投影片 1

Quantum Computing 3

投影片 2

Five common operations

$$I: \begin{matrix} |0\rangle & \to & |0\rangle \\ |1\rangle & \to & |1\rangle \end{matrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$X: \begin{matrix} |0\rangle & \to & |1\rangle \\ |1\rangle & \to & |0\rangle \end{matrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

$$Y: \begin{matrix} |0\rangle & \to & -|1\rangle \\ |1\rangle & \to & |0\rangle \end{matrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$Z: \begin{matrix} |0\rangle & \to & |0\rangle \\ |1\rangle & \to & -|1\rangle \end{matrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

投影片 3

Five common operations

Hadamard gate :

$$H: \begin{matrix} |0\rangle \to \sigma(|0\rangle + |1\rangle) \\ |1\rangle \to \sigma(|0\rangle - |1\rangle) \end{matrix} = \sigma \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Hadamard gate
可以變成疊加態

投影片 4

unitary

It states that if M is unitary, then $MM^* = \pm I$.

M*:conjugate transpose
如果 M都是實數 那M* = M^T

投影片 5

Cloning

Cloning isn't possible

如果你想要複製一個測量完已知狀態的qubit很簡單
但如果我們想複製的是還沒測量的qubit

投影片 6

Proof

U: $U(|a0\rangle) = |aa\rangle$

$U(|a0\rangle) = |aa\rangle$ $\quad$ $|c\rangle=\sigma(|a\rangle+|b\rangle)$

$U(|b0\rangle) = |bb\rangle$ $\quad$ $U(|c0\rangle) = |cc\rangle$

$|b\rangle$ orthogonal to $|a\rangle$

投影片 7

Proof

$|c0\rangle = |c\rangle \otimes |0\rangle$

$= \sigma(|a\rangle + |b\rangle) \otimes |0\rangle$

$= \sigma(|a0\rangle + |b0\rangle)$

$U(|c0\rangle) = U(\sigma(|a0\rangle + |b0\rangle))$

$= \sigma((U|a0\rangle) + (U|b0\rangle))$

$= \sigma(|aa\rangle + |bb\rangle)$

因為 U是linear

投影片 8

Proof

$U(|c0\rangle) = |cc\rangle$

$= |c\rangle \otimes |c\rangle$

$= \sigma(|a\rangle + |b\rangle) \otimes \sigma(|a\rangle + |b\rangle)$

$= \sigma^2|aa\rangle + \sigma^2|ab\rangle + \sigma^2|ba\rangle + \sigma^2|bb\rangle$

$= \sigma^2(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle)$

$\neq \sigma(|aa\rangle + |bb\rangle)$ →←

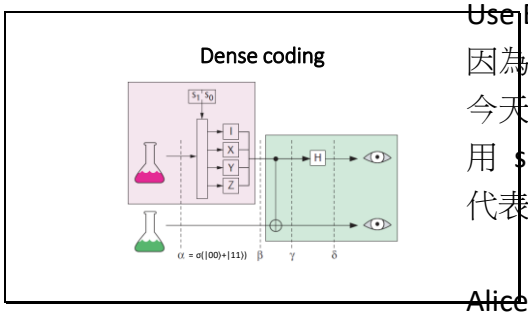
投影片 9

Dense coding

今天Alice想傳訊息給Bob
假設他今天想傳一個400bits的訊息
那正常他就一定要傳400bits的訊息給Bob

但如果之前他們已經共有200 EPR pairs
而Bob可以使用這EPR pairs來解出 Alice的訊息

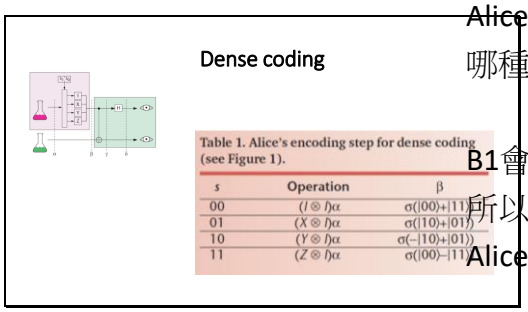
投影片 10



Use EPR
因為傳送方式都是一樣
今天假設Alice要送2bit的訊息
用 s1跟s0表示
代表十位數的0~3

Alice拿出她的”EPR Pair 0, Qubit 0.” a0
Bob就獲得EPR Pair 0, Qubit 1.” a1
這個EPR我們叫做a

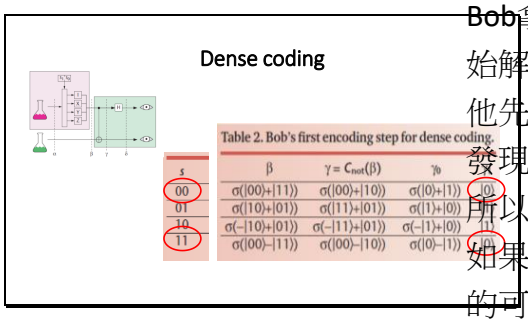
投影片 11



Alice會根據他s1.s0決定要對a做哪種運算得到B

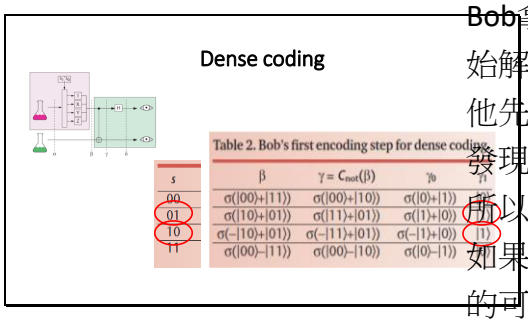
B1會改變但B2不會受運算影響
所以B只是A改變第一個qubit
Alice就可以寄給Bob一個qubit

投影片 12



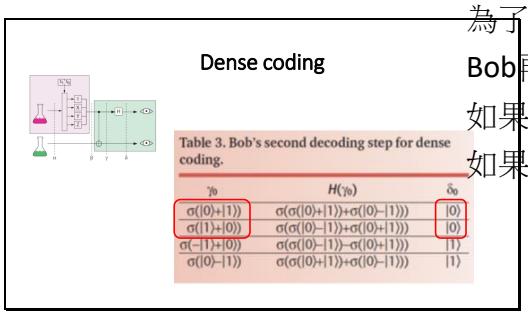
Bob拿到Alice寄的qubit後可以開始解碼了
他先用Cnot gate 將B轉成r
發現r變成非糾纏態
所以Bob就可以先測量r1
如果r1是0那他就知道Alice要寄的可能是0或3
如果r1是1那就是1或2

投影片 13



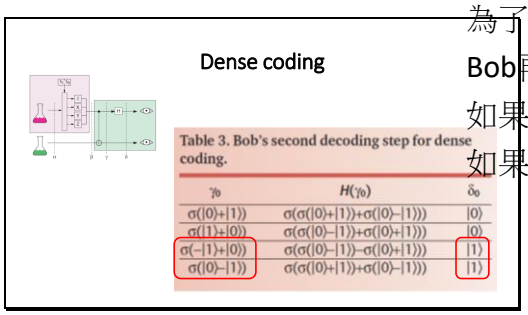
Bob拿到Alice寄的qubit後可以開始解碼了
他先用Cnot gate 將B轉成r
發現r變成非糾纏態
所以Bob就可以先測量r1
如果r1是0那他就知道Alice要寄的可能是0或3
如果r1是1那就是1或2

投影片 14



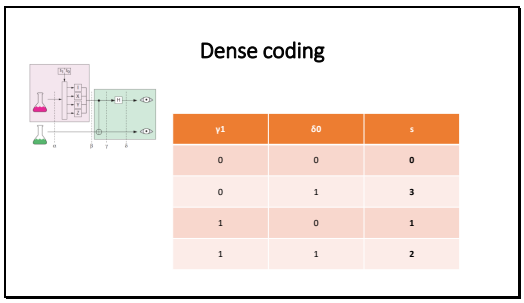
為了要確定訊息是甚麼
Bob再對r0做H運算得到δ0
如果δ0=0，那可能是0或1
如果δ0=1，那可能是2或3

投影片 15

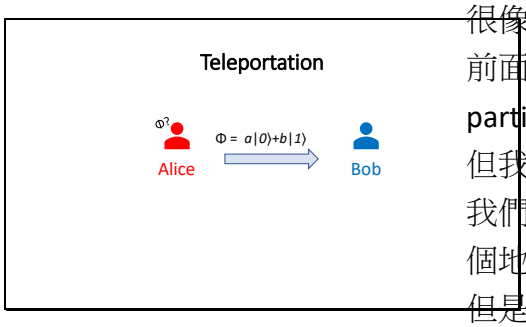


為了要確定訊息是甚麼
Bob再對r0做H運算得到δ0
如果δ0=0，那可能是0或1
如果δ0=1，那可能是2或3

投影片 16



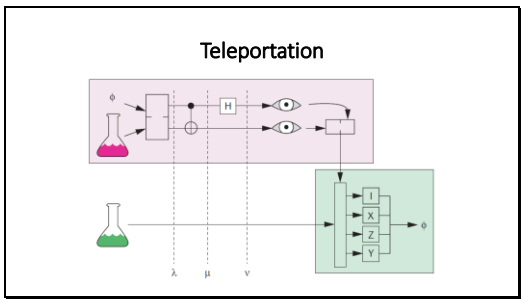
投影片 17



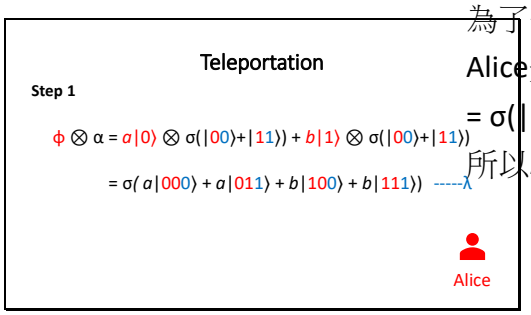
很像dense coding
前面已經證明不能複製quantum particle
但我們現在可以用另一個方式
我們可以再產生一個粒子再另一個地方
但是我們原本的要把他毀掉

像dense coding
Alice跟Bob共享一個EPR pair α
假設Alice有一個qubit ϕ 想傳給Bob
但Alice不知道他的狀態也不想測量他
儘管Alice不知道a或b但他希望Bob可以得到同樣狀態的ϕ
這個過程跟dense coding的反向很類似

投影片 18



投影片 19

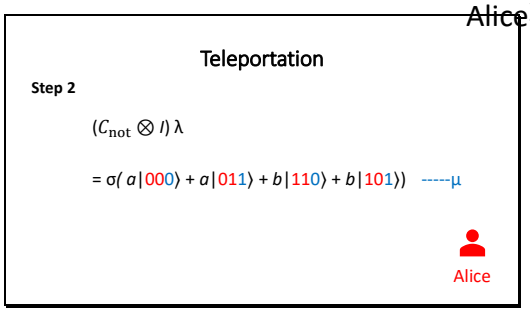


為了傳給Bob

Alice先對ϕ做tensor product 跟 α = σ(|00>+|11>)做運算

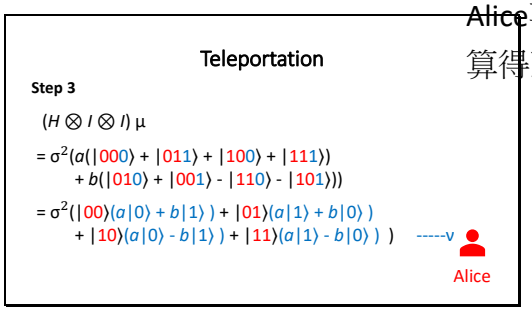
所以Alice現在叫做λ

投影片 20



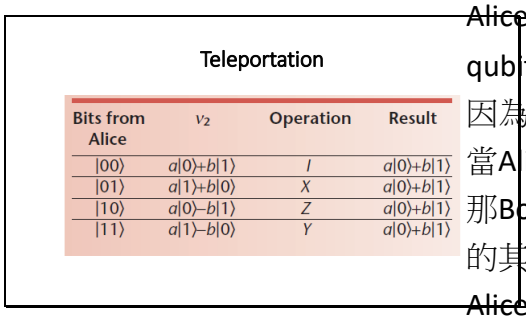
Alice再對λ做(Cnot⊗I)運算得到μ

投影片 21



Alice再對μ的第一個qubit做H運算得到v

投影片 22

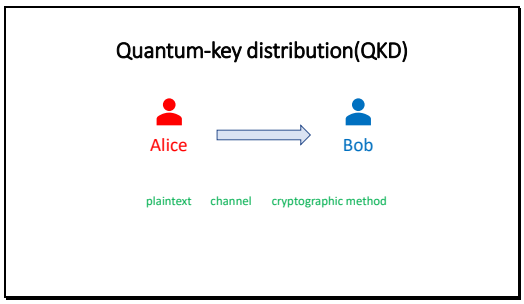


Bits from Alice	v_2	Operation	Result
$\|00\rangle$	$a\|0\rangle+b\|1\rangle$	I	$a\|0\rangle+b\|1\rangle$
$\|01\rangle$	$a\|1\rangle+b\|0\rangle$	X	$a\|0\rangle+b\|1\rangle$
$\|10\rangle$	$a\|0\rangle-b\|1\rangle$	Z	$a\|0\rangle+b\|1\rangle$
$\|11\rangle$	$a\|1\rangle-b\|0\rangle$	Y	$a\|0\rangle+b\|1\rangle$

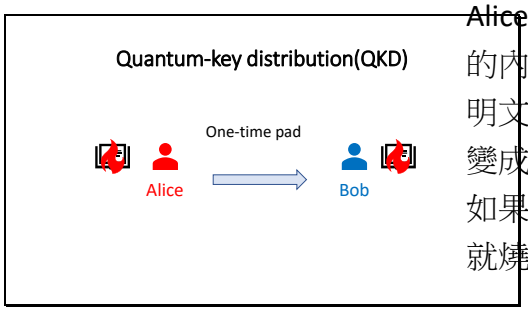
Alice的最後一步是測量前兩個qubits
因為v1糾纏α(v2)的qubit 1
當Alice測輛v1
那Bob的qubit就會陷入4個狀態的其中一個
Alice會測量前兩個qubit 可以表示0-3
然後寄給Bob

Bob就能用Alice寄的qubit決定他要做哪種運算 變回ϕ

投影片 23



投影片 24



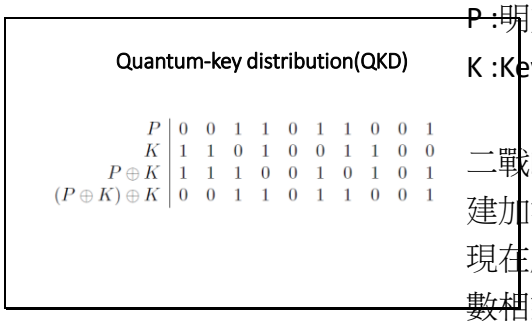
Alice跟Bob都有一本同樣的書 書的內容就是很多隨機數
明文第一個字+書的第一個數字變成密文
如果一頁到底就翻頁 2面都用完就燒掉

Bob
解密就減掉數字得到明文
一樣用完就燒掉

One-time pad

後來就創了one-time key

投影片 25



P	0	0	1	1	0	1	1	0	0	1
K	1	1	0	1	0	0	1	1	0	0
$P \oplus K$	1	1	1	0	0	1	0	1	0	1
$(P \oplus K) \oplus K$	0	0	1	1	0	1	1	0	0	1

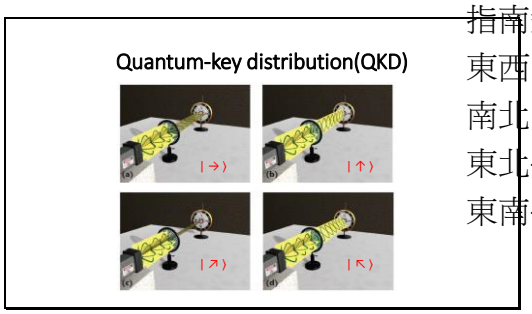
P :明文
K :Key

二戰的enigma就是一個複雜的創建加密key的機器
現在廣泛使用的是RSA 就是兩質數相乘產生金鑰

One-time key 最麻煩的是雙方都必須提前見面去交換key的副本然後保證他們的安全性
如果有一種方式能夠要在時再建立跟交換key那就好了

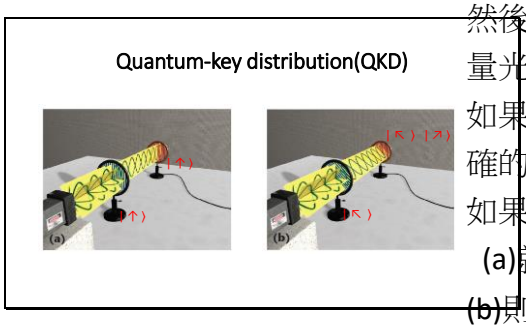
這就是量子計算給我們的!!!

投影片 26



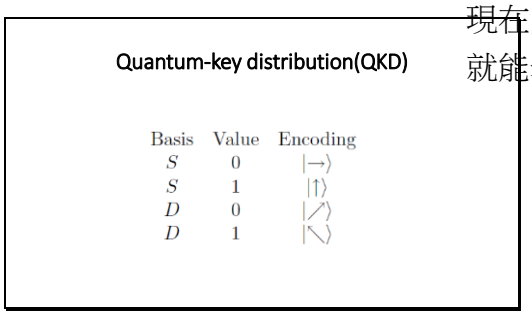
指南針!
東西
南北
東北-西南
東南-西北

投影片 27



然後我們可以用一個探測器去測量光子
如果探測器跟光柵一樣 就能正確的量測到
如果不一樣會獲得一個隨機的
(a)就能正確的量測
(b)則會有50%的機率得到↖ 50%的機率得到↗

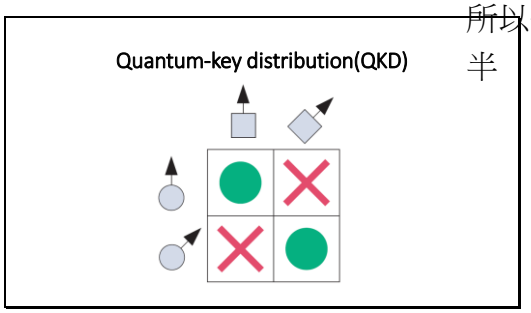
投影片 28



Basis	Value	Encoding
S	0	$\|\rightarrow\rangle$
S	1	$\|\uparrow\rangle$
D	0	$\|\nearrow\rangle$
D	1	$\|\nwarrow\rangle$

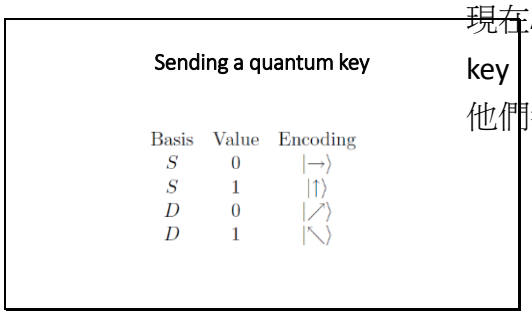
現在只用直的跟45度的兩個光柵就能表現出4種狀態的光子

投影片 29



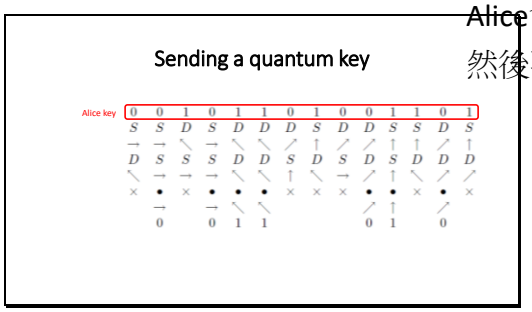
所以偵測到對的光子的機率是一半

投影片 30



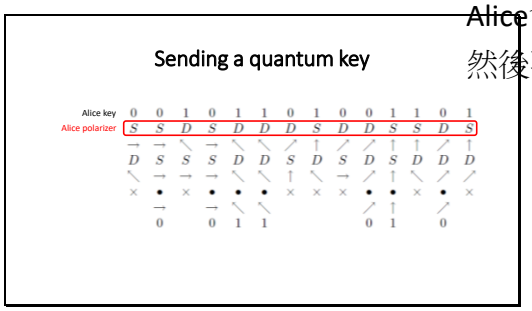
現在Alice跟Bob要交換 quantum key
他們都遵守這個規則

投影片 31



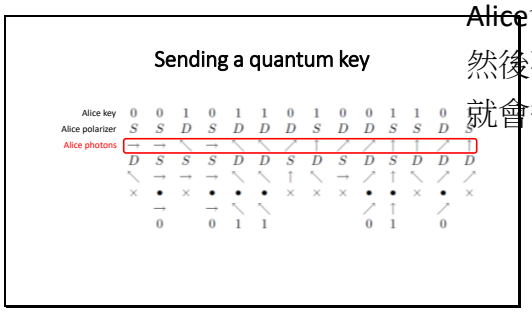
Alice會隨機產生一組key
然後再隨機使光柵是S或D

投影片 32



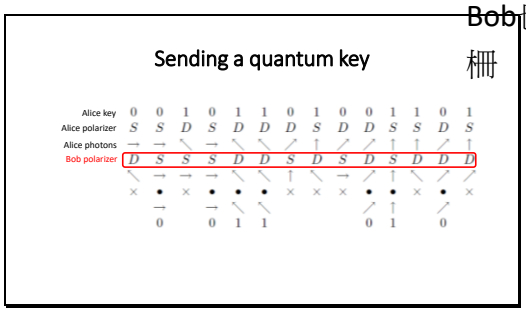
Alice會隨機產生一組key
然後再隨機使光柵是S或D

投影片 33



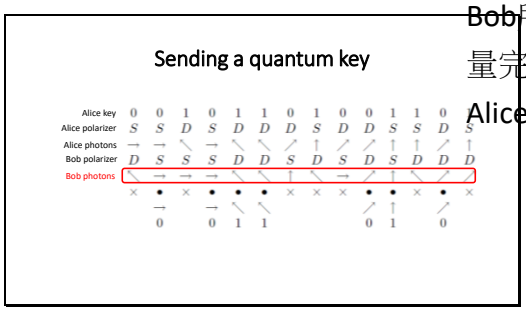
Alice會隨機產生一組key
然後再隨機使光柵是S或D
就會寄出他的光子

投影片 34



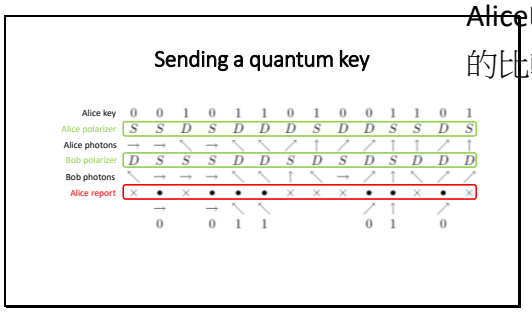
Bob也會隨機產生一組S&D的光柵

投影片 35



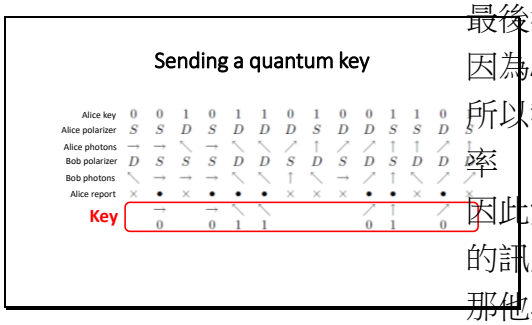
Bob所量到的光子會長這樣
量完他會把他設定的光柵寄給Alice

投影片 36



Alice收到Bob的設定後會跟自己的比較然後將對錯寄給Bob

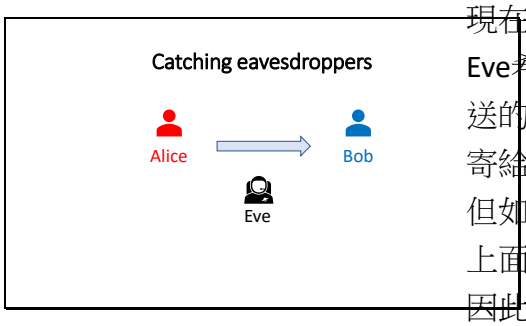
投影片 37



最後猜對的就會變成key
因為Alice跟Bob都是隨機的產生
所以我們期待Bob有50%的猜對率
因此如果Alice想加密一個n-bits的訊息
那他必須先寄2n-bits的光子

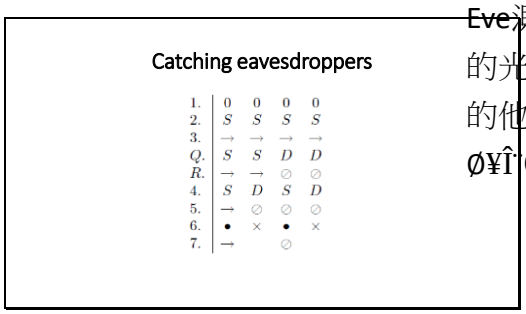
而且這樣做
如果有人在竊聽他們的key時
Alice跟Bob能夠察覺
因為會大約有25% Bob寄回去的bits是錯的

投影片 38



現在Eve想竊聽 Alice&Bob
Eve希望能在途中擷取Alice所發送的光子然後複製完再一樣繼續寄給Bob
但如果要不測量他且複製 我們上面有證明過這是不可能的
因此Eve會擷取每個光子然後測量它們再複製一個相同的狀態給Bob

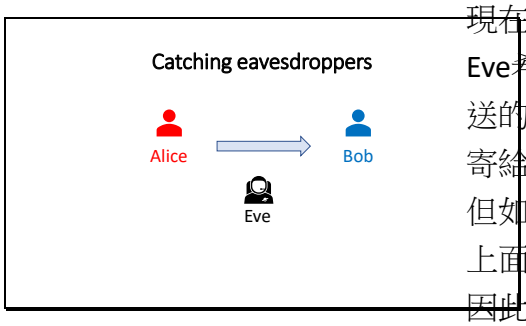
投影片 39



1.	0	0	0	0
2.	S	S	S	S
3.	→	→	→	→
Q.	S	S	D	D
R.	→	→	⊘	⊘
4.	S	D	S	D
5.	→	⊘	⊘	⊘
6.	•	×	•	×
7.	→		⊘	

Eve測量時因為他也不知道Alice的光柵設定 所以依照前一篇說的他有50-50的機率猜對
Ø¥Î¨Ó¥Nªí¤@-ÓÀH¾÷ªºµ²ªG

投影片 40



現在Eve想竊聽 Alice&Bob
Eve希望能在途中擷取Alice所發送的光子然後複製完再一樣繼續寄給Bob
但如果要不測量他且複製 我們上面有證明過這是不可能的
因此Eve會擷取每個光子然後測量它們再複製一個相同的狀態給Bob