Introduction to Quantum Cryptography

Francesco Biccari

biccari@gmail.com

Metodi Avanzati di Fisica della Materia
Prof. P. Calvani, Prof. P. Mataloni
Università La Sapienza di Roma

2007-11-05

Outline

Cryptography

Etymology

From Greek: κρυπτός "hidden" and γράφω "write"
the art of rendering an information unintellegible to any unauthorized party

Terminology

encryption/decryption: rendering an intellegible information unintellegible / viceversa;
cryptosystem or cipher: an algorithm for performing encryption and decryption (usually public)
key: an input parameter for cipher (usually private)

Example of Historical Cryptography

Giulio Cesare cipher (monoalphabetic substitution). The key is the shift.
Leon Battista Alberti cipher(polyalphabetic substitution). The key is the random alphabet.
Bellaso–Vigenère cipher (polyalphabetic substitution). The key is a phrase.

Cryptography

Symmetric–Key Algorithm

Same key for encryption and decryption
The problem is how to keep the key hidden
Usually distributed by a public-key cryptosystem.

Examples

one-time pad is the only secure chiper (Shannon 1949)
the key is as long as the message and it can be used only one time;
$s = message \oplus key$ (binary addition)

DES (1976) Data Encryption System
the key is 56 bits long. The rest is computational complexity.

Asymmetric–Key Algorithm

Different key for encryption and decryption
Based on the computational difficulty to "invert" the public key to obtain the private key (thus insecure)
RSA (1977): based on the factorization of the prime numbers.

Quantum Mechanics and Qubit

Useful Features of QM

- Measure operation: $|\alpha\rangle \xrightarrow{A} |a\rangle$ ($\hat{A}$ autoket);
- Heisenberg uncertainty principle of two not–commutative observable operators;
- Quantum Entanglement (violation of Bell's inequality).

Quantum Bit: Qubit

qubit is a state of a two–dimensional Hilbert space. $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$
where $|0\rangle$ and $|1\rangle$ form an orthogonal basis.
An example is a system of spin 1/2 with $|0\rangle = |z\uparrow\rangle$ and $|1\rangle = |z\downarrow\rangle$.

Qubit Representation

$$|\phi\rangle \doteq \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Density Operator:

$$\hat{\rho} = \sum_i p_i |\phi_i\rangle\langle\phi_i|$$

Quantum Mechanics and Qubit

Single Qubit Operators

Time Evolution $\hat{U}$;

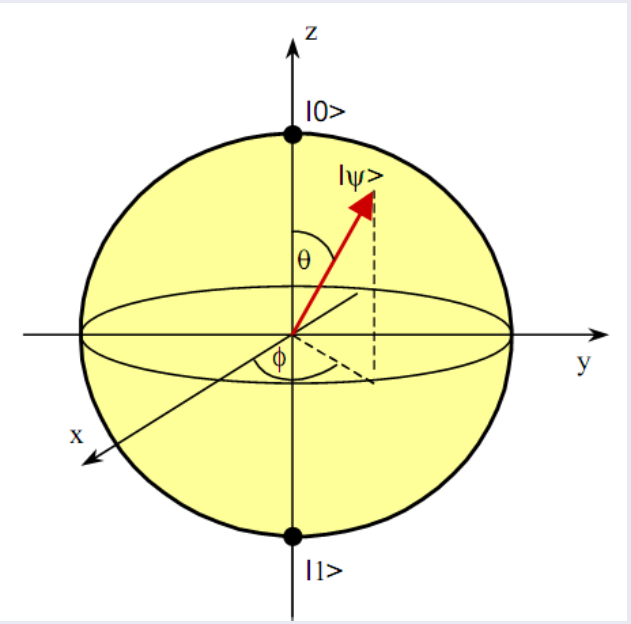
Hadamard ($\pi/4$ rotation) $\hat{H} \doteq \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Pauli

$\hat{I} \doteq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \hat{\sigma}_x \doteq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \hat{\sigma}_y \doteq \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \hat{\sigma}_z \doteq \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Bloch–Poincaré Sphere Representation

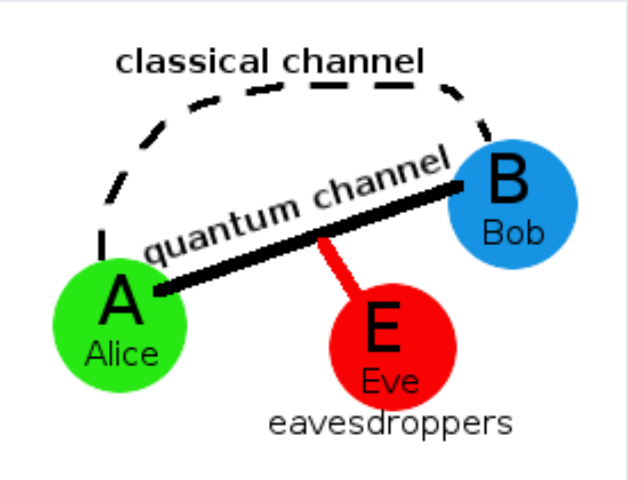
$|\phi\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\varphi} \sin(\frac{\theta}{2})|1\rangle$
The corresponding pure density operator is: $\hat{\rho}(\theta, \varphi) = \frac{1}{2}(\hat{I} + \vec{r} \cdot \vec{\hat{\sigma}})$
where
$\vec{r} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\varphi)$
belongs to a sphere of radius 1.
Instead mixed states are represented by the internal point of this sphere.



The Idea of Quantum Cryptography

The Idea

Wiesner (1980)
Bennet, Brassard (1984)



1. A sends key (qubits) by QC;
2. B measures the key;
3. A sends by CC part of the key;
4. B checks if E "measured" the key;
5. if not, A encrypts data using the key and sends them by CC; otherwise try another key.

Quantum Cryptography is useful to share, in a secure way, the private key in symmetric cryptography.
(better QKD: Quantum Key Distribution)
One–Time Pad + QKD $\longrightarrow$ perfect cryptography!

Most Famous Protocols

The BB84 Protocol (Bennet–Brassard 1984)

Based on the Heisenberg uncertainty principle.
2 conjugate bases of a 2 state system. e.g.: $|\langle\uparrow \mid \leftarrow\rangle|^2 = 1/2$
Usually qubits encoded in polarization of photons along different axis.

Basis	0	1
+	↑	→
X	↗	↘

Alice's random bit	0	1	1	0	1	0	0	1
Alice's random sending basis	+	+	X	+	X	X	X	+
Photon polarization Alice sends	↑	→	↘	↑	↘	↗	↗	→
Bob's random measuring basis	+	X	X	X	+	X	+	+
Photon polarization Bob measures	↑	↗	↘	↗	→	↗	→	→
PUBLIC DISCUSSION OF BASIS								
Shared secret key	0		1			0		1

Raw key (before classical comm.): 25% error rate;
Sifted key (after classical comm.): 50% of Raw key, 0% error rate

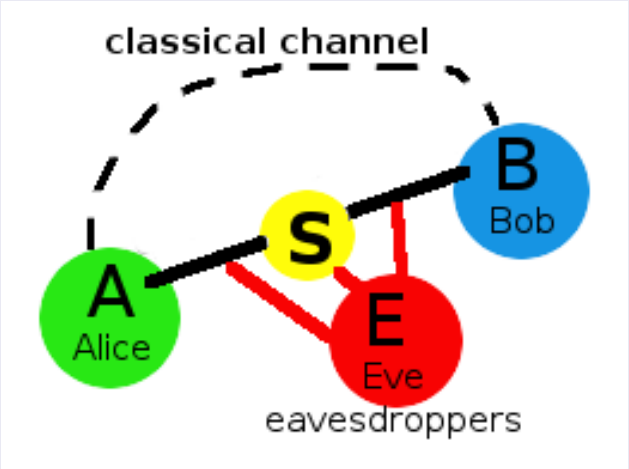
Eavesdropping

E can interfere with both classical and quantum channel.
In the first case Eve cannot obtain any information. If she change the data of the classical channel or measures the quantum channel, A and B discover the change by error rate of qubits received in the same basis.
For real eveasdropping E should be able to copy the qubit.

Most Famous Protocols

The "EPR" Protocol (Ekert 1991)

Based on the properties of a maximum entangled system of two photons.
e.g. $|\phi\rangle = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle)$
These can be made by Alice, Bob or by a third person (including Eve).
After the measurement in random basis, they communicate by classical channel and keep the qubit if the basis is the same.
(one of two inverts the qubits)



Eavesdropping

E can interfere with both classical and quantum channel.
Same sistuation as in the BB84 protocol.
For real eveasdropping E should be able to copy the qubit.
Ekert protocol uses a third basis. Even if the good choice of basis is reduced, there are enough data to test Bell's inequality to understand if the Source is Eve.

Eavesdropping and No–Cloning Theorem

No–Cloning Theorem

Wigner (1961), Ghirardi (1981), Wooters–Zurek (1982).
(pure state and unitary time evolution copier)

$$\hat{U}|\phi\rangle_A|e\rangle_B = |\phi\rangle_A|\phi\rangle_B$$

$$\hat{U}|\psi\rangle_A|e\rangle_B = |\psi\rangle_A|\psi\rangle_B$$

for all $|\phi\rangle$ and $|\psi\rangle$.
With the inner product of the two previous expressions: $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$ that is not true for all $|\phi\rangle$ and $|\psi\rangle$.
The no cloning theorem holds in full generality.

Eavesdropping

Thus the only possibility for Eve to attack the system is acting as Bob for Alice and Alice for Bob, performing two QKD. (Man in the middle attack).
Useful only if A and B don't have an authentication protocol.

Technological Aspects

Practical Interests

QKD is useful for application where the distance between A and B is very short (Credid Card and ATM machine) or very large.
The first possibility is impossible with present technology.
We will concentrate only on such large distance system.
(First experiment in 1992 was performed at 30 cm distance)

Medium, Detectors and Sources

- free space: good for present detector at 800nm;
- optical fiber: good for large distance but need new detectors near 1300 nm or 1550 nm.

The latter choice is preferred. Low attenuation: 0.3dB/km, free space attenuation is 2dB/km.

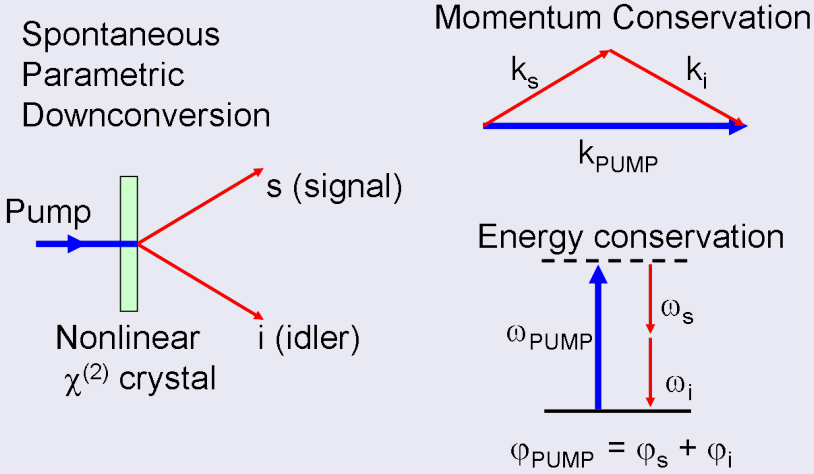
Technological Aspects: Photon Source

Faint Laser Pulses

- Poisson Distribution: $P(n,\mu) = \frac{\mu^n}{n!} e^{-\mu}$.
- Very small μ (mean number) to have low probability $P(n>1) \simeq \frac{\mu}{2}$
- Problem! $P(n=0) \simeq 1-\mu \longrightarrow$ Detector dark counts! $0.01 < \mu < 0.10$

Entangled Photon Pairs

- Spontaneous Parametric Downconversion (Non linear effect $\chi^{(2)}$)
- First photon triggers the second one: Single photon without empty pulses
- Inefficient (10^{-10}) and not–deterministic
- It can be used for Photon Pairs creation $\longrightarrow$ Ekert protocol

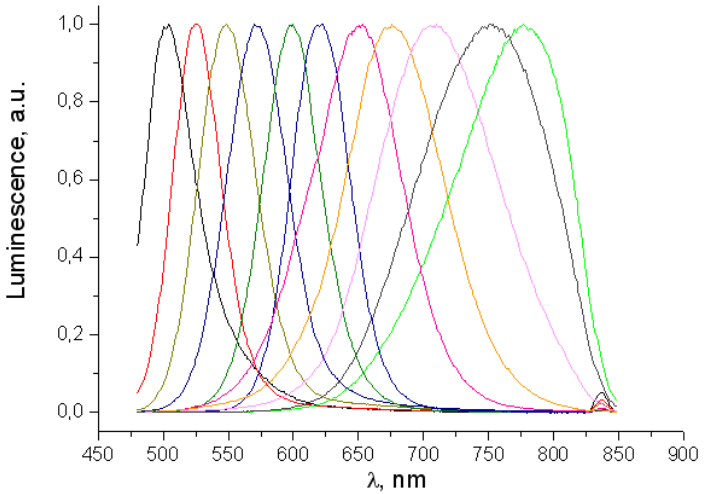


Technological Aspects: Photon Source

Photon Gun

The ideal single–photon source. Not yet available for QKD.

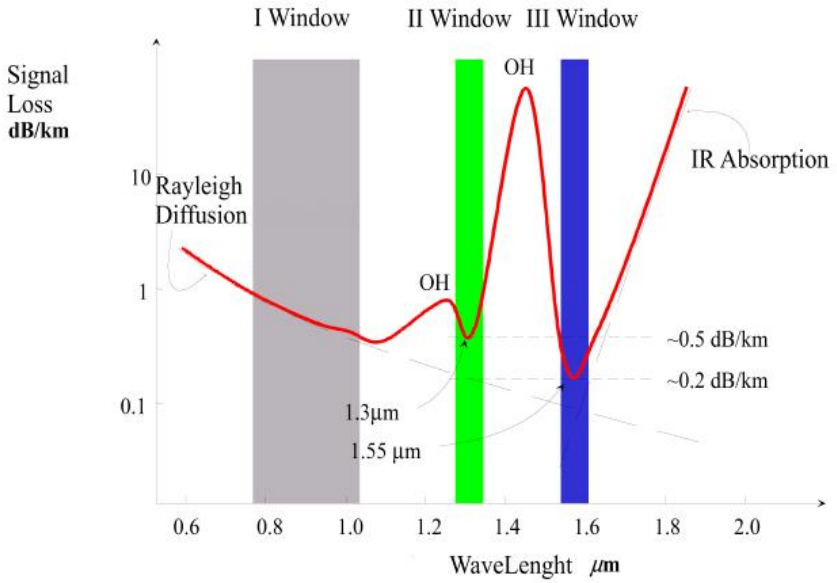
- single two–level quantum system. e.g.: trapped ions. (Technically difficult) Promising candidate is vacancy in diamond (large bandwidth): fluorescence exhibits strong photon antibunching
- mesoscopic p–n junction: extremely low temperature, inefficient.
- semiconductor quantum–dot: hole–electron recombination. After excitation each quantum–dot emits a single photon with the frequency depending of its radius.



Technological Aspects: Quantum Channel

Optical Fiber

- waveguide: refractive index $n(x, y)$
- attenuation 2dB/km at 800nm, 0.2dB/km at 1550nm
- mode: solution of Maxwell equation in the fiber. (pattern)



Problems

- mode coupling: not stable relation input–output $\longrightarrow$ single–mode fibers (only bound mode: monotonically decay of $\vec{E}$ and $\vec{B}$ in the trasverse direction; two indipendend polarizations)
- chromatic dispersion effects (timing resolution limitation) $\longrightarrow$ narrow bandwidth (difficult in parametric down conversion)
- polarization effects: geometric phase, birefringence, polarization mode dispersion, polarization–dependent loss

Technological Aspects: Quantum Channel

Polarization Effects in the Optical Fibers

- geometric phase (Berry) $\longrightarrow$ aligment of A and B systems
- birefringence: due to the asymmetry in the fiber. Different phase velocities for two orthogonal polarization states. Compensation by alignment.
- polarization mode dispersion: Different group velocities for two orthogonal polarization states. $\approx 0.1 ps/km$ Orthogonal modes couple. Remedy: source high coherence time.
- polarization–dependent loss (neglegible in fibers)

Free Space

- transmission window at 770 nm (good detectors!)
- atmosphere is not birefringent (no polarization change)
- energy spread out
- ambient light $\longrightarrow$ high error rate
- turbulent medium (corrected by a reference pulse n ns before each pulse)
- diffraction

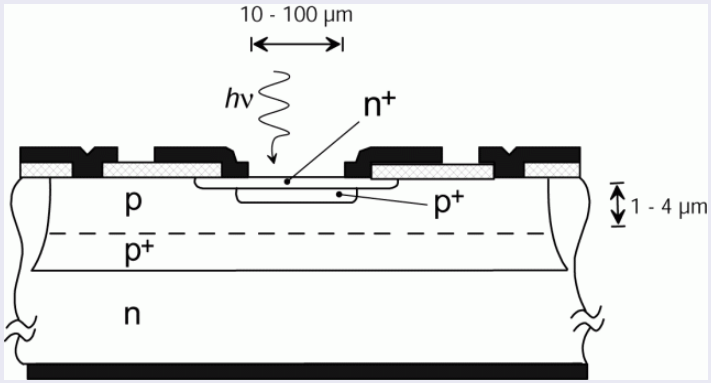
Technological Aspects: Detector

Ideal detector

- high quantum efficiency over a large spectral range
- low dark counts
- good timing resolution (low jitter)
- short recovery time (to reach high data rates)
- practical!

APD: Avalanche Photodiodes

- Currently APD is the best choice
- Geiger–mode: applied voltage exceeds the breakdown voltage ($\approx 10^5\, V/cm$; gain $\approx 10^6$)
- Self–sustaining avalanche (ns rise time; mA current range; ps jitter)
- How to stop the avalanche and reset the APD?



Technological Aspects: Detector

Single–Photon APD Reset Methods. Quenching Circuit

- passive–quenching: a single resistor (100 kΩ or more) in series to the APD. The avalanche current self-quenches because it develops a voltage drop across the APD. Then the APD bias slowly recovers to V_A, and therefore the detector is ready again. Maximum count rate reach MHz
- active–quenching: bias is actively lowered below V_B. Higher count rate: till 100 MHz. Circuits are much more complicated!
- gated–mode: the most used method. Bias is kept below V_B. It is raised above V_B only for a time window synchronized with photon arrival. Data rate: till 100MHz. Useful when arrival time is well known (single–photon).

APD and Quantum Channel

- free space and fiber ($\nu_{ph} \lesssim 1\mu m$): Silicon commercial APD is enough for QKD. 76% quantum efficiency, jitter 28ps, count rate 5MHz. Dark count rate at -20° is 50Hz.
- fiber and ν_{ph} 1.3 μm or 1.55 μm: Ge and InGaAs/InP. Lower efficiency, higher dark counts, complicated setup. Not yet commercial products.

Quality of QKD

QBER

Quantum Bit Error Rate

$$QBER = \frac{N_{wrong}}{N_{tot}} = \frac{N_{wrong}}{N_{right} + N_{wrong}} = \frac{R_{error}}{R_{sift} + R_{error}} \approx \frac{R_{error}}{R_{sift}}$$

$$R_{sift} = \frac{1}{2} R_{raw} = \frac{1}{2} q f_{pulse} \mu t_{link} p_{phot}$$

$$R_{error} = R_{opt} + R_{det} + R_{acc}$$

- f_{pulse}: number of laser pulses per second
- μ: mean number of photon per pulse
- t_{link}: probability for a photon arriving to the analyzer
- p_{phot}: probability to detect a photon
- q: correction factor for some setups

Quality of QKD

R_{opt}

Probability to end up in the wrong detector (optics).

$$R_{opt} = R_{sift}\, p_{opt}$$

p_{opt}: probability of a photon's going in the wrong detector

R_{det}

Probability to keep a dark count (detector)

$$R_{det} = \frac{1}{2}\bigg|_{sifting} \frac{1}{2}\bigg|_{det} f_{pulse}\, p_{dark}\, n_{det}$$

p_{dark}: probability to register a dark count per time window and per detector

R_{acc}

Probability to have two non correlated photons (only for EPR)

$$R_{acc} = \frac{1}{2}\bigg|_{sifting} \frac{1}{2}\bigg|_{det} f_{pulse}\, t_{link}\, p_{acc}\, p_{phot}\, n_{det}$$

Quality of QKD

QBER

$$QBER = p_{opt} + \frac{p_{dark}\, n}{t_{link}\, p_{phot}\, 2q\mu} + \frac{p_{acc}}{2q\mu} = QBER_{opt} + QBER_{det} + QBER_{acc}$$

- $QBER_{opt}$ is a measure of the optical quality of the setup ($\simeq 1\%$)
- $QBER_{det}$ increases with distance (t_{link} decreases while p_{dark} is constant)

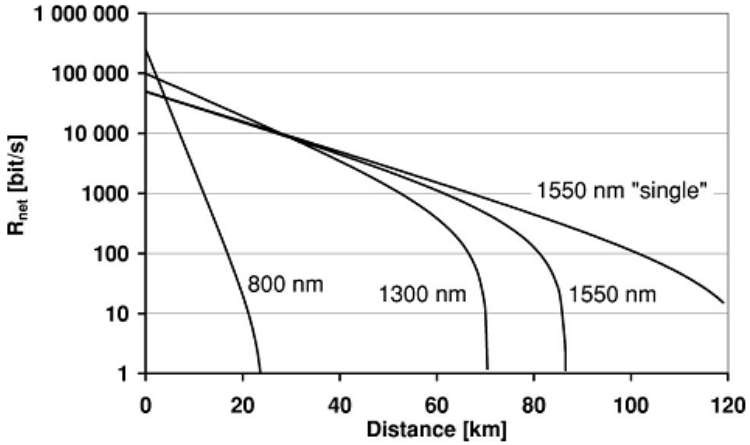


FIG. 11. Bit rate, after error correction and privacy amplification, vs fiber length. The chosen parameters are as follows: pulse rates of 10 MHz for faint laser pulses ($\mu = 0.1$) and 1 MHz for the case of ideal single photons (1550-nm "single"); losses of 2, 0.35, and 0.25 dB/km; detector efficiencies of 50, 20, and 10; dark-count probabilities of 10^{-7}, and 10^{-5}, and 10^{-5} for 800, 1300, and 1550 nm, respectively. Losses at Bob's end and $QBER_{opt}$ are neglected.

Experimental Setups with Faint Laser Pulses

Polarization Coding

Encoding the qubits in the polarization of photons
For instance BB84 protocol: 4 states (0° and 90°, $+45^\circ$ and -45°), 2 bases.
First QKD experiment: 1992. 30cm in free space
1995: QKD over a distance of 23km in optical fiber!

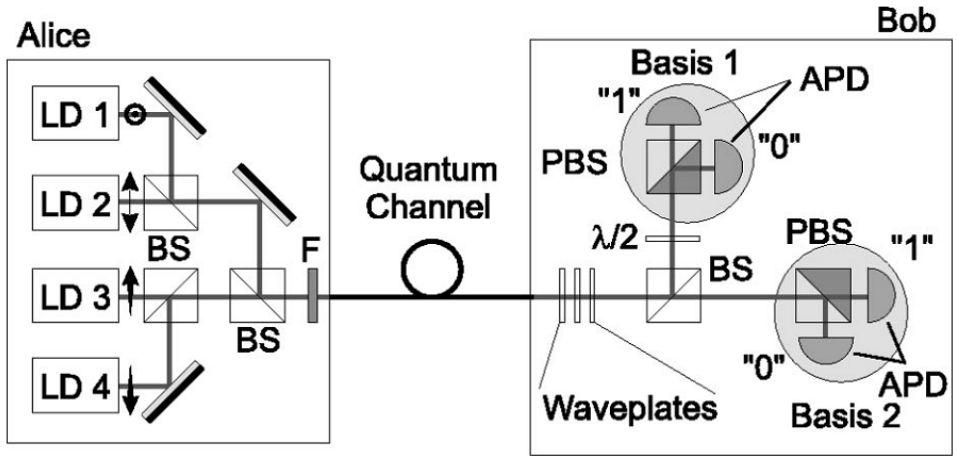


FIG. 12. Typical system for quantum cryptography using polarization coding: LD, laser diode; BS, beamsplitter; F, neutral density filter; PBS, polarizing beamsplitter; λ/2, half waveplate; APD, avalanche photodiode.

- F: to reduce μ
- Waveplates: compensation of the optical fiber effects
- $\lambda/2$: to rotate the polarization of 45°, to use the same detector alignment for both basis

Experimental Setups with Faint Laser Pulses

Phase Coding

Encoding the qubits in the relative phase of photons
For instance BB84 protocol: 4 states ($\phi = 0$, π, $\pi/2$, $3\pi/2$), 2 bases.
Detection implemented by (single–mode) optical fiber interferometers
Most common: Mach–Zehnder interferometer.

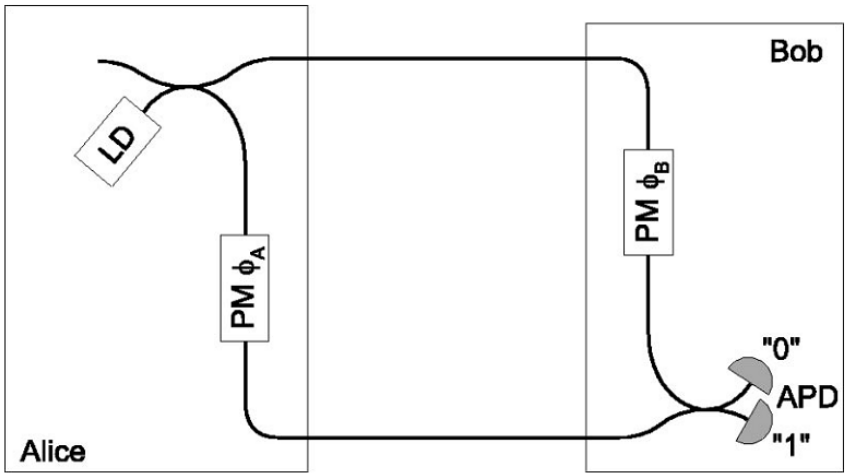


FIG. 14. Conceptual interferometric setup for quantum cryptography using an optical fiber Mach-Zehnder interferometer: LD, laser diode; PM, phase modulator; APD, avalanche photodiode.

- $I_0 = I \cos^2\left(\frac{\phi_A - \phi_B + k\Delta L}{2}\right)$
- qubit encoded by ϕ_A modulator
- Bob chooses a basis using ϕ_B modulator (0 or $\pi/2$)
- Classical communication

Experimental Setups with Faint Laser Pulses

Alice			Bob	
Bit value	ϕ_A	ϕ_B	$\phi_A - \phi_B$	Bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

Phase Coding Example

Compatible bases when ϕ is equal to 0 or π

Stability of Path Difference ΔL

ΔL must be stable in time! Impossible over more than few meters.
1992 Bennett proposed the double Mach–Zehnder implementation

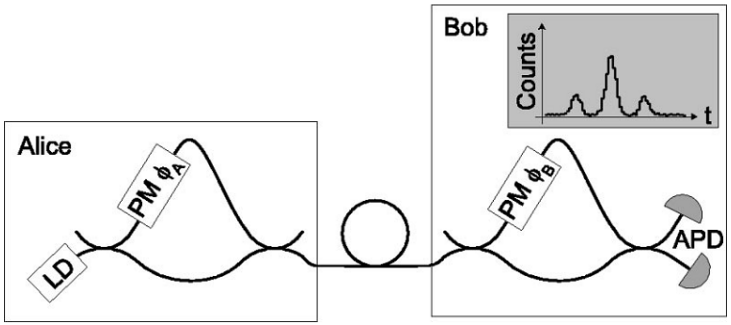


FIG. 16. Double Mach-Zehnder implementation of an interferometric system for quantum cryptography: LD, laser diode; PM, phase modulator; APD, avalanche photodiode. The inset represents the temporal count distribution recorded as a function of the time passed since the emission of the pulse by Alice. Interference is observed in the central peak.

- a series of 2 Mach–Zehnder
- single fiber!
- interference produced by undistinguishable paths: short–long or long–short (central peak)

Conclusions

Applications of the QKD

The current commercial systems are aimed mainly at governments and corporations with high security requirements.
QKD was used in Swiss national election!

Industry and QKD

id Quantique (Geneva), MagiQ Technologies (New York) and SmartQuantum (France)

World Records

March 2007, optical fiber, BB84, 148.7 km at Los Alamos/NIST
2006 (BB84) and 2007 (Ekert), free space, 144 km between two Canary Islands

References

- Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, Hugo Zbinden
  Rev. Mod. Phys, vol. 74, 145, January 2002
- Francesco De Martini, Fabio Sciarrino
  Progress in Quantum Electronics 29 (2005) 165–256