On the security of the Quantum Key Distribution protocols

Gonzalo Álvarez and Fausto Montoya
Dep. Tratamiento de la Información y Comunicación, Instituto de Física Aplicada,
Consejo Superior de Investigaciones Científicas
Serrano144, E-28006 Madrid, Spain
and
Amalia Orúe
Facultad de Ingeniería Eléctrica, Universidad de Oriente
Santiago de Cuba, Cuba

ABSTRACT

The advent of quantum computers may compromise the security of today's conventional cryptosystems. Quantum key distribution protocols are proposed to ward off such threat; but, for the moment, the proposed quantum protocols are an hybrid of classical and quantum mechanisms and, as a consequence, they will result compromised as easily as conventional cryptography by quantum cryptanalysis.

Keywords: Cryptography, Protocols, Security, Quantum computers, Random numbers.

1. INTRODUCTION

Quantum computing is a burgeoning field of research that applies concepts of quantum physics to building more efficient computers. Although only rudimentary quantum computers have been built so far, many researchers believe that quantum computing has great potential. In recent years, there has been extensive studies about the possibilities offered by quantum computation to cryptology.

From the point of view of quantum computing researchers, after the advent of high power quantum computers, conventional cryptography may be no longer secure. Cryptanalysis tasks would be dramatically accelerated with the help of quantum computers, if such computers are ever build. The state of a quantum computer is a superposition of exponentially many basis states, each of which corresponds to a state of a classical computer of the same size. By taking advantage of interference and entanglement in the system, a quantum computer could readily perform tasks that would take much longer on classical computers.

A few general observations can be made to demonstrate it:

- Public key cryptosystems, based on the difficulty of factoring large integers and finding discrete logarithms, can be broken in a period of time growing exponentially with the key digit number using today's computers. However, with the quantum factoring algorithm proposed by Shor, running in a quantum computer, such problems could be solved in a period of time growing only quadratically with the key digit number ([SHO97]).
- Quantum mechanics can alleviate brute force attacks on secret key cryptosystems too. Grover's efficient algorithm can reduce the time needed for searching applications over unsorted data from $\mathcal{O}(N)$ to $\mathcal{O}\left(\sqrt{N}\right)$, being N the key digit number ([GRO97]). This means that the key length of secret key algorithms should be doubled to withstand this attack.
- The hash function security will be likewise compromised as shown by Brasard, Høyer and Tapp in [BRA97]. They have developed a quantum algorithm to solve the collision problem in arbitrary r−to−one functions,

reducing the computation time from $\mathcal{O}\left(\sqrt{N}\right)$ to $\mathcal{O}\left(\sqrt[3]{N/r}\right)$.

Hence, it is proposed to switch from conventional cryptographic algorithms to quantum cryptography, whose security, as stated by these researchers, "is based on fundamental principles of quantum mechanics, rather than in unproven computation assumptions" ([GOT00]).

Vernam's one time pad cryptosystem is the only cryptosystem to remain secure under these and any other foreseeable attacks, because it is the only system up to date with provable security.

2. QUANTUM CRYPTOGRAPHY

Quantum cryptography is a modern version of the one time pad system. Although thoroughly unbreakable, the one time pad still needs that the secret key be transmitted between the communicating parties. The Achilles 'heel of the traditional one time pad system lies in this need of a trusted courier for the key distribution. Quantum cryptography comes to the rescue, substituting the trusted courier by photon transmission.

The core of quantum cryptography is the fact that given a single photon in one of four possible polarization angles: vertical, horizontal, +45° and –45°, it is impossible to distinguish with certainty which polarization angle it has really.

The quantum no-cloning theorem establish that an unknown quantum state cannot be copied, because the photon state under observation would be disturbed with a polarization measurement. Consequently, the result of a measurement has a 50% of uncertainty and any copy would be unfaithful.

Precise measurement can be made if photons are transmitted with only two orthogonal angles. Suppose that photons are transmitted rectilinearly (horizontally or vertically) polarized. A birefringent calcite crystal oriented in one of the two angles will accurately separate photons in two different paths, according to their polarization. But, if diagonally polarized photons (+45° or –45°) are received as well, the same calcite crystal will classify them either as vertical or horizontal at random with equal probability.

3. QUANTUM KEY DISTRIBUTION PROTOCOLS

Bennett and Brassard proposed the first quantum cryptosystem in the early 1984, named BB84 ([BEN84]). Actually, it was a quantum key distribution (QKD) protocol, allowing two separated users to generate a random key, and then share securely. A simpler QKD scheme, the B92 was proposed in 1992 by Bennett, using only two different non-orthogonal states, instead of four ([BEN92]). Both protocols were photon polarization based schemes. The difficulty of these systems is to keep stable polarizations over long distances.

Another interesting scheme, that overcomes this difficulty, is known as Plug an Play QKD and was proposed by Muller et all ([MUL97]). It was based on phase encoding of photons and detection with Faraday mirrors, avoiding the need of controlling polarization variation effects. This scheme was successfully implemented over a 23 km long regular telecom optical fiber, with present date technology at bit rates of 1 Kb/s.

A ground-based free-space demonstration experiment in daylight over a distance of 500 m through air has been reported recently in Los Alamos National Laboratory, US ([HUG99]), showing the feasibility of secure quantum communication in ground-satellite links.

Given present date technology, bit rates of 100 bits/s can be achieved over distances between 45 km and 70 km. It is supposed that in the near future the maximum distances will be limited to 100 km, for the same bit rate ([ZBI98]).

4. THE B92 PROTOCOL

In order to appreciate how quantum cryptography works, it is instructive to examine Charles Bennett's B92 quantum key distribution protocol.

Suppose that Alice and Bob will employ a quantum channel and a classical public channel to communicate with each other. Single photons are being used to carry the information across the quantum channel, which could be either an optical fiber or free space. The public channel could be any conventional one, like a telephone line or computer network, for example.

Table 1 illustrates how such protocol works.

Alice raw key	1	0	1	1	0	0	0	1
Alice polarization	/	|	/	/	|	|	|	/
Bob raw key	0	1	1	1	0	0	1	0
Bob polarization	\	—	—	—	\	\	—	\
Photon passes Bob analyzer?	no	no	no	yes	no	yes	no	no
Distilled and shared key				1		0		

Table 1

In general, this protocol consists of a bit by bit comparison of linearly polarized single photons that Alice transmits to Bob. First, Alice generates a raw truly random bit stream, which records and transmits to Bob. She transmits single photons, in one of the two following polarization directions: vertical (to symbolize “0”) and +45^{o}(to represent “1”).

Bob also has two polarizers (analyzers), one oriented in the horizontal direction (to symbolize “1”) and the other at –45^{o} (corresponding to “0”). He selects one polarizer at random each time that Alice sends a single photon, and records whether the photon passes or not (Y or N) through his chosen polarizer and which was the polarizer he used.

Every time Bob uses the analyzer that do not agree to the polarization states sent by Alice, each result (Y or N) can occur with a probability $p_1 = 50\%$. For instance, if Alice sends a vertically polarized photon and Bob selects his +45 polarizer, there is a probability $p_2 = 50\%$ that this photon pass through his analyzers. However, if he had chosen his horizontal polarizer, he would not have detected the photon. It is clear, thus, that when Bob does detect a photon, he knows certainly that both have the same bit value.

After the transmission of all the photons, Bob sends a copy of his successes and failures (Y or N) to Alice over the public channel, not revealing the polarizers he employed to measure each bit.

Finally, Alice and Bob keep only the distilled sequence of bits for which Bob’s result was “Y” and these bits become the shared secret key. The average of successful bits is 25%, therefore 75% of original sequence would be lost, being this inefficiency the price to pay on behalf of secrecy.

In a real life system, optical imperfections and detector noise will introduce additional errors, as high as 1.6%, that should be necessarily corrected.

To guarantee an error free quantum key, Alice and Bob carry out an information reconciliation procedure, using standard error correcting codes over the public channel ([CAC97]). During this procedure some bits are revealed to an occasional eavesdropper listening at the public channel, so they must also be discarded, lowering the amount of usable distilled key bit number.

Thanks to the no cloning theorem, a passive eavesdropper (Eve) listening and retransmitting at the quantum channel, will result in 25% of errors, that will be found by Alice and Bob when performing the information reconciliation, revealing Eve's manipulations. In such case, Alice and Bob will drop the whole sequence.

4.1 PRACTICAL CONSIDERATIONS

There are a few practical issues that affect dramatically the QKD performance and security. The generation, propagation and detection of single photons are far from being a solved problem.

It is extraordinarily difficult to generate a single photon state because of the Poisson statistics of real light sources. Instead of generating photons, very tiny laser pulses are used. The experimental set-up consists of two solid estate pulsed lasers and two electro-optic polarizers, pulses are dimmed and then combined with a passive coupler. The problem is that a pulse may contain several photons, allowing Eve to divert some of them with a beamsplitter, therefore gaining knowledge of the photon polarization without being detected. To avoid this threat, laser pulses are attenuated to a level such that less than 1% of pulses contain more than one photon. The price to be paid is that the probability that the pulse contains one photon is about 10%. This means that about 90% of pulses contain no photons, thus reducing the data rate drastically.

The difficulty with polarization based systems is the need to keep stable polarizations over long distances. Due to the birefringence of optical fibers and the environment effects, the output polarization fluctuates erratically. Polarization variation effects are compensated by means of Pockels-cells or liquid crystals. To compensate the short term polarization changes the laser is switched each millisecond from quantum operation to continuous wave operation, thus originating an additional reduction of effective data rate.

Another propagation problem is that optical fibers are not perfectly circular, causing polarization dependent loses. Similar effects are present in other passive optical devices.

Measuring photon polarization is also a delicate problem. Lack of precision in the positioning of polarization analyzers may cause different measured value of p_1 and p_2 probabilities.

5. ATTACKS ON QKD PROTOCOL

It is a well proven fact that QKD protocols are unconditionally secure against passive eavesdropping attacks, ([BIH97] and [MAY98]), still taking into account that Eve can read about 1% of bits.

But no QKD ordinary protocol can stand the classic “man in the middle attack”. It is an active attack in which a malicious active attacker (Mallory) impersonates Bob while communicating with Alice and impersonates Alice while communicating with Bob, because he is sitting in between, both in the quantum channel and in the public channel, carrying out two separated communication sessions with Alice and Bob. This threat can be overcome by authentication of the public channel messages.

The preferred public channel message authentication procedure chosen by quantum computing researchers is based on the old secret key signatures proposed by Wegner and Carter ([WEG81]), rather than in public key signatures. This technique requires that Alice and Bob share a small initial secret key to begin with. The final sequence distillation and the information reconciliation procedure will consume some bits of the initial secret key step by step, thus exhausting the initial key material after a few operations. To overcome this depletion, the secret key can be replenished from the new fresh key material generated by the QKD ([HUG95]).

6. SECURITY OF QKD PROTOCOLS

There are some claims of proof of unconditional security of QKD against passive wiretaps carried out by Eve. One of the most widely accepted was given by Lo and Chau [LOC99]. However, although QKD is always performed in two stages, over a quantum channel first and over a public channel next, all proofs focus on the quantum channel only. But it will be naive to think that this kind of attacks are the only threat against a quantum cryptographic system. Eve or Mallory could try to attack the public channel instead of the quantum channel.

The security of a system is as weak as the security of its weakest part. For QKD to work, a short initial key material must be interchanged between Alice and Bob. And this initial key intended for mutual authentication must be shared using a classical protocol, before entering any quantum negotiation.

According to the previous section, the whole security of quantum cryptography relies on the authentication procedure of the conventional channel. As described in [WEG81], the authentication mechanism is a hash function of the message and a portion of the short initial key shared by both partners. Thus, if the hypothetic quantum computer announced by the quantum computing researchers will be ever built, the security of this kind of signature will also be cast in doubt.

Researchers in quantum computing state that the advent of quantum computers “will lead to a retroactive total security break with catastrophic consequences". But they remark that "Ironically, quantum mechanics also comes to the rescue", thanks to quantum cryptography ([HOI98]). This assertion is a sophism, because, at least, the security of quantum cryptography is reduced to the security of a conventional cryptosystem, supposedly insecure under a quantum attack.

If for some lucky reason the Wegner algorithm resulted secure against a quantum attack, what is the quantum cryptography utility?, to which extent does it help to the communications security? In that case it will suffice to use conventional cryptography based in the Wegner algorithm, thus avoiding the messy, slow and inefficient quantum protocols.

Next, we must point out the problem inherent to the way of replenishing the exhausted short initial key, with new fresh key material generated by the QKD. The use of an old key to negotiate a new one, that will substitute the former, is a cryptographic bad practice that should be by all means avoided.

It is self evident that if the short initial key, or any intermediate key, is compromised, then all the future transactions will be compromised as well, leading to a permanent security break.

Theoretical demonstration of unconditional security against passive eavesdropping attacks of QKD protocols assumes that the final distilled quantum key sequence is perfectly random. But it should be remarked that randomness of practical implementations rely on the mechanical accuracy of optical devices and mechanical absolute perfection is an impossible goal.

Low (and perhaps asymmetrical) detection probability of different polarization states of laser pulses, unequal pulse amplitudes of different lasers, inaccuracies in the polarization variation effects compensation, polarization dependent loses and uneven polarization analyzers positioning, all together, may lead to an imbalanced distribution of ones and zeros of the finally distilled quantum key, thus not satisfying the inexcusable Golomb randomness postulates ([GOL67]). Certainly, Eve will exploit this fact to mount an attack against the key. Unfortunately, quantum cryptography researchers do not seem to be aware of this threat and no suitable measures are proposed to ward it off, if there exist any.

Raw bit sequences produced by real life quantum number generators are not balanced, bit distributions of about 40/60 of ones and zeros are typical ([STE99]). But cryptographically secure unbiased sequences can be build, starting from the raw imbalanced ones, by appropriate mathematical procedures ([PER92]).

Obviously, QKD information reconciliation procedures may include a method to test and fix any bias of the raw quantum key. But it is unclear, until now, that such task could be performed using a public channel without revealing any information to Eve.

Finally, unless a remarkable breakthrough in quantum communications speed takes place, QKD will never be able to generate enough key material as to encrypt big volumes of information, such as real time audio or, worst, video. Even though considerably large improvements in speed are accomplished, in the mid term, QKD will only be useful for classical key distribution, thus depending again on classical cryptography for the encryption of bulk information.

7. CONCLUSIONS

Quantum cryptography must be regarded as a very interesting field of applied physics research, but not as a solid spare candidate for the present day cryptographic techniques. This observation will hold true as long as its security is just sustained on the security of the conventional cryptographic algorithms that it is intended to substitute.

Today's quantum cryptography is an hybrid of classical and quantum mechanisms and much work must be done yet to achieve secure full quantum cryptographic protocols, not just QKD protocols.

More attention should be paid to practical implementation aspects, heavily dependent on the optical devices mechanical precision, that can affect adversely the quantum key statistics and consequently its security.

Therefore, it would be better to pay attention to well established fundamental principles of cryptography, rather than entrusting unproven quantum mechanics statistical assumptions.

Acknowledgements

This work was supported by CICYT, Spain, under grant TEL98-1020 and by MEC under Programa de estancias de Científicos y Tecnólogos Extranjeros en España.

REFERENCES

[BEN84] C.H. Bennett and G. Brassard, "Quantum cryptography: "Public key distribution and coin tossing", in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, (1984) 175-179

[BEN92] C.H. Bennett, "Quantum cryptography using any two nonorthogonal states". Phys. Rev. Lett. **68** (1992) 3121-3124

[BIH97] Eli Biham, Tal Mor, "Bounds on Information and the Security of Quantum Cryptography", Phys. Rev. Lett. **79**, (1997) 4024-4037

[BRA97] Gilles Brasard, Peter Høyer and Alain Tapp, "Quantum Algorithm for Collision Problem", Los Alamos preprint archive quant-ph/9705002

[CAC97] Crhistian Cachin and Uely Maurer, "Linking information reconciliation and privacy amplification". *Journal of Cryptology*, **10** (2) (1997) 97-110

[GOL67] S. Golomb, "Shift Register Sequences". Prentice-Hall Inc. 1967

[GOT00] Daniel Gottesman and Hoi-Kwong Lo. "From Quantum Cheating to Quantum Security". Phys. Today **53** (11) (2000) 22-27

[GRO97] L. K. Grover, "Quantum Mechanics helps in searching for a needle in a Haystack". Phys. Rev. Lett. **79** (2) (1997) 325-328

[HOY98] Hoy–Kwong Lo, "Quantum Cryptology", in Introduction to Quantum Computation and Information, World Scientific (1998)

[HUG95] Richard J. Hughes et all. "Quantum Cryptography". Contemporary Physics **36** (1995) 149-167

[HUG99] R. Hughes and J. Nordholt, "Quantum cryptography takes to the air". Phys. World **12** (5) (1999) 31-35

[LOC99] H.-K. Lo and H. F. Chau, "Unconditional Security Of Quantum Key Distribution Over Arbitrarily Long Distances", Science **283** (1999) 2050-2056

[MAY98] D. Mayers, "Unconditional Security in Quantum Cryptography", Submitted to Journal of ACM; arXiv:quant-ph/9802025 v4 (1998)

[MUL97] A. Muller et all, "Plug and Play systems for quantum cryptography", App. Phys. Lett. **70** (7) (1997) 793-795

[PER92] Y. Peres. The Annals of Statistics **20** (1992) 590-597

[SHO97] P.W. Shor, "Algorithms for Quantum Computation: Discrete logarithms and factoring", SIAM J. Computing **26** (1997) 1484-1509

[STE99] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard and H. Zbinden. "Optical Quantum Random Number Generator", quant-ph/9907006, (1999)

[WEG81] M.N. Wegman, J.L. Carter, "New hash function and their use in authentication and set equality". Journal of Computer and System Sciences, **22** (1981) 265-279

[ZBI98] H. Zbinden, H. Beechman-Pasquinucci, N. Gisin and G. Ribordy "Quantum cryptography", Appl. Phys. B **67** (1998) 743-748