(3) $i|0\rangle + \sqrt{3}|1\rangle$ recall: want $|a|^2 + |b|^2 = 1$

$|a+bi| = \sqrt{a^2+b^2}$
$|a+bi|^2 = a^2+b^2$

1. check: length $= |i|^2 + |\sqrt{3}|^2 = 1 + 3 = 4$

   normalize: $\frac{i}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ has length $\left|\frac{i}{2}\right|^2 + \left|\frac{\sqrt{3}}{2}\right|^2 = \frac{1}{4} + \frac{3}{4} = 1$

2. measure: (w.r.t. basis $|0\rangle, |1\rangle$)
   - $|0\rangle$ prob. $\left|\frac{i}{2}\right|^2 = \frac{1}{4}$
   - $|1\rangle$ prob $\left|\frac{\sqrt{3}}{2}\right|^2 = 3/4$.

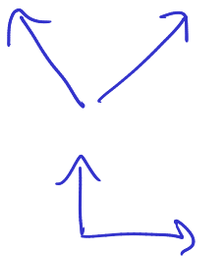
Eg. $\frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle$

length $= \left|\frac{1+i}{2}\right|^2 + \left|\frac{1-i}{2}\right|^2 = \frac{1^2+1^2}{2^2} + \frac{1^2+1^2}{2^2} = \frac{2}{4} + \frac{2}{4} = 1$

Photons w/ 2 bases:

V basis

L basis



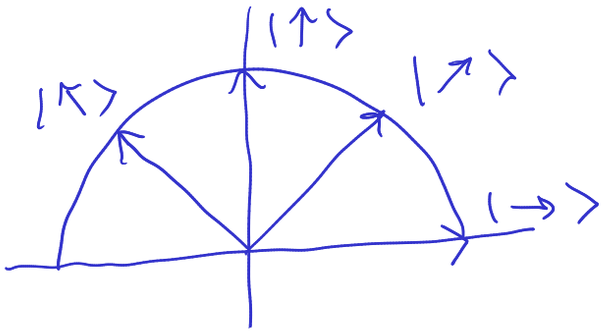
V basis L basis

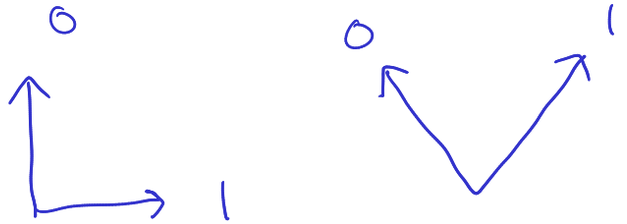
eg. $|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$

measurement:

in L basis: $\begin{cases} |\uparrow\rangle \text{ w/ prob } \frac{1}{2} \\ |\rightarrow\rangle \text{ w/ prob } \frac{1}{2} \end{cases}$

in V basis $\begin{cases} |\nearrow\rangle \text{ w/ prob } 1 \\ |\nwarrow\rangle \text{ w/ prob } 0 \end{cases}$





$$|\nwarrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\rightarrow\rangle$$

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\rightarrow\rangle$$

$$|\uparrow\rangle = \frac{1}{\sqrt{2}}|\nwarrow\rangle + \frac{1}{\sqrt{2}}|\nearrow\rangle$$

$$|\rightarrow\rangle = \frac{-1}{\sqrt{2}}|\nwarrow\rangle + \frac{1}{\sqrt{2}}|\nearrow\rangle$$

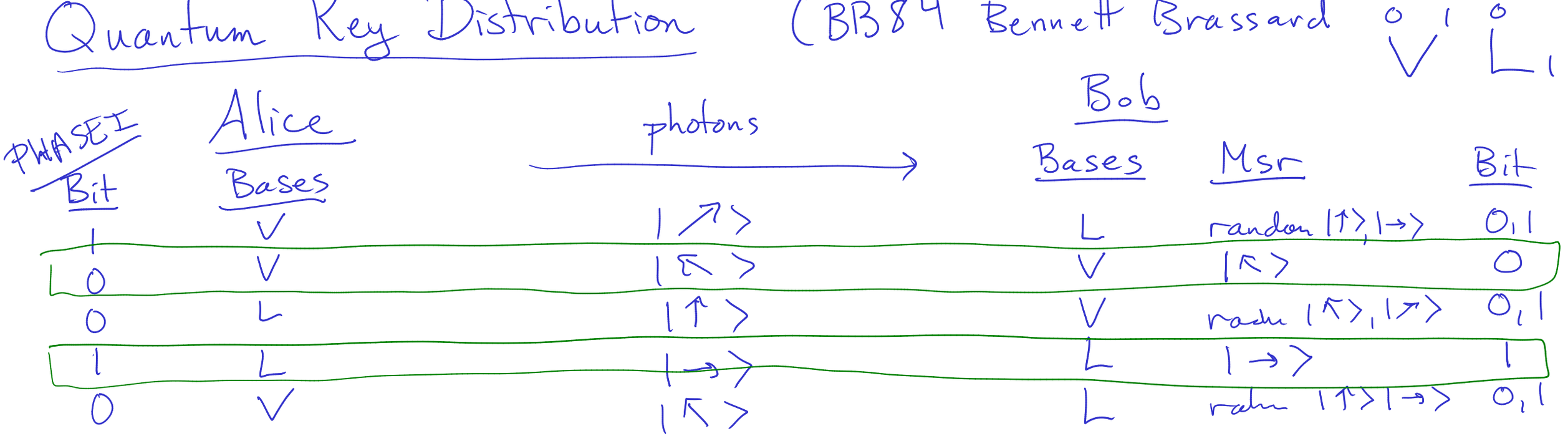
① Bit + basis $\Rightarrow$ create photon coding that bit in that basis

	V	L
0	$\|\nwarrow\rangle$	$\|\uparrow\rangle$
1	$\|\nearrow\rangle$	$\|\rightarrow\rangle$

② From photon & basis, read a bit

	$\|\uparrow\rangle$	$\|\rightarrow\rangle$	$\|\nearrow\rangle$	$\|\nwarrow\rangle$
L	0	1	rand 50/50	rand 50/50
V	rand 50/50	rand 50/50	1	0

Quantum Key Distribution (BB84 Bennett Brassard)



1) Alice gen. bits randomly
   Alice gen. bases randomly
   } { Bob chooses bases randomly.

2) Generates ₿ sends photons
   } { Bob measures photons in his basis
   ₿ interprets as a bit

PHASE 2

Alice phones Bob (classical channel, no encryption)
and they compare bases.

They keep the rows of the table where the bases agree.
Those bits form the shared secret.

Our example: 0, 1

Could an Eavesdropper see the secret?

To learn anything about a quantum state, must measure.

eg. (1) Alice send $|\uparrow\rangle$ (L basis)
Eve msrs in V basis
$\Rightarrow$ the photon becomes $|\nwarrow\rangle$ or $|\nearrow\rangle$ w/ 50-50 prob.

Bob msrs in L basis, gets $|\uparrow\rangle$ or $|\rightarrow\rangle$ w/ 50-50 prob.

Ack: Eve's activity screws up the shared bit w/ probability 1/2.

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

Eve msrs in L basis

$\Rightarrow$ she reads $|\uparrow\rangle$ w/o changing anything.

Bob msr in L basis, get $|\uparrow\rangle$, bits agree, no change.

Eve succeeds

Bottom Line: If Eve can't predict bases, she's in situation ① or ② w/ 50-50 probability. So 1/4 of the time, she messes up the shared bit.

Phase III (Check for Eve)

A & B Choose some # of the supposed shared bits randomly to reveal & compare & discard.

Agree: Probably no Eve.

Disagree: Caught Eve, throw away entire secret.

If we check 1 bit, Eve gets away with it $3/4$ time.
2 $(3/4)^2$
3 $(3/4)^3$ etc.

So total # of bits to send: $\approx 2\times$ (# of bits needed + # of bits to achieve confidence Eve isn't there.)