_1 = \mp 2$.

$\Rightarrow \quad C = \pm 2$. or $|C| = 2$.

If state is quantum, we talk about expectation values:

- Operators are Z_1, X_1, $W_2 = \frac{Z_2 + X_2}{\sqrt{2}}$, $V_2 = \frac{Z_2 - X_2}{\sqrt{2}}$.
- each with eigenvalues ± 1.
- For $|\varphi^+\rangle$ state

$$\langle Z_1 W_2 \rangle = \langle \phi^+ | Z_1 \otimes \frac{Z_2 + X_2}{\sqrt{2}} | \phi^+ \rangle.$$

$$= \frac{1}{\sqrt{2}} \langle \phi^+ | Z_1 \otimes Z_2 + Z_1 \otimes X_2 | \phi^+ \rangle$$

$$= \frac{1}{\sqrt{2}} \langle \phi^+ | \frac{|00\rangle + |11\rangle}{\sqrt{2}} + \underbrace{\frac{|01\rangle - |10\rangle}{\sqrt{2}}}$$

$$= \frac{1}{\sqrt{2}} \left[\frac{\langle 00| + \langle 11|}{\sqrt{2}} \frac{|00\rangle + |11\rangle}{\sqrt{2}} + 0 \right]$$

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

$$\langle Z_1 \otimes V_2 \rangle = \frac{1}{\sqrt{2}}.$$

$$\langle X_1 \otimes W_2 \rangle = \frac{1}{\sqrt{2}}$$

$$\langle X_1 V_2 \rangle = -\frac{1}{\sqrt{2}}.$$

$\rightarrow$ CHSH Inequality.

$$|\langle C \rangle| = \langle Z_1 W_2 \rangle + \langle Z_1 V_2 \rangle + \langle X_1 W_2 \rangle - \langle X_1 V_2 \rangle$$

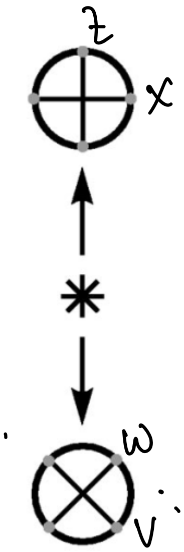
$$= \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}} - \left(-\frac{1}{\sqrt{2}}\right)$$

$$= 2\sqrt{2} > 2.$$

Correlation C is violated by Bell states.

CHSH Inequality

How to do experimentally:



Test of Bell inequality

$$\langle \varphi^+ | X_1 W_2 | \varphi^+ \rangle$$

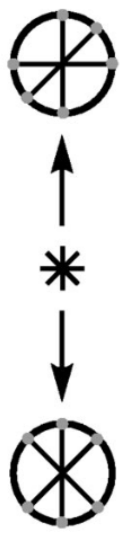
$$\mathrm{Tr}\left(X_1 \otimes W_2 \, |\varphi^+\rangle\langle\varphi^+| \right).$$

$$\langle AB \rangle = \underline{(+1)(+1)\, P(0,0)} + \underline{(-1)(-1)\, P(1,1)}$$
$$+ (+1)(-1)\, P(0,1) + (-1)(+1)\, P(1,0)$$

$$= P(\text{outputs are same}) - P(\text{outputs are different})$$

Ekert 91 Protocol

Alice



Ekert protocol

Bob.

$\underbrace{x, z}, w : = \theta_i^A$

$z, \underbrace{w, v} : = \theta_i^B$.

- Alice prepares a state $|\varphi^+\rangle := \frac{1}{\sqrt{2}}\left[|00\rangle + |11\rangle\right]$.
- She sends 2nd qubit to Bob.
- Alice measures in θ_i^A each qubit i
- Bob " " θ_i^B " " i
- They announce $\{i, \theta_i^{A,B}\}$.
- when $\theta_i^A = \theta_i^B$.

  happens - $\frac{2}{9}$. times.

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}\left[|0_A 0_B\rangle + |11\rangle\right].$$

- Both Measure in Z-basis: $|0\rangle_A \Rightarrow |0\rangle_B \Rightarrow$ bit values 0,0.

$|1\rangle_A \Rightarrow |1\rangle_B \Rightarrow$ bit values 1,1.

$\Rightarrow$ when Basis are same $\theta_i^A = \theta_i^B$, bit values are same.

They keep them as key: happens $\frac{2}{9}$ times.

- If one measures in Z and ~~o~~ther in X.

$$= \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\left[|0\rangle_A\left(|+\rangle_B + |-\rangle_B\right) + |1\rangle\left(|+\rangle - |-\rangle\right)\right]$$

$$0 = \frac{1}{2}\left[|0+\rangle + |0-\rangle + |1+\rangle - |1-\rangle\right].$$

$\therefore$ Bit values. $\quad$ 0 0 $\quad$ $\cancel{0}$ 1 $\quad$ 1 0 $\quad$ 1 1.

- when $\theta_i^A \neq \theta_i^B$. use to check CHSH inequality

$\theta_i^A = X, Z. \quad \theta_i^B = W, V.$

$\frac{7}{9}$ times.

CHSH $= 2\sqrt{2}$.

- Estimate error rate
- Do error correction + Privacy amplification.

BBM92 Protocol:

- Alice prepares an entangled state $|\phi^+\rangle$.
- She sends 2nd qubit to Bob.
- Both measure randomly in Z or X basis
- They announce the basis publicly..
- Thier bit values exactly match when basis are same.

  They keep the bit values as key where basis match.
- They discard the rest.
- They are error estimation.