Quantum Cryptography: A Short Historical overview and Recent Developments

Ioannis P. Antoniades

Informatics Department, Aristotle University of Thessaloniki, Thessaloniki 541 24, Greece

Vasilios G. Chouvardas

Informatics Department, Aristotle University of Thessaloniki, Thessaloniki 541 24, Greece

Miltiades K. Hatalis

Informatics Department, Aristotle University of Thessaloniki, Thessaloniki 541 24, Greece

and Georgios L. Bleris

Informatics Department, Aristotle University of Thessaloniki, Thessaloniki 541 24, Greece

Abstract

This paper presents a short review of theoretical developments in Quantum Cryptography, a field that has attracted significant attention and multi-disciplinary scientific effort mainly in the past ten years. Since its birth (about two decades ago) advances in Quantum Cryptography have yielded important results from a conceptual as well as practical point of view. Today Quantum Cryptography is seen as a field that is most likely to be the first to produce commercial applications based solely on quantum first principles. We discuss the importance of formal mathematical methods in practical advances in cryptography (both classical and quantum). We present a short historical overview of theoretical milestones in Quantum Cryptography. Finally we present some recent developments that appeared in the past couple of years.

Keywords: *Quantum Cryptography, information theory.*

1. Introduction

The previous century has been marked with by three major scientific revolutions: Quantum theory, information theory and Relativity. All three have given results that not only are important from a practical point of view (quantum theory and relativity have accurately explained macroscopic and microscopic experimental facts not explained by any classical theory) but they presented revolutionary impact on the entire classical framework of thought. Quantum theory introduced a non-classical logical framework upon which description of physical reality is based; the state of a system may exist in linear superpositions of orthogonal state vectors (a yes-no state system may exist in states that are linear superpositions of 'yes' and 'no'!) and collections of physical systems may exist in collective states in which knowledge of properties of the individual parts is not accessible to measurement (entanglement). Information theory on the other hand, introduced the concept of information and showed that any computational process is a physical process and vice versa. Moreover, information theory has made conceptually profound statements about computability and decidability of a well-posed mathematical problem and defined computational complexity in formal terms. Finally, relativity has changed the way we view the geometry of space and time. As these basic theories were developed quite independently of one another, it was natural for scientists to attempt to combine their lines of thought. In several respects this proved to be a very difficult task. Until today, for example, there is no known theory of gravity consistent with both relativity and quantum theory. On the other hand, attempts towards a quantum information theory have left open questions in the foundations of classical information theory such as whether Church-Turing thesis holds also for quantum computational processes. Moreover, up until twenty years ago, no-one had realized that quantum theory might provide completely non-classical, yet practically realizable, means of computations that would offer an exponential speed-up relative to known classical algo-

Corresponding author:V.Chouvardas:
email: vchou@csd.auth.gr

rithms. For example, the well-know algorithm of Shor [1] was shown to solve the problem of factorization of a large integer in polynomial time, whereas no known classical algorithm exists that can achieve this task. Finally, the proof of existence of quantum error correction codes in the past decade has provided optimism that the creation of a powerful computer operating merely on quantum principles is possible in practice.

Among the fervent enthusiasm in the field of quantum information theory the possibility of defining cryptographical methods in completely quantum terms was also quite early realised [2,3]. The emerged field of Quantum Cryptography (QC) "lies at the intersection of quantum mechanics and information theory and that, moreover, the tension between quantum mechanics and relativity—the famous Einstein-Rosen-Podolsky (EPR) paradox (Einstein *et al.*, 1935)—is closely connected to the security of QC" [4,5]. QC has provided cryptographical protocols with provable unconditional security independent on future technological advancements. This is in contrast to all but one (the one-time pad) classical cryptography protocols for which only *computational* security is proved, i.e. security is based solely on the computational difficulty of solving certain 'hard' problems for which no polynomial-time algorithms is thought to exist (but not provably so). Despite theoretical proofs of security of QC methods under ideal conditions, security of QC protocols is (only) compromised by unavoidable technological shortcomings of the apparatus used for their practical implementation (noisy communication channels, deficiencies in detectors and elementary particle sources, etc). Most of the efforts in the past years are to improve security bounds of QC protocols operating in non-ideal conditions. It is encouraging that, despite the fact that QC protocols do not guarantee perfect security in a non-perfect world, the degree of security achieved can still be much higher than their classical counterparts. Furthermore, QC protocols have now been experimentally demonstrated many times using present technology a fact that has lead to the wide belief that QC will provide the first commercial applications of systems functioning solely on basic quantum mechanical principles in the near future. In this paper, we first discuss the importance of formal mathematical methods for the advancement of both classical as and quantum cryptography. We then give a short overview of basic QC principles and protocols. Thirdly, we give a short review of the most important historical findings. Finally, since a very thorough review of both theoretical and experimental achievements in QC has been published in 2002 by Gisin *et. al.* [5], we selectively present some major theoretical developments in the past couple of years.

1. Formal mathematical methods and Cryptography

"Cryptography is about communicating in the presence of an adversary" [6]. Modern cryptography has been based on the principle that security of a cryptographical method (algorithm) does not have to depend on keeping the method itself secret. In fact, the exact algorithm upon which a cryptographical method is based for all practical purposes is required to be publicly known. What is necessarily kept secret is a short message (the 'key'), which is shared among valid users of the protocol and not accessible to an invalid one. Discrete mathematics, group theoretical methods and function theory have provided the means to achieve a great variety of cryptographical tasks such as encryption, message authentication, digital signatures, secure electronic monetary transactions etc. based on the above requirement. Cryptography, on the one hand qualifies as a field of applied mathematics, however, it is important to stress that formal mathematical proof in Cryptography is not only an academic matter, but it is absolutely crucial for whether a cryptographical method can be trusted for practical applications: A cryptographical protocol for digital signatures, for example, must be proved secure if it is ever to trusted for real-life applications and if this is not possible, mathematics should at least quantify security restrictions or define security prerequisites.

It is a bit embarrassing that no known provably secure cryptographical method exists, in the sense that an adversary with unlimited resources (computational power) is guaranteed not to be able to by-pass the protocol. The only exception is the "one-time pad" encryption method, in which a binary message is encrypted by XORing each of the bits with a random bit sequence (the key) shared by all valid users. New messages should be encrypted with different random bit sequences. This method guarantees that the probability of an adversary obtaining the correct message given the encrypted text (cipher-text) is exponentially small in the size of the message (and thus the key). However, the one-time pad is totally impractical for most real-life applications: First, the key must be as long as the total length of all the messages that are ever to be exchanged and secondly, valid users should share the exact same key, which would compromise security if this (long) key must be somehow distributed to distant users.

The most widely used *public-key* cryptography methods (mainly used in digital signatures and

message authentication), on the other hand, are only proved to be *computationally* secure. The security of these methods is based on the present inability to solve certain 'hard' mathematical problems, such as the factorisation of a very large integer, in polynomial time. However, the existence of a classical polynomial time algorithm that would solve these problems has not been disproved. This means that a sudden mathematical breakthrough that would reveal such an algorithm would cause all systems based on these methods to collapse overnight! The uneasiness that this possibility causes was further enhanced when in 1994 Shor published an algorithm based on a quantum computer that can factorise a large integer in polynomial time [1].

It is apparent how much relief it would bring if a direct proof of the fact that there exist decision problems in NP (the set of all decision problems for which the solution may be *verified*, once found, in polynomial time) that are not in P (the set of all decision problems whose solution can be *found* and *verified* in polynomial time). For now it is known that $P \subseteq NP$.[1]

Even if it is proved that no classical algorithm can be found that can solve a computationally hard problem in polynomial time, the threat from a realization of a quantum computer always exists.

2. Quantum Cryptography principles and the BB84 protocol

The first QC protocol appeared in 1984 [2], although ideas closely related to QC were presented by Wiesner about a decade earlier [3].[2] The principles upon which these ideas were based come from two of the most basic QM facts:

(1) One cannot make a measurement of a quantum state without perturbing the state, unless the state is an *eigenstate* of the operator corresponding to the measured quantity. (2) One cannot create a perfect copy of an unknown quantum state [7]. These two facts nicely lead to the possibility of performing secure communications by encoding information with quantum means. Suppose that Alice (usual name for the legitimate sender of a message) wants to send a message M to Bob (usual name for the recipient) under presence of (malicious) Eve (usual name for an eavesdropper). Alice may encode such a binary message as a sequence of two distinct quantum states ψ_1 and ψ_2. These states can be realized by (for example) two different polarization states of photon particles and send them to Bob through a classical communications channel. Eve may also obtain the same sequence by intercepting the sent sequence on the channel measuring the states and resending to Bob. However, by principle (1) Alice would have inadvertently disturbed the states, a fact that Alice and Bob can easily discover latter. Eve can neither make copies of the states and measure them at her ease later (something that is trivial for classically encoded information), because this is not allowed by quantum principle (2). It must be stressed that in order for (1) to hold, states ψ_1 and ψ_2 must be *non-orthogonal*, otherwise Eve would cause no disturbance by measuring in the proper basis. Let us now describe the first implementation of a quantum cryptography protocol that appeared in 1984 known as the BB84 Quantum Key Distribution (QKD) Protocol:

Alice generates a random bit string. She then encodes the string using two *pairs* of *orthogonal* quantum states: ψ_{11}, ψ_{12} ($\psi_{11}\cdot\psi_{12}=0$) for the first pair and ψ_{21}, ψ_{22} ($\psi_{21}\cdot\psi_{22}=0$) for the second. States within the same pair are orthogonal whereas, any two states chosen from *different* pairs must be *non-orthogonal*. For example, ψ_{11}, ψ_{12} can be the left-right polarization states of a photon and ψ_{21}, ψ_{22} the $+45^o$ -45^o polarizations. Either one of ψ_{11}, ψ_{12} will encode bit 0 and either one of ψ_{21}, ψ_{22} bit 1. Alice randomly chooses one of the 4 states for each bit and sends it to Bob.

Bob measures each individual state also choosing randomly between the two bases using a different random number generator than Alice. If for a particular bit he chooses the same basis as Alice, then he will get the same state as the one sent by Alice. If he chooses a different basis, then he will get 50% uncorrelated results. In total, Bob will have an average of 25% error rate in the bit string he obtains.

This error rate is large but can be corrected in a straightforward manner: After his measurements Alice and Bob announce over a public channel the basis they measured each one of the bits, without revealing the results of their measurements. Therefore, each time they used a different base, they discard the corresponding bit keeping only those for which they measured in the same basis. In this way, they get a 50% reduced size final random bit sequence upon which they both agree. This key sequence may now be used as the secret key to some symmetric classical encryption scheme (such as DES) or in one-time pad communications.

Since Eve cannot make copies of the sequence and since after interception she must send something to Bob (otherwise she would be easily de-

[1] Conversely, the proof of the opposite, i.e. that NP=P would cause much distress.

[2] Actually, Wiesner published his early thoughts on QC in the 70's as late as 1983.

tected), the best she can do is receive each bit, measure it and then send a different photon prepared in the same state as the results of her measurement. In this way Eve would have a 50% chance to send the same state as the original Alice sent. In such cases Bob and Alice will not be able to discover her intervention. However in the rest 50% of the cases Eve will choose an opposite base. Thus, she will introduce an *extra* error in the final sequence obtained by Bob. This will result in an extra 25% error in Bob's sequence even after Alice and Bob compare bases. Thus Eve's intervention would be detected, in which case they would abort communications.

Privacy amplification

The above protocol can be proved secure *under ideal conditions*, since any intervention by Eve is guaranteed to be detected for long enough bit sequences. However, in practice the apparata (photon source, photon detectors) used by Alice and Bob and the classical communication channel (optical fibre, free space) are not ideal. Basic problems are: (i) Alice's photon source is assumed ideal if it can produce single photons. In practice multiple photons may be produced in the same state, giving Eve the advantage of keeping one copy for herself. (ii) The communication channel is noisy. Noise causes decoherence of single particle states a fact that introduces an error that Bob must correct. (iii) Bob's photon detector may also 'fire' when there is no incoming photon, giving the so called *dark counts*. These problems can significantly compromise the security and fidelity of the protocol. It must be noticed, however, that these are technological problems and not inherent problems of the quantum protocol itself. Much of the challenge faced by QC research is to devise methods to ensure security even in non-ideal conditions.

In this section we discuss the security problem caused by noisy communication channels and how it is dealt by the BB84 protocol. The problem is that a noisy channel would increase the error rate in the string Bob obtains after step 2 above. If this additional rate is ε%, and assuming that Eve measures only to 4ε% of the signal sent by Alice, in the end Eve would be able to obtain 2ε% of the information contained in the signal causing an additional error of ε% after Alice and Bob perform step 3. However, Bob now does not know if this error was due to an Eavesdropper or due to noise in the channel. The only solution would be for Alice and Bob to measure the error rate of the channel and thus be able to detect statistical deviations from it. Finally, Alice and Bob may perform some additional steps that would reduce Eve's information about the key down to zero at the cost of obtaining an even shorter key. This procedure is called *privacy amplification* [8,9] and it has been proved that it would work only if Eve has initially less information about the key than Bob [5]. Whether the latter condition holds can be detected by the legitimate users as follows: After step 3 is performed, leaving Alice and Bob with the reduced key, they publicly announce a random subset of their bits comparing the results. This way they can estimate the error rate. Actually, they estimate the joint probability distribution P(a,b) of random variables a, b, i.e. the random bits of the keys possessed by Alice and Bob respectively. Then, they can calculate the mutual information, I(a,b) shared among Alice and Bob and also the mutual information $I(a,\varepsilon)$ between Bob and Eve. Of course, they discard all the bits that they publicly announced. If condition

$$I(a,\varepsilon) \leq I(a,b) \quad (1)$$

is not satisfied, they abort, else they continue by applying some classical error correction techniques that would a) correct all errors (*error correction*) and b) reduce Eve's information down to zero (*privacy amplification*). An example of such technique is the following: a) error correction: Alice chooses pairs of bits and announces their XOR value (sum modulo 2). If Bob has the same XOR he replies 'accept' else 'reject'. In the first case, they both keep the value of the first bit and discard the second, whereas in the second case they discard both bits. After, this error correction step Alice and Bob possess identical (shorter) keys. b) privacy amplification: In order to reduce possible information Eve may possess on the final reduced size key, Alice randomly chooses pairs of bits and computes their XOR value. Instead of announcing this value, she announces only which pairs of bits she chose. Then, both Alice and Bob replace the two bits by their XOR value. In this way, Alice and Bob end up with a yet shorter (error-free) key, but at the same time they effectively reduce Eve's information down to an arbitrarily short value. This is because, if Eve has some partial information about any of the two bits, she has less information about their XOR value. For example, if Eve knows the value of the first bit and nothing about the second, then she has zero information about their XOR. Equivalently, if she knows the values of both bits with 60% probability then she would know the value of their XOR only with probability $(60\%)^2 + (40\%)^2 = 52\%$. In practice, more efficient algorithms than the one presented here are used (e.g. [10].)

Other protocols

It has been proved that privacy amplification can also work even if condition (1) is not satisfied,

assuming a two-way communication between Alice and Bob (i.e. Bob may send signals back to Alice as well). For such protocols see [11-12].

The BB84 protocol works with a 4 state quantum system. It has also been shown that QKD may be equally achieved by a two state system [13]. A *six-state* protocol has also been proposed, which provides better accuracy rates than the two and four-state protocols and reduces Eve's optimal information gain [14,15]. Another conceptually interesting historical protocol is the Einstein-Podolsky-Rosen protocol proposed by Artur Erkert in 1991 [16] and came as an independent invention of Quantum Cryptography using a different route. This protocol replaces the channel shared by Alice and Bob by a common trusted source emitting *maximally entangled* photons to both Alice and Bob. The security of this protocol is based on the violation of Bell's inequalities, i.e. of the inability to reproduce measurement results on entangled quantum states by any classical local theory.

3. Eavesdropping in imperfect QC environment and ultimate security proofs

Imperfect qubit sources and imperfect qubit detection on the parts of Alice and Bob present additional security compromises in any practical realisation of a QC protocol. The security proof for QC with perfect apparatus and noise free channels is straightforward. Assuming perfect apparatus, conditional security can also be proven in case of noisy channels, the only limitation coming from the error rate of the channel. One can obtain theoretical upper bounds to the error rate due to noisy channels consistent with condition (1) for one-way communications. With two-way communications these bounds are father relaxed. It has been proven that (e.g. in [5] the technique of privacy amplification presented above would reduce Eve's information down to zero, if the *Quantum Bit Error Rate* (QBER) is less than

$$\mathrm{QBER} \le \frac{1-1/\sqrt{2}}{2} \cong 15\% \quad (2)$$

In case of two-way communications this bound may increase to 30% [17,18]. Eq. (2) holds only when Eve performs single-qubit attacks (*individual attacks*). However, possibility exists for *collective attacks* on more than one qubits called also *coherent* attacks or *joint* attacks. How much extra advantage Eve can gain under these attacks is still an open question. However, an upper bound for security (again assuming perfect apparatus) can be calculated [5,19,20] yielding a maximum QBER of about 11%.

However, other sources of error besides the communication channel provide Eve with an advantage. For example, if Alice's photon source produces multiple photon pulses (all encoding the same qubit in the same quantum state), Eve may keep one photon for herself and send the others to Bob. In single photon pulses Eve keeps the copy and sends nothing to Bob. If Eve uses a more efficient communication channel than Alice, then in principle Bob will not be able to detect the reduction in incoming qubit rate, which may be attributed to channel loss instead. Moreover, if the 'dark count' rate of Bob's faulty detectors is comparable to channel losses, then Eve may obtain full information about the signal without being detected. Of course, Eve must be able to measure the number of photons in a multiple photon pulse without disturbing the qubits. In principle, this is possible through what are called *quantum non-demolition measurements*, i.e. measurements that determine the number of photons without affecting the quantum state. Under present technology such measurements are not possible, but they are a foreseeable possibility for the near future. This possibility has received significant attention in recent literature since it presents some realistic scenarios for eavesdropping. The debate is not yet settled. Gisin argues that the assumption that Eve possesses unlimited technological power is too strict and unrealistic. For example, in order to rage a quantum non-demolition attack, Eve must (i) perform nearly perfect non-demolition experiments (an impossible task today but foreseeable in the future), (ii) maintain the quantum state of the qubits she intercepts until Alice and Bob reveal their bases (this would require a lossless quantum loop circuit or quantum memories that would stay decoherence-free for unlimited time, a difficult task since Alice and Bob may wait for an adequate time until they reveal their bases) and (iii) Eve would have to use a more efficient communications channel than Alice and Bob. Especially the latter requirement is quite optimistic for Eve. Gisin argues that the efficiency of communication channels is limited by physical reasons rather than technological ones and thus, Eve cannot be expected to do better than Alice and Bob in practice.

The discussion in this section points to the conclusion that *ultimate proofs* of security of QC require security under non-ideal conditions for Alice and Bob but ideal technological conditions for Eve, a somewhat unrealistic assumption. In any case, ultimate proofs must be distinguished from

practical ones where technological limitations on Eve are also present.

Despite the above, a more 'realistic' class of attacks on QC protocols have been recently proposed [21-23], the *beam-splitter* attack. According to this Eve splits all pulses in two, analyzing each half in one of the two bases, using photon-counting devices able to distinguish between pulses with 0, 1, and 2 photons. This requires nearly perfect detectors, but at least one does not need to assume technology completely out of today's realm. Whenever Eve detects two photons in the same output, she sends a photon in the corresponding state to Bob. In all other cases she sends nothing. An analysis of Eve's information gain is given in [5]. Here we state the conclusion, namely that Even can undetectably obtain twice as much information on the signal than with a simply intercept-resend strategy. Practical solutions to limit Eve's information exist, at the cost of reducing the transmitted bit rate of the communications channel. This way Eve would be limited in that she would be able to attack smaller portions of the signal in order to remain undetected.

In the end, multi-photon pulses do not constitute a threat to security; there are counter-measures to limit Eve's advantage to arbitrarily small amounts unfortunately at the cost of arbitrarily lowering the achieved secret bit rate.

Despite the fact that QC can be proven secure ideally, based on quantum principles alone, the technological implementation would always be questionable. In this sense the relationship

Infinite security $\Rightarrow$ infinite cost $\Rightarrow$ zero practical interest

(as presented by Gisin *et al*. [5]) is very relevant in QC systems as well. Then, what is the reason one would be interested in QC over classical methods? There are clear reasons: (i) "It is much easier to forecast progress in technology than mathematics" [5]. The possibility that a scientific mathematical breakthrough would render all classical public-key cryptography obsolete overnight is negligible for QC. The security of the latter depends only on technological limitations. (ii) The security of QC depends on technology possessed by an adversary at *the time of realisation of the protocol*. In the classical case, an enemy can 'store' a secret until technology advances may enable the breaking of the encoding. This is simply not possible with information encoded with quantum means. The latter point is, of course, relevant to secrets whose value is maintained through large time periods.

4. Some recent developments in QKD

An interesting proposal on how to overcome the beam-splitter attack in the case of high-detector loss was published by Hwang [24]. The author proposed that Alice intentionally (and randomly) replaces part of her qubits with multi-photon pulses (decoy pulses). Then, Alice and Bob estimate the loss in the decoy pulses. If they are significantly less that signal losses, they abort the protocol. The author argued that the security bound of the QC protocol is significantly improved provided that the decoy source and signal multi-photon statistics are designed to be as similar as possible.

A recent work by Barbosa et. al. [25] has demonstrated a multi-base QC system for message communication (not just key distribution). This protocol enables Alice to encode a binary message by mapping the bits to a set of M bases, according to a predetermined short key K, initially shared by Alice and Bob. The authors prove that this protocol is secure in noisy environments under cipher-text only attacks provided that M is large enough. This protocol has also the nice feature that detection of Eve's intervention is not necessary for security, i.e. there are no conditions under which the protocol must be aborted. Another nice feature is that in this protocol channel noise works to the advantage of Alice and Bob and to the disadvantage of Eve.

Another interesting cryptographic task, apart from secure message communication is *bit commitment*. In bit commitment one party (Alice) must decide on the value of a single bit (1 or 0) and commit to this value without actually revealing the value to Bob. At a later time, when Alice decides will reveal the value she chose so that Bob will be able to prove that this was indeed the value Alice committed to. For a successful completion of the protocol, Bob must not be able to have any information about the value Alice chose, before she actually reveals it and at the same time Alice must not be able to undetectably reveal a different value from what she initially chose. Bit commitment is an important protocol, because it finds applications in many other cryptographic tasks, such as playing a game of chance from a distance. It is known that there is no classical algorithm for secure bit commitment (only computationally secure algorithms exist). Unfortunately, quantum bit commitment was also shown to be an impossible task. Remarkably, a recent work by Adrian Kent [26] has proved that quantum *string* commitment is possible. String commitment is a task under which Alice commits N logical bits of information so that Bob may at most extract $M<N$ bits prior to Alice revelation.

Security is defined as follows: Given security bounds M and ε, the probability that Bob extracts more than $N'=N-M$ bits prior to Alice's revelation as well as the probability of Alice cheating when revealing any bit both are less than ε. We do not present the details of Kent's quantum protocols here, but instead comment on a very interesting fact: whereas classically, bit string commitment is equivalent to single bit commitment (any multiple bit encoding scheme may be used to encode a single logical bit), this is not the case with quantum encoded information. Quantum single bit commitment and quantum string commitment are not equivalent problems. Thus, one cannot do the first while the second is possible. This demonstrates the fact that equivalence in classical cryptographic tasks does not necessarily imply equivalence in their quantum counterparts.

5. Conclusions

In this paper we attempted a short review of the foundations of quantum cryptography and main theoretical milestones. QC protocols have certain advantages over their classical counterparts in that QC are proven secure under ideal technological implementation, whereas security proofs extent to certain cases of non-ideal implementation. The importance of mathematical proof from a practical point of view was demonstrated. Ultimate security is not likely to be achieved, as technological implementation may never be perfect. The QC paradigm still remains strong, however, in that it transfers the security burden to the technological rather than the theoretical arena, which is preferable in the sense that technological advances are slower and better predictable.

It is also remarkable that research into QC has also offered deeper insight into the principles of quantum information theory as well as classical cryptography itself. On the other hand, there are still several open questions: Firstly, complete and realistic analyses of the security issues are not available. There exist formal calculations of security bounds under specific conditions, but these analyses have not reached a satisfactory degree of generality. Secondly, comparison between different QC implementations is not adequately based on quantitative indicators. Thirdly, there exist experimental demonstrations of quantum key exchange over distances of the order of a few tenths of kilometres but these distances are two limited and the bit rates are still too low. Despite these facts the general belief is that QC will present the first commercial applications of systems based fully on quantum mechanical principles.

References

[1] Shor, P5. W., (1994), *Proceedings of the 35thSymposium on Foundations of Computer Science*, , pp. 124–134. Goldwasser, S. (Ed). IEEE Computer Society, Los Alamitos, California.

[2] Bennett, C. H., and Brassard G.,(1984) In*Proceedings of the IEEE Internationa Coference on Computers, Systems and Signal Processing*, Bangalore, India, pp.75–179. IEEE, New York.

[3] Wiesner, S., (1983), *SIGACT News* **15**, 78–88.

[4] Einstein, A., Podolsky, B. and Rosen, N., (1935), *Phys. Rev.* **47**, 777–780.

[5] Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., (2002), *Rev. Mod. Phys.*, **74**(1), 145-196.

[6] Goldwasser S., Bellare, M. (1996), Cryptography: Lecture Notes, (compiled for a summer course in cryptography taught at MIT in July 1996).

[7] Wootters, W. K., and Zurek, W. H., (1982), *Nature* (London) **299**, 802–803.

[8] Bennett, C. H., G. Brassard, and J.-M. Robert, (1988), *SIAM J. Comput*. **17**, 210–229.

[9] Bennett, C. H., G. Brassard, C. Crepeau, and Maurer, U. M., (1995), *IEEE Trans. Inf. Theory* **41**, 1915–1923.

[10] Brassard, G., and Salvail, L. (1994) In: *Advances in Cryptology—EUROCRYPT '93 Proceedings*, Lecture Notes in Computer Science, Vol. 765, pp. 410. T. Helleseth (Eds). Springer, New York.

[11] Maurer, U. M., (1993), *IEEE Trans. Inf. Theory* **39**, 733–742.

[12] Maurer, U. M., and Wolf, S., (1999), *IEEE Trans. Inf. Theory* **45**, 499–514.

[13] Bennett, C. H., (1992), *Phys. Rev. Lett.* **68**, 3121–3124.

[14] Bruss, D., (1998), *Phys. Rev. Lett.* **81**, 3018–3021.

[15] Bechmann-Pasquinucci, H., and Gisin, N., (1999), *Phys. Rev. A* **59**, 4238–4248.

[16] Ekert, A. K., (1991), *Phys. Rev. Lett.* **67**, 661–663.

[17] Gisin, N., and Wolf S., (2000), *Advances in Cryptology—Proceedings of Crypto 2000*, Lecture Notes in Computer Science, Vol. 1880, pp. 482–500. Bellare, M. (Ed.) Springer, New York.

[18] Gisin, N., and Wolf, S., (1999), *Phys. Rev. Lett.* **83**, 4200–4203.

[19] Shor, P. W., and Preskill, J., (2000), *Phys. Rev. Lett.* **85**, 441–444.[20]Lo, H.-K., and

Chau, H. F., (1999), *Science* **283**, 2050–2056.

[21] Dusek, M., M. Jahma, and Lütkenhaus, N., (2000), *Phys. Rev. A* **62**, 022306.

[22] Lütkenhaus, N., (2000), *Phys. Rev. A* **61**, 052304.

[23] Felix, S., A. Stefanov, H. Zbinden, and Gisin, N., (2001), *J. Mod. Opt.* **48**, 2009–2021.

[24] Hwang, W. Y., (2003), *Phys. Rev. Lett.* **91**, 057901.

[25] Barbosa, G.A., Corndorf, E., Kumar, P. and Yuen, H. P., (2003), *Phys. Rev. Lett.* **90**, 227901.

[26] Kent, A., (2003), *Phys. Rev. Lett.* **90**, 237901.