Quantum Cryptography

Entanglement can, in principle, be used to send secure messages. To see how it works, we first need to know a bit about how cryptography works. Most cryptography is based on a secret key. Both parties need to know the key.

For example, suppose you want to send the ASCII code for "X"

"X" = 01011000

and suppose the key is 01001001. You can encode the message using the "XOR" operation. If both digits in the message and the key match, encode "1", otherwise encode "0".

Message:	"X" =	0 1 0 1 1 0 0 0
Key:		0 1 0 0 1 0 0 1
Encoded message:		1 1 1 0 1 1 1 0

Now, Bob sends the encoded message to Alice who decodes it with the same key

Encoded Message:	1 1 1 0 1 1 1 0	
Key:	0 1 0 0 1 0 0 1	
Decoded message:	0 1 0 1 1 0 0 0	= "X"

it worked!

This method is perfectly secure provided no one else knows the key. The question is how to create a key which both parties have but no one else knows. If you try to send the key over some transmission, there's always a possibility it gets intercepted by an evesdropper. But ... quantum entanglement provides a way around this.

Quantum Cryptography

Here's the idea: Alice and Bob each have a Stern-Gerlach apparatus which can be oriented along the z-axis, or the x-axis. The two randomly and independently orient their SG apparatuses (by, say, flipping a coin).

Bob now creates an entangled e^+e^- pair and sends one of the particles to Alice. They instruct each other to measure the spin of the particles in rapid succession and repeat many times recording the results.

Later, Bob and Alice call each other, and let each other know the orientations of the SG Apparatus.

① Whenever their axes are the same, they agree to use Bob's measurement $|+\rangle$ or $|-\rangle$ as either 1 or 0 for the key. Of Course Alice knows Bob's measurements because it is opposite of hers (singlet state)

$$|\chi\rangle = \frac{1}{\sqrt{2}}\left[\,|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\,\right]$$

② There is no problem if someone intercepts their call where they say how they set the apparatus. That eavesdropper (EVE) would know which pairs are used to form the key, but would not know the results of the measurement (spin up or down)... theres a 50-50 chance of each.

Some sample data is listed on the next page.

Quantum Cryptography

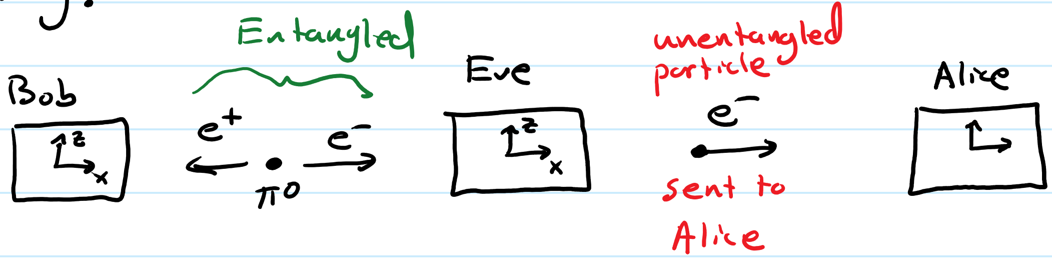
Alice		Bob		Key
Orientation	Result	Orientation	Result	
z	+	z	−	0
z	+	z	−	0
x	−	z	−	
z	+	x	+	
x	+	x	−	0
x	−	x	+	1
x	−	x	+	1
z	−	z	+	1
x	+	z	−	
z	−	x	+	

Randomly Generated by coin flip

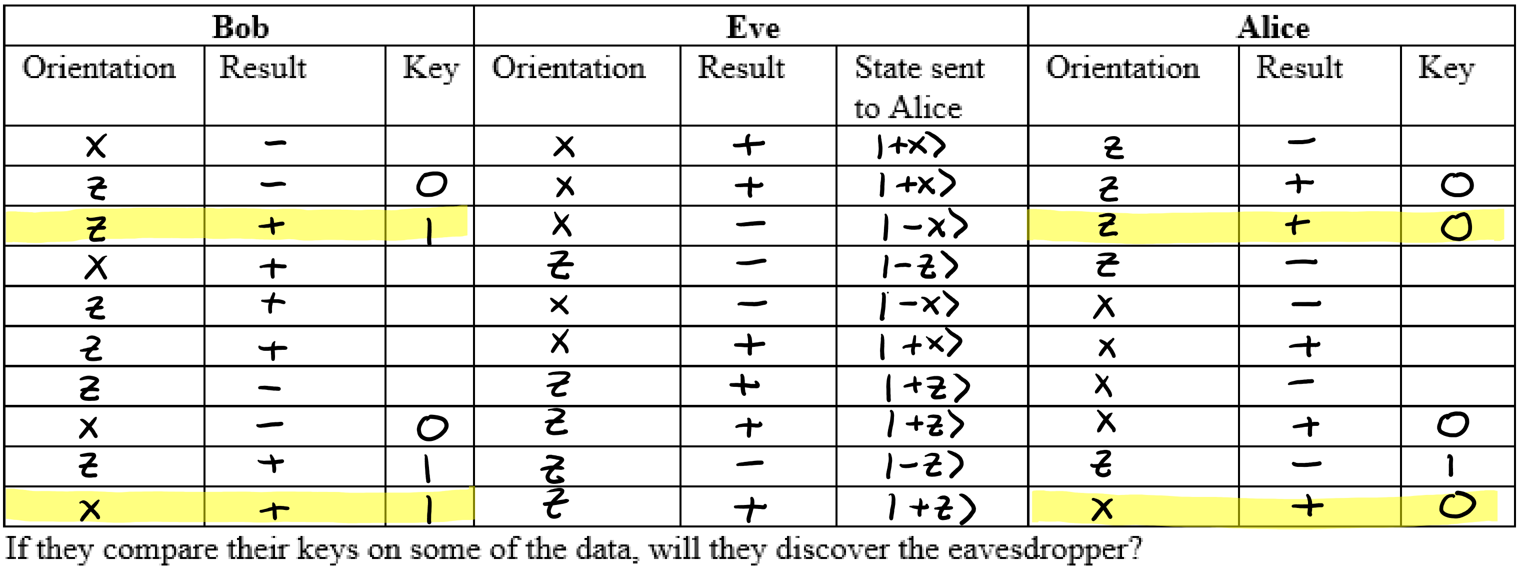
Each result is random (QM!)

But when the apparatuses are set to the same axis, Bob & Alice will get opposite spins (entanglement).

Even better, this setup could be used to detect an eavesdropper. If someone intercepted & measured particle sent to Alice, they'd collapse the quantum state. Of course, Alice would notice if the particles didn't arrive, so the listener (EVE) would have to send some particles so as not to give herself away. But, Eve could never recreate the original state which is entangled with Bob's particle. If Bob and Alice compare some samples of their measurements, they'd notice that some of their results are <u>not</u> perfectly anticorrelated and they'd know someone was listening!



Quantum Cryptography



Bob			Eve			Alice		
Orientation	Result	Key	Orientation	Result	State sent to Alice	Orientation	Result	Key
x	-		x	+	$\|+x\rangle$	z	-	
z	-	0	x	+	$\|+x\rangle$	z	+	0
z	+	1	x	-	$\|-x\rangle$	z	+	0
X	+		z	-	$\|-z\rangle$	z	-	
z	+		x	-	$\|-x\rangle$	X	-	
z	+		x	+	$\|+x\rangle$	x	+	
z	-		z	+	$\|+z\rangle$	x	-	
x	-	0	z	+	$\|+z\rangle$	x	+	0
z	+	1	z	-	$\|-z\rangle$	z	-	1
x	+	1	z	+	$\|+z\rangle$	X	+	0

If they compare their keys on some of the data, will they discover the eavesdropper?

Note the highlighted entries. In those entries, Bob & Alice had the apparatuses aligned, but got the same result. Someone must have broken the quantum state (by observing it) and so Eve is detected.