Tues: Exam I

   Covers all   Lectures 1→11

                    HW 1→6

   Bring :: ~~½ single side letter s~~
            ½ letter sheet single side.

BB84 Scheme - no evesdropping

In the BB84 scheme Alice + Bob choose to prepare/measure states in the bases:

$$Z = \{ |0\rangle, |1\rangle \}$$

$$X = \left\{ \underbrace{\frac{|0\rangle + |1\rangle}{\sqrt{2}}}_{|+\rangle}, \underbrace{\frac{|0\rangle - |1\rangle}{\sqrt{2}}}_{|-\rangle} \right\}$$

Their schemes for translating between bit values and states/outcomes are

Alice				Bob		
Bit value	Basis	State		Measurement	outcome	bit value
0	Z	$|0\rangle$		Z	0	0
1	Z	$|1\rangle$		Z	1	1
0	X	$|+\rangle$		X	+	0
1	X	$|-\rangle$		X	−	1

The protocol is as follows

Alice	Bob

Alice uses a classical procedure to generate a random stream of bits

🧍📦 ~ 0 1 1 0 ⟩ 1 0 1 0 ⟩ 0 0 1 0

Alice uses a classical procedure to randomly choose one basis per bit

🧍 ~▷ Z X Z X ⟩ X Z X X ⟩ X X X X

Bob uses a classical procedure to randomly choose a measurement type/basis. He records this

🧍 X X Z Z ⟩ Z Z Z X ⟩ Z X X Z

Alice records both of these. For each she prepares a qubit in the relevant state and transmits to Bob

He measures each qubit in the basis and records the result. An example is

#1   #2   #3   states unknown to Bob
🔵   🔵   🔵

$$0\ 1\ 1\ 0 \begin{Bmatrix} 1\ 0\ 1\ 0 \end{Bmatrix} 0\ 0\ 1\ 0$$
$$Z\ X\ Z\ X \begin{Bmatrix} X\ Z\ X\ X \end{Bmatrix} X\ X\ X\ X$$
$$|0\rangle|{-}\rangle|1\rangle|+\rangle\ |{-}\rangle|0\rangle|{-}\rangle|+\rangle\ |+\rangle|+\rangle|{-}\rangle|+\rangle$$

#1 2 3 4 5 6 7 8

Alice transmits qubits to Bob

Choice	X	X	Z Z	Z Z Z X	Z X X Z
Result	0	+	1 −	0 0 1 +	1 + − 0
Bit value	0	1	1 1	0 0 1 0	1 0 1 0

|+⟩ |1⟩ |−⟩ |0⟩ ↙

🔵   🔵   🔵   🔵
#4   #3   #2   #1

Bob does <u>not</u> know the <u>states</u>

At this stage he does not know her choices

Quantum physics predicts:
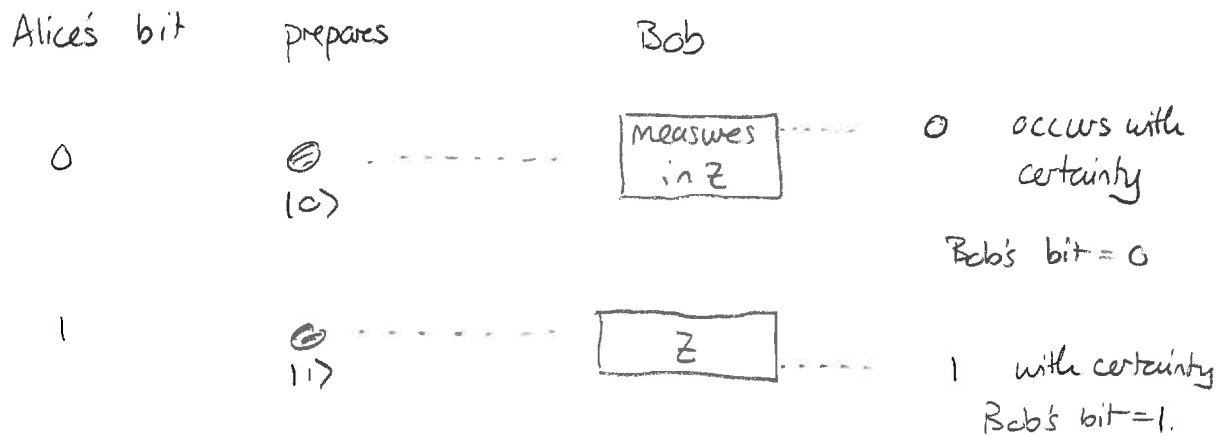
    1) For a qubit where Alice + Bob use the same basis then
       their bit values will agree with certainty

    2) For any qubit where Alice + Bob use different bases
       their bit values will not agree with certainty. On average
       they will agree about ½ the time
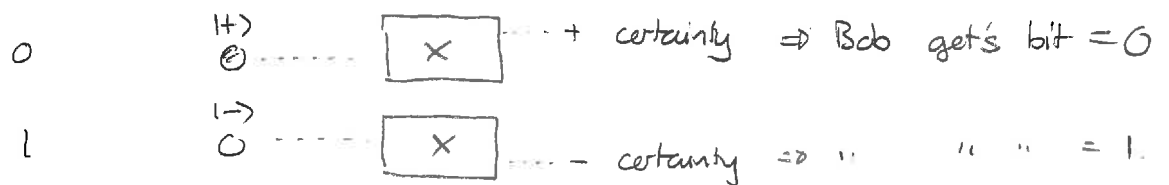
We will analyze these in detail in an exercise.

1 BB84 – no eavesdropping

a) Consider a qubit for which Alice and Bob use the same basis. Show that for all possible choices of bit value and basis, Bob will obtain the same bit value as Alice.

b) Consider a qubit for which Alice uses the Z basis and Bob uses the X basis. For each choice of bit value that Alice might use, determine the probability that Bob gets the same bit value. What is the overall probability that Alice and Bob agree on bit values for this situation?
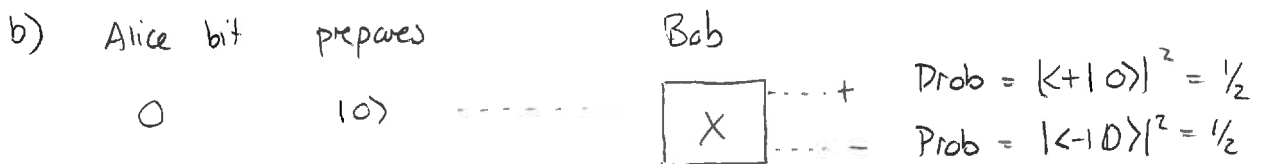
Answer: a) Suppose they both use Z. Then

Alice's bit   prepares   Bob
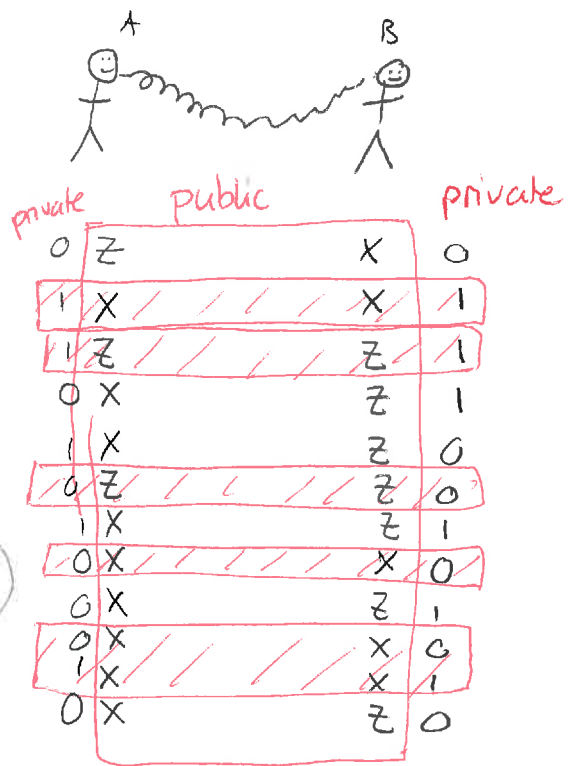
0                  $|0\rangle$ measures in Z 0 occurs with certainty

                                                                Bob's bit $= 0$

1                  $|1\rangle$ Z 1 with certainty

                                                                Bob's bit $= 1$.

Similarly if they use X

0                  $|+\rangle$ X $+$ certainty $\Rightarrow$ Bob gets bit $= 0$

1                  $|-\rangle$ X $-$ certainty $\Rightarrow$ '' '' '' $= 1$.

They match.

b)   Alice bit   prepares   Bob

0                  $|0\rangle$ X $+$ Prob $= |\langle +|0\rangle|^2 = \frac{1}{2}$
                                                    $-$ Prob $= |\langle -|0\rangle|^2 = \frac{1}{2}$

So Bob gets value 0 with prob $\frac{1}{2}$ and bit value 1 with prob $\frac{1}{2}$.

Similarly if Alice's bit is 1

So overall prob of agreement $= \frac{1}{2}$

The next stage of the BB84 protocol is:

After transmission + measurement Alice + Bob communicate their choices of basis but keep the bit values secret.

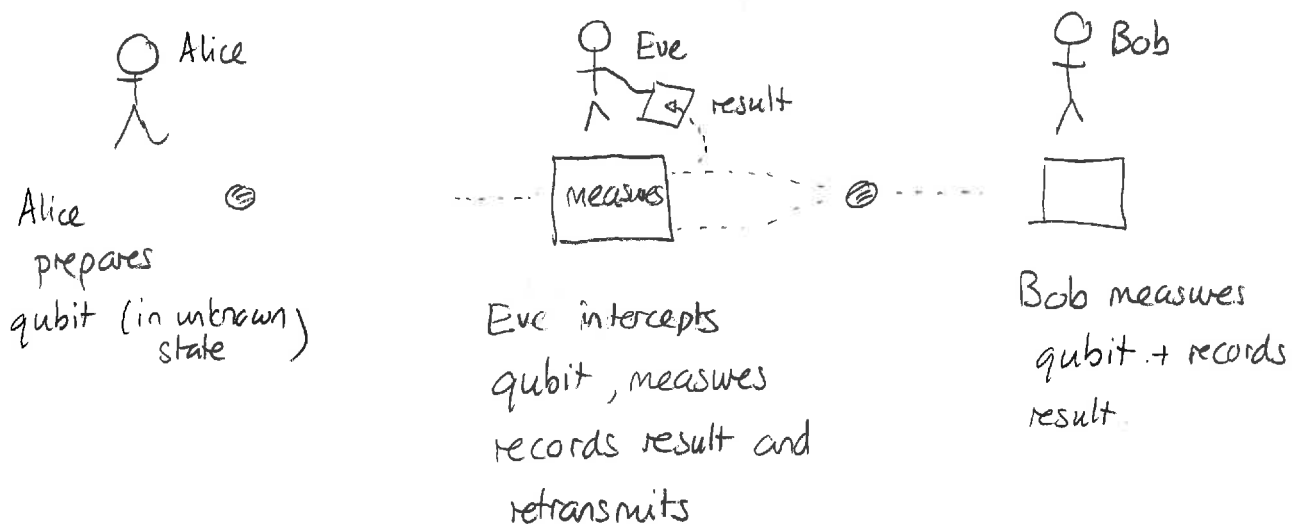They then reject all runs where they disagree + keep those where they agree.

private	public		private
0	Z	X	0
1	X	X	1
1	Z	Z	1
0	X	Z	1
1	X	Z	0
0	Z	Z	0
1	X	Z	1
0	X	X	0
0	X	Z	1
0	X	X	0
1	X	X	1
0	X	Z	0

At this stage quantum physics predicts that for the runs which they retained their bit values will be identical with certainty. Since it is no longer possible to intercept the qubits (they could be destroyed) no more measurements can occur. They have a secret string of bits that is private to just them.

Note that the success rate per actual qubit sent is about ½.

BB84 - with eavesdropping

Now consider the possibility of eavesdropping. An eavesdropper could try many strategies but in each her goal is to learn the key without being detected.

We consider one relatively simple strategy

Alice prepares qubit (in unknown state)

Eve intercepts qubit, measures records result and retransmits

Bob measures qubit + records result

Eve does this before Bob measures and therefore before Alice + Bob have communicated their basis choice. So she has to randomly choose a basis in which to measure although it will be one of X or Z.

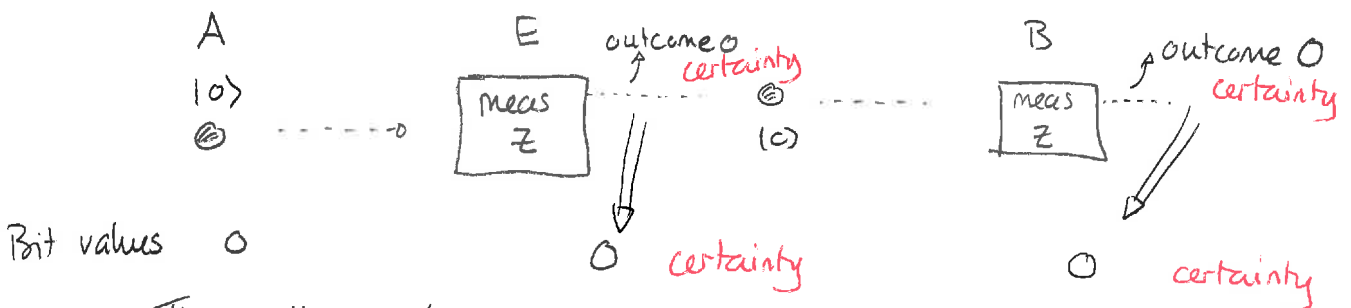We could consider all possibilities of basis choices for A, B and E

However, we can restrict analysis to choices where A and B use the same basis since they reject those where their bases are different.

We will analyze these possibilities. But recall that in these cases, in the absence of Eve, Alice + Bob will always agree on the bit value.
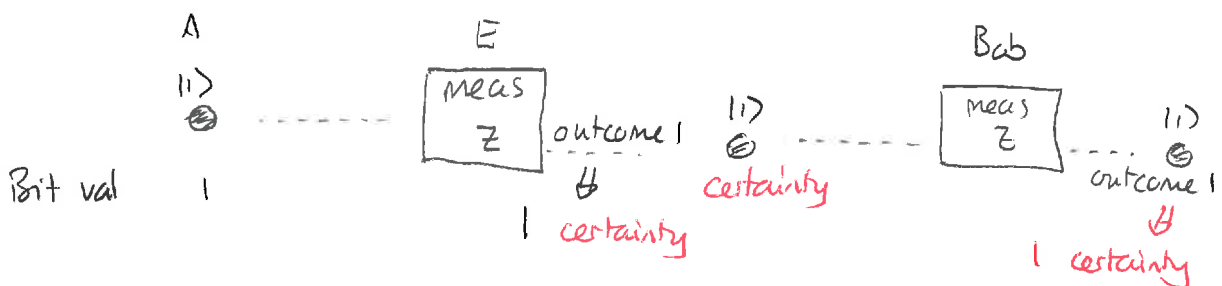
2 BB84 – with eavesdropping

a) Suppose that Alice and Bob both choose to use the Z basis for a particular qubit. Suppose that Eve chooses the same basis. For each bit values that Alice could use determine the probabilities with which Eve will extract either 0 or 1 and the probabilities with which Bob will extract either 0 or 1. Does this ever produce a mismatch between Alice and Bob's bits? Could Bob and Alice detect the presence of Eve?

b) Suppose that Alice and Bob both choose to use the Z basis for a particular qubit. Suppose that Eve chooses the X basis. For each bit values that Alice could use determine the probabilities with which Eve will extract either 0 or 1 and the probabilities with which Bob will extract either 0 or 1. Does this ever produce a mismatch between Alice and Bob's bits? Could Bob and Alice detect the presence of Eve?

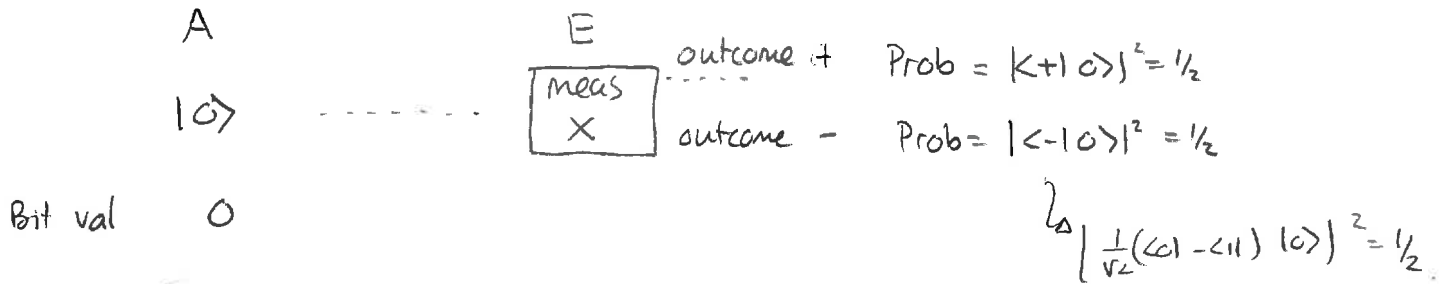Answer a)   Suppose   Alice's bit value is 0. Then

Bit values   0

They all match,

Suppose   Alice's bit value is 1. Then

Bit val   1

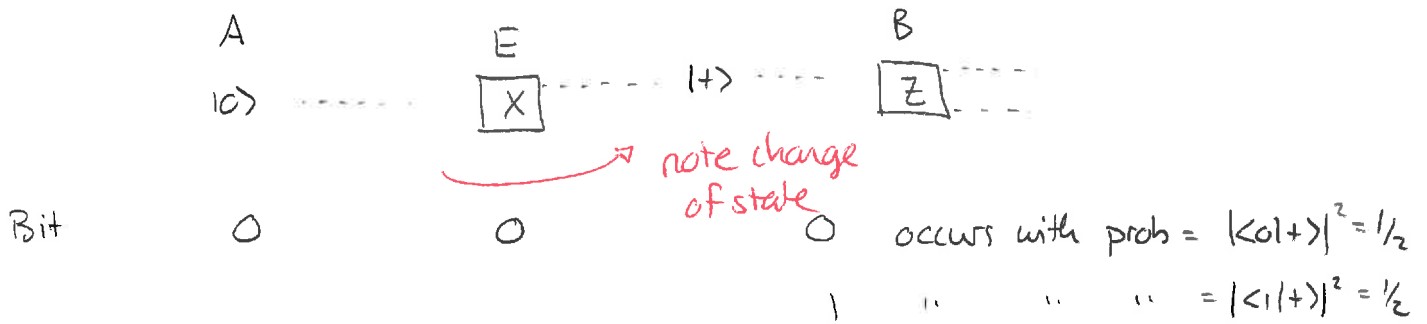They all match.

So   A, B and E's   bit values all match. Based on their own actions observations, there is no difference to the case where Eve is absent. So they cannot detect her.
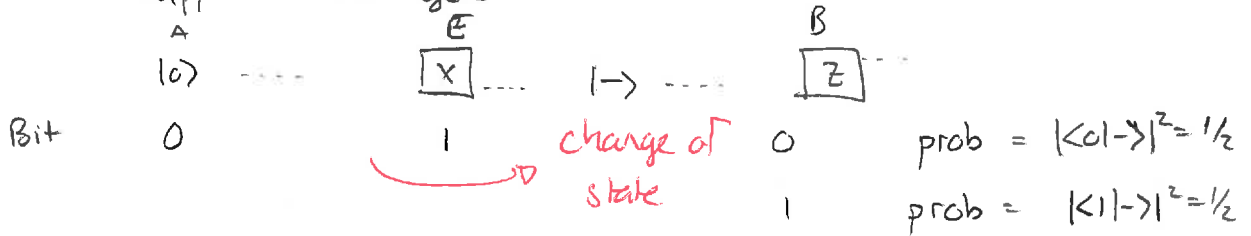
b)   Suppose Alice prepares bit 0

A   E

$|0\rangle$ - - - - - - - -   [meas X]   outcome +   Prob $= |\langle +|0\rangle|^2 = \frac{1}{2}$

                           outcome −   Prob $= |\langle -|0\rangle|^2 = \frac{1}{2}$

Bit val   0 $\left| \frac{1}{\sqrt{2}}(\langle 0| - \langle 1|) |0\rangle \right|^2 = \frac{1}{2}$

Both outcomes are equally likely for Eve's measurement. Suppose she gets +. Then

A   E   B

$|0\rangle$ - - - - -   [X] - - - - $|+\rangle$ - - - - [Z] - - -

                    note change of state

Bit   0   0   0   occurs with prob $= |\langle 0|+\rangle|^2 = \frac{1}{2}$

                                     1   "   "   " $= |\langle 1|+\rangle|^2 = \frac{1}{2}$

Suppose she gets −. Then

        A   E   B

$|0\rangle$ - - - -   [X] - - - - $|-\rangle$ - - - [Z] - -

Bit   0   1   *change of state*   0   prob $= |\langle 0|-\rangle|^2 = \frac{1}{2}$

                                          1   prob $= |\langle 1|-\rangle|^2 = \frac{1}{2}$

So we can summarize:

Measure choices   A ⟿ Z

                          E ⟿ X

                          B ⟿ Z

Alice bit	Eve bit	Bob bit	Prob
0	0	0	$\frac{1}{4}$
0	0	1	$\frac{1}{4}$
0	1	0	$\frac{1}{4}$
0	1	1	$\frac{1}{4}$

Similarly if Alice uses bit 1 we get:

Alice	Eve	Bob	Prob
1	0	0	1/4
1	0	1	1/4
1	1	0	1/4
1	1	1	1/4

The table indicates that in these cases Alice + Bob's bits match with probability 1/2. They mismatch with probability half

So we see that, for the cases where A,B use same basis:

1) When Eve uses same basis, she learns bit value with certainty and A,B cannot detect her presence (this scenario occurs with probability 1/2)

2) When Eve uses a different basis (this occurs with prob 1/2) she learns bit value with prob 1/2. Also with prob 1/2 there will be a mismatch between A,B's bits.
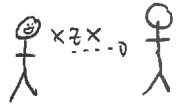
Thus for this type of attack
  i) Eve learns bit value with prob 3/4.
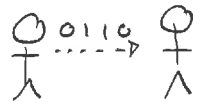 2) Alice + Bobs bits mismatch with prob 1/4.

So quantum theory has forced Eve to reveal her presence.

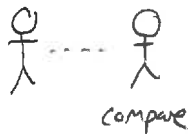The remaining step is that Alice + Bob need to check for the presence of Eve. They do this by:

After measurements A, B compare basis choices and reject runs where they used different basis

Of the surviving runs, A,B randomly choose a subset for inspection. Alice reveals the bit values of this subset. Bob compares these "sampled bits"
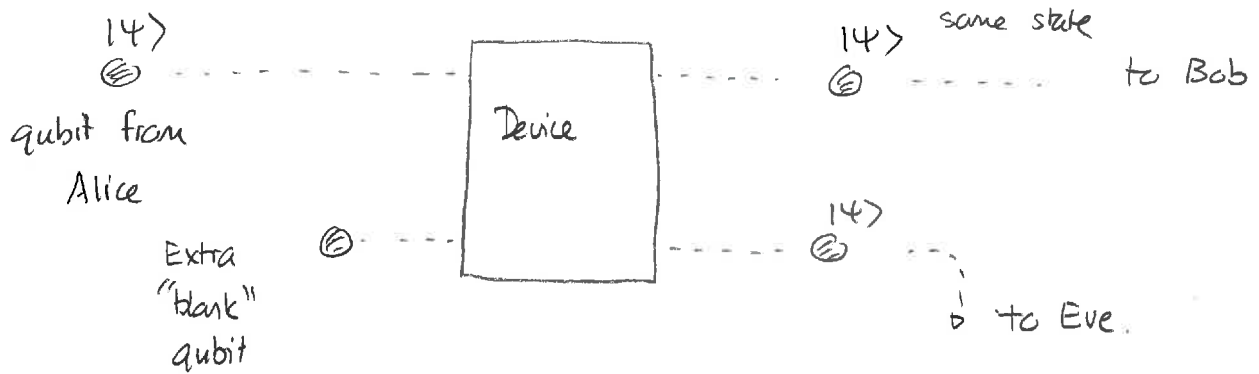
If Eve has done the previous attack about 25% of the "sampled bits" will have a mismatch.
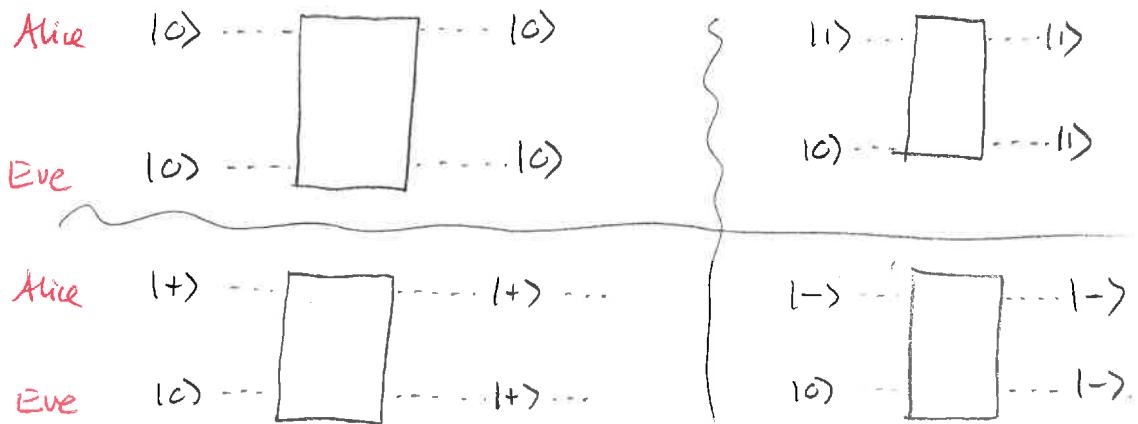
In this way they can detect Eve

More sophisticated eavesdropping?

Eve could try more sophisticated strategies. Perhaps she could copy the state that Alice sends. This would require a copying device that needs to do:

$|\psi\rangle$
qubit from Alice

Extra "blank" qubit

Device

$|\psi\rangle$ same state
to Bob

$|\psi\rangle$
to Eve.

Specifically we would need:

Alice $|0\rangle$ ---- [ ] ---- $|0\rangle$

Eve $|0\rangle$ ---- [ ] ---- $|0\rangle$

$|1\rangle$ ---- [ ] ---- $|1\rangle$

$|0\rangle$ ---- [ ] ---- $|1\rangle$

Alice $|+\rangle$ ---- [ ] ---- $|+\rangle$ ---

Eve $|0\rangle$ ---- [ ] ---- $|+\rangle$ ---

$|-\rangle$ ---- [ ] ---- $|-\rangle$

$|0\rangle$ ---- [ ] ---- $|-\rangle$

Is such a device possible? If so one can "clone" an unknown quantum state. We will show that a general requirement of quantum physics prohibits this