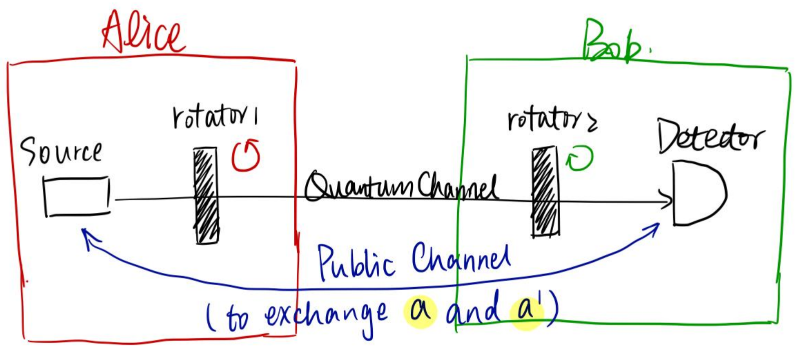
BB84 Protocol

The process of creating shared seret key

initial key a	0	1	1	0	1	0	0	1
⇓ change into qubit								
initial key a (qubit)	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	$\|1\rangle$
randomly Hadamard transform: Hadmard transform on a if basis is "x". do nothing for "+"								
random rotatation string b	0	0	1	0	1	1	1	0
⇓ 0 stands for "+", 1 stands for "x"								
corresponding rotation basis	+	+	×	+	×	×	×	+
the qubit key to be Transmitted (transmit photons): dirac notation	$\|0\rangle$	$\|1\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\|1\rangle$
direction	↑(90°)	→(0°)	↖(135°)	↑(90°)	↖(135°)	↗(45°)	↗(45°)	→(0°)
Quantum Channel								
the key after transmission	$\|0\rangle$	$\|1\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\|1\rangle$
randomly inverse Hadamard transform: Inverse Hadmard transform on a if basis is "x". do nothing for "+"								
random rotation string b'	0	1	1	1	0	1	0	0
⇓ 0 stands for "+", 1 stands for "x"								
corresponding rotation basis	+	×	×	×	+	×	+	+
final qubit key	$\|0\rangle$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\|1\rangle$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}$	$\|0\rangle$	$\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}$	$\|1\rangle$
⇓ measure								
a'	0	0 or 1	1	0 or 1	0 or 1	0	0 or 1	1

For all i when a[i] = a'[i], there must be b[i] = b'[i], otherwise it means that a third person have been eavesdropping.

Shared secret key [Probabilisticly, it's half of the length of a/a'/b/b']



Attention:

1. For the left table:

   — : The bit string randomly generated by alice

   — : The bit string randomly generated by Bob

2. Randomly choosing "+" or "-" as basis, is equivalent to randomly doing Hadamard transform

$$|0\rangle \rightarrow \boxed{H} \rightarrow \frac{\sqrt{2}|0\rangle+\sqrt{2}|1\rangle}{2}$$

$$|1\rangle \rightarrow \boxed{H} \rightarrow \frac{\sqrt{2}|0\rangle-\sqrt{2}|1\rangle}{2}$$

Hadamard gate in matrix: $H=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}1\\ 0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\ 1\end{bmatrix}$$

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}\begin{bmatrix}0\\ 1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ -1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\ 0\end{bmatrix}-\frac{1}{\sqrt{2}}\begin{bmatrix}0\\ 1\end{bmatrix}$$

3. Inverse transform of Hadamard gate:

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

$$H^{-1}=\frac{1}{-\frac{1}{2}-\frac{1}{2}}\begin{bmatrix}-\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}}\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$$

∴ Inverse Hadamard transform = Hadamard transform