CUC 2004 Talk, Full article

Title: New directions in quantum cryptography
Author: dr. Mario Stipčević, Ruđer Bošković Institute, Zagreb

Submission date: 16. August 2004.

Introduction

Today we live in the age of knowledge and communications. Possessing knowledge and means of communication and intelligently managing these resources, rather than fighting wars, is the best way to gain power and profit. The biggest profit is achieved not by producers of goods but by those who produce know-how and critical information on how to produce goods. Global two-way communications (especially since invention of the world-wide-web) seem to be the most important accelerator of marketing as well as for producing and spreading of knowledge. Further examples of using of global communication channels are: e-business (communicating and signing confidential documents), e-banking (issuing bank orders), e-shopping etc. Many of these are of wide public interest. In short, a lot of critical data is stored or travel through communication channels (computer networks, telephone lines, internet, etc.) and there is a clear need to protect such data. This brings us to the art and science of data protection, namely the cryptography.

The most basic problem in cryptography is establishing a secret key between two parties that have no previous common information, in the presence of an eavesdropper. By the Kerchoff's principle it is assumed that the eavesdropper obtains a maximum possible quantity of information from the communication channels and that he/she is familiar with the protocol.

Generally, cryptography can be divided into two types: classical and quantum. In classical cryptography an eavesdropper has all the information needed to calculate the secret key with a high probability. In quantum cryptography an eavesdropper can at most obtain a limited information about the secret key and the upper bound on his/her information can be made arbitrarily small.

Consequently we say that classical cryptography is "computationally secure", whereas quantum cryptography offers so called "unconditional security".

Classical cryptography

Roughly speaking, contemporary classical cryptography makes use of existence of mathematical problems which can be easily defined but are very hard to solve. Nevertheless they can *in principle* be solved if enough computational resources and/or time is available.

For example, it is quite easy (and can be done fast on modern computer) to multiply 1000 prime numbers and obtain a resulting large integer number. However, a task of finding all prime factors of the same large number typically takes many millions of years of calculation on the same modern computer. In a slightly different setup security of the famous RSA public key protocol relies on apparent hardness of the factoring problem.

The main problem with the classical cryptography is that hardness of underlying mathematical problems hasn't yet been strictly proven. This means that one day someone could invent better algorithms for factoring and finding discrete logarithms and that the whole cryptography would collapse instantly. Yet another threat comes from apparent possibility to construct quantum computers which are already known to be able to solve this two particular mathematical problems with great speed. A quantum computer with mere 2000 quantum bits of memory could break PGP or RSA in a blink of an eye.

Quantum cryptography

Fortunately there exists another cryptographic technique, namely the quantum cryptography, which is completely immune to computational attacks by both classical and even quantum computers. The main characteristics of the QC are the following:

1. an eavesdropper can not have exactly the same information as the legitimate users;
2. legitimate users can calculate an upper limit to the amount of information leaked to the eavesdropper (colloquially: they can detect eavesdropping);
3. legitimate parties can obtain a highly secret key about which the eavesdropper can have at most limited amount of knowledge which limit is under control of the legitimate parties.

Quantum cryptography (QC) is a set of cryptographic primitives which rely on laws of quantum physics rather than on unproven mathematical puzzles. The most important and the most studied primitive is the quantum key distribution protocol (QKD). This protocol makes possible to establish a (highly) secret key between two parties which do not share a secret initially. It is an equivalent of (or substitute for) the classical public key protocol, except that here an interactive two-way communication is needed to establish a single key. Interactivity is the price paid for going from computational to unconditional security.

The main technical requirement for QC is existence of a quantum channel between any two points that wish to communicate a secret key - usually it means an uninterrupted mono-mode optic fiber link. Alternatively, single quanta of light can be sent over the clear air.

In this presentation we will review several interesting QC techniques pursued today.

Quantum Key Infrastructure (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 central task of QKI 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. Solution to this problem is known as Secret Sharing Scheme (SSS). Eventually QKI is to superseede completely existing classical QKI which is a very ambitious task.

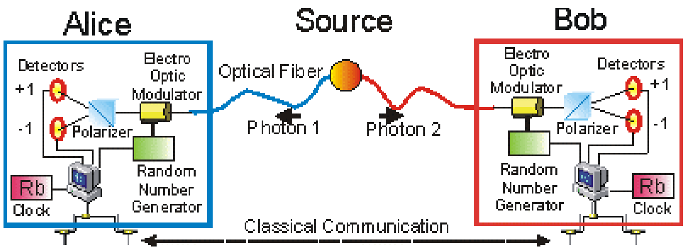
Quantum cryptography with EPR pairs

In 1991. Eckert has published his famous paper about a new cryptographic technique later named EPR. It consists of a source of entangled photon pairs delivering each of the two photons to the two legitimate parties who want to establish a secret key and/or to exchange a message in secrecy. The EPR protocol is an upgrade to the earlier BB84 invented by C.H. Bennet and G. Brassard in 1984. Such photon pairs were known for their paradoxical behavior described by so called "Einstein Podolski Rosen paradox", therefore the name to the protocol.

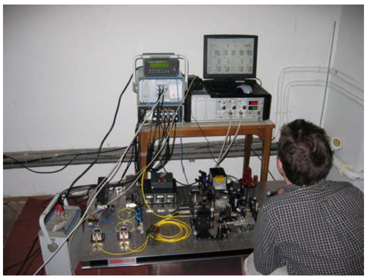
Group from Vienna univ. led by prof A. Zeilinger realized in 1999 the EPR protocol. Key to this success was a device for producing pairs of entangled photons using non-linear optical crystals. The obtained key rate was 550 bit/sec.

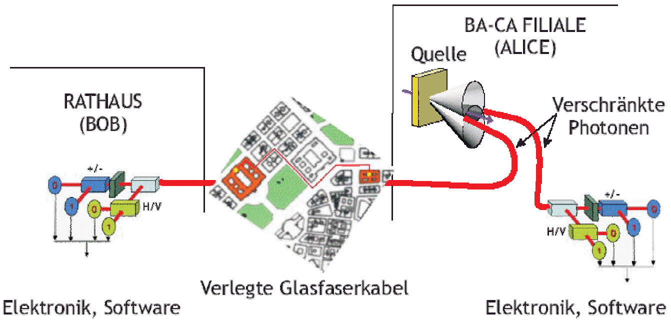
Although logically equivalent to BB84 this system has advantages:

1. intrinsic randomness of distributed key
2. extremely low probability of double photons



This technique was publicly displayed recently (on 1. April 2004.) in an demonstration of worlds first ever bank payment made by virtue of the Quantum Cryptography.

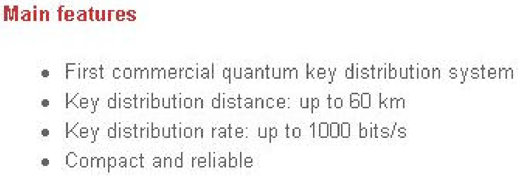




The first commercial Quantum Cryptographic machine

In summer 2002 Swiss firm IdQuantique announced the first ever commercial device for Quantum Key Distribution capable of operating over an unpreceeded distance. An actual experiment was performed was performed with two stations 67 km apart. The link between was a commercial optic fiber normally used in telephone communication. The device is capable of continuous key generation at a speed pf 1000 bits/sec.

Price: cca 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

A year and the half later, in November 2003, US based firm MagiQ announced the second ever product which uses Quantum Cryptography. "QPN Security Gateway" (code name "Navajo") 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. It can be easily integrated into any computer network. QPN's physical infrastructure is tamper-free or tamper-evident.

Range: up to 120 km. Cost of a basic set is cca. 100.000 US$

MagiQ QPN
QPN datasheet
Presenting the first commercial quantum cryptography solutions.
QPN™ Research
QPN datasheet

One incredible thing about MagiQ is that they boldly claim to have produced the first commercial Quantum Cryptographic machine and that most American news magazines reporting about the announcement of the QPN blindly follow this obvious manipulation. MagiQ has alsorecieved a medal This situation along with the retoric wrapping the European project SECOQC described below shows that the Quantum Cryptography has startled some tensions.

Swiss QKI initiative

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

A major step happened in October 2003. when IdQuantique, WISEKey and OISTE joined 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

European scientists against eavesdropping and espionage

In September 2001 European Commission has issued a 194 page long report on espionage and surveill ance network ECHELON. This network is a result of an alliance (named UKUSA) among English-speaking countries: United States, the UK, Canada, Australia and New Zealand, capturing telephone calls, faxes and e-mail around the world. ECHELON is estimated to intercept up to 3 billion communications every day.

As an answer to that EU seeks a counter-measure in deploying super-secure links based on Quantum Cryptography. One of the projects to that end is Framework 6 project for **Development of a Global Network for Secure Communication based on Quantum Cryptography** (SECOQC).

Goal of SECOQC: 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 for SECOQC: "stop significant financial losses due to industrial espionage performed by activities of the ECHELON communication surveillance and interception network".

At the same time, American NSF for 2004. gives over 300 MUS$ for research in computer security: more than for biomedicine or nano-technology.

Local activity

In the Institute Ruđer Bošković we are conducting two pilot projects concerning Quantum Cryptography.

First is about development of hardware devices and instrumentation for commercial Quantum Cryptography.

The other project is CARNet pilot project nr. 650-103/03, "Secure communication over the Internet" in which we are developing a new unconditionally secure key distribution protocol. Web site of this project is:
http://www.irb.hr/users/stipcevi/carnet2003/index.html .

Open questions

- So far the QC has been limited to distances of some 100 kilometers through optic fiber and some 40 kilometers through the air.
- Current price is approx. 100.000 US$ for a pair of transcieving stations, but one can expect drastic price cut in next 5-10 years.
- It is too early to speak about availability of products but restrictive export rules of this technology to "problematic" countries can be expected.
- Quantum signature seems problematic without some additional theoretical studies and availability of quantum memories which currently does not exist.

Conclusion

Increasing security concerns stimulate search for new cryptographic solutions. A solution which apparently offers a qualitative leap in security is the quantum cryptography. In spite the fact that it is only about one decade old, the QC has already became an emerging technology. The infrastructure needed to support quantum cryptography 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. This makes quantum cryptography even more appealing.

Preparations for the quantum key infrastructure (QKI) have already begun. For example in Europe FP6 project "SECOQC" which started on 1. April 2004. gathers 12 countries with a budget of 11.6 MEur. It will be interesting to follow further development of this intriguing technique.

Literature

[1] C. Shannon, Communication Theory of Secrecy Systems, Interna publikacija Bell Systems, 1946 (zabrana tajnosti skinuta 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/