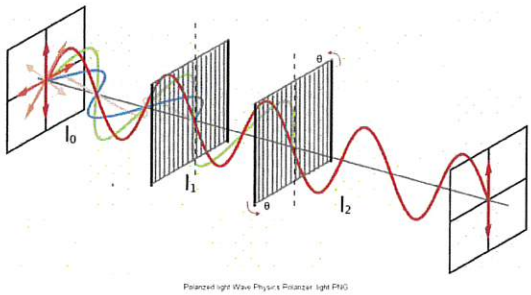
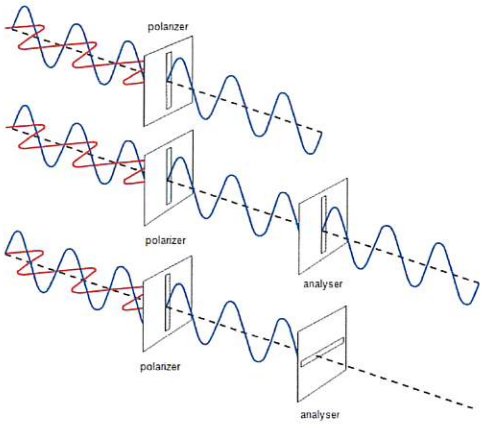
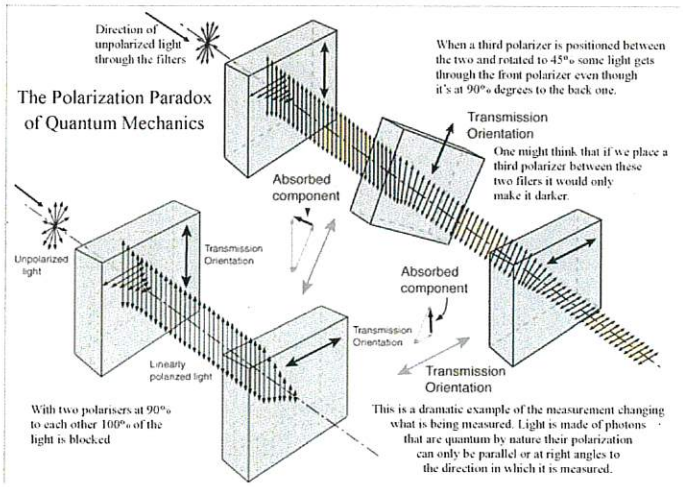
光的偏振實驗

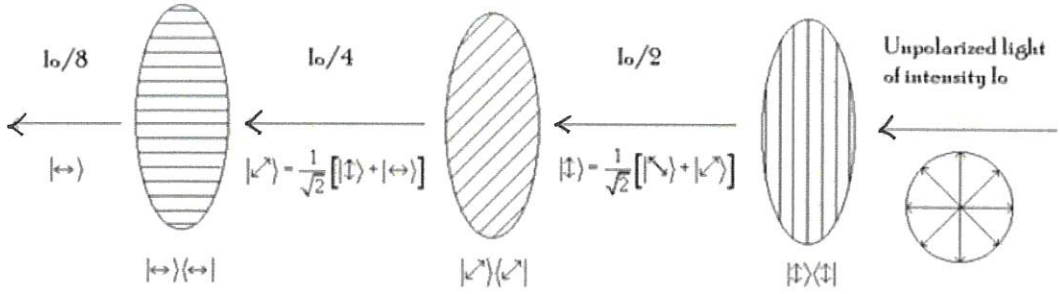


Polarized light Wave Physics Polarizer light PNG





0 $\frac{1}{4}$



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

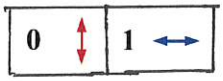
$$|\nearrow\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle + |1\rangle\right]$$

- 直线基：$\oplus = \{|0\rangle, |1\rangle\} = \{|\uparrow\rangle, |\rightarrow\rangle\}$
- 对角基：$\otimes = \{|+\rangle, |-\rangle\} = \{|\nearrow\rangle, |\searrow\rangle\}$

$$\begin{cases} |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$

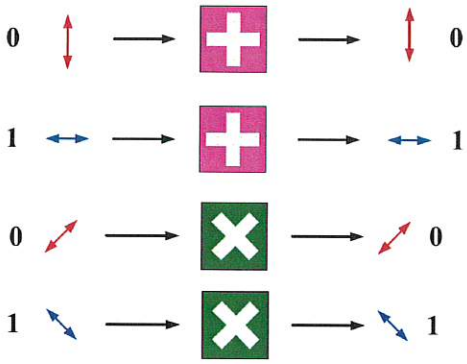
不同的基

直线基1:水平和垂直



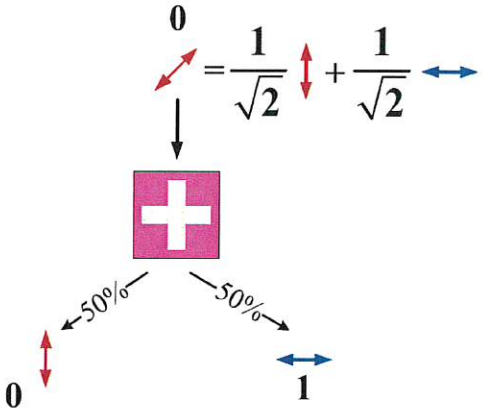
对角基2:对角

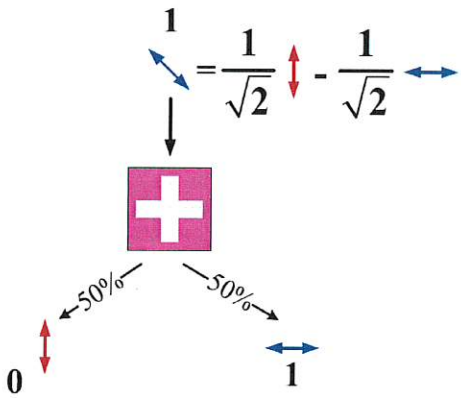
在相同的基下测量



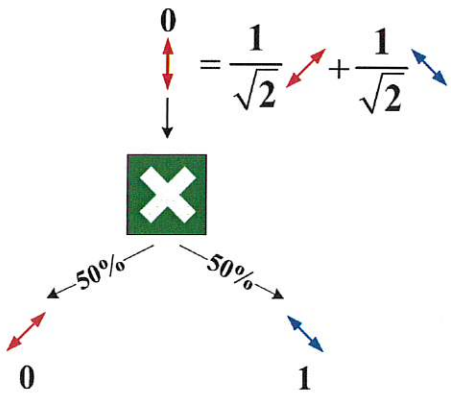
在不同的基下测量

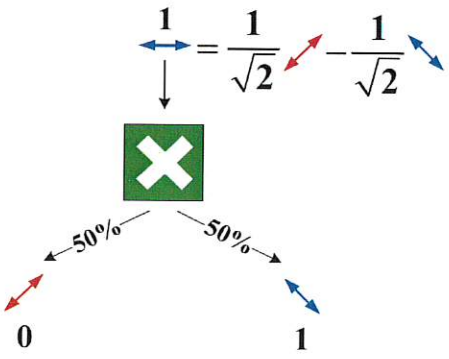
$$\begin{cases} |\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases}$$





$$\begin{cases} |0\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\searrow\rangle) \\ |1\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\searrow\rangle) \end{cases}$$





结论：
- 在相同的基下测量：bits 相同
- " 不同 " " ：$Pr\{\text{"}\ \text{"}\} = \frac{1}{2}$

Quantumn key Distribution (QKD)

No.
Date: / /

BB84 (Bennett & Brassard '84) protocol

Protocol

(I) Quantumn channel

(1) A: randomly chooses $a_1 a_2 \cdots a_{2n}$, $a_i \in \{0, 1\}$
$B_1 B_2 \cdots B_{2n}$, $B_i \in \{\oplus, \otimes\}$

encode $a_i \xrightarrow{B_i} |g_i\rangle$ $\left(\begin{array}{l} 0 \to |0\rangle, |+\rangle \\ 1 \to |1\rangle, |-\rangle \end{array}\right)$
$\oplus$ $\otimes$

sends $|g_i\rangle \to B$

(2) B: randomly chooses $B_i' \in \{\oplus, \otimes\}$, measure $|g_i\rangle \xrightarrow{B_i'} b_i$
$(1 \le i \le 2n)$

(II) Public channel (檢測 Eve 存在, 決定 key)

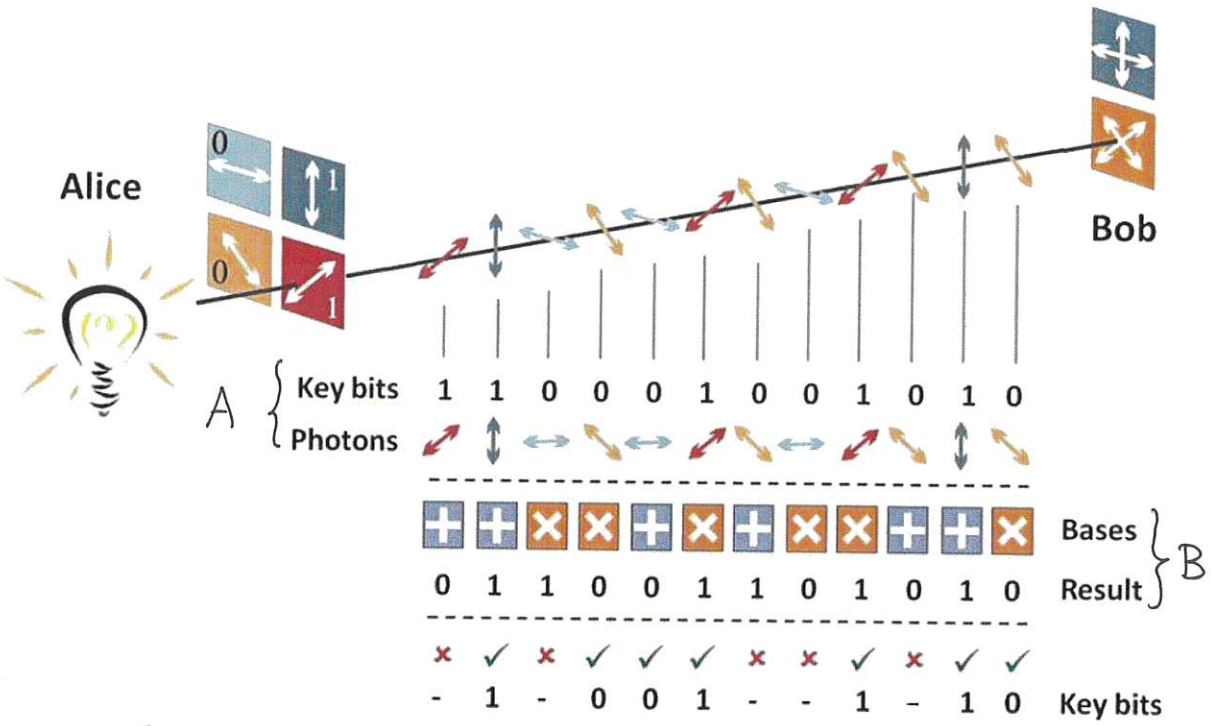
(1) Raw keys: (i) $B \xrightarrow{B_1' \cdots B_{2n}'} A$
(ii) $A \xrightarrow{B_1 \cdots B_{2n}} B$
keep a_i, b_i if $B_i = B_i'$
(iii) remaining a_i, b_i as raw keys $a_1' a_2' \cdots a_n'$, $b_1' b_2' \cdots b_n'$ $(n' \approx n)$

(2) Eve 存在?: Exchange + Compare $a_1' \cdots a_m'$, $b_1' \cdots b_m'$ (由 raw keys 任選 m bits)

(a) Eve 不存在: $a_1' \cdots a_m' = b_1' \cdots b_m'$

(b) Eve 存在: $\begin{cases} Pr(a_1' \cdots a_m' = b_1' \cdots b_m') = (\frac{3}{4})^m \\ Pr(\quad \neq \quad) = 1 - (\frac{3}{4})^m \end{cases}$

(3) Remaining $n-m$ bits as key



BB84 协议

		1	2	3	4	5	6	7	8	9	10	11	12
Alice	所发送比特值	0	1	0	1	1	0	0	1	1	1	0	1
	偏振光滤波器	⊗	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊕	⊗	⊗	⊗
	偏振光态	↗	↔	↕	↘	↘	↕	↗	↔	↔	↘	↗	↘
Bob	偏振光检测器	⊗	⊕	⊗	⊕	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊗
	观测值	↗	↔	↘	↕	↔	↕	↗	↕	↔	↔	↕	↘
	观测比特值	0	1	1	0	1	0	0	0	1	1	0	1
比较滤波器和检测器的结果		真	真	假	假	假	真	真	假	真	假	假	真
	单时拍	0	1				0	0		1			1

Eve 扰乱数据以后 Bob 所观测到的比特值

		1	2	3	4	5	6	7	8	9	10	11	12
Alice	所发送比特值	0	1	0	1	1	0	0	1	1	1	0	1
	偏振光滤波器	⊗	⊕	⊕	⊗	⊗	⊕	⊗	⊕	⊕	⊗	⊗	⊗
	偏振光态	↗	↔	↕	↘	↘	↕	↗	↔	↔	↘	↗	↘
Eve	偏振光检测器	⊕	⊗	⊗	⊕	⊕	⊕	⊗	⊕	⊗	⊗	⊗	⊕
	观测值	↔	↘	↗	↕	↔	↕	↗	↔	↘	↘	↗	↕
	观测比特值	1	1	0	0	1	0	0	1	1	1	0	0
Bob	偏振光检测器	⊗	⊕	⊗	⊕	⊕	⊕	⊗	⊗	⊕	⊕	⊕	⊗
	观测值	↘	↔	↗	↕	↔	↕	↗	↘	↕	↕	↕	↘
	观测比特值	1	1	0	0	1	0	0	1	0	0	0	1
	单时拍	1	1				0	0		0			1