

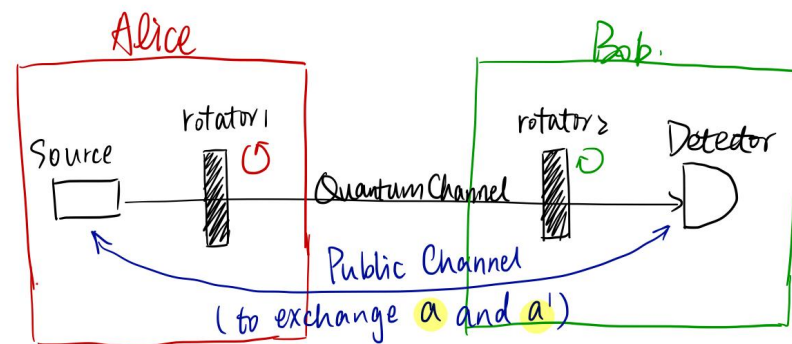
# BB84 Protocol

The process of creating shared secret key

initial key <b>a</b>	0	1	1	0	1	0	0	1
↓ change into qubit								
initial key <b>a</b> (qubit)	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 0\rangle$	$ 1\rangle$
randomly Hadamard transform	Hadamard transform on a if basis is "x". do nothing for "+"							
random rotation string <b>b</b>	0	0	1	0	1	1	1	0
↓ 0 stands for "+", 1 stands for "x"								
corresponding rotation basis	+	+	x	+	x	x	x	+
the qubit key to be transmitted (transmit photons)	$ 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	$\uparrow(90^\circ)$	$\rightarrow(0^\circ)$	$\swarrow(135^\circ)$	$\uparrow(90^\circ)$	$\swarrow(135^\circ)$	$\nearrow(45^\circ)$	$\nearrow(45^\circ)$	$\rightarrow(0^\circ)$
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 Hadamard transform on a if basis is "x". do nothing for "+"							
random rotation string <b>b'</b>	0	1	1	1	0	1	0	0
↓ 0 stands for "+", 1 stands for "x"								
corresponding rotation basis	+	x	x	x	+	x	+	+
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	0	0 or 1	1	0 or 1	0 or 1	0	0 or 1	1

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

Shared secret key [ Probabilistically, 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

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

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

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

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

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

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