Filippos Vogiatzian

Quantum Key Distribution

Quantum Cryptography

Motivation

- Cryptography relies on adversarial computational power

Motivation

- Cryptography relies on adversarial computational power
- Backwards unreliable secrecy

Motivation

- Cryptography relies on adversarial computational power
- Backwards unreliable secrecy
- As soon as we have quantum computers:
  - Shor's Algorithm: Integer factorisation in polynomial time!

Motivation

- Cryptography relies on adversarial computational power
- Backwards unreliable secrecy
- As soon as we have quantum computers:
  - Shor's Algorithm: Integer factorisation in polynomial time!

Can’t we obtain perfect security ?

Motivation

- Cryptography relies on adversarial computational power
- Backwards unreliable secrecy
- As soon as we have quantum computers:
  - Shor's Algorithm: Integer factorisation in polynomial time!

Can’t we obtain perfect security ?

One-Time Pad !!!

Motivation

- Cryptography relies on adversarial computational power
- Backwards unreliable secrecy
- As soon as we have quantum computers:
  - Shor's Algorithm: Integer factorisation in polynomial time!

Can’t we obtain perfect security ?

One-Time Pad !!!

When Classical Cryptography fails…

When Classical Cryptography fails…

Quantum Cryptography

Post-quantum Cryptography

When Classical Cryptography fails...

Quantum Cryptography

- Perfect Security
- Relies only on the laws of nature

Post-quantum Cryptography

When Classical Cryptography fails...

Quantum Cryptography

- Perfect Security
- Relies only on the laws of nature

Post-quantum Cryptography

- Quantum Computational Security
- Relies on primitives that are equally hard for classical and quantum computers to solve
  - Lattice-Based Cryptography

QKD 2PC and more

- Quantum Key Distribution (QKD): Two parties (Alice and Bob) communicate with perfect secrecy in the presence of an eavesdropper (Eve) [1,3,4]
- Two-Party Cooperation (2PC): Two parties that don’t trust each other cooperate in a secure way
- How to encrypt or authenticate a quantum state
- Implementations

$$\langle \phi_k | \phi_{k'} \rangle = \langle \phi_k | \int_{-L/2}^{L/2} dx\, |x\rangle\langle x| \phi_{k'} \rangle$$

$$\Rightarrow \left(\frac{2\pi}{L} n + k_0\right)\frac{L}{2} = \frac{\pi}{2}(2l-1),\ l = 1, 2, \ldots \Rightarrow k_0 = -\frac{\pi}{L}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$\langle \phi_k | \phi_{k'} \rangle = \int_{-L/2}^{+L/2} dx\, \phi_k^*(x) \cdot \phi_{k'}(x)$$

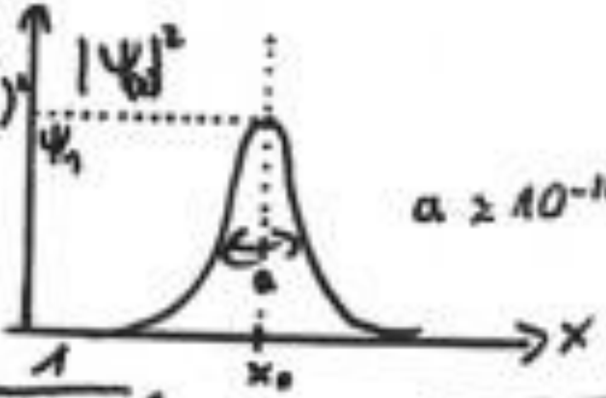
$$\psi_n(x) = \sqrt{\frac{2}{L}} \cos\left[\frac{\pi}{L}(2n-1)x\right];\ \varphi_a - \varphi_b = \pi;\ \psi_n(x) = \sqrt{\frac{2}{L}} \sin\left[\frac{2\pi}{L} n x\right]$$

$$\langle \phi_k | \phi_{k'} \rangle = \frac{1}{L}\int_{-L/2}^{+L/2} dx\, e^{-ikx} e^{ik'x} \stackrel{!}{=} 0;\ k \neq k'$$

$$\hat{H}\psi_{ns}(x) = -\frac{\hbar^2}{2m}\partial_x^2 \psi_{ns}(x) = \frac{\hbar^2}{2m}\left(\frac{\pi}{L}[2n-1]\right)^2 \psi_{ns}(x)$$

$$E_{ns} = \frac{\hbar^2}{2m}\frac{\pi^2}{L^2}(2n-1)^2,\ n = 1, 2, \ldots;\ \hat{H}\psi_{na}(x) = \frac{\hbar^2}{2m}\left(\frac{2\pi}{L}\right.$$

$$|\psi(x)|^2 = |\psi_0|^2 e^{-\frac{(x-x_0)^2}{2a^2}}$$



$$\int_{-\infty}^{+\infty} dx\, e^{-Ax^2} = \sqrt{\frac{\pi}{A}}$$

$$a \approx 10^{-10}\,m$$

$$\hat{H}\psi_a = -\frac{\hbar^2}{2m}\partial_x^2\psi_a(x) = \frac{\hbar^2}{2m}\frac{1}{2a^2}\psi_a(x) - \frac{\hbar^2}{2m}\frac{1}{4a^4}(x-x_0)^2\psi_a(x)$$

$$= -\frac{\hbar^2}{2m}\left(-\frac{1}{2a^2} + \left(\frac{1}{2a^2}(x-x_0)\right)^2\right) e^{-\frac{(x-x_0)^2}{4a^2}}\psi;\ V(x) = \frac{\hbar^2}{2m}\frac{1}{4a^4}(x-x_0)^2$$

$$A = \frac{1}{2a^2} \Rightarrow |\psi_0| = \frac{1}{(2\pi a^2)^{1/4}}$$

$$\hat{H} \to \hat{H} = -\frac{\hbar^2}{2m}\partial_x^2 + V(x);\ \hat{H}\psi_a = \frac{\hbar^2}{2m}\frac{1}{2a^2}\psi_a = E_a\psi_a$$

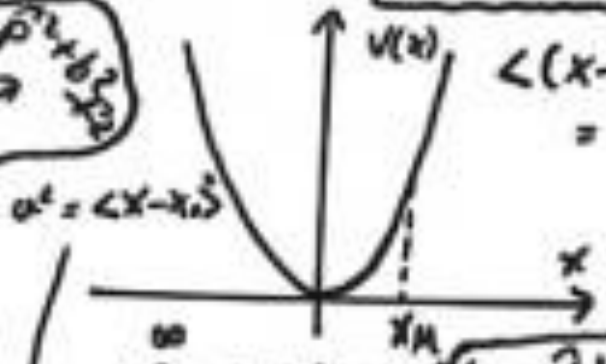
$$V(x) = \frac{1}{2}m\omega^2(x-x_0)^2 \to m\omega^2 = \frac{\hbar^2}{m4a^4} \Rightarrow \boxed{\omega = \frac{\hbar}{2ma}}$$

$$E_a = \frac{\hbar^2}{2m}\frac{1}{2a}$$

$$[\hat{p}, \hat{x}] = \frac{\hbar}{i};\ \hat{p} = \frac{\hbar}{i}\partial_x\ /\ \hat{H} = \frac{\hat{p}^2}{2m} + \frac{1}{2}m\omega^2\hat{x}^2$$

$$a^2 + b^2 = (a+ib)(a-ib);\ a, b \in \mathbb{R};\ 2\ (a\hat{p}\ ib\hat{x})(a\hat{p} - ib\hat{x}),\ a, b \in \mathbb{R}$$

$$= a^2\hat{p}^2 + iba\hat{x}\hat{p} - iab\hat{p}\hat{x} + b^2\hat{x}^2 = a^2\hat{p}^2 + b^2\hat{x}^2 - ba\hbar$$



$$\langle (x-x_0)^2 \rangle = \langle \psi_a | (x-x_0)^2 | \psi_a \rangle$$

$$\hat{H} = (a\hat{p} + ib\hat{x})(a\hat{p} - ib\hat{x}) + ba\hbar;\ a^2 = \frac{1}{2m};\ b^2 = \frac{1}{2}m\omega^2$$

$$\int_{-\infty}^{\infty} dx\, |x\rangle\langle x| = \mathbb{I}$$

$$\text{Def: } c^+ = \frac{1}{\sqrt{\hbar\omega}}(a\hat{p} + ib\hat{x});\ c^- = \frac{1}{\sqrt{\hbar\omega}}(a\hat{p} - ib\hat{x}) \Rightarrow \hat{H} = \hbar\omega c^+ c + \frac{1}{2}\hbar\omega$$

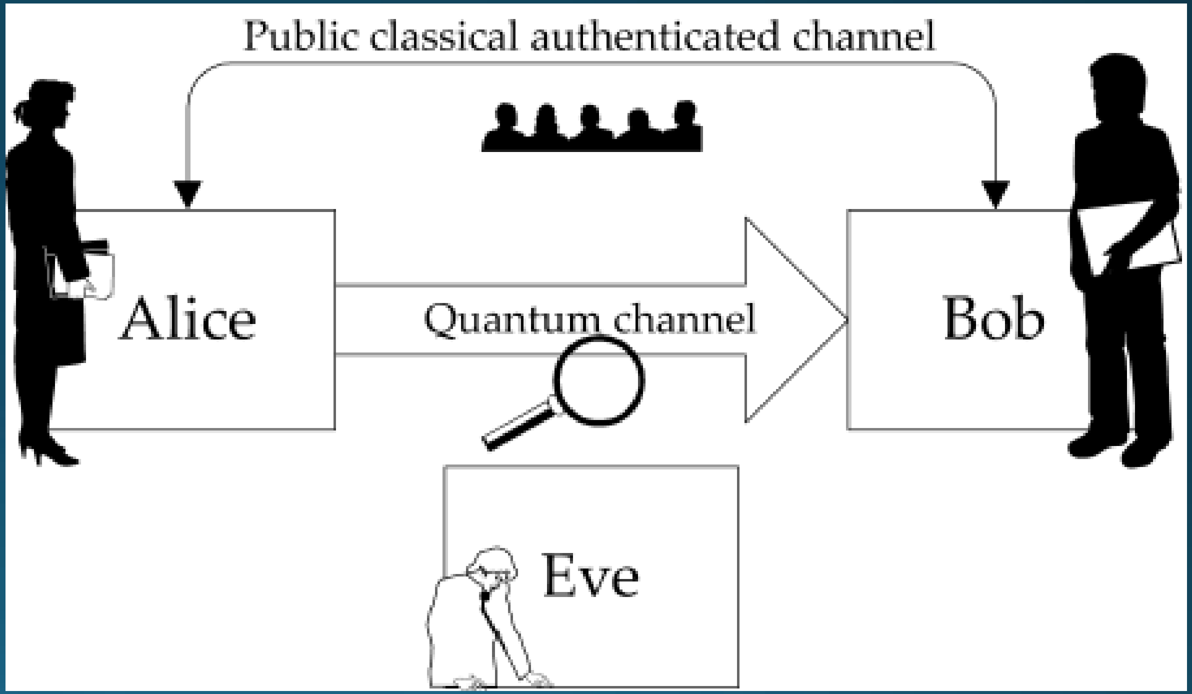
$$\psi_a^*(x)\langle \psi_a |$$

$$\hat{x}|x\rangle = x|x\rangle$$

$$= \int_{-\infty}^{\infty} dx\, \psi_n^*(x)(x-x_0)^2\psi_a(x)$$

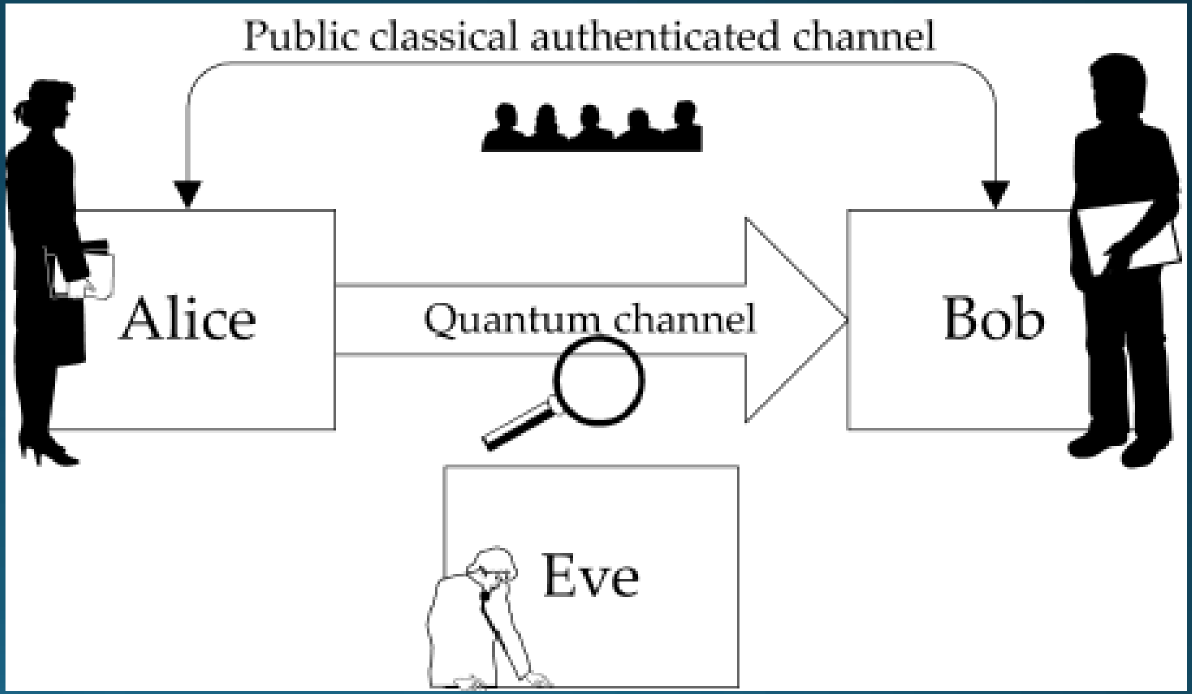
$$\left\{\left(\frac{w}{-\bar{t}}\ \frac{t}{\bar{w}}\right) \middle| w, t \in \mathbb{C}\right\}\ \{\pm 1\};\ SU(2) \cong S^3\quad A \mapsto wAw^{-1}$$

Quantum Channel



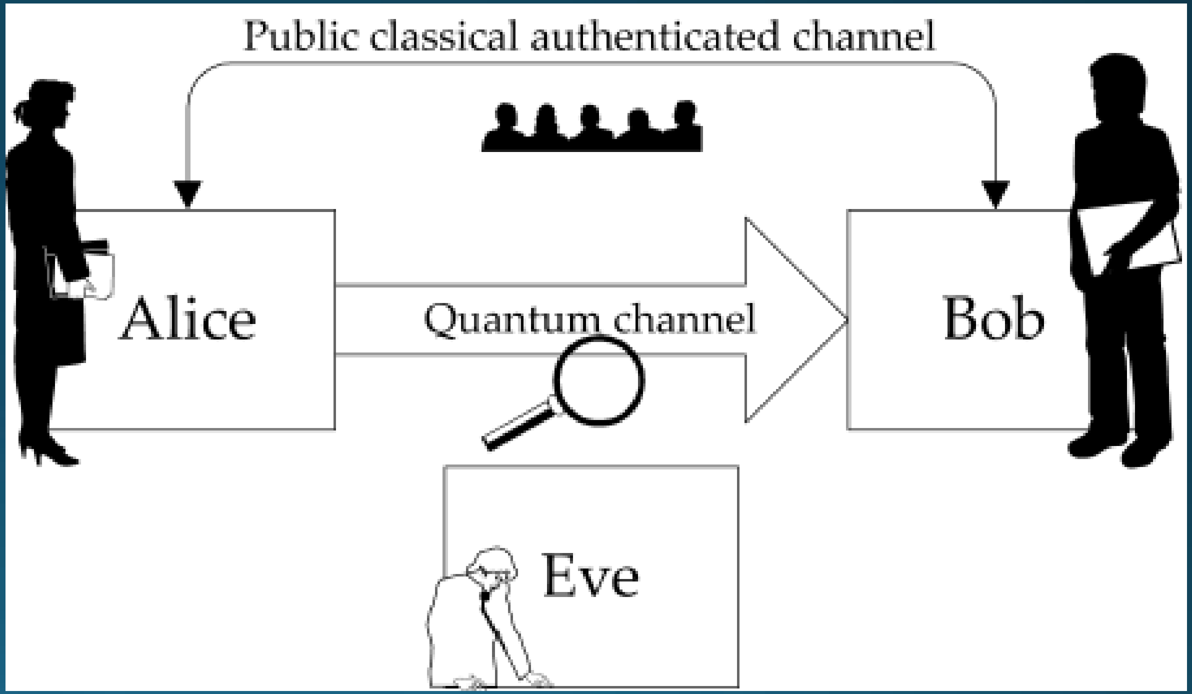
Quantum Channel

- Eve has complete control over the channel



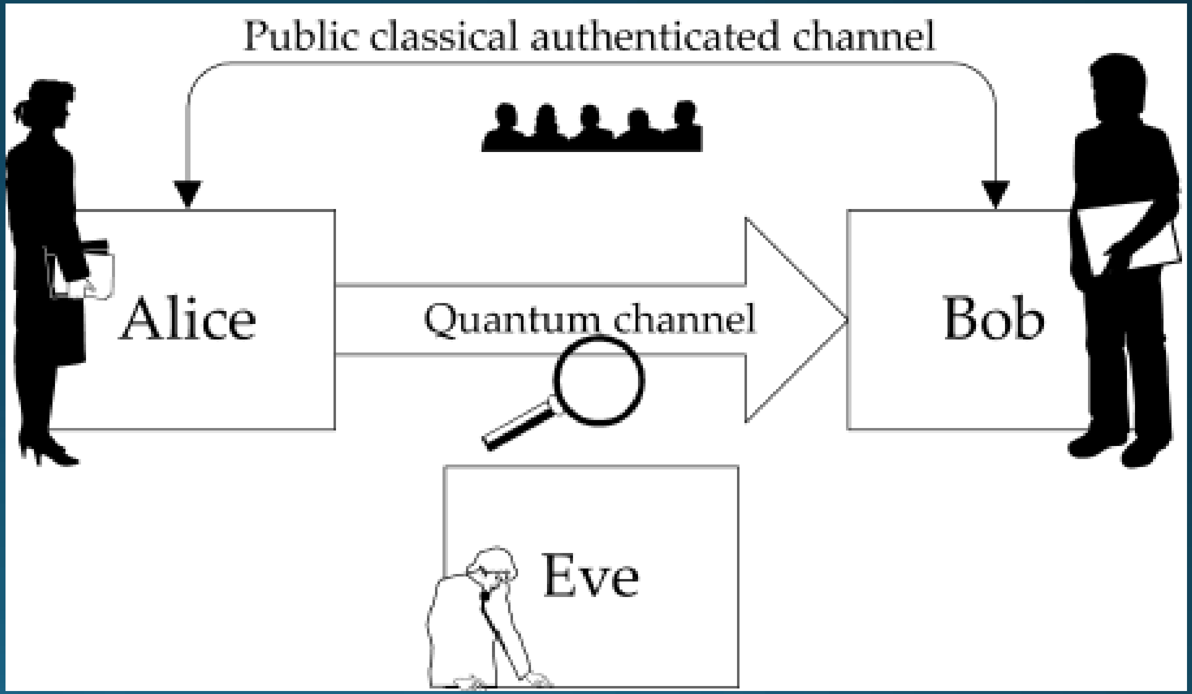
Quantum Channel

- Eve has complete control over the channel
- She can intercept or measure the sent qubits



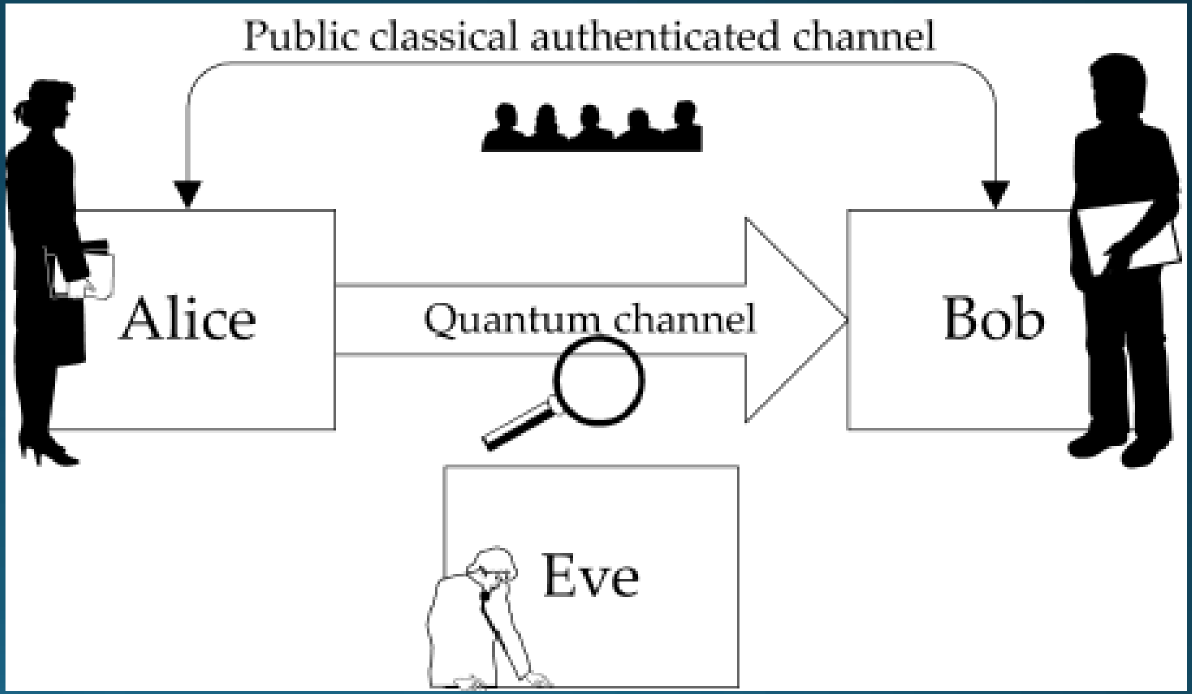
Quantum Channel

- Eve has complete control over the channel
- She can intercept or measure the sent qubits
- No cloning theorem: Forbidden to clone of an unknown quantum state (Wooters and Zurek and Dieks 1982)



Quantum Channel

- Eve has complete control over the channel
- She can intercept or measure the sent qubits
- No cloning theorem: Forbidden to clone of an unknown quantum state (Wooters and Zurek and Dieks 1982)
- Eve can block the channel by sending random qubits and prevent communication over the channel



Quantum Key Distribution

- Alice and Bob use the public quantum channel to agree on a private secure key
- Eve has no information about the key
- Having a private key they can use any other classical encryption scheme to communicate through the public classical channel
- If they use OTP they can communicate with perfect secrecy!

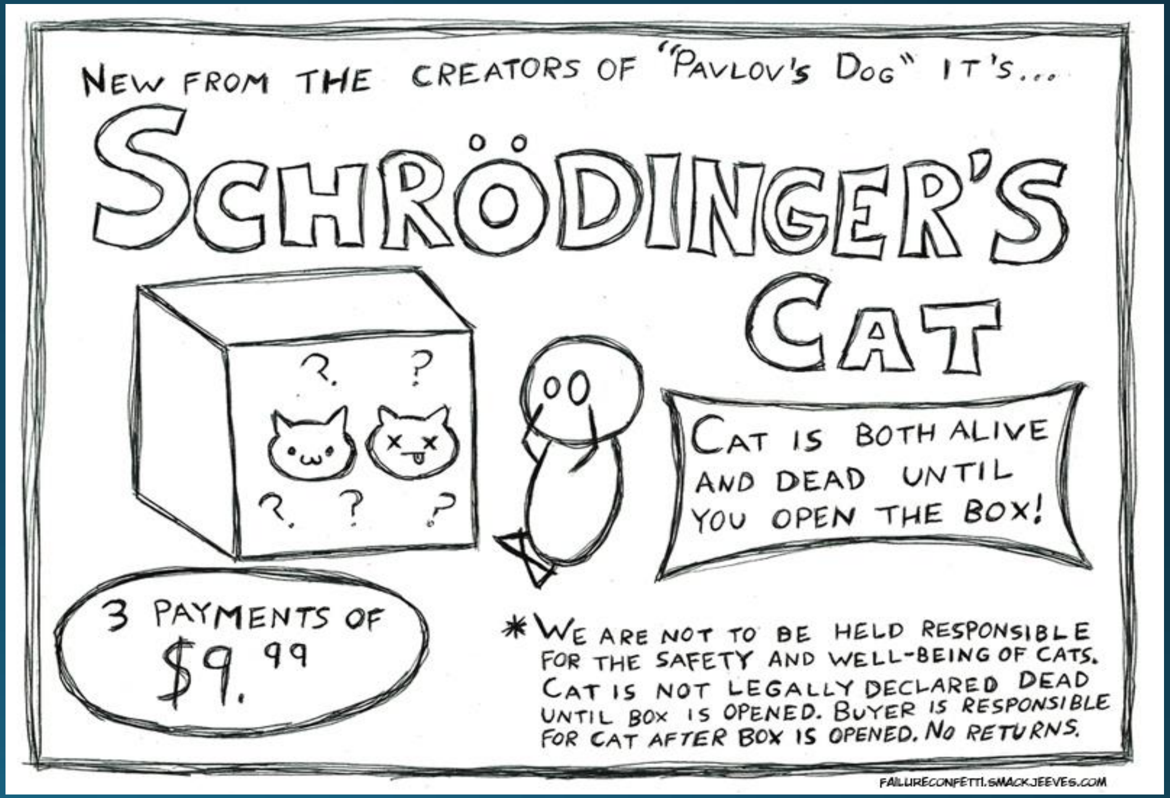
Quantum Bits (qubits)

Quantum Bits (qubits)

- Two-state quantum-mechanical system

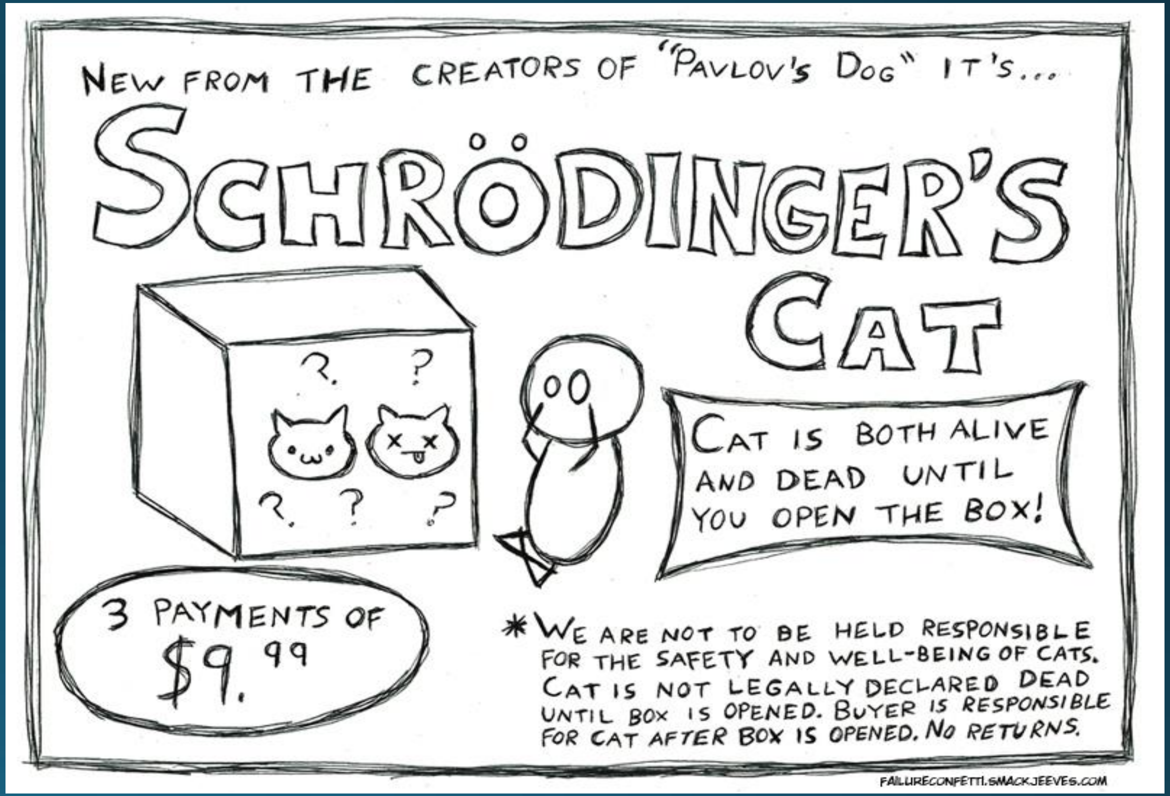
Quantum Bits (qubits)

- Two-state quantum-mechanical system



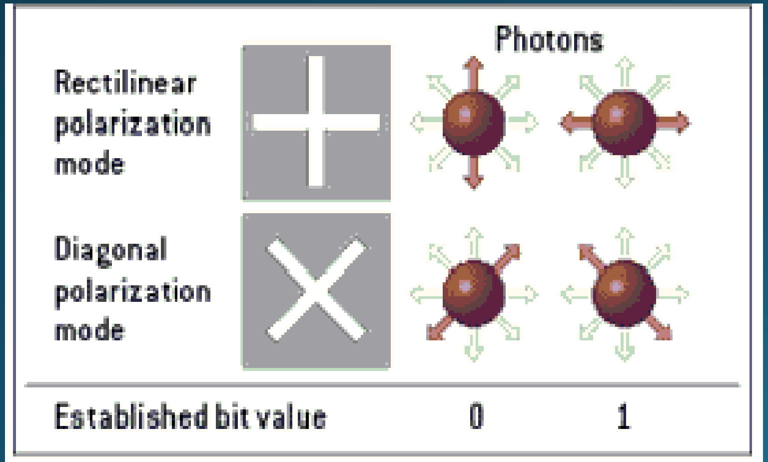
Quantum Bits (qubits)

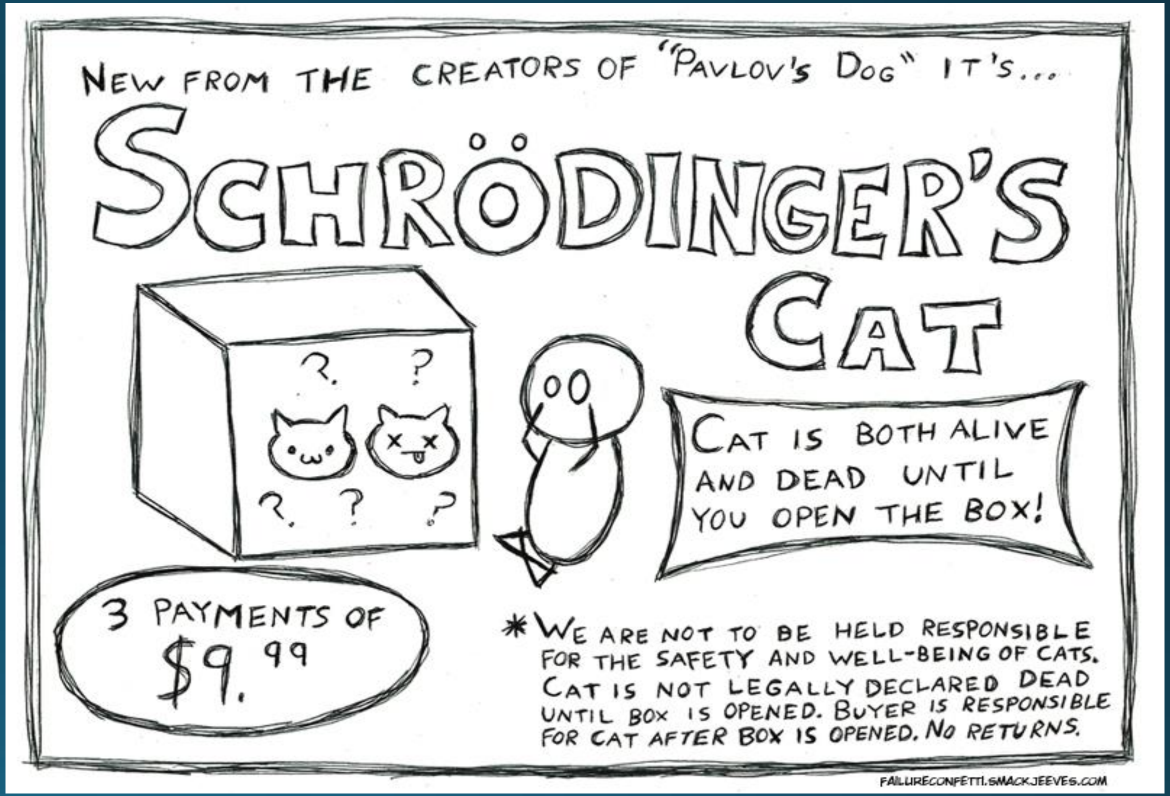
- Two-state quantum-mechanical system
- Polarisation of photon
  - rectilinear / diagonal polarization



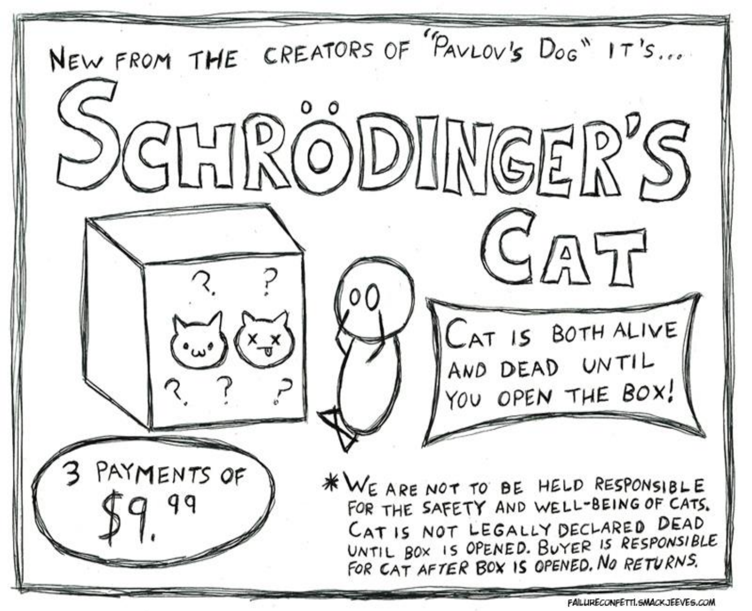
Quantum Bits (qubits)

- Two-state quantum-mechanical system
- Polarisation of photon
  - rectilinear / diagonal polarization



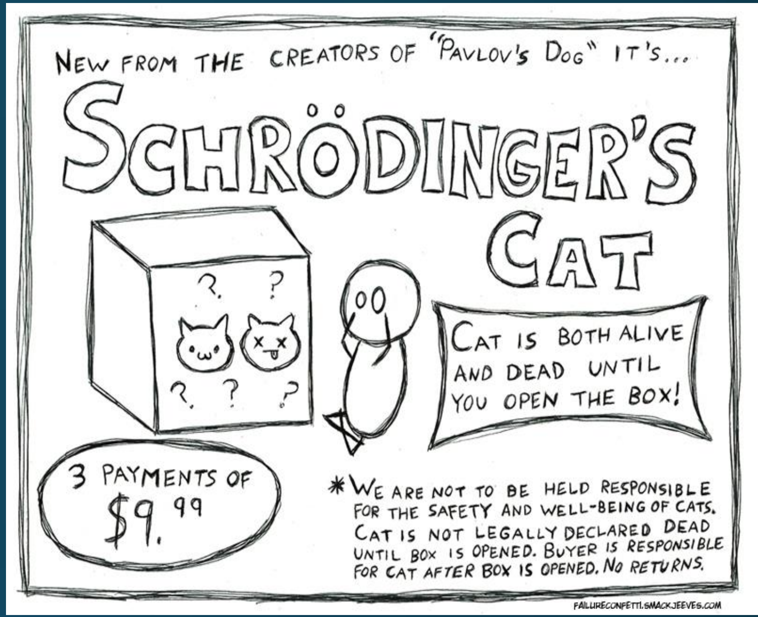


Measuring Qubits



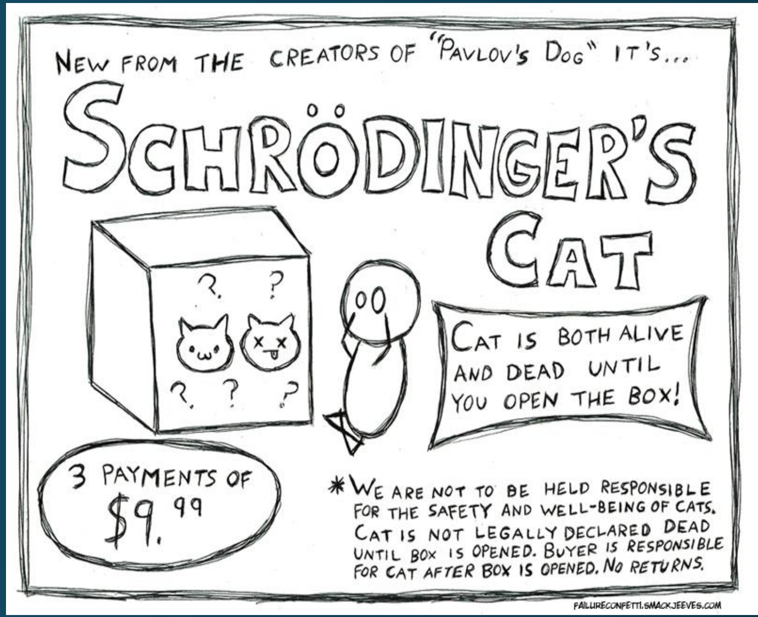
Measuring Qubits

- Measuring a qubit:
  - opening the box



Measuring Qubits

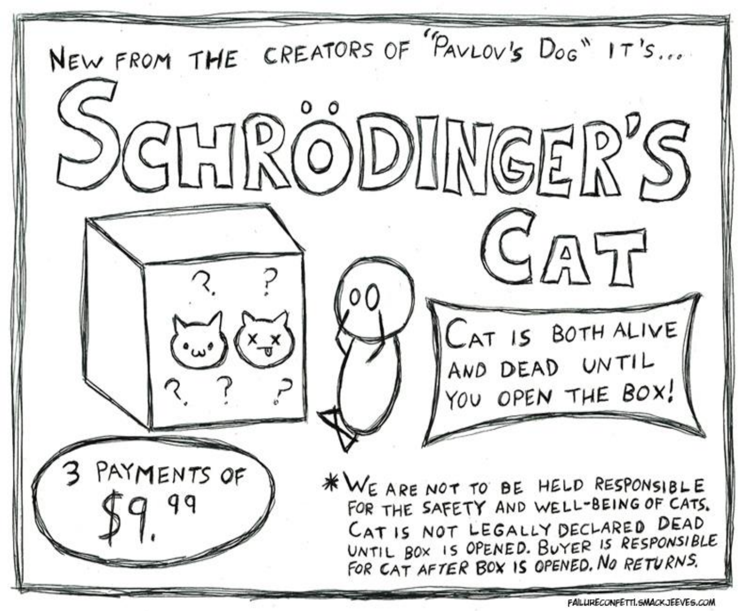
- Measuring a qubit:
  - opening the box



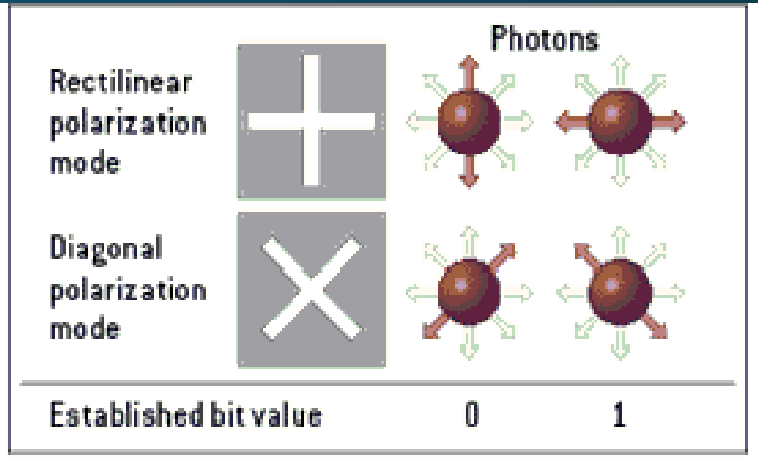
- Collapses the wavefunction to one of the two states:
  - The cat is DEAD or ALIVE

Measuring Qubits

- Measuring a qubit:
  - opening the box

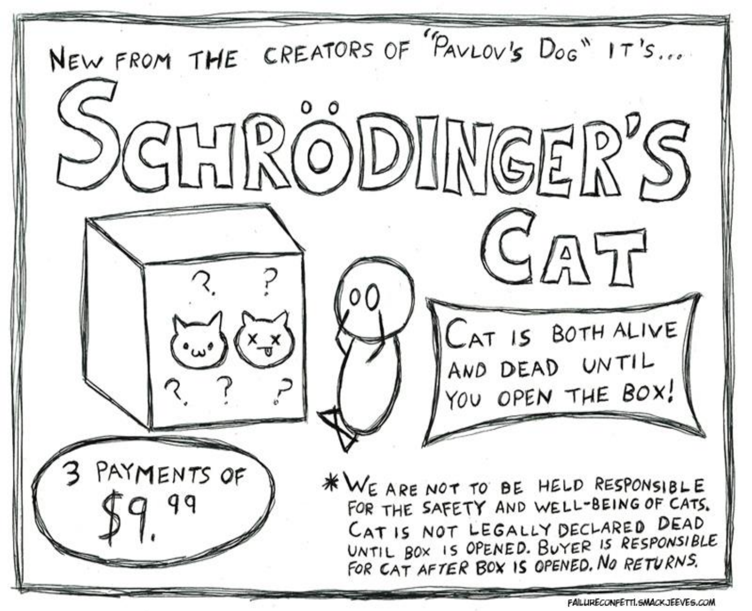


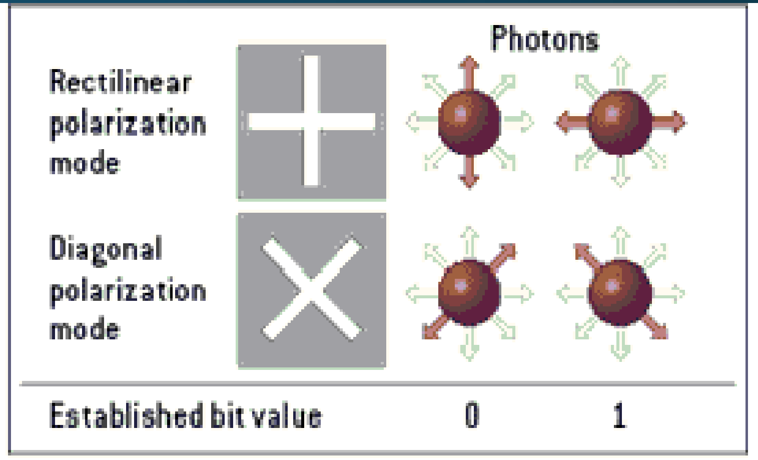
- Collapses the wavefunction to one of the two states:
  - The cat is DEAD or ALIVE



Measuring Qubits

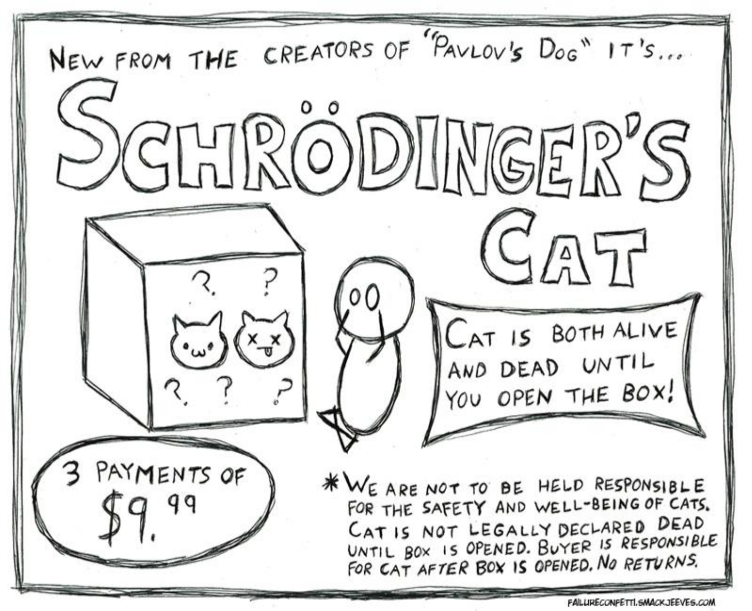
- Measuring a qubit:
  - opening the box
  - filter the photon through one of the modes
- Collapses the wavefunction to one of the two states:
  - The cat is DEAD or ALIVE

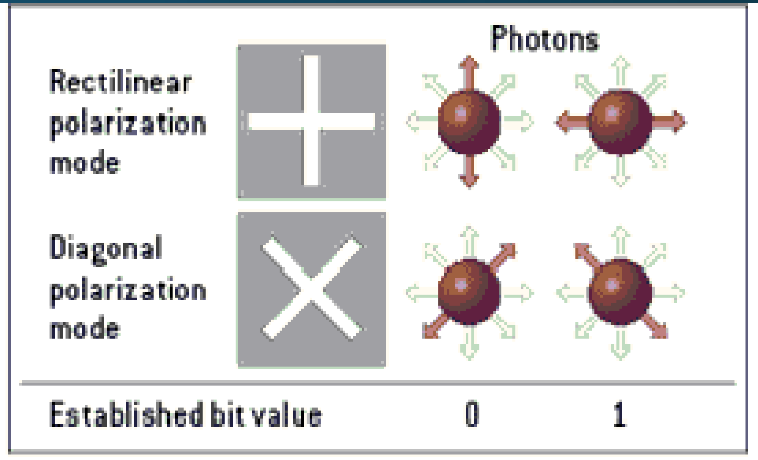




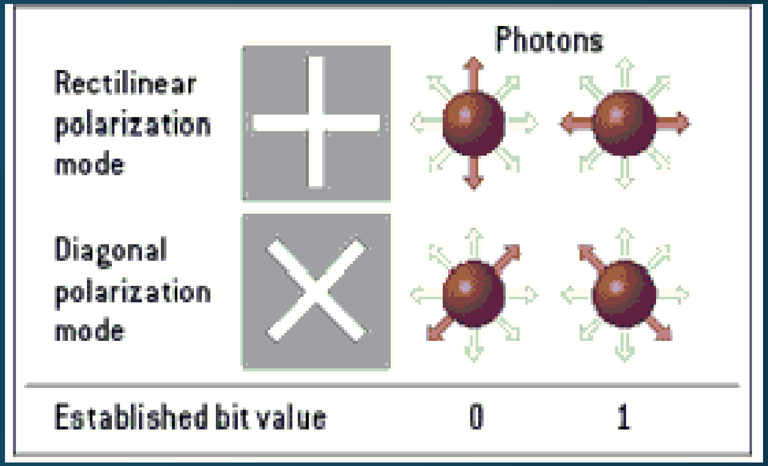
Measuring Qubits

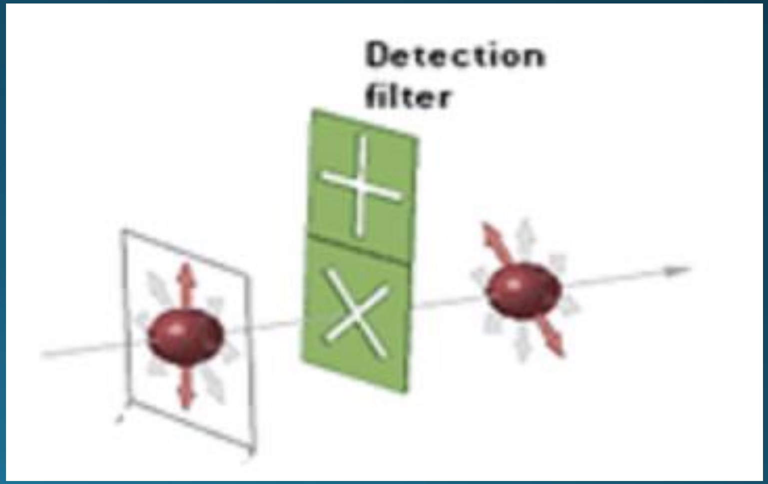
- Measuring a qubit:
  - opening the box
  - filter the photon through one of the modes
- Collapses the wavefunction to one of the two states:
  - The cat is DEAD or ALIVE
  - The polarization is VERTICAL or HORIZONTAL
  - The bit is 0 or 1





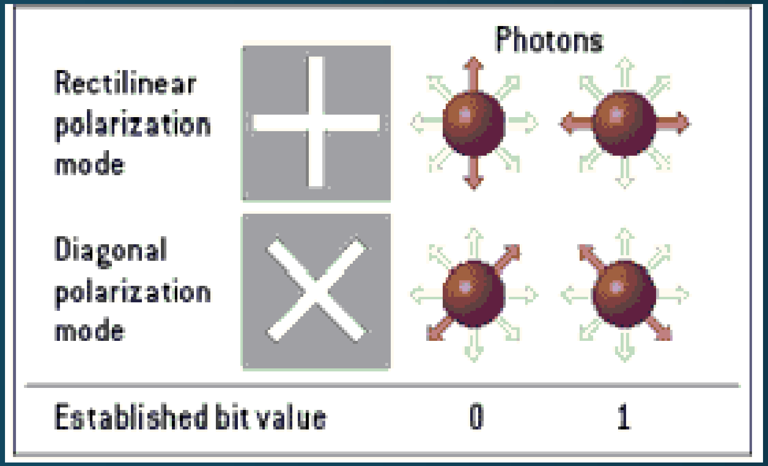
Measuring Qubits

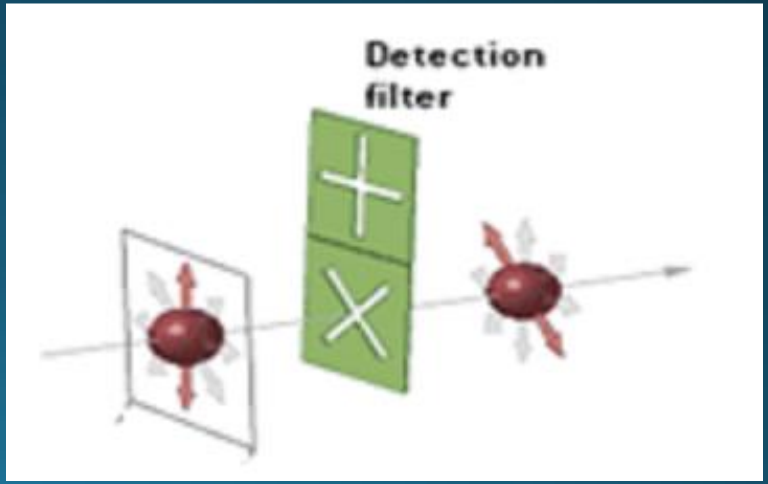




Measuring Qubits

1. Measuring the qubit in the "wrong basis"

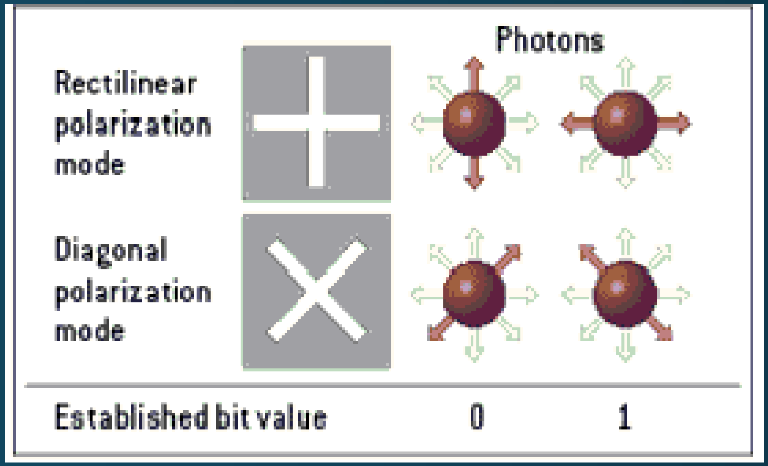


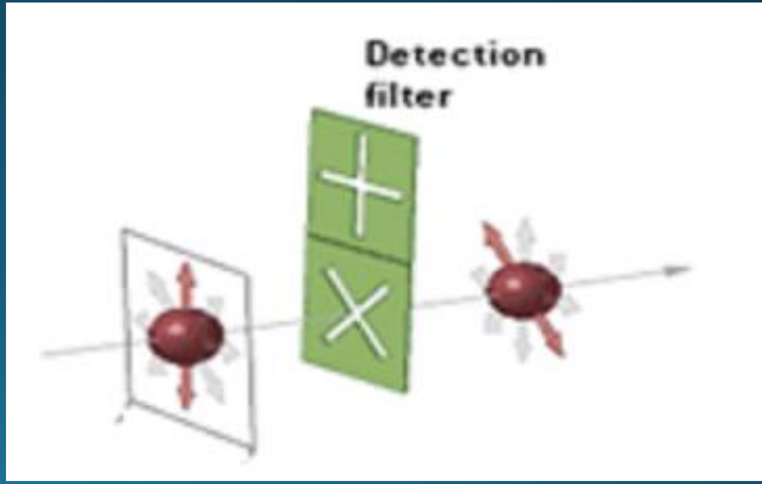


Measuring Qubits

1. Measuring the qubit in the "wrong basis"

2. No information gain! (we get 0 or 1 with P=0.5)



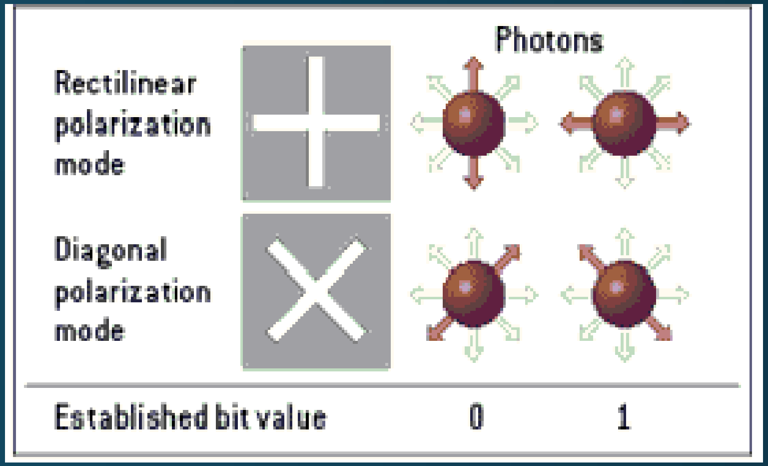


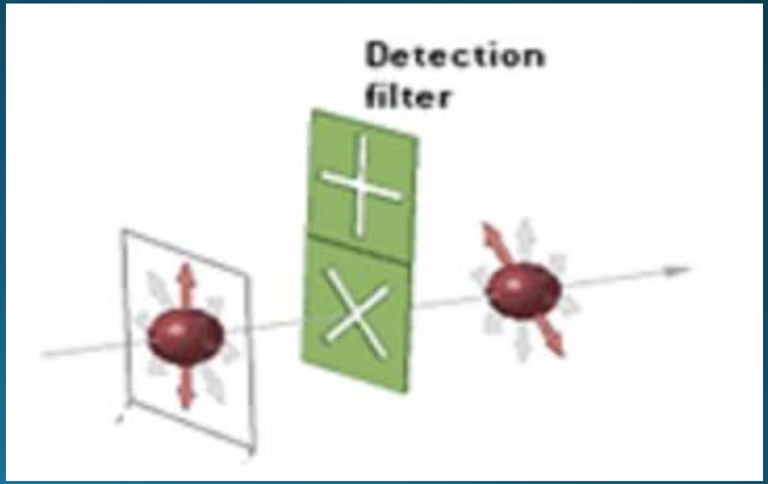
Measuring Qubits

1. Measuring the qubit in the "wrong basis"

2. No information gain! (we get 0 or 1 with P=0.5)

3. It changes the state to one of the states corresponding to the new basis

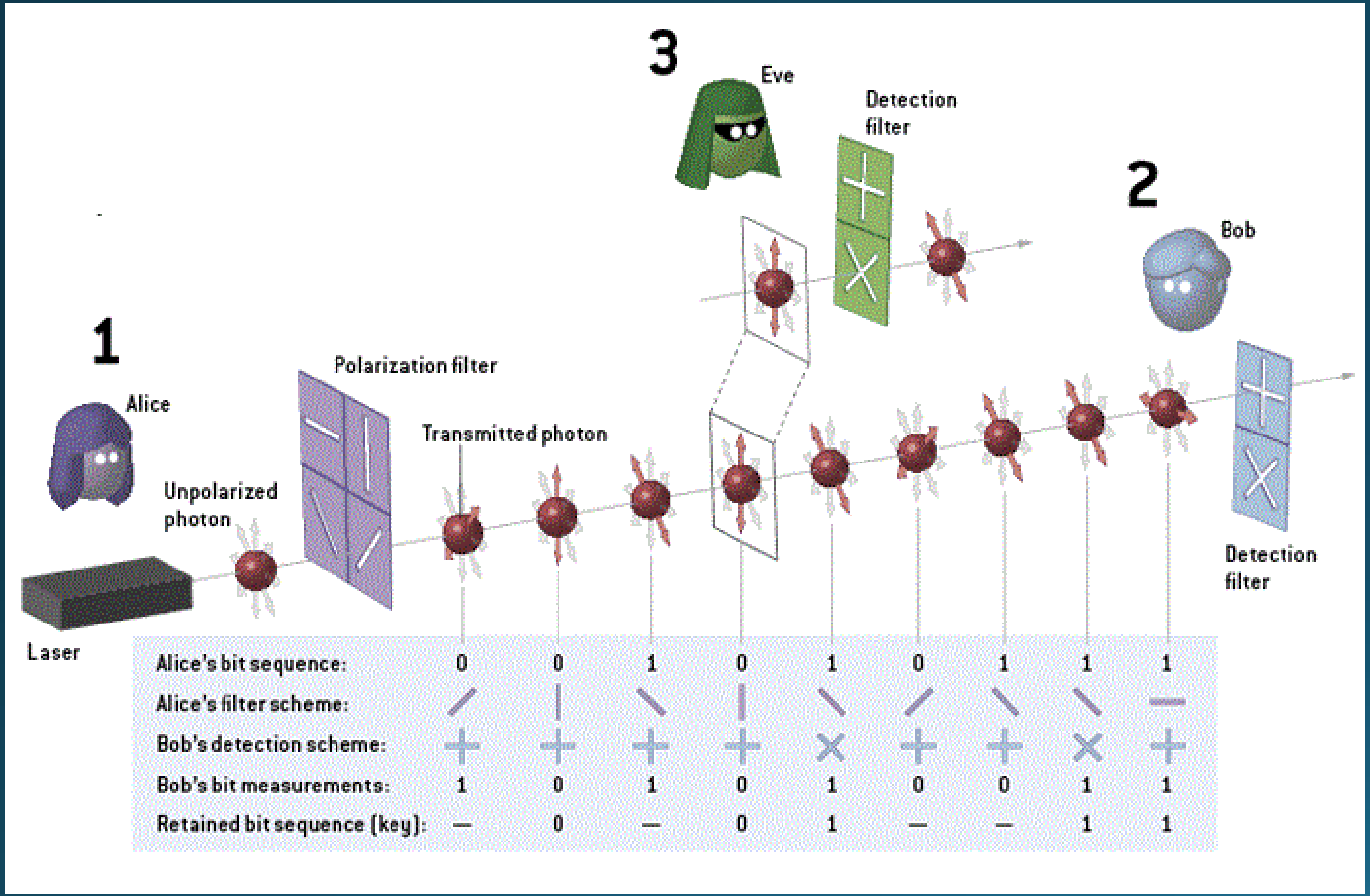




BB84 QKD Scheme

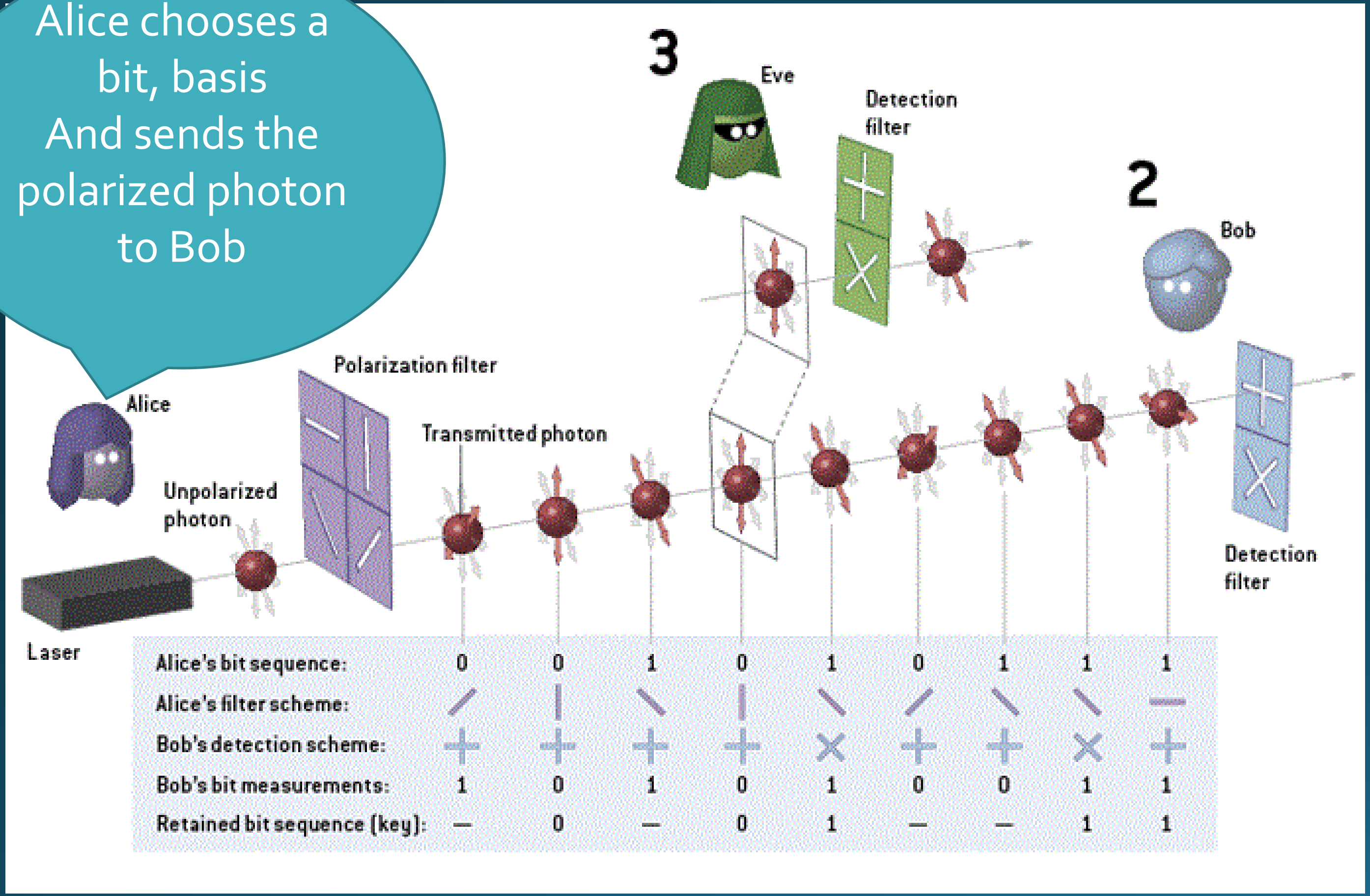
1. Alice chooses a random bit (0,1) and basis (+ or X)
2. She sends the qubit to Bob with the appropriate polarization
3. Bob measures the qubit with a random basis
4. Alice and Bob compare the string of bases they used and only keep those bits where they used the same basis
5. Error estimation and correction
6. Privacy amplification

BB84 QKD in Action



BB84 QKD in Action

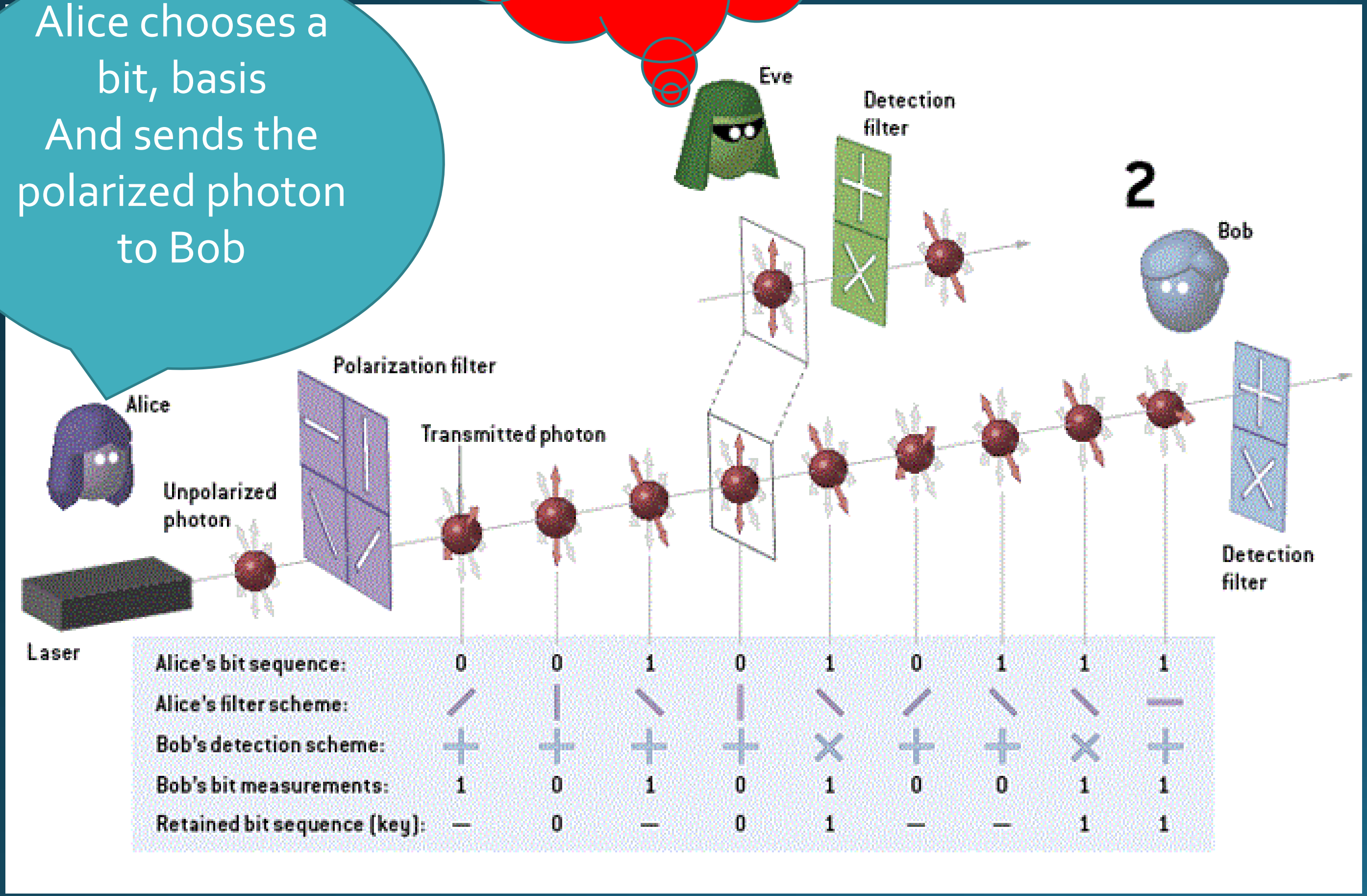
Alice chooses a bit, basis
And sends the polarized photon to Bob



BB84 Q… ction

Knows
some bits!!

Alice chooses a bit, basis
And sends the polarized photon to Bob

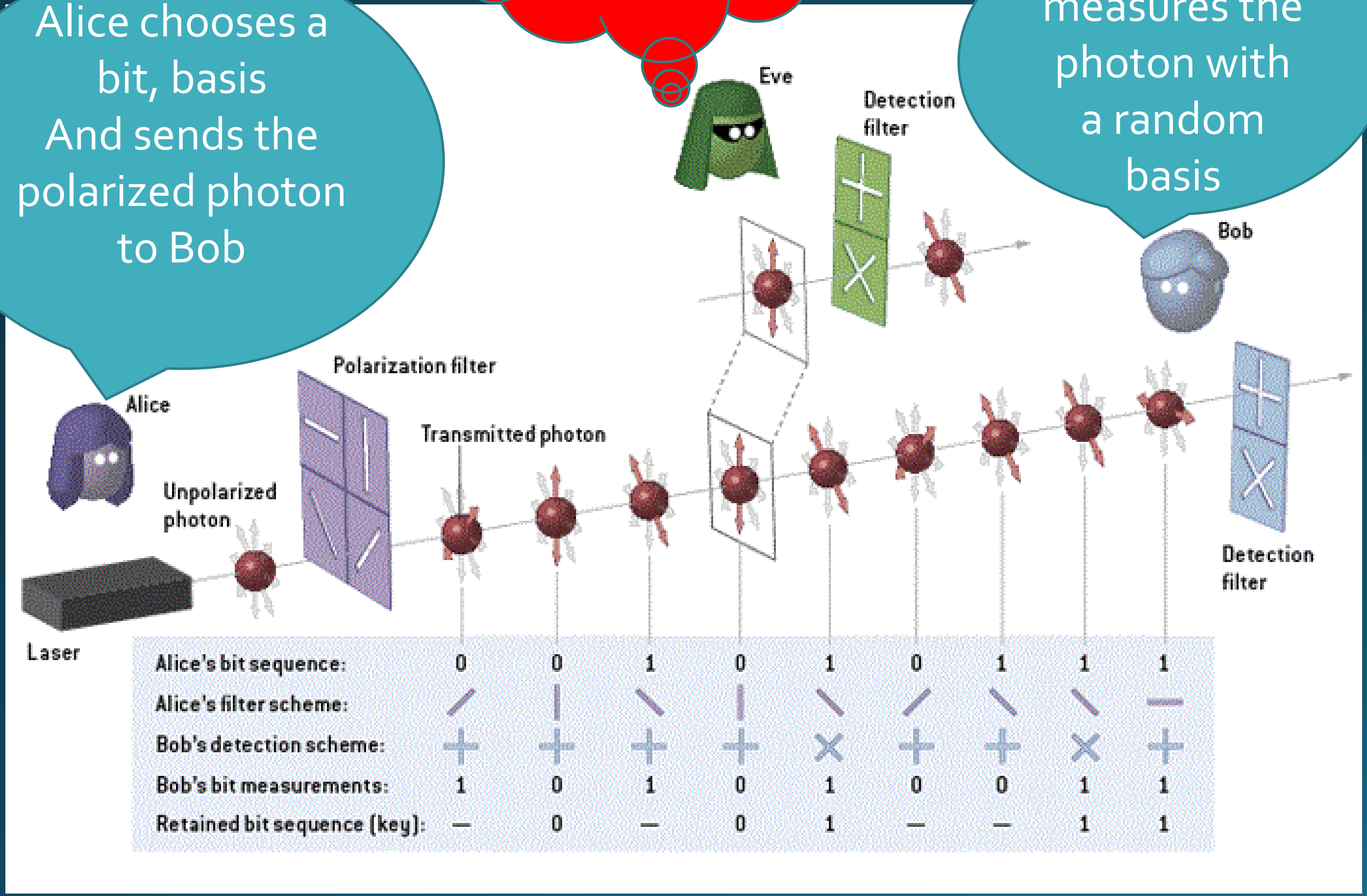


BB84 Q… Action

Knows some bits!!

Alice chooses a bit, basis
And sends the polarized photon to Bob

Bob measures the photon with a random basis

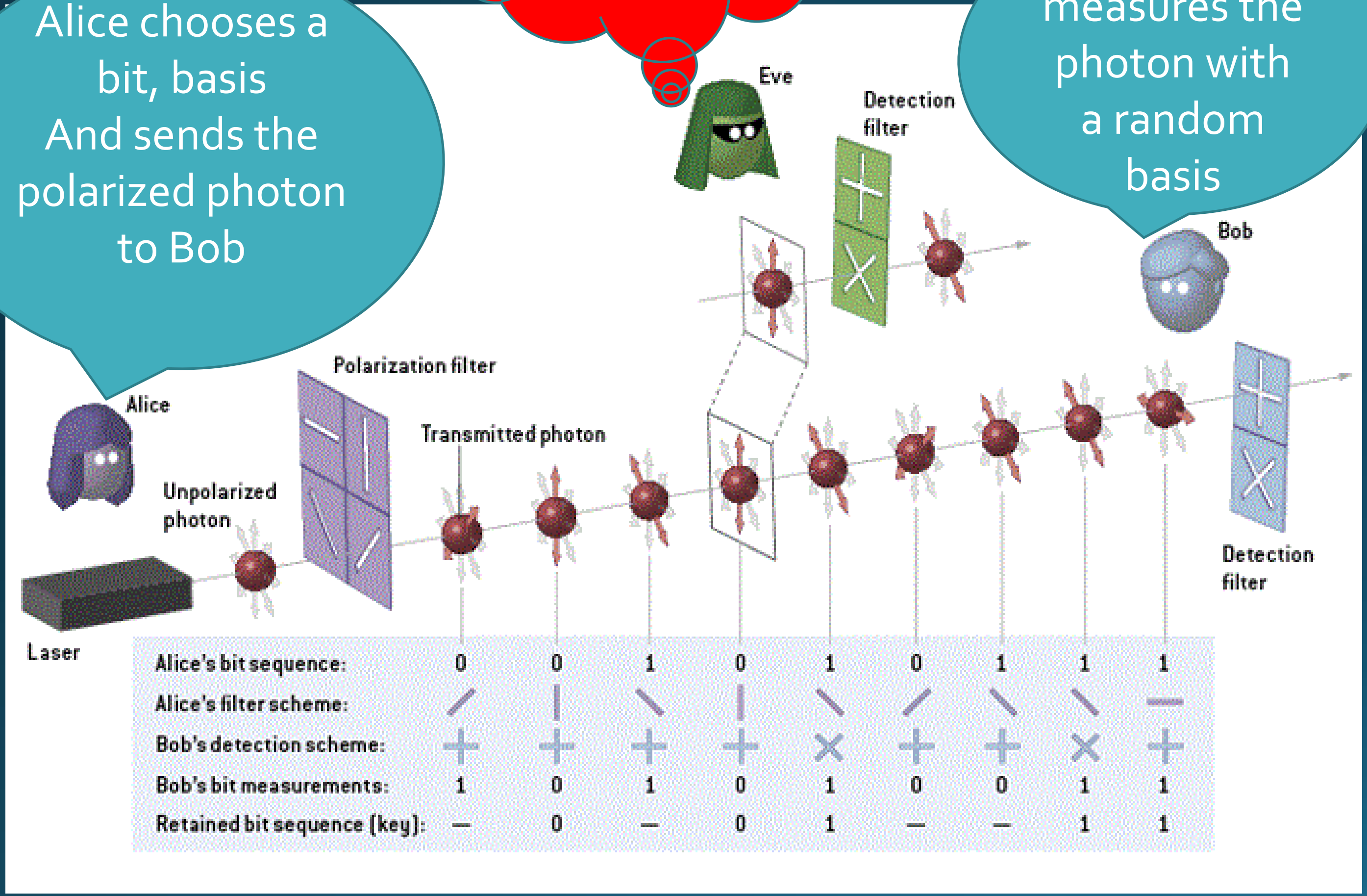


BB84 Q … Action

Alice chooses a bit, basis
And sends the polarized photon to Bob

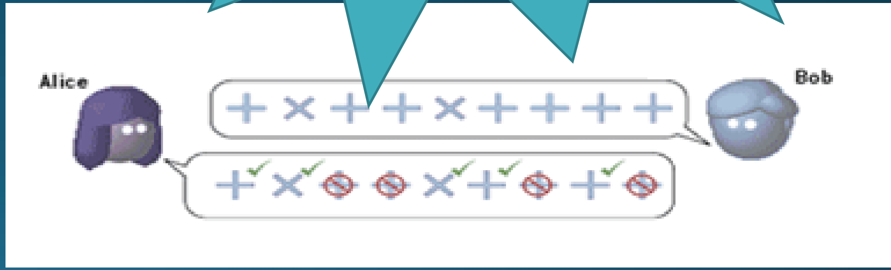
Knows some bits!!

Bob measures the photon with a random basis



Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	—	0	—	0	1	—	—	1	1

-Confirm bases used
-Error estimation
-Privacy Amplification

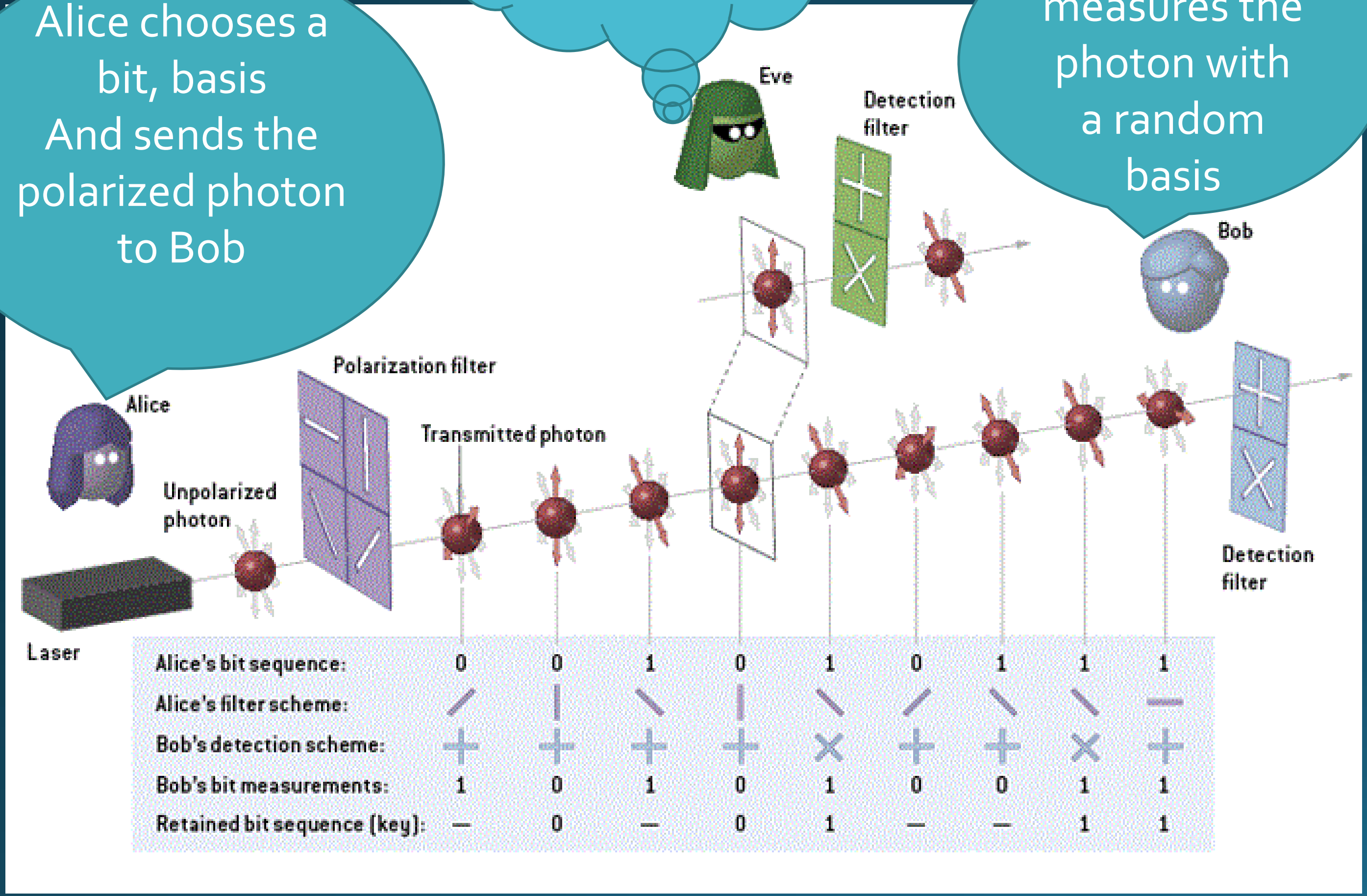


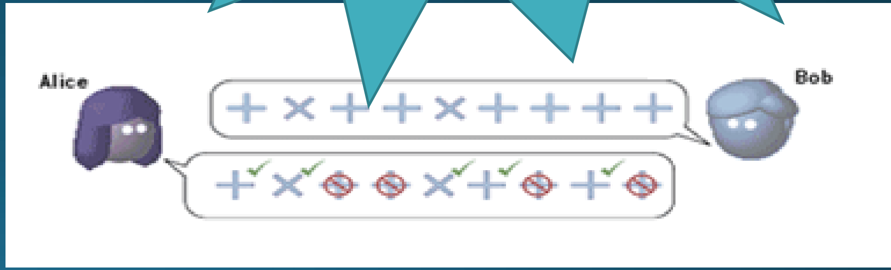
BB84 Q ??? ction

Alice chooses a bit, basis
And sends the polarized photon to Bob

Bob measures the photon with a random basis

-Confirm bases used
-Error estimation
-Privacy Amplification



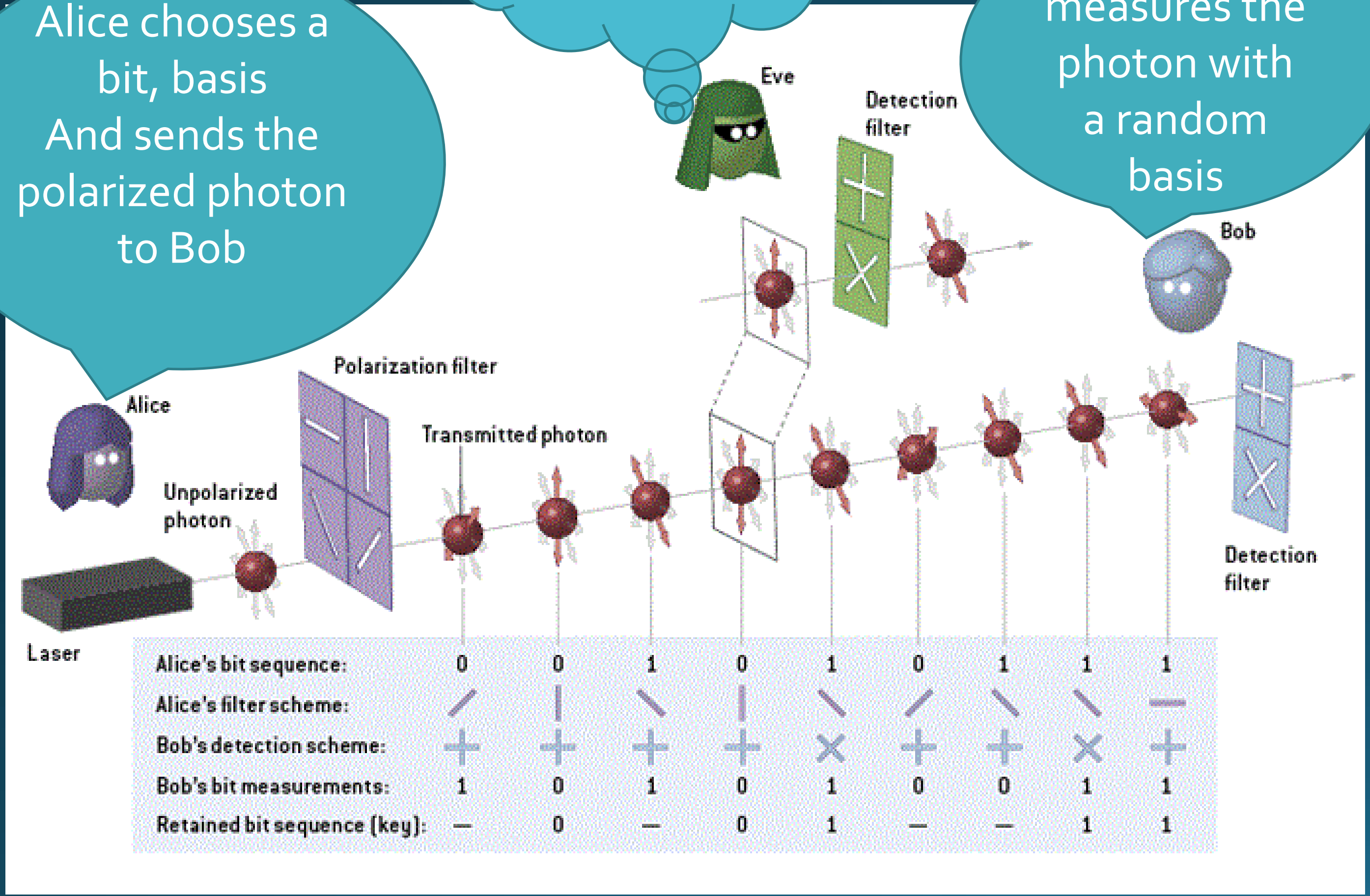


BB84 Q ction

???

Alice chooses a bit, basis
And sends the polarized photon to Bob

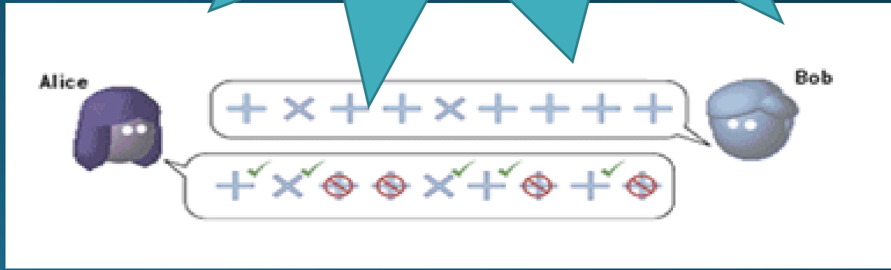
Bob measures the photon with a random basis



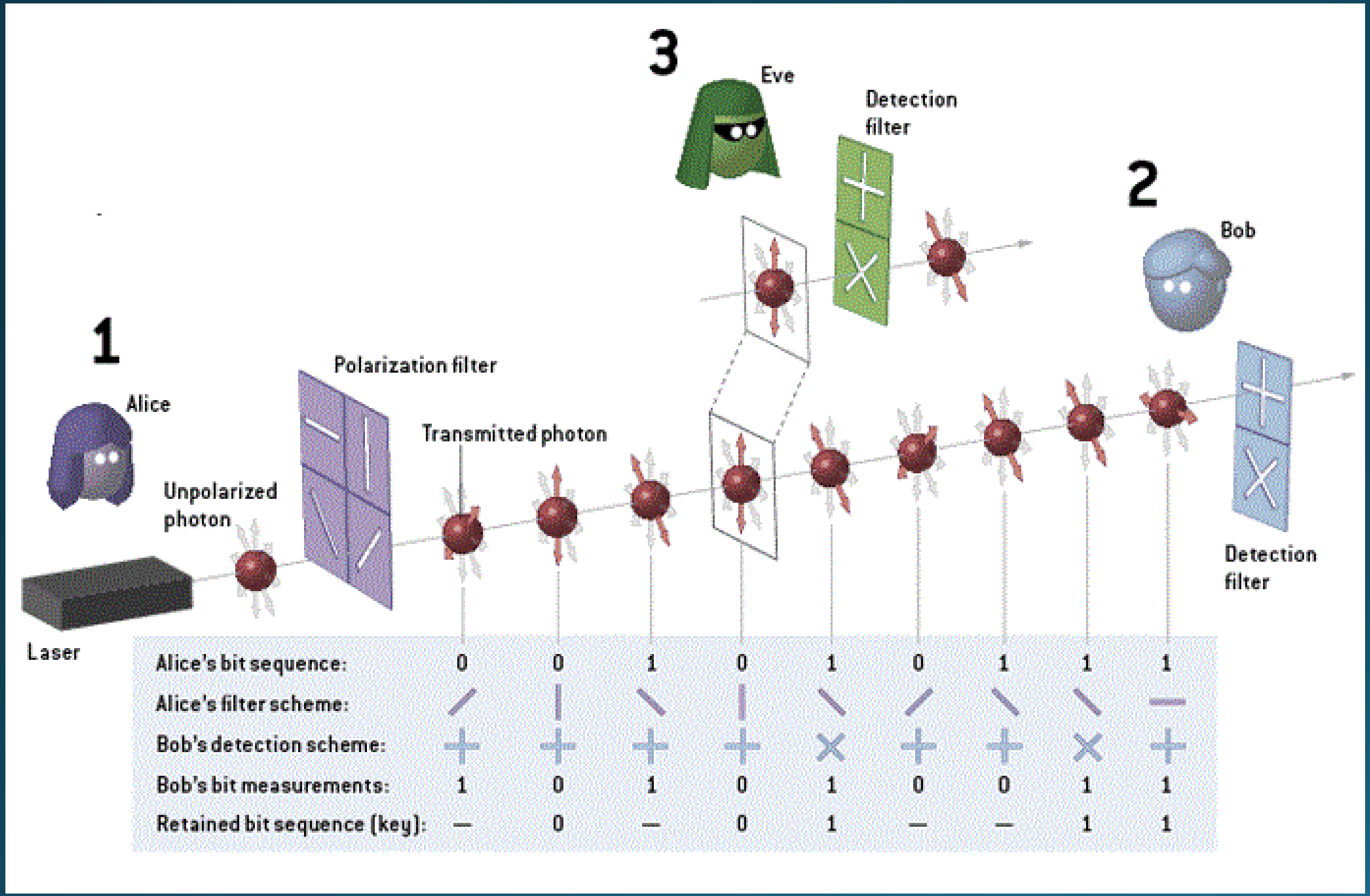
Alice's bit sequence:	0	0	1	0	1	0	1	1	1
Alice's filter scheme:	/	|	\	|	\	/	\	\	—
Bob's detection scheme:	+	+	+	+	×	+	+	×	+
Bob's bit measurements:	1	0	1	0	1	0	0	1	1
Retained bit sequence (key):	—	0	—	0	1	—	—	1	1

This scheme can be proven to be perfectly secure!

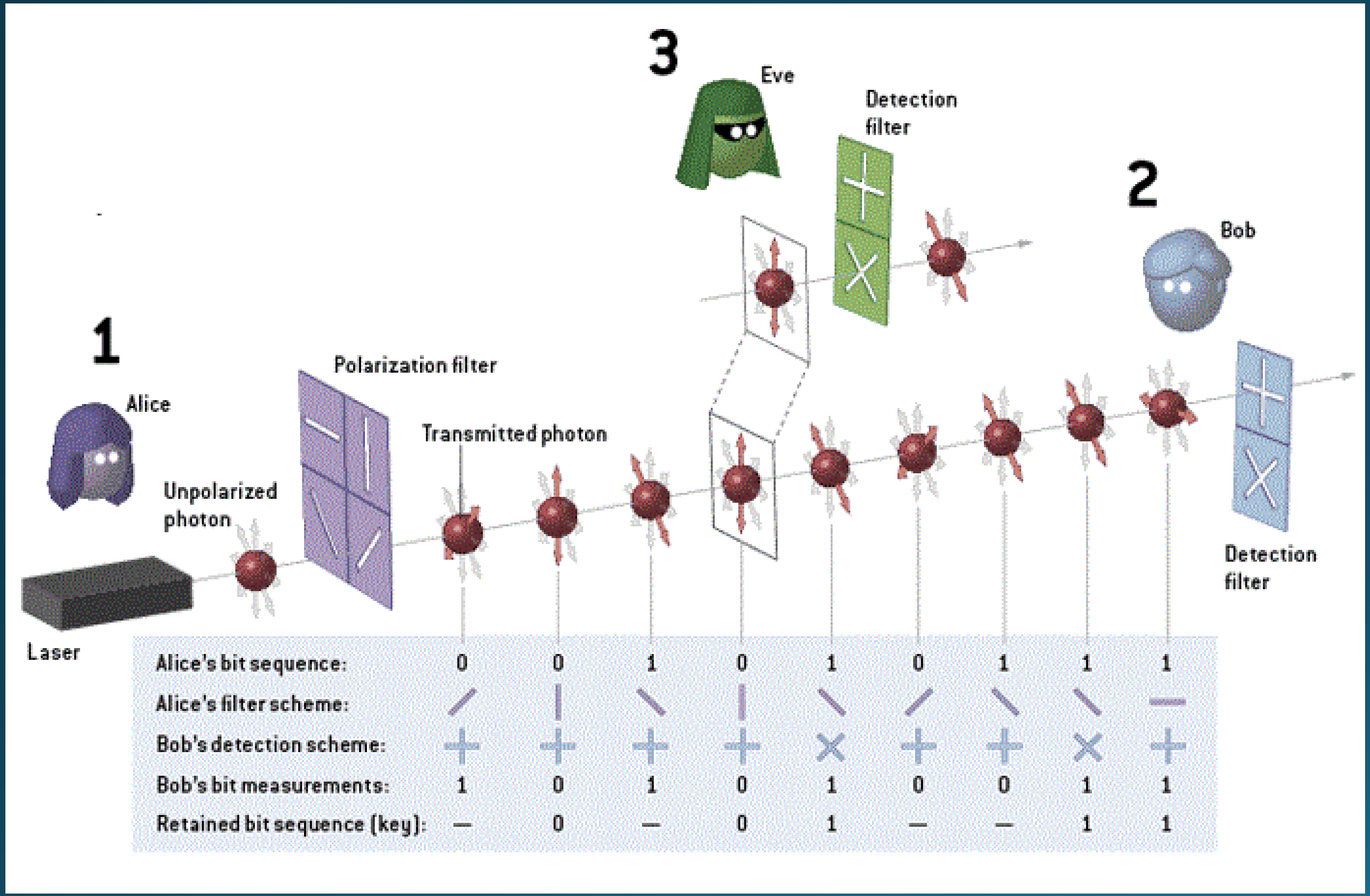
-Confirm bases used
-Error estimation
-Privacy Amplification



Detecting an eavesdropper

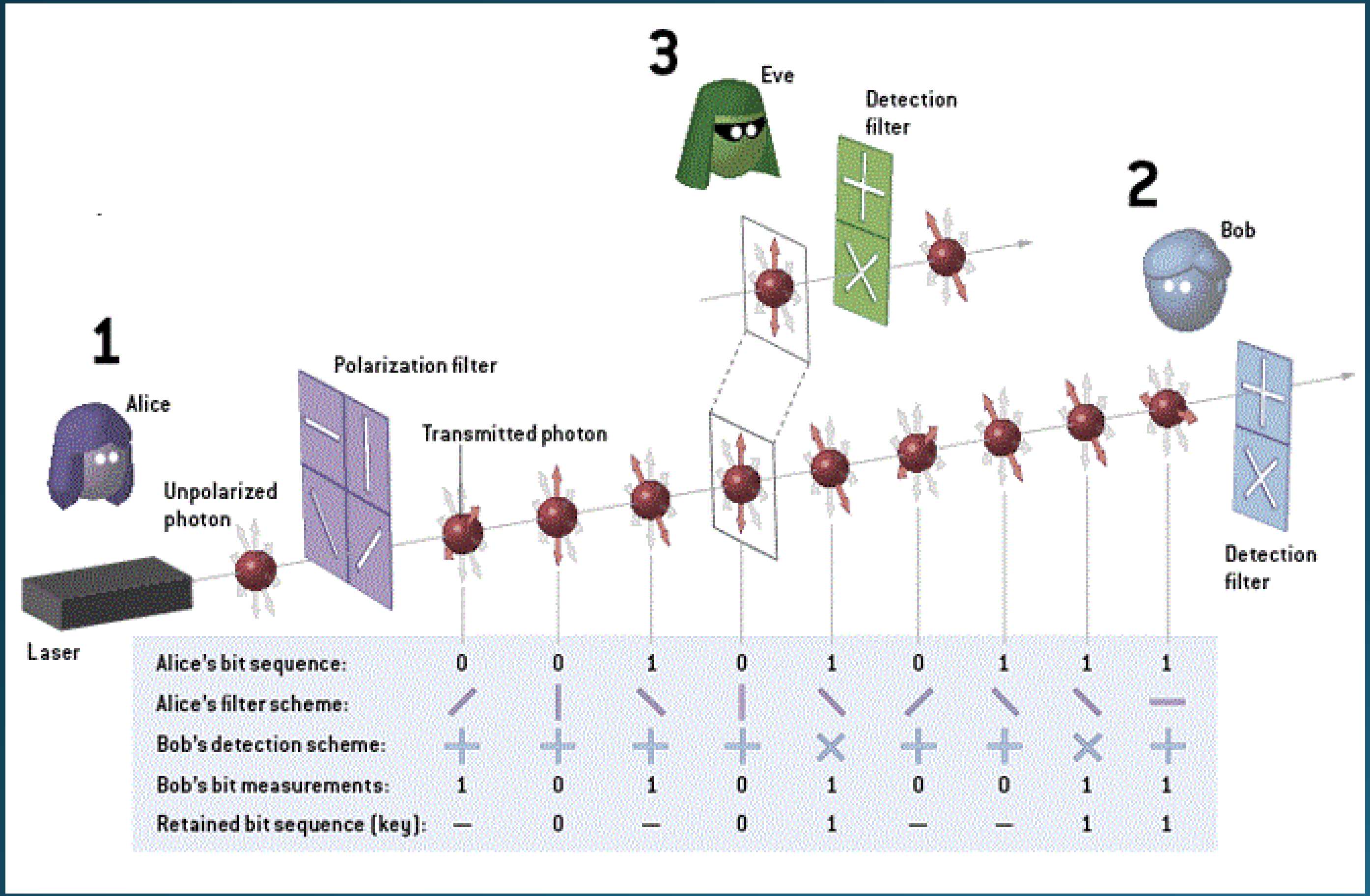


Detecting an eavesdropper



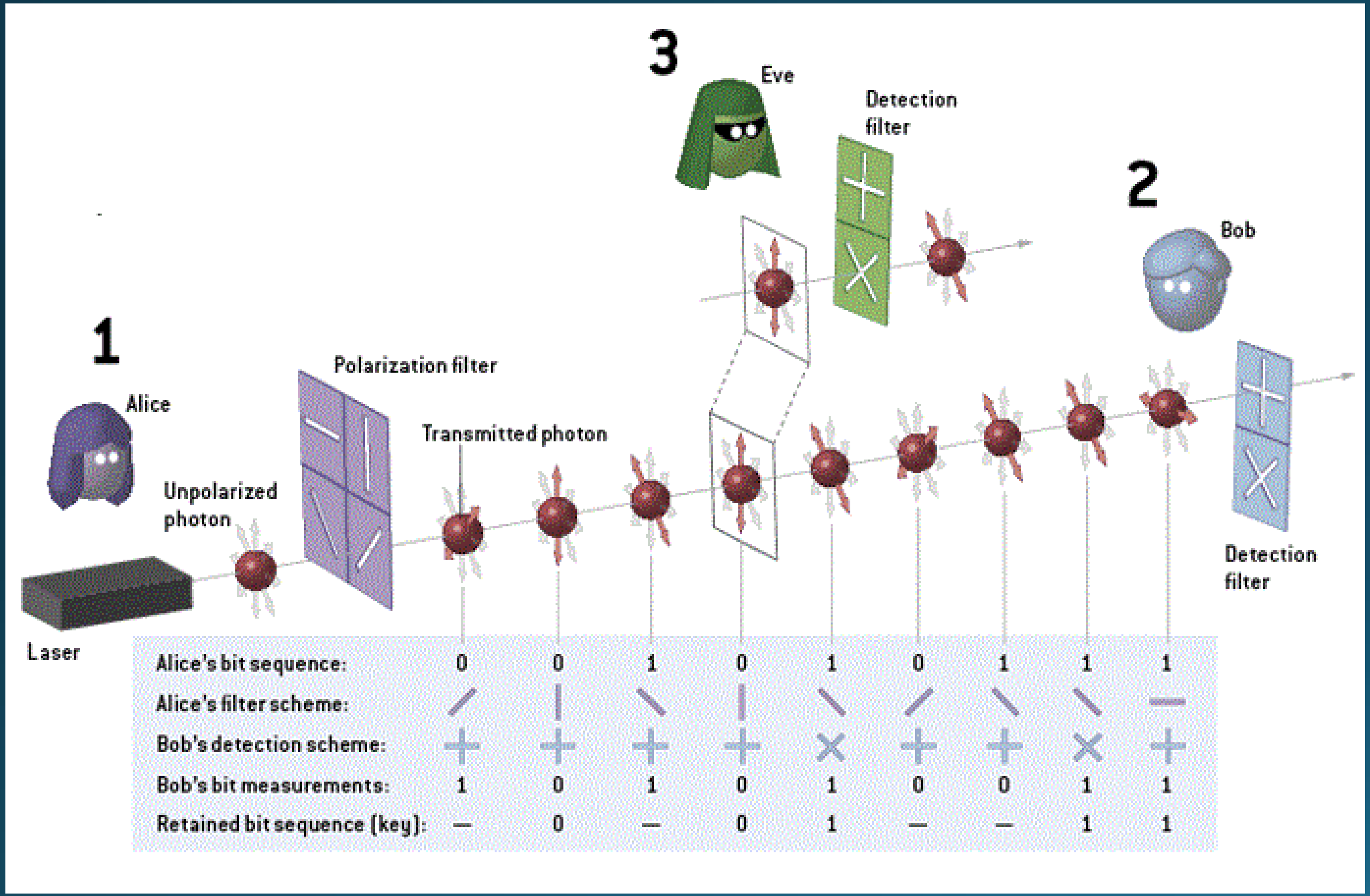
- If Eve measures a state in the wrong basis she will change the state of the photon

Detecting an eavesdropper



- If Eve measures a state in the wrong basis she will change the state of the photon
- This might introduce errors that can be detected by Alice and Bob

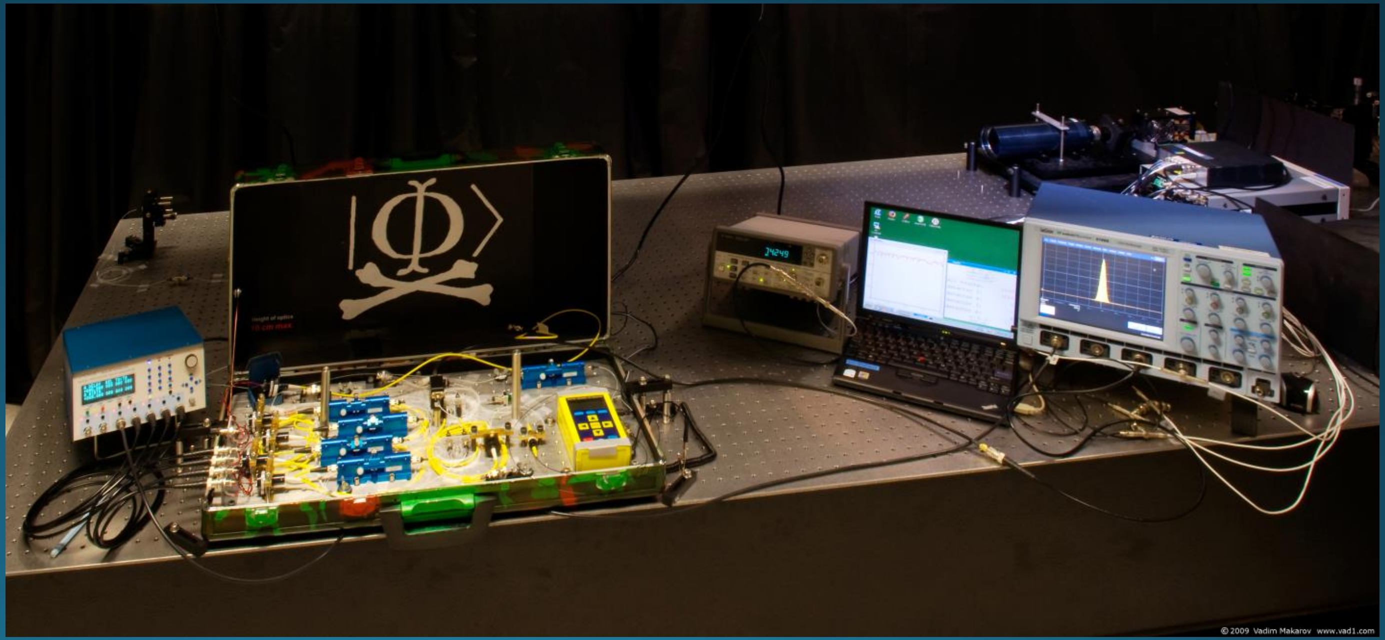
Detecting an eavesdropper



- If Eve measures a state in the wrong basis she will change the state of the photon
- This might introduce errors that can be detected by Alice and Bob
- If too many errors are detected they know that there was an eavesdropper and abort

Applications

- Commercial QKD systems already exist
- 2007 Voting in Geneva [5]
- Approximately 4 commercial companies
- and 5 Quantum Key Distribution Networks



Too good to be true?

- Distances: ~200km using optic fiber
  and much less through free space (air)
- Expensive equipment
- Imperfect implementations, at least two successful attacks

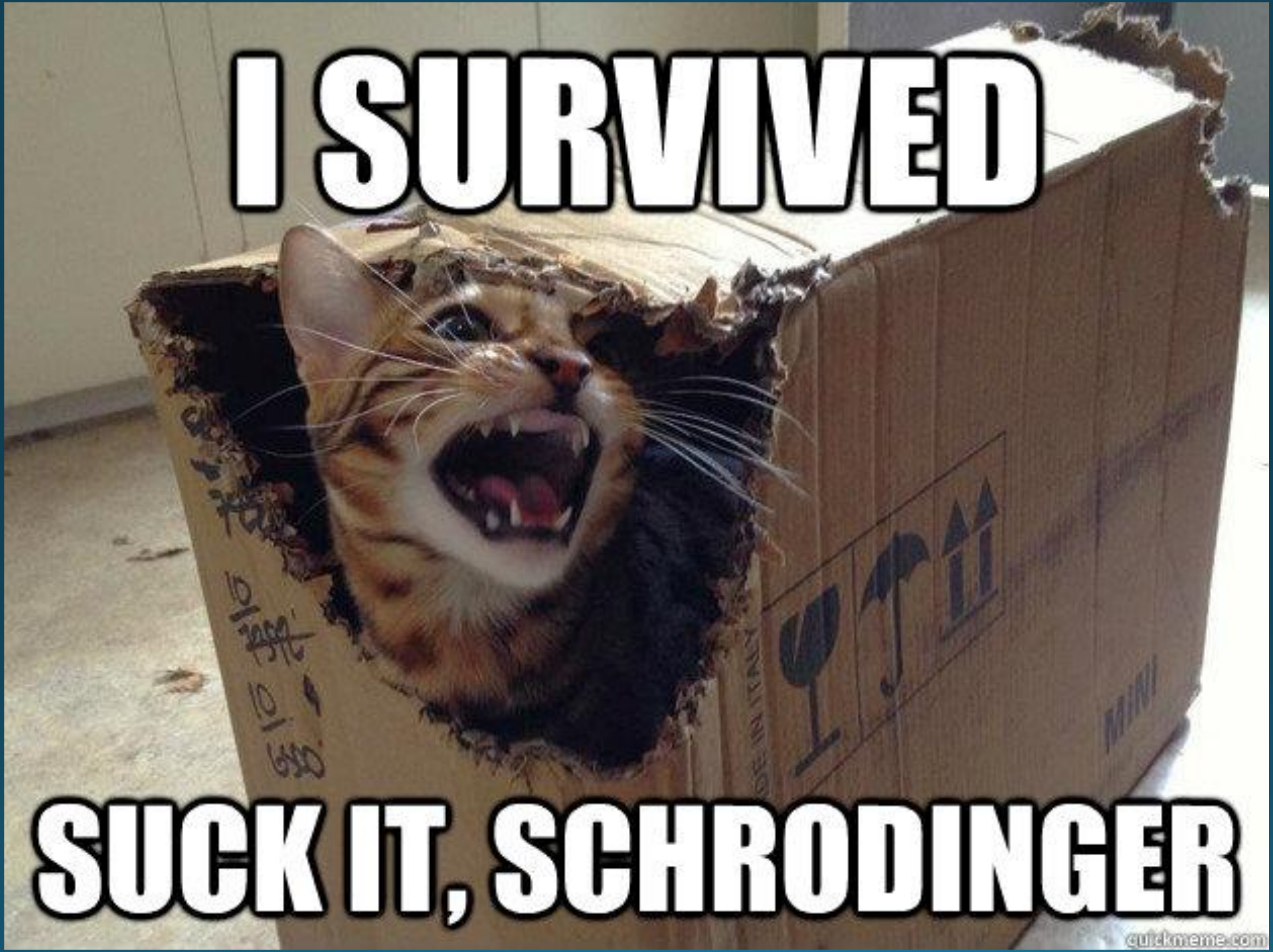
Conclusions

- Quantum Cryptography only relies on laws of nature
- Post-quantum cryptography relies on primitive that are difficult for quantum and classical computers
- Quantum Key Distribution allows two parties to share a key using a public quantum channel
- QKD schemes are perfectly secure, possible and work in practice

  although the implementation of them so far is not perfect

References

1. **Quantum Cryptography**, S Fehr, Foundations of Physics 2010
2. **Quantum Computing**, Lecture Notes, R de Wolf (Ch. 5)
3. **Quantum Cryptography: Public Key Distribution and Coin Tossing**, Bennett and Brassard 1984
4. **Assumptions in Quantum Cryptography**, NJ Beaudry, PhD Thesis, ETHZ 2014
5. **Quantum protocols for anonymous voting and surveying,** JA Vaccaro,J Spring, A Chefles, Physical Review A 75, 012333 2007
6. http://www.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election.html#.VEoePxbcBkA


I SURVIVED
SUCK IT, SCHRODINGER