Lecture 9

Sunday, September 29, 2024 8:59 AM

No-Cloning Thereom → The main concept of QKD

Assume U is a cloning gate on $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

$U|\varphi\rangle|0\rangle = |\varphi\rangle|\varphi\rangle \rightarrow |0\rangle|0\rangle$, $|1\rangle|1\rangle$

$$U \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \otimes \begin{pmatrix}1 \\ 0\end{pmatrix} = \begin{pmatrix}\alpha \\ \beta\end{pmatrix} \otimes \begin{pmatrix}\alpha \\ \beta\end{pmatrix}$$

$$\begin{pmatrix} U_{11} & U_{12} & U_{13} & U_{14} \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ U_{41} & \cdots & \cdots & U_{44} \end{pmatrix} \begin{pmatrix}\alpha \\ 0 \\ \beta \\ 0\end{pmatrix}^{4\times1} = \begin{pmatrix}\alpha^2 \\ \alpha\beta \\ \beta\alpha \\ \beta^2\end{pmatrix}^{4\times1}$$

$\mathbb{R} \rightarrow \mathbb{R}^2$

U can't be linear

U can't satisfy $|\alpha^2|^2 + |\alpha\beta|^2 + |\beta^2|^2 = 1$ not true

$|\alpha|^2 + |\beta|^2 = 1$

We can setup 4 equations:

$U_{11}\alpha + U_{13}\beta = \alpha^2$

$U_{21}\alpha + U_{23}\beta = \alpha\beta$

$U_{31}\alpha + U_{33}\beta = \alpha\beta$

$U_{41}\alpha + U_{43}\beta = \beta^2$

$$U = \begin{pmatrix} \alpha & 0 & 0 \\ \vdots & \ddots & \vdots \\ \vdots & & \ddots \\ \cdots & & \beta \end{pmatrix}$$

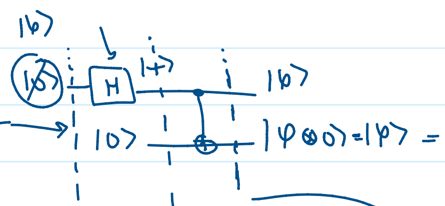
One solution

$U_{11} = \alpha$, $U_{13} = 0$, $U_{41} = 0$, $U_{43} = \beta$

We have to know α & β to construct U.

But $|\varphi\rangle$ will collapse

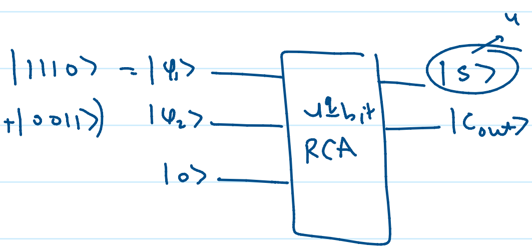
How to create a Bell state



$|00\rangle$ $|0+\rangle$ $|\Phi^+\rangle$

$\frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Quantum Parallelism



$\frac{1}{\sqrt{2}}(|0001\rangle + |0011\rangle)$

$\frac{1}{\sqrt{2}}(|1111\rangle + |\cdots\rangle)$ T

$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$$\left.\begin{array}{l} |0\rangle + |0\rangle \\ |0\rangle + |1\rangle \\ |1\rangle + |0\rangle \\ |1\rangle + |1\rangle \end{array}\right\}$$ at the same time