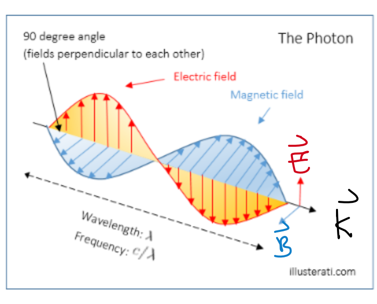
Quantum cryptography: Photons and BB84

Photons as qubits

- The energy associated to light is quantized in units of hν, where h=6.62 × 10^{-34} Js is called Planck's constant and ν is the frequency of light in Hertz. Each quanta of light is called "photon".
- In the 1st week of class we established an analogy between electron spin (states up/down) and classical waves of light (polarization state E//x or E//y). It turns out that this analogy is a complete equivalence: The polarization of a photon is actually a two level system just like a qubit:



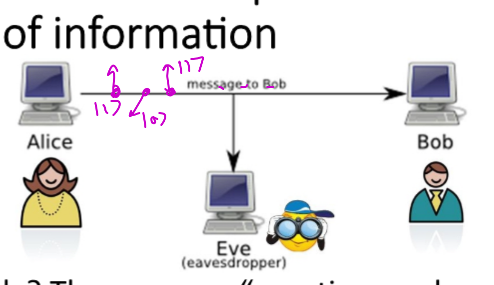
PHOTON PROPAGATING ALONG $\vec{k}$ WITH POLARIZATION

$\vec{E} \parallel \hat{x} \Rightarrow |\vec{k}, \vec{E}\parallel\hat{x}\rangle \equiv |0\rangle$, $|\vec{k}, \vec{E}\parallel\hat{y}\rangle \equiv |1\rangle$ } A PERFECT FLYING QUBIT!

$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |\vec{k}, \vec{E} \parallel \frac{\hat{x}+\hat{y}}{\sqrt{2}} = 45° \text{ Pol.}\rangle$

ALSO $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) = |\vec{k}, \vec{E} \parallel \frac{\hat{x}+i\hat{y}}{\sqrt{2}} = \text{RIGHT Circ. Pol.}\rangle$

Quantum communication: Each photon transmitted in an optical fibre sends one bit of information



- But how to send securely? They can use "one-time pad encryption". First Alice and Bob must share a private key: A *random* n-bit string:

$$\boldsymbol{S} = 010001111001110\cdots$$

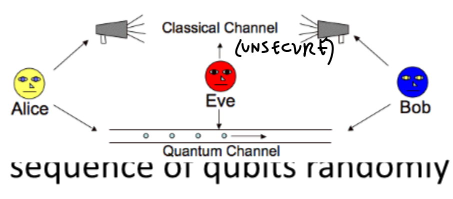
- Alice encodes her message $\boldsymbol{M}_1$ by transmitting $\boldsymbol{M}_1 \oplus \boldsymbol{S}$. Bob knows the key $\boldsymbol{S}$ so he can decode the message:

$$(\boldsymbol{M}_1 \oplus \boldsymbol{S}) \oplus \boldsymbol{S} = \boldsymbol{M}_1$$

- This method is 100% secure against eavesdropper "Eve", but only for the first n bits transmitted. If Alice sends another message $\boldsymbol{M}_2 \oplus \boldsymbol{S}$, Eve can do $(\boldsymbol{M}_1 \oplus \boldsymbol{S}) \oplus (\boldsymbol{M}_2 \oplus \boldsymbol{S}) = \boldsymbol{M}_1 \oplus \boldsymbol{M}_2$ and use letter-frequency code breaking to decode $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$.

Quantum key distribution: BB84 protocol (Bennet, Brassard 1984)

- Problem: How can Alice and Bob share a key remotely without allowing Eve to learn the key? Quantum mechanics provides a 100% secure method for that!



- BB84: Alice sends Bob a sequence of qubits randomly chosen to be in one of four states:

$$|0\rangle, |1\rangle, H|0\rangle, H|1\rangle$$

PHOTON POLARIZED: x, y (TYPE-1 BASIS), +45°, −45° (TYPE-H BASIS)

- As each qubit arrives Bob randomly decides whether to measure in the type-1 basis (with an x-polarizer) or in the type-H basis (with a 45^0 polarizer).

BB84

- After Bob measured all the qubits (and recorded his sequence of 0s and 1s), Alice tells him over an insecure channel which qubits were sent type-1 and which type-H. However, *she does not reveal* which state she prepared for each qubit: Whether it was |0>, |1>, or H|0>, H|1>.
- On average, half of Bob's choice of basis will coincide with Alice's choice of basis. For those qubits (the "coincidence qubits"), Bob will learn the actual random bit 0 or 1 that Alice chose to send. Finally, Bob tells Alice over an insecure channel which qubits coincided (without revealing their state!). Now they both share a list of ~ n/2 random bits that they can use as a one-time pad!

		1	2	3	4	5	6	7	8	9 . . .
Alice:	Type:	1	H	H	H	1	1	H	1	H . . .
	State:	0	1	0	1	1	0	1	0	0 . . .
Bob:	Measure-ment type:	H	H	H	1	1	H	1	1	1 . . .
	Outcome:	1	1	0	0	1	1	1	0	0 . . .

Security against Eve

- Alice randomly switched between type-1 and type-H to provide security against Eve: If Alice had instead sent them all type-1, Eve could acquire the same type of information as Bob without being detected (provided Eve knew it was type-1).
- With Alice switching randomly, the best Eve can do is to read-out randomly in type-1 and type-H (just like Bob), and then sending over to Bob. Once she learns about the sequence of coincidence bits Alice and Bob agreed upon, only an unknown ~ half of her measurements will agree with Alice's choice (type-1 or H). On average half of these qubits (1/4 of the pad) will be "corrupted" by Eve's measurement, so a ¼ of Bob's code pad will disagree with Alice's.
- This makes Eve's intervention detectable. All Alice and Bob need to do is to sacrifice a few of their secret bits, sharing them over the unsecure channel. If ¼ of them don't agree, they will learn that Eve is systematically listening to their conversation! If instead only a tiny fraction disagrees, they can set an upper bound on the security of their channel.

Let's play the Alice-Eve-Bob game?

Complete the table by *flipping a coin* when appropriate.

(a) Assume Eve is *not* listening.

1) Alice chooses which qubits are type-1 and which are type-H, and whether to send 0 or 1.
2) Bob chooses whether to measure in type-1 or type-H *by flipping a coin*. Bob reads-out (use coin to get result when appropriate).
3) Mark the coincidence list and obtain your one-time code pad (the private key). How long is it?

		1	2	3	4	5	6	7	8	9	10
	Qubit:	1	2	3	4	5	6	7	8	9	10
ALICE	Type:	1	H	1	1	H	1	H	H	1	1
	State:	1	0	0	1	0	0	1	1	1	0
EVE	TYPE:	H	H	1	1	1	H	H	1	1	H
	STATE:	1	0	0	1	0	0	1	0	1	0
BOB	Meas. Type:	H	H	1	H	H	H	H	1	1	1
	Outcome:	~~0~~ 1	0	0	1	1	0	1	0	1	1

⇒ ALICE'S PAD: 000110
BOB'S PAD: 001111
EVE'S PAD: 000110

FOR THESE CHOICES, IT HAPPENED THAT EVE'S PAD COINCIDED WITH ALICE'S! SO EVE IS ABLE TO READ THE MESSAGE. BOB'S PAD HAD 1/3 OF ITS QUBITS CORRUPTED. IF BOB CROSS-CHECKS WITH ALICE, THEY WILL LEARN THAT SOMEONE IS LISTENING!

(b) Assume Eve *is* listening.

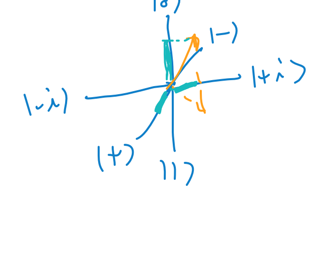
Repeat the same procedure, but before Bob measures, Eve reads out. Choose a sequence of type-1 or type-H measurements for Eve (random or not, your choice!), and decide on outcomes of Eve's measurements using a coin when appropriate. Compile the list for Bob's measurements and compare Bob's one-time pad to Alice's. Which fraction disagrees?

Quantum tomography

- Say Alice holds an *unknown* 1-qubit state (e.g. outcome of a complicated QC):

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

- Each measurement she makes (after applying a unitary transf. of her choice) yields either 0 or 1 and destroys the state! It is impossible for her to learn the value of complex coefficients α and β. However, if she can create the state |ψ> over and over again, she can come up with an approximation for α, β after doing statistics on a large number N of measurements (precision $\sim 1/\sqrt{N}$).
Question: How many different basis she needs to measure on? (Good question for final exam).
- The process of approximating α, β is called *quantum tomography*. It's a very costly process.



Summary

- Single photons are flying qubits: They provide a practical means to do quantum communication. We showed that the polarization state of a photon can encode a single qubit.
- Secure communication requires a private key, a random string of bits only known by the sender and the receiver. Quantum mechanics (BB84) provides an ingenious method for two parties to share a random string of bits! This allows the sender and receiver to share their key remotely with 100% security and ability to detect a possible eavesdropping event. Note: Quantum mechanics does not enable private communication of meaningful messages – it only enables private communication of a random message!