New directions in Quantum Cryptography

dr. Mario Stipčević, Institut Ruđer Bošković

CARNet Users Conference 2004

27-29 September 2004, FER, Zagreb

Final version

E-mail: Mario.Stipcevic@irb.hr

Why do we need cryptography ?

We live in the age of **knowledge** and **communications**
Investment in those two brings up the highest **profit**

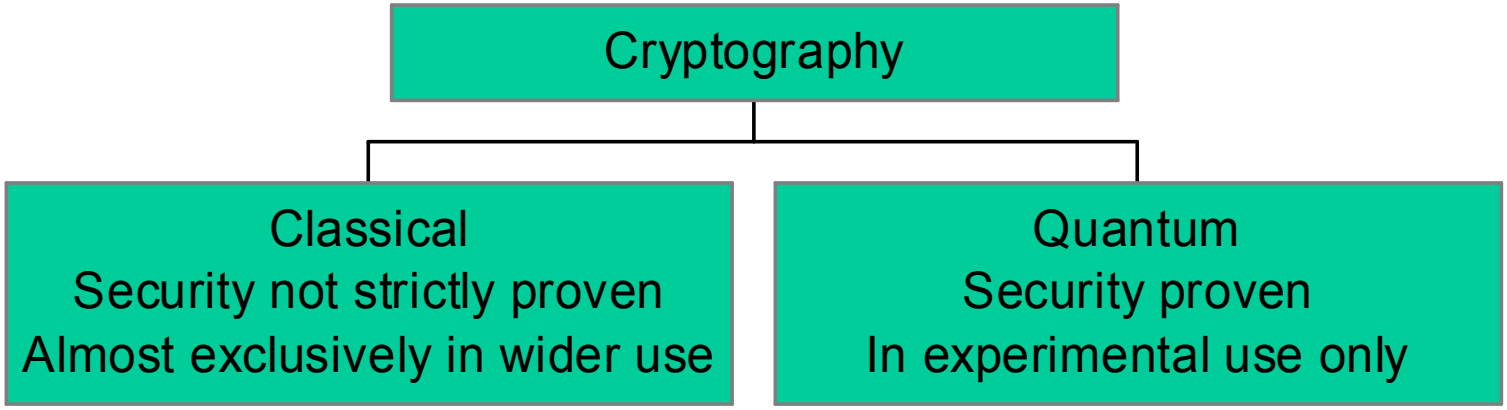
Communications play an increasingly important role in everydays life:
- transfer of knowledge (sensitive data)
- logging onto remote systems
- electronic business (B2B)
- e-commerce
- e-banking (for business and citizens)
- e-government, etc.

Data often need to be secured when transferred through an insecure environment such as the Internet or telephone lines

$\Rightarrow$ **cryptography**

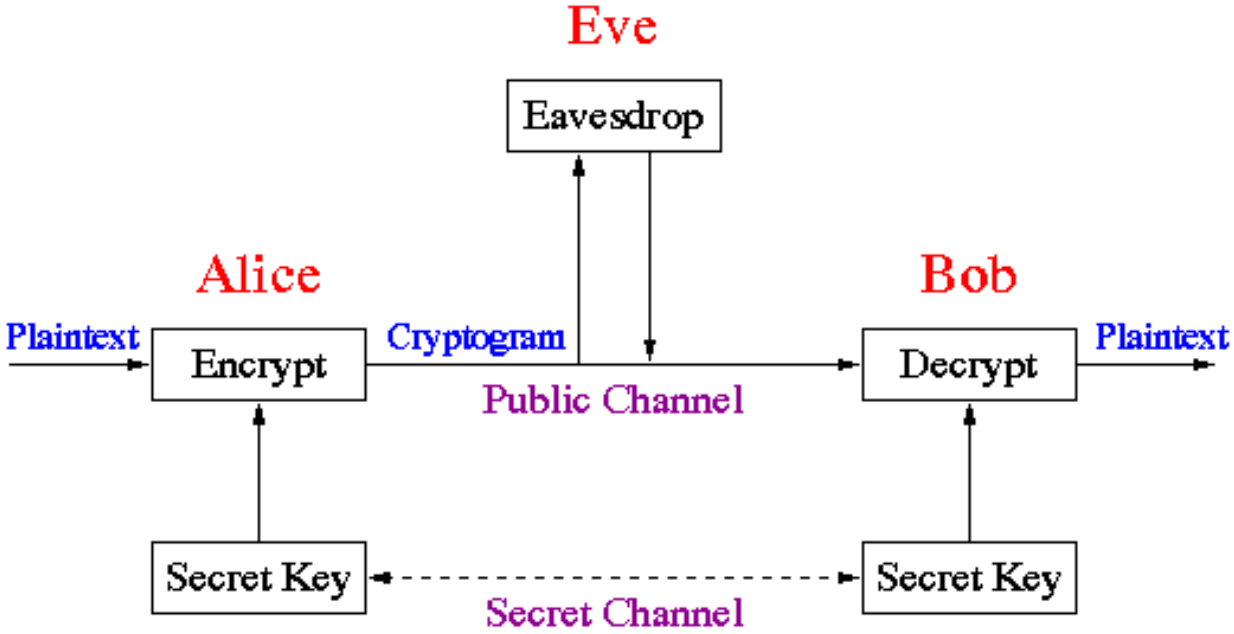
Cryptography

The art and science of data protection.



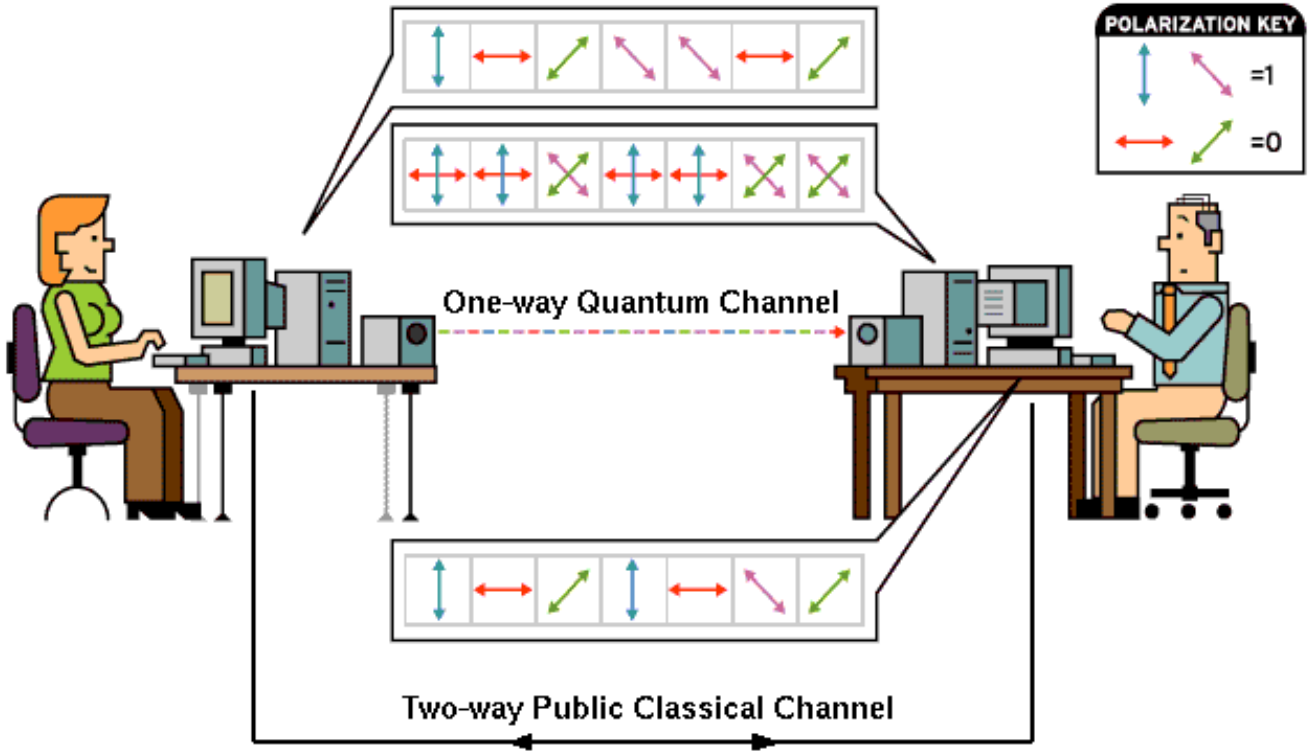
• Classical cryptography consists of mathematical puzzles. But this puzzles can in principle be solved.
• Quantum cryptography relies on laws of physics and puzzles that cannot be solved.

Classical Shannon's cryptosystem



- This system is only secure if eavesdropper does not have access to the secret channel
- The only protocol proven to be **unconditionally secure** is the One Time Pad (OTP). Other known protocols, including Public Key protocols, are at best **computationally secure**
- Eve is supposed to be able to **copy perfectly** and **without interference**

Quantum cryptosystem



- This system can be made **unconditionally secure** (eg. protocol EPR)
- Eve is able to **copy perfectly** and **without interference** from the CC
- Only **imperfect copies** of info. sent through the QC are possible but the legitimate parties can correct errors by power of **interaction**

Computational vs Unconditional security

Computational security:

- Cryptosystem can *in principle* be broken if enough computational resources (CPU, memory) and/or time is available.

Unconditional security:

- Cryptosystem can not be broken even with unlimited computational resources and time: there is simply not enough information leak for an eavesdropper to calculate the message (or key).

Unconditional security comes with a price tag: legitimate parties now MUST INTERACT in order to establish mutual secret key.

Classical vs Quantum Cryptosystem

Almost all contemporary comm. channels are “classical” meaning:
1. information ***can be copied*** without errors
2. copying process does ***not*** introduce ***detectable interference***
3. channel is virtualy ***noiseless***.

Quantum crypto makes use of the “quantum channel” from which:
1. perfect ***copies*** of original information are ***not possible***
2. copying process introduces ***detectable interference***
3. ***noise*** is inherent to this type of channel.

Quantum channel consists of a medium (such as optic fiber) which can carry a single quantum of energy (eg. a photon).

Security of the QC relies on impossibility to copy without error the information carried by a single quantum of energy. This is so called “no cloning theorem”.

Quantum Key Distribution (QKD)

The heart of Quantum Cryptography is a protocol for establishing a symmetric secret key between two distant parties

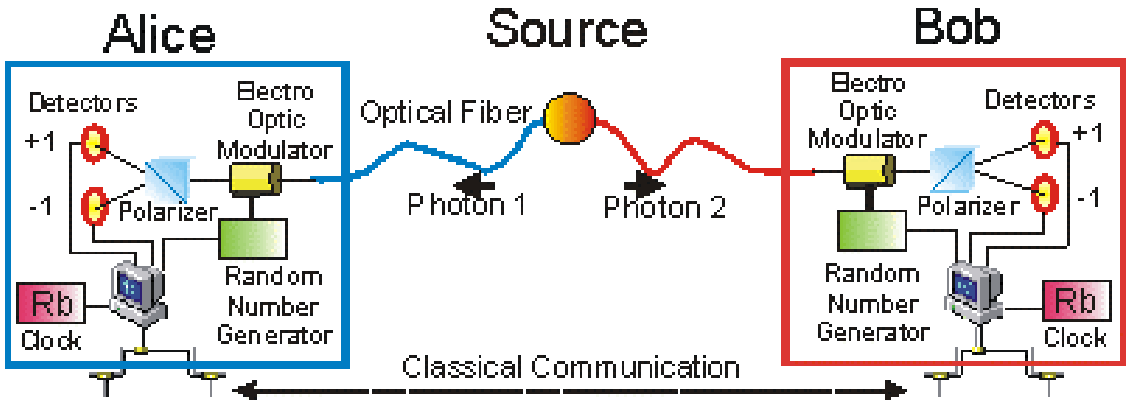
- In 1984. C.H.Bennett (IBM) i G. Brassard (U.Montreal) published first QKD protocol named **BB84**. They performed a successful experiment in 1991. This was the birth of Quantum Cryptography

- 1992. Bennett published simplified BB84 protocol named **B92**

- 1991. Eckert published the **EPR** protocol which avoids weaknesses of BB84 and B92. This protocol makes use of so called “Einstein Podolski Rosen pairs” of entangled photons. EPR and its variants is what is actually used today.

Q. Cryptography with EPR pairs

Group from Vienna univ. led by prof A. Zeilinger realized in 1999 the EPR protocol. Key to this success was a device for producing pairs of entangled photons using non-linear optical crystals.

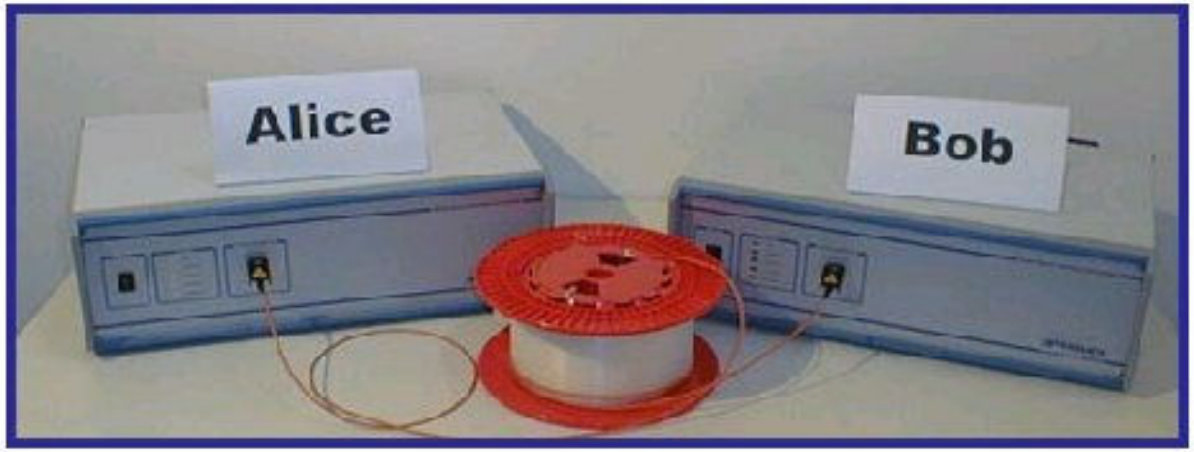


Although logically equivalent to BB84 this system has advantages:

- intrinsic randomness of distributed key
- extremely low probability of double photons (exploitable for attacks)

IdQuantique's QKD device

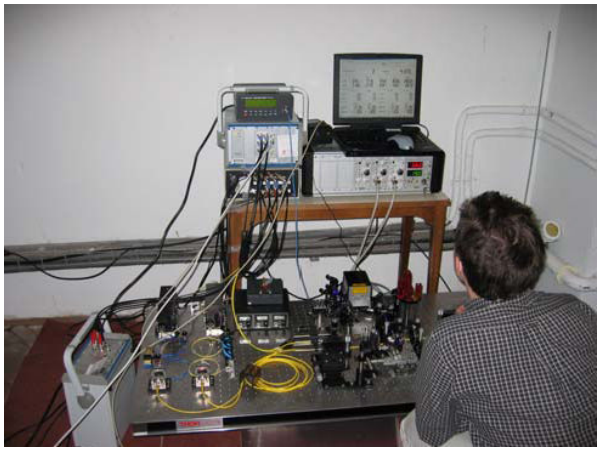
In summer 2002 Swiss firm IdQuantique produced the first comercial device for QKD capable of operating over an unpreceeded distance of 67 km. The link between is optic fiber. Price: 100.000 Eur.



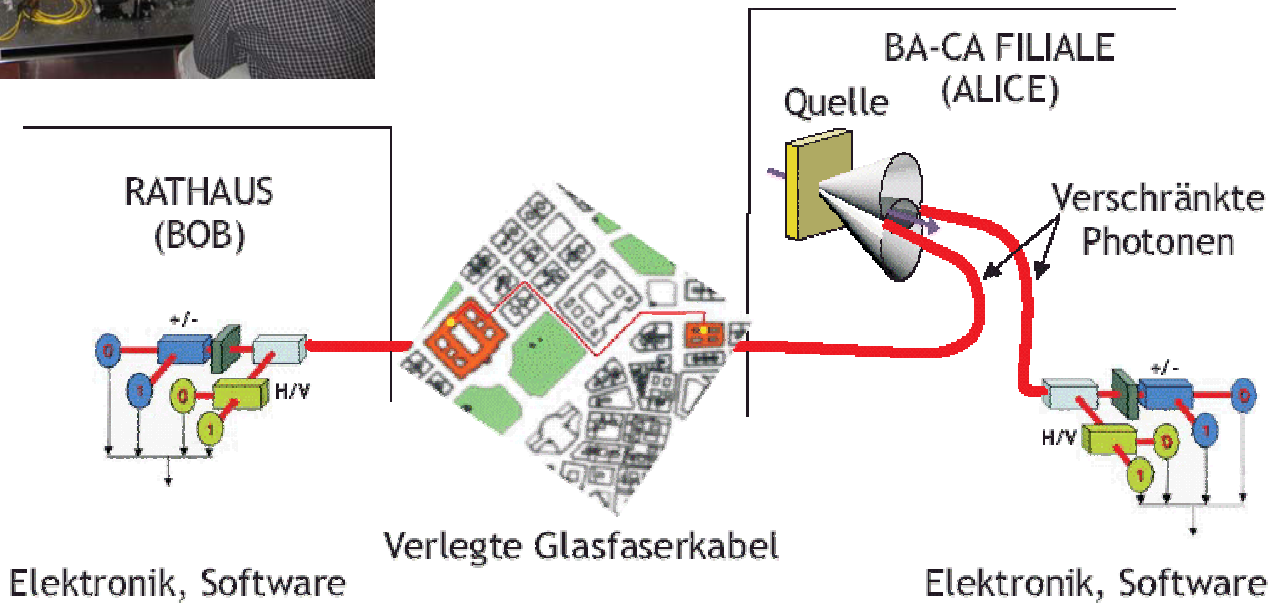
Main features

- First commercial quantum key distribution system
- Key distribution distance: up to 60 km
- Key distribution rate: up to 1000 bits/s
- Compact and reliable

1.04.2004 - first Quantum bank transaction (Vienna)



Group from Vienna Univ. exhibits a public display of world's first payment secured by virtue of a Quantum Cryptographic protocol, between Vienna Rathaus and Bank of Austria.



MagiQ's QPN

- MagiQ is an USA based start-up company

- Their QPN Security Gateway uses combination of Classical Cryptography and Quantum Cryptography to achieve nearly-perfect security.

- Symmetric secret keys are generated by QKD and refreshed at a rate of 100 keys/sec

- Any intrusion into system is immediately detected

- QPN has a great computer network support and is compatible with existing PKI infrastructure but it also requires optic fiber connections

- Range: they claim to be able to chain stations up to 120 km apart

- QPN physical infrastructure is tamper-free or tamper-evident

- Available in 2003. Cost of a basic set: cca. 150.000 US$

Quantum PKI (QKI)

- QKI is term for quantum equivalent of Public Key Infrastructure (PKI)
- It is not yet clear what QKI will offer but the general idea is to give some network support to the QKD
- The problem is to establish a secret key between very distant parties over a set of **partially trusted** servers, such that neither of servers "has" all the information about the key but that a qualified majority of servers can compute the key (Secret Sharing Schemes).
- Eventually QKI is to superseede completely existing classical QKI - **this is a huge task**.

Swiss QKI initiative

- In 1998. Swiss firm OISTE has designed a certification system **Root**

- 2001. Swiss World Internet Secure Key (WISEKey) has become the world's most trusted e-security infrastructure for delivery of digital certificates including OISTE Root.
  A mountain bunker protects its algoritmic code. It takes 7 weeks to get entry clearance to the bunker.

- October 2003. IdQuantique, WISEKey and OISTE join forces to develop a first ever Quantum Key Infrastructure based on the OISTE Root and Quantum Cryptography.

Government departments, banks and financial institutions looking to archive information over ultra secure links are expected to be the first users of the technology

EU Framework 6 project SECOQC

"European scientists against eavesdropping and espionage"

• **Goal:** Development of an entirely secure communications network based on Quantum Cryptography. Ten countries from the EU, Switzerland, Canada. Budget: 11.4 MEur.

• "Within four years, the cost-effective production of quantum key distribution shall start. A near-to-market prototype for encrypted connections between two points will be developed, as well as a high performance network infrastructure for spanning greater distances."

• Reason: stop significant financial losses due to industrial espionage performed by activities of the ECHELON communication surveillance and interception network.

• American NSF 2004. gives over 300 MUS$ for research in computer security: more than for biomedicine or nano-technology

Local activity

Two activities concerning Quantum Cryptography are under way at the Institute Ruđer Bošković

• CARNet project nr. 650-103/03 " Secure communication over the Internet" aims to develop a new unconditionally secure key exchange protocol. Project's site: http://www.irb.hr/users/stipcevi/carnet2003

• Development of hardware devices and instrumentation for commercial Quantum Cryptography, a collaboration between Dept. of experimetlal physics and Dept. of electronics

Open problems

- So far QKD has been limited to distances up to cca. 100 km through the optic fiber and 40 km through the air
- Current price of a pair of transcieving stations is cca. 100 kEur
- A wide-spread network of high quality optic fiber is a vital prerogative
- Political export restrictions currently in practice may limit availability of the QC technology

The infrastructure needed for QC is quite demanding, but the trends are that a large portion of it, namely the fiber optic going to or close to the end user, will be widely used anyhow for other purposes such as the cable TV or broadband internet.

QKI and beyond

QKI promisses enhanced security for critical applications:

- Last year, the State of Geneva has demonstrated first ever biometric Voice Recognition e-voting system for blind and partially sighted people (WSIS) for facilitating electronic voting.

- This year, WISEKey released a new generation of authentication devices which includes Biometric Identity fingerprint reader on a USB flash memory drive

Allthough these two has nothing to do with QKI, it is believed that only QKI offers level of security needed for such a major issues as full-scale e-voting for governmental and parliamenraty elections.

For that purpose central Government's servers would be connected with local county servers via Quantum Channels.

Conclusions:

- Quantum Cryptography is a quickly growing science and technology
- Protocols exist which are proven to be **unconditionally secure**: no matter what advances occur in digital computing, Quantum Cryptography can never be broken
- Practical solutions exist, but still in testing phase, clumsy and very expensive
- QC technology has the potential of becoming miniature and cheap
- Increasing security concerns boost investment in research of the QC as a candidate for an **ultimate cryptographic technique**
- We can expect that in next 10 years QC becomes a part of cryptographic techniques available to widest public (eg. e-banking)

Literature

[1] C. Shannon, Communication Theory of Secrecy Systems, Internal publication of Bell Systems, 1946 (revealed in 1949)

[2] A. Einstein, B. Podolski, N. Rosen, Phys. Rev. **41**(1935)777

[3] C.H.Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India 1984, pp 175-179

[4] A. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**(1991)661-663

[5] W.K. Wooters, W.H. Zurek, A Single Quantum Cannot be Cloned, Nature, **299**(1982)802-803

[6] C.H.Bennett, F.Besette, G.Brassard, L.Savail, J.Smolin, Experimental Quantum Cryptography, Proc. Eurocrypt 1980, pp. 253-265

[7] C.H.Bennet, G.Brassard, J-M.Robert, Privacy amplification by public discussion, SIAM J. on Computing **17**(1988)210-229

[8] http://www.quantum.univie.ac.at/research/crypto/index.html

[9] http://www.magiqtesh.com/

[10] http://www.idquantique.com/

[11] http://www.secoqc.net/