

$$|+\rangle + i|-\rangle$$

~~~~~

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle + i\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

$$= \frac{1+i}{\sqrt{2}}|0\rangle + \frac{1-i}{\sqrt{2}}|1\rangle$$

$$\sim \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle$$

↓

$$\left|\frac{1+i}{2}\right|^2 = \frac{1}{2}$$

↓

$$\frac{1}{2}$$

$$\boxed{\begin{aligned} |\alpha a|^2 + |\alpha b|^2 &= |\alpha|^2 (|a|^2 + |b|^2) \\ |a|^2 + |b|^2 &= 1 \end{aligned}} \quad \boxed{\begin{aligned} |a+bi|^2 &= a^2 + b^2 \\ |1+i|^2 &= 1^2 + 1^2 \\ &= 2 \end{aligned}}$$

$$\left|\frac{1+i}{\sqrt{2}}\right|^2 + \left|\frac{1-i}{\sqrt{2}}\right|^2$$

$$(1+i)(1-i)$$

$$= \frac{2}{2} + \frac{2}{2} = 2$$

# Quantum Key Distribution (BB84 Bennett, Brassard)

Cheat sheet  
 $\begin{matrix} \uparrow^0 \\ \rightarrow^1 \end{matrix}$ 
 $\begin{matrix} \nearrow^0 \\ \nwarrow^1 \end{matrix}$

## Phase I (BASES SECRET)

| Alice |       | photon                | Bob   |                                                    |        |
|-------|-------|-----------------------|-------|----------------------------------------------------|--------|
| Bit   | Basis |                       | Basis | Msr                                                | Bit    |
| 1     | V     | $ \uparrow\rangle$    | L     | random $ \uparrow\rangle$ or $ \rightarrow\rangle$ | 0 or 1 |
| 0     | V     | $ \nwarrow\rangle$    | V     | $ \nwarrow\rangle$                                 | 0      |
| 1     | L     | $ \rightarrow\rangle$ | L     | $ \rightarrow\rangle$                              | 1      |
| 0     | L     | $ \uparrow\rangle$    | V     | random $ \nwarrow\rangle$ or $ \nearrow\rangle$    | 0 or 1 |
| 1     | L     | $ \rightarrow\rangle$ | V     | random $ \nwarrow\rangle$ or $ \nearrow\rangle$    | 0 or 1 |

## Phase II Classical channel (public)

Alice & Bob compare lists of bases

& keep the rows where bases agreed.  $\leftarrow$  "shared secret"

Attacks? Can Eve listen in? i.e. measure photon en route

eg. ① Alice sends  $|\uparrow\rangle$  (L basis)

Eve msrs in V basis

$\Rightarrow$  the photon becomes  $|\nwarrow\rangle$  or  $|\nearrow\rangle$  w/ 50-50 chance

Bob measures in L basis : get  $|\uparrow\rangle$  or  $|\rightarrow\rangle$  w/ 50-50 chance

Eve screens up bit  
 Bob's w/ 50% prob

(w/o Eve, would have measured  $|\uparrow\rangle$  w/ 100% prob)

(2) Alice sends  $|\uparrow\rangle$  (L basis)

Eve undetected  
(she does get bit)  
Eve msrs in L basis  
 $\Rightarrow$  the photon is unchanged

Bob msrs in L basis : gets  $|\uparrow\rangle$  w/ 100% prob

If Eve can't predict bases, she's in situation (1) or (2) w/ 50-50 chance.

$\Rightarrow$  So Eve screws up the bit (gets caught if bits are compared)  
w/  $\frac{1}{4}$  probability.

Phase III . (Check for Eve)

Choose some # of bits of shared secret (randomly)  
to reveal & compare & discard.

Agree: No Eve, use secret  
(probably)

Disagree: Throw away everything & start over.

If we check 1 bit, Eve gets away with it w/ prob  $3/4$   
 " " 2 bits, " "  $(3/4)^2$   
 " " k bits, " "  $(3/4)^k \rightarrow 0$

Choose  $k$  s.t.  $(3/4)^k$  is a small & acceptable risk.