COMP232:

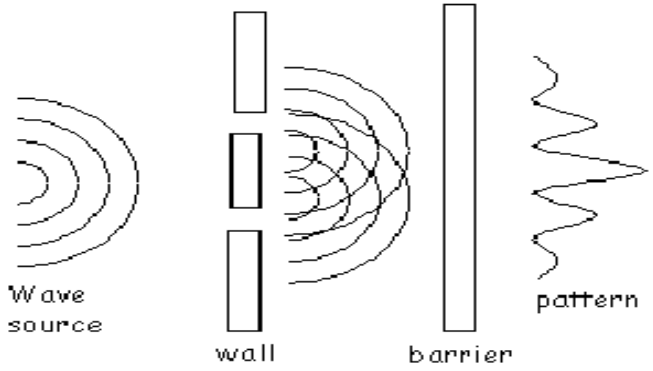
Quantum cryptography & quantum computing

Plan

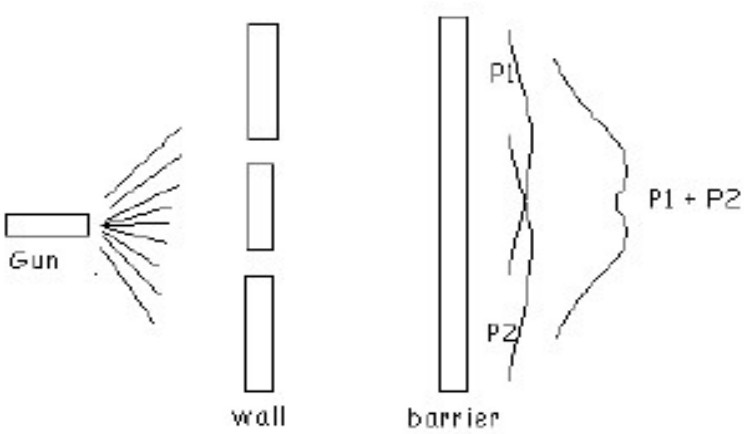
- *For thousands of years, code-makers and code-breakers have been competing for supremacy. Their arsenals may soon include a powerful new weapon: quantum mechanics.*
- *Daniel Gottesman and Hoi-Kwong Lo (2001)*

- Quantum cryptography;
- Quantum computing and cryptanalysis;

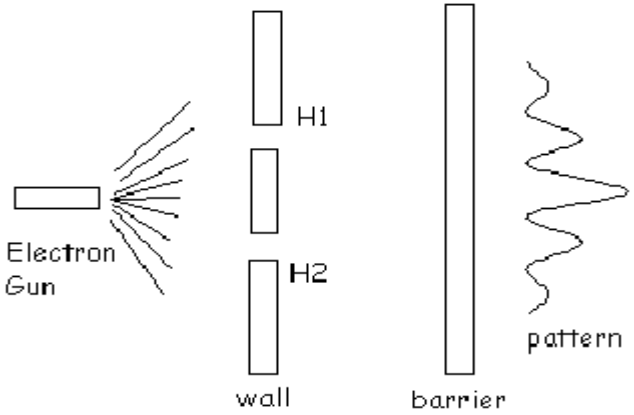
Waves or particles?



Light



Paintballs



Electrons

QM:

- particles may be in a "superposition" of several states at the same time;
- electron may be in a combination of state "at H1" and "at H2";
- when measured we always get a definite state

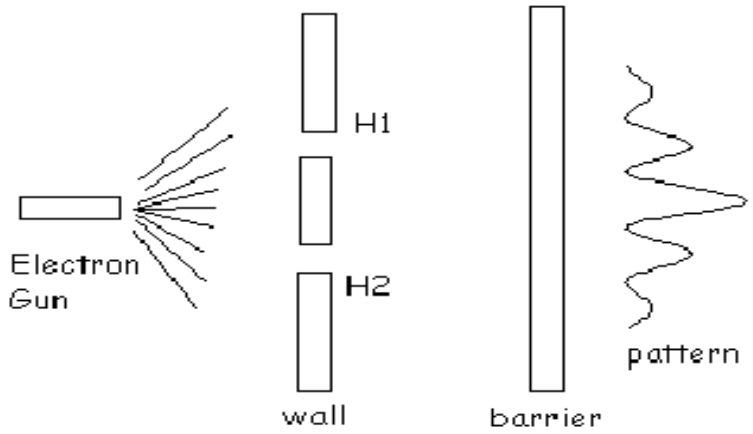
QM principles

- a particle can be in a superposition of several states at the same time;
- particle characteristics are best described as blends or superpositions of base values;
- when characteristics are measured, the superposition *collapses* into a single state, losing any information about the state before measurement. *(← special importance for quantum cryptography: you cannot measure the system without disturbing it)*

Qubits

- Qubit (quantum bit) is a quantum system with *two discrete* states, usually denoted by $|0\rangle$ and $|1\rangle$;
- A state of qubit is an arbitrary superposition of basis states, I.e. linear combination $a|0\rangle + b|1\rangle$, where *a* and *b* are *complex numbers*, called amplitudes;
- The *norm squared* of the amplitude of a state is the *probabilities* of measuring the system in that state: $|a|^2$ for $|0\rangle$ and $|b|^2$ foı $|1\rangle$

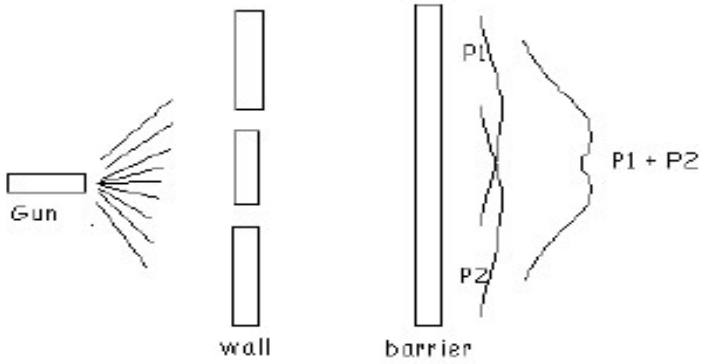
Example



If electron has equal probabilities to go through either H1 or H2 then it position might be superposition of two states: $1/\sqrt{2}\,|H1\rangle + 1/\sqrt{2}\,|H2\rangle$

<=

If one tries to measure the position of electron either at H1 or at H2 then probability of finding electron there would be ½ . A|t the same time measurements destroy superposition of states and one gets the following distribution =>



Measurements

- Measuring of any quantum system (e.g. qubit) *projects* the state vector of the system onto a new state vector;
- The measurements in a set, called “basis”, are a description of what can be observed. In our example the basis is states H1 and H2;
- In short, any measurement is defined by a basis. The result of the measurement is a (state) vector of the basis.The probability to get such a result is defined by amplitude assigned to a particular basis state vector;
- Often quantum systems can be described with many *different*, but related, bases.

Photon measurement with different bases

Polarization of photon:

- superposition of two basis states;
- many possible bases
- we co → ler two ↑ ferent bases: +
  1. ↗ and ↖ denoted by X
  2. and denoted by

Polarization	↑	→	↗	↖	↑	→	↗	↖
Basis	+	+	+	+	X	X	X	X
Result	↑	→	↑ or → (50/50)	↑ or → (50/50)	↗ or ↖ (50/50)	↗ or ↖ (50/50)	↗	↖

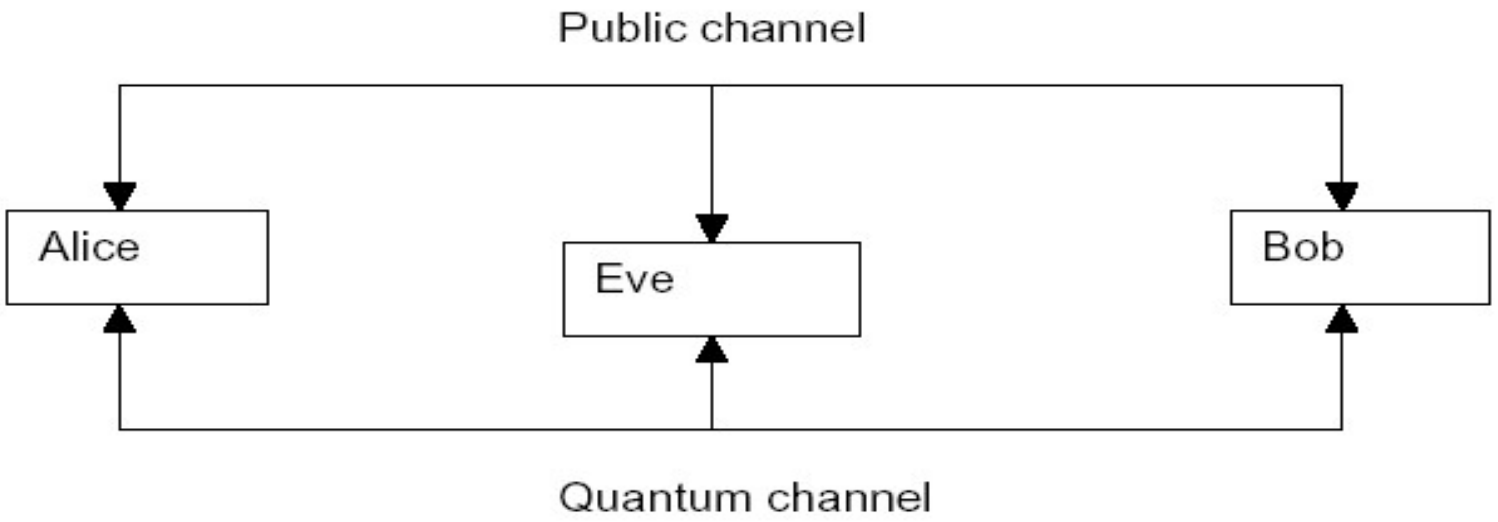
Quantum Key Distribution

- Charles H. Bennett and Gilles Brassard, 1984 (BB84):
- QKD protocol ensures:
- that either the distributed key will be perfectly secure;
- or that parties will learn that someone is listening and

therefore not use the key.

- In this protocol, Alice and Bob agree in advance on representation of 0 and 1 in each of two basis for photon polarization, e. g.:
- → and ↗ represent 0
- /|\ and ↖ represent 1.

BB84 protocol. General scheme



Picture by P.E. Black at al.

- Alice and Bob use two channels, quantum and classical;
- Both channels may be overheard by Eve the adversary

BB84 protocol

- Alice sends to Bob a stream of polarized photons, choosing randomly between , →, , ↗ d ↖ olarizations. (Quantum channel)
- When receiving a photon, Bob chooses randomly between + and x bases.
- When the transmission is complete, Bob sends Alice the sequence of bases he used to measure the photons. (Public channel).
- Alice tells Bob which of the bases were the same ones she used.
- (Public channel)
- Alice and Bob discard the measurements for which Bob used a *different* basis than Alice.
- The remaining 50% (on average) of measurements form a shared key: Bob will get the same polarization that Alice sent.

BB84 protocol (cont.)

Sent by Alice	→	→	↑	↑	↗	↖	↗	→	→	↑	↖	↖	↖	↑	→	↗
Basis used by Bob	X	+	X	X	+	X	+	+	+	X	X	+	X	+	+	X
Bob's result	↖	→	↗	↖	→	↖	↑	→	→	↖	↖	→	↖	↑	→	↗
Key		0				1		0	0		1		1	1	0	0

• When Eve is listening only public channel she cannot learn anything about the key itself (because for a given basis Alice sends random polarizations)

BB84 protocol (cont.)

- What if Eve is trying to listen quantum channel?
  - She has to guess correct basis at each step (50% on average) to make measurements;
  - But when Eve measures a photon, its state is altered to conform to the basis Eve used, so Bob will get the wrong result in approximately half of the cases where he and Alice have chosen the same basis:

Sent by Alice	→	→	↑	↑	↗	↖	↗	→	→	↑	↖	↖	↖	↑	→	↗
Basis used by Eve	+	+	X	+	+	+	X	+	X	X	+	+	X	+	X	+
Eve's result	→	→	↗	↑	→	↑	↗	→	↖	↖	↑	→	↖	↑	↗	→
Basis used by Bob	X	+	X	X	+	X	+	+	+	X	X	+	X	+	+	X
Bob's result	↖	→	↗	↖	→	↗	↑	→	→	↖	↗	→	↖	↑	→	↗
Key		0				err		0	0		err		1	1	0	0

BB84 protocol

- Next, Alice and Bob publicly compare small parts of their raw keys to estimate the error rate, then delete these publicly disclosed bits from their key, leaving the *tentative final key*.
- If the error rate exceeds a pre-determined error threshold, indicating possible interception by Eve, they start over from the beginning to attempt a new key.

Practical Implementations

- **Los-Alamos Laboratory:**
- implementation of the protocol with quantum channel; distance = 184.6 km (fibre optic), september 2006;
- quantum channel through the air; distance > 10 km;
- **University of Munich**: quantum key exchange with the airplane (>20km, 300km/h) (2012)
- **Italian Space Agency & Padova Uni & Chinese space agency:** Quantum communication with a satellite; distance > 1000 km (2015)
- **Commercial implementations:** ID Quantique …

- **Quantum RND:** ID Quantique …

Quantum computing

- Quantum systems may be used to perform computations;
- Computations involve:
  - Performing controlled evolution of quantum system;
  - Suitable measurements;
- Quantum models of computations and quantum algorithms:
  - R.Feynman, 1982: the idea of using quantum effects to perform massive computations;
  - D. Deustch, 1985: formal model of Universal Quantum Computer;
  - P. Schor,1994: quantum computers could factor large numbers efficiently, in polynomial time !!

Quantum cryptanalysis

- Shor's algorithm for factoring large numbers has complexity, so it is polynomial in the length of input number *N;*
- Could be used for efficient breaking of RSA encryption, if implemented;
- Many technical difficulties, but:
  - Implemented by IBM in Dec 2001 on 7-qubit computer to factorise 15
  - Michigan University, Dec 2005: first quantum chip (1 qubit)
  - Innsbruck University, Dec 2005: first Quantum Byte (8 qubit system)
  - Bristol University, 2011: implementation of Shor's algorithm, factorized 21)
  - First commercial quantum computer (annealer) by D-Wave Systems, the company claims to have a 2000 qbit processor in their 4th generation quantum computer
  - IBM Q experience (online): https://quantumexperience.ng.bluemix.net/qx/experience
- Post-quantum cryptography: active development of methods for which quantum attacks are not known