0.1 QUANTUM CRYPTOGRAPHY (*O. HADERKA, M. HENDRYCH, M. DUŠEK*)

For ages people have wished to find a way to communicate in secrecy so as to allow nobody to overhear their messages. This wish or desire may come true with the aid of cryptography. Cryptography may be defined as the art of writing and deciphering messages in code.

The use of cryptography in everyday life has grown enormously during recent years. The outburst of electronic communications between banks, state agencies and various institutions handling private data, as well as the fast development of e-business on the Internet, has lead to a huge increase of demand for secure cryptographic methods and devices. Today most of cryptographic tasks are solved with the help of cryptosystems [1] that rely on computational complexity, e.g., on the difficulty to factor large numbers. However, advances in mathematical algorithms and computing power compromise the security of these methods, which is maintained by continual lengthening of cryptographic keys. Classical cryptography also faces an increasingly serious menace arising from the construction of quantum computers. Algorithms capable of breaking public-key ciphers have already been developed [2]. Although the construction of a practical device is still hypothetical, experimental advances are very fast. Another threat to classical systems comes from single-purpose massively parallel optoelectronic devices [3].

In contrast to classical cryptographic methods, the security of quantum cryptography is based on the fundamental laws of physics. It is guaranteed by the Heisenberg uncertainty principle and is independent of any mathematical or technological developments.

Today it is only a little more than one decade since the first prototype of quantum cryptographic apparatus came into existence [4]. In the meantime, quantum cryptography has become a well-known technique of communication in a provably secure way, and together with an intensive research in the field of quantum computers it has given rise to a whole new branch of science—quantum information theory [5]. Viewed from this perspective, quantum cryptography today is only a subset of a broad field of quantum communications that also include quantum teleportation, quantum dense coding, quantum error-correcting codes, quantum data compression, etc.

The purpose of this review is to give an overview of both theoretical and experimental achievements in the field with a focus on recent developments.

0.1.1 Cryptographic tasks

Current classical cryptographic methods are used to solve a number of tasks. One of the most important ones is *secure message exchange*, which allows two parties to communicate in such a way that their messages are unintelligible to any third party. An unconditionally secure method that enables to achieve this goal is the so-called Vernam cipher [6], or a one-time pad, which was

invented in 1917. The principle of this cipher is that addition of a string of random bits, called the key, to a message, renders the resulting string also completely random. For this cipher to be unconditionally secure, three requirements must be satisfied: (i) the key must be as long as the message; (ii) it must be purely random; (iii) it may be used once and only once. The only way to reveal the contents of the original message is to subtract the key. Thus the task of secure message exchange can be reduced to the problem of secure distribution of the cryptographic key.

Other tasks challenging cryptographers include mutual identification, secret sharing or multi-party computations. The goal of *mutual identification* is for individual parties to assure each other of their identities. *Secret sharing* is a method that enables us to split a secret string, e.g. a vault password, into several shares in such a way that individual shares contain absolutely no information about the secret, however, certain minimal subsets of the shares, pieced together, can recover the original secret. *Multi-party computations* allow two or more parties to perform a common computation without disclosing the input data of individual participants. After each party submits its input, every participant learns the output, computed from the inputs, without learning the inputs of the others, except those inferable from the output. This can be used, e.g., for ballots.

It should be mentioned that all these tasks can be solved classically, but they suffer either from the key-distribution problem or from the absence of an unconditional-security proof, and therefore from vulnerability to future decrypting techniques, quantum or classical.

On the other hand, quantum physics enables us to design a cryptographic primitive, which resolves at least part of the tasks mentioned above. This primitive is called quantum key distribution.

0.1.2 The principle

The quantum key distribution procedure (QKD) allows two parties to establish a common random secret key. It takes advantage of the fact that quantum mechanics does not allow us to distinguish non-orthogonal states with certainty. The security of QKD is guaranteed by their overlap.

Within the framework of classical physics, information encoded into a property of a classical object, can be acquired without affecting the state of the object. However, if information is encoded into a property of a quantum object, any attempt to discriminate its non-orthogonal states inevitably changes the original state with a nonzero probability. And since eavesdropping is also governed by the laws of quantum mechanics, these changes cause errors in transmissions and reveal the eavesdropper.

An eavesdropper could also try to amplify the signal and split off its part, however, cloning of quantum states is also forbidden by quantum principles [7]. Thus QKD cannot prevent from eavesdropping, but it enables legitimate users to discover it. If any eavesdropping is detected, the key is simply thrown

away and a new one is generated. No leakage of information occurs, since the key is just a random sequence.

0.1.2.1 Communication protocol BB84 The first QKD protocol was proposed by C. H. Bennett and G. Brassard in 1984 [8] (therefore the acronym BB84), following the first ideas by S. Wiesner [9]. At present time this protocol has been best elaborated, both theoretically and experimentally. The properties that may be employed to encode information are, e.g., polarization of photons, phase, or quantum correlations (entanglement) of quantum systems. And how does this protocol work? Let us first describe a system, where information is encoded into linear polarizations of photons:

At the beginning, the two parties that wish to communicate, traditionally called Alice and Bob, agree on two polarization bases mutually rotated by 45°, and determine which polarization in each basis corresponds to a logical 1 and 0, e.g.,

base $+$:	$\updownarrow$	$=$	0	$\leftrightarrow$	$=$	1
base $\times$:	$\nwarrow\!\!\searrow$	$=$	0	$\nearrow\!\!\swarrow$	$=$	1

Then Alice generates random bits, chooses randomly between the two polarization bases, and sends photons with corresponding polarizations to Bob. Bob also chooses randomly (and independently of Alice) his detection bases, i.e., the orientation of his polarization analyzer. The two outputs of the analyzer are fed to detectors. One detector corresponds to a '1', the other to a '0'. Next, Alice and Bob say each other through a public channel (computer network, telephone, etc.), which bases they used for individual photons. Note that they communicate *bases only*, not particular polarizations of photons. They keep only those bits when their bases coincided. In those cases their bits should be identical as the results of Bob's measurements are deterministic. Thus they obtain a shared key. When they used different bases, the outcomes of Bob's measurements are random, and are discarded. Afterward Alice and Bob "sacrifice" a random part of this sequence by publicly comparing it. Their strings should be identical; possible differences reveal an eavesdropper's activity. The disclosed part of the key must be thrown away and cannot be used for any other purposes. The whole procedure is summarized in the following table:

(1)	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
(2)	×	+	×	+	+	+	+	+	×	×	+	×	×	×	+
(3)	$\nwarrow$	$\leftrightarrow$	$\nearrow$	$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$	$\updownarrow$	$\updownarrow$	$\nearrow$	$\nwarrow$	$\leftrightarrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\leftrightarrow$
(4)	+	×	×	+	+	×	×	+	×	+	×	×	×	×	+
(5)	1		1		1	0	0	0		1	1	1		0	1
(6)	+		×		+	×	×	+		+	×	×		×	+
(7)			OK		OK			OK				OK		OK	OK
(8)			1		1			0				1		0	1
(9)					1									0	
(10)					OK									OK	
(11)			1					0				1			1

I. Quantum distribution:

(1) Random bits generated by Alice;
(2) Polarization bases randomly chosen by Alice;
(3) Polarizations of photons sent by Alice;
(4) Random orientations of Bob's polarization analyzer;
(5) Bits obtained by Bob (blank spaces mean that the photon was lost).

II. Public discussion:

(6) Bob announces his polarization bases;
(7) Alice announces coincidences of their bases;
(8) Random shared sequence of bits (in the absence of an eavesdropper and noise, these bits must be identical with the bits sent by Alice).

III. Test for eavesdropping:

(9) Bob picks a random part of his bits and makes them public in order to detect eavesdropping;
(10) Alice checks these bits and informs Bob if they are correct (eavesdropping would have caused errors);
(11) Secret bits shared by Alice and Bob—the key.

0.1.2.2 Eavesdropping on quantum states Let us suppose that two parties, Alice and Bob, want to interchange a secret key by means of a channel which is accessible to a third party, eavesdropper, traditionally called Eve. Eve is allowed to use all the power of quantum mechanics. What happens if Eve is listening? First, we should realize that classical eavesdropping is out of the question. Eve simply cannot draw out a small part of the signal. Since a single particle is used for each bit, she can get either nothing or the whole particle. In the latter case the particle is lost for Bob and the corresponding bit is not contained in the key (some loss is tolerated). Eve cannot even copy (or clone) the quantum state of the particle [7]. The simplest reasonable Eve's strategy is to use a measuring device, similar to that of Bob, to measure the polarization of incoming photons, and resend each bit again to Bob with the help of a device similar to Alice's one. If Eve chooses the "wrong" polarization basis for her measuring and preparation apparatuses (i.e., different from Alice's and Bob's ones), she inevitably changes the polarization state of the photon and then there is a nonzero probability that Bob gets a result different from the original Alice's bit. These differences enable Alice and Bob to disclose Eve.

Of course, Eve may use some more sophisticated measurements (e.g., such that does not swallow up the original photon). However, it can be shown that the resultant effect is qualitatively the same (see section 0.1.4). In general any interaction modifies the states of a photon.

Eve is assumed to know the types of bases Alice and Bob use. This is why Alice and Bob must alternate randomly and independently between two conjugated bases (e.g., polarization bases rotated by 45°). Now, even if Eve has known the bases, she could hit the right one only in 50 % of cases on

average. Thus continual eavesdropping using the described strategy causes a 25 % error rate. By comparing part of transmitted bits, Alice and Bob can estimate the error rate and detect Eve's activity.

Note that Eve could also modify the "auxiliary" information transmitted through the classical open channel. For example, she can cut both channels and pretend to be Bob in front of Alice. Therefore *authentication* of the messages sent over the open channel is necessary [1, 10]. The recipient must be able to check that the message has come from the "proper" sender and that it has not been modified. This requires of Alice and Bob to share a small amount of secret information (an authentication password) at the beginning. After each transmission, this password is replaced by a new one, obtained from the transmitted sequence. Therefore, the QKD cryptosystem works rather as an "expander" of shared secret information.

In any real apparatus, there is noise which may also cause errors. Therefore some small amount of errors have to be tolerated. Of course, it is possible to correct errors by standard *error correction* procedures [4, 11]. Nevertheless, we cannot exclude the possibility that the errors are due to Eve and not due to "technological" noise. Fortunately, the amount of information, which could have leaked out to Eve, can be estimated from the error rate for a large class of eavesdropping strategies [4, 12, 13]. To minimize Eve's information, a *privacy amplification* procedure can be applied to the key at the cost of its shortening [4, 14]. Finding the limit of the amount of information Eve can obtain for the most general attack allowed by quantum mechanics, is the cornerstone of the efforts to provide the ultimate security proof of quantum cryptography (see sec. 0.1.4).

0.1.2.3 Other communication protocols Besides BB84, other protocols were designed. The B92 protocol [15] uses only two non-orthogonal states. A strong reference pulse is used to prevent an eavesdropper from misusing vacuum states on a lossy quantum channel. The same trick may be used to enhance the security of BB84—this protocol is known as the 4+2 protocol [16]. In the six-state protocol, three non-orthogonal bases are used [17]. Though the latter protocols offer security improvements compared to BB84, they have not attracted the attention of experimentalists yet.

Another class of QKD protocols is based on entangled quantum systems [19]. Both Alice and Bob receive one member of a pair of particles obtained from the parametric down-conversion process [18]. These particles feature nonclassical properties: results of suitably chosen measurements on the particles exhibit, even when spatially separated, correlations that cannot be explained by any classical theory consistent with local realism. When Alice and Bob decide to establish a key, they perform independent measurements in randomly chosen bases (from a given non-orthogonal set), and using a public channel they arrive at a secret shared key in a way similar to BB84. Later developments showed a way to improve the security of this protocol by means of the so-called entanglement-purification techniques [20].

We note that also protocols using orthogonal states have been designed [21]. Superpositions of quantum states are employed. A superposition is divided into parts, which are sent separately with a time delay larger than the time distance between Alice and Bob. This requirement, however, makes such schemes difficult to implement.

There have also been a large number of other, more or less, exotic proposals.

0.1.3 Quantum cryptographic methods in practice

The quantum communication protocols described above may be used to implement quantum counterparts to the classical solutions of cryptographic tasks mentioned in sec. 0.1.1. Until now most of the efforts were devoted to a quantum solution of the key-distribution problem, which may readily be applied to secure message exchange or can be used as a building block for different cryptographic schemes.

0.1.3.1 Quantum key distribution. The first QKD prototype operated over a distance of 32 cm in free space [4]. Since then, experimental techniques have undergone a tremendous progress and today QKD systems at almost a commercial level are offered [22]. A number of problems must have been solved. Communication distance has reached several tens of kilometers in optical fibers [23, 24, 25, 26]. Also free space systems are being developed with earth-satellite communication on mind [27]. It should be noted that only a few systems presented until now have exhibited parameters that would ensure a secure key generation.

Two main conceptions of QKD apparatuses have been followed. Until late 90's, most of the attention was devoted to the construction of QKD devices, which used dim laser pulses as the source of photons. Pulses from a laser diode are attenuated down below one photon per pulse. Since laser pulses exhibit Poisson statistics in photon-number distribution, this ensures that about 90 % of pulses contain no photons at all, about 9 % of pulses contain exactly one photon, and only a small fraction of pulses contain two or more photons. Bit values are encoded into polarization states of the laser pulses [24, 28, 27] or into phase differences in a large Mach-Zehnder interferometer [23, 25, 22, 26]. The former method requires stabilization of polarization over the communication distance, which is achieved by active stabilization. It was shown that it is possible to operate such a system in field conditions over a distance of 23 km [24]. The interferometric method achieves the stabilization of the Mach-Zehnder interferometer over the communication distance by splitting the interferometer into two unbalanced interferometers and by using time-multiplexing over a single transmission fiber. This method has been successfully applied over 46 km in the field [25]. While polarization measurements are more precise than phase interferometry, the latter method seems to gain more popularity amongst experimentalists after the development of highly stable interferometric schemes employing Faraday mirrors [22, 26]. Er-

ror rates below one percent are achievable. The main obstacles both these methods face are attenuation in optical fibers, and low efficiency and high noise level in currently available detectors. These factors result in a serious limitation of the secure transmission distance.

Free-space QKD also advances at a fast pace. Filtering of the stray light is achieved by means of carefully adjusted telescopes and by tight spectral- and time-filtering. It was shown that under good atmospheric conditions, QKD is feasible up to 1.6 km [27], a distance approaching the effective turbulent atmospheric thickness in a surface-to-satellite path. Observed error rates were around 5 % and 3 % by day and night, respectively.

Quite recently interest in correlated photon pairs has been revived, though the original Ekert's proposal comes already from 1991 [19]. It was shown that the entanglement can be preserved over large distances [29]. To discover an eavesdropper, the communication protocol can either test the Bell inequalities [19, 30, 31], or a variant of the BB84 can be applied [30, 32]. Both energy-time [19, 31] and polarization [30, 33, 34] entanglements have been used. A novel source of entangled photons brings cryptography with correlated photons closer to applications [35, 31]. At the present experimental level, error rates fall only slightly below 10 percent at communication distances approaching 10 km.

Another way to employ correlated photons pairs in quantum cryptography has been suggested [36, 37]. The idea is to take advantage of the fact that in the down-conversion process photons are always created as in pairs. Performing a photon-number measurement in one of the beams, only single-photon states can be selected in the other beam. Such a source would not only extend the distance limit of secure QKD, but it would also conform with the ultimate security proofs which were derived under the assumption that single-photon states are used. A more detailed investigation [38] shows that even though physical imperfections in real experiments keep such sources far from single photons, they still offer certain benefits compared to dim laser pulses.

The development of QKD also stimulated the construction of high-quality random-number generators [39]. This is an important question, because to preserve the level of security, Alice's and Bob's choices of encoding and measurement bases and bit values must be truly random. Quantum generators based on the division of a weak photon flux at a beam-splitter seem to accomplish this task. Some schemes let the Nature make this random work already within the setup.

0.1.3.2 Quantum identification. Attempts have been made to build a quantum identification system [40] by first implementing another cryptographic primitive, the so-called bit commitment [41]. This task, however, has been proved impossible to implement in a secure way [42].

Later a secure solution of this task was found. It combines a classical three-step identification procedure with QKD [43]. The identification procedure uses random sequences which are used just once, and the QKD procedure

supplies the users with new key material. Moreover, the identification procedure may easily be incorporated into the public discussion within the QKD, which substantially simplifies the system.

Other ways to solve mutual identification were proposed using correlated particles [44, 45]. Here again, modifications of the QKD procedure are used. In the latter case, a third communicating party, trusted arbitrator, is required.

0.1.3.3 Quantum secret sharing. A theoretical proposal of how to implement secret sharing in a quantum way was proposed in [46]. This method uses three-particle quantum entanglement of Greenberger-Horne-Zeilinger states, which, however, have not neatly been produced in the laboratory yet. Later a modification of the secret sharing protocol was developed, which expediently utilizes the entanglement of EPR photon pairs, and which is already within the reach of today's technologies [47]. This task has already been implemented experimentally too [48].

0.1.3.4 Multi-party computations. The hope for secure quantum implementation of multi-party computations using a cryptographic primitive, called oblivious transfer [49], was dashed together with the bit commitment [42]. Until now, no other solution has been published.

0.1.4 Security

Provided that quantum theory is a right description of our physical world, quantum cryptography offers, in principle, unconditional security. However, there are several problems in practice. First, each real apparatus and transmission line exhibit losses, imperfections, and misalignments. This results in non-zero error rates during transmissions even in the absence of an eavesdropper. The unconditional security is imperiled. Second, there is no easy-to-use single-particle carrier in the optical domain where naturally quantum cryptography is likely to be employed. The sources used until now suffer from a certain content of vacuum or multiphoton states, both of which open security risks. Multiphoton events can in principle be identified by Eve and she can eavesdrop on them by splitting and diverting part of the signal without risking disclosure. Vacuum states, on the other hand, can be used for manipulations that can hide the consequences of eavesdropping.

These actualities force communicating parties to undertake steps (privacy amplification [4, 14]) to eliminate information possibly leaked to an eavesdropper. Since it is impossible to discriminate between errors caused by technology and by eavesdropping, legitimate users must attribute all the errors to Eve's activity. To estimate the amount of Eve's knowledge from the detected error rate, one has to consider possible eavesdropping strategies; not only those technologically possible today but all strategies possible in principle. The intercept-resend attack, described in section 0.1.2.2, was investigated in detail first [4, 50, 51, 52]. Then more general attacks on single quantum

bits (qubits)—such that Eve could use positive-operator-valued measurement (POVM)—were considered [50, 12]. Other generalizations of eavesdropping strategies "enable" Eve to use "probes" interacting with information carriers. These probes could be stored and measured (by POVM) later—after the announcement of Alice's and Bob's bases [13]. Next step has covered the so-called collective and coherent attacks. In these cases it is supposed that an eavesdropper can carry out measurements not only on individual qubits, but on the key as a whole by means of collective measurement on non-entangled probes corresponding to individual qubits (collective attack), or by means of an unrestricted, arbitrarily complex "common" probe (coherent or joint attack) [53]. Proofs of security of the BB84 scheme against the most general attack, even in the presence of noise, have been finally obtained [54]. Fortunately, it seems that if the technological error rate is low enough, quantum key distribution could still be unconditionally secure.

However, all the proofs mentioned in the previous paragraph are idealized in the following sense: A proof of security is independent of the physical implementation of signal states as long as they have the correct overlap probabilities and if the recipient is able to detect exactly the same set of states as are sent. But the latter condition represents a serious difficulty in practice. Real detectors are usually not able to distinguish the number of impinging particles. It could be overcome by sending quantum states of exactly one particle. Unfortunately, it is also a hard technological problem. If Alice cannot guarantee one-photon signals and Bob's detectors just either fire or they do not fire, an eavesdropper can split and read some signals without the recipient detecting it. The difficulties implied, for example, by the use of weak coherent states in combination with lossy lines have been pointed out and their various aspects have been discussed in [16, 51, 55, 37, 56]. This subject has been further analyzed in [36, 37, 38], where bounds on coverable distances were given. Positive security proofs for individual attacks for sufficiently short distances taking account of realistic signals are given in [37]. It has been shown that with the best current technology (transmission line made of optical fiber at 1550 nm, Ge or InGaAs avalanche detectors, and weak laser pulses as a source of quantum state carriers), the distance allowing secure QKD is limited to about 25 km. The hope for extending this range above 120 km by using a source based on postselection from correlated photon pairs has been weakened when a more realistic treatment found a limit of about 55 km achievable with present laboratory skills [38]. There is also some work in progress on the positive security proof for the case of coherent attacks [57]. On the other hand, the eavesdropping attacks which may undermine the secrecy of the key for setups exceeding these secure distances, are still quite complicated. The eavesdropper needs perform a non-demolition measurement of the total photon number in the signal state, then she has to split off one photon providing a multi-photon signal has occurred, store that photon, and then, finally, measure it after the public discussion.

0.1.5 Prospects

It is clearly apparent that quantum cryptography is now ready to offer efficient and user-friendly systems providing an unprecedented level of security. While classical methods are still safe enough for short-lifetime encryption, quantum cryptography may prove valuable when thinking with longer prospects. The development of quantum computers can play a significant role in speeding up the increase of the need for QKD in the IT market.

Still there is a lot to be done. While the security of single-photon methods is already quite well defined, the security of cryptography with correlated pairs is much less understood. It would also be useful to make a rigorous analysis of what is the optimum protocol. QKD itself is now well elaborated, but its further propagation to other areas of cryptography (or discovery of another quantum primitive) still stands ahead.

Theoretical progress will no doubt be immediately followed by experimental advances. The development of new technologies can extend the limit of secure communication. Mainly detectors in the 1550-nm fiber-optic communication window require a big improvement. Any reduction of the fiber attenuation would also greatly contribute to extending the communication range.

It should be stressed that future practical applications of quantum cryptography are by far not the only benefit of this area of research. As already mentioned, a whole new field has been stimulated, which has helped us better understand the Nature. It is believed that this resource is still far from being exhausted.

Acknowledgments

This work was supported by The Ministry of Education of the Czech Republic (projects LN00A015) and The Czech National Security Authority (project 19982003012).

REFERENCES

1. For references on classical cryptography see, e.g., D. R. Stinson, *Cryptography: Theory and Practice*, CRC Press, Boca Raton, 1995.

2. P. W. Shor, *Proc. 35th Ann. Symp. Found. Comp. Sci.*, S. Goldwasser, ed., IEEE, Los Alamitos (1994).

3. A. Shamir, presented at *Int. Conf. Theor. Appl. Crypt. Techniques*, Prague, (1999). Available at `http://jya.com/twinkle.eps`.

4. C. H. Bennett , F. Besette, G. Brassard, L. Salvail, J. Smolin, *J. Crypt.* **5**, 3 (1992).

5. For a review see C. H. Bennett, P. W. Shor, *IEEE Trans. Inf. Theory* **44**, 2724 (1992).

6. G. S. Vernam, *Journal of the American Institute of Electrical Engineers* **45**, 109 (1926).

7. W. K. Wootters, W. H. Zurek, *Nature* **299**, 802 (1982).

8. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore, India*, IEEE, New York, 1984, p. 175.

9. S. Wiesner, *SIGACT News* **15**, 78 (1983).

10. M. N. Wegman, J. L. Carter, *Journal of Computer and System Sciences* **22**, 265 (1981).

11. G. Brassard and L. Salvail, in: *Advances in Cryptology: Proc. of Crypto '93, Vol. 765 of Lecture Notes in Comp. Science*, Springer-Verlag, Berlin, 1994, p. 410.

12. N. Lütkenhaus, *Phys. Rev. A* **54**, 97 (1996).

13. C. Fuchs, N. Gisin, R. B. Griffits, C.-S. Niu, A. Peres, *Phys. Rev. A* **56**, 1164 (1997).

14. C. H. Bennett, G. Brassard, C. Crépeau, U. M. Maurer, *IEEE Trans. Inf. Theor.* **41**, 1915 (1995).

15. C. H. Bennett, *Phys. Rev. Lett.* **68**, 3121 (1992).

16. B. Huttner, N. Imoto, N. Gisin, T. Mor, *Phys. Rev. A* **51**, 1863 (1995).

17. D. Bruss, *Phys. Rev. Lett.* **81**, 3018 (1998).

18. See, e.g., D. F. Walls, G. J. Milburn, *Quantum Optics*, Springer, Berlin, 1995, chap. 5.

19. A. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

20. D. Deutch, A. K. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, A. Sanpera, *Phys. Rev. Lett.* **77**, 2818 (1996).

21. L. Goldenberg, L. Vaidman, *Phys. Rev. Lett.* **75**, 1239 (1995); A. Peres, *Phys. Rev. Lett.* **77**, 3264 (1996); *L. Goldenberg, L. Vaidman, Phys. Rev. Lett.* **77**, 3265 (1996); M. Koashi, N. Imoto, *Phys. Rev. Lett.* **79**, 2383 (1997).

22. G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, *J. Mod. Opt.* **47**, 517 (2000).

23. C. Marand, P. D. Townsend, *Opt. Lett.* **20**, 1695 (1995)

24. A. Muller, H. Zbinden, N. Gisin, *Europhysics Lett.* **33**, 335 (1996).

25. R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, C. Simmons, *Lect. Notes in Comp. Sci.* **1109**, 329 (1996).

26. M. Bourennane, D. Ljunggren, A. Karlsson, P. Jonsson, A. Hening, J. P. Ciscar, *J. Mod. Opt.* **47**, 563 (2000).

27. W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, C. G. Peterson, *Phys. Rev. Lett.* **84**, 5652 (2000).

28. J. D. Franson, B. C. Jacobs, *Electron. Lett.* **31**, 232 (1995)

29. P. R. Tapster, J. G. Rarity, P. C. M. Owens, *Phys. Rev. Lett.* **73**, 1923 (1994); W. Tittel, J. Brendel, H. Zbinden, N. Gisin, *Phys. Rev. Lett.* **81**, 3563 (1998); G. Weihs, T. Jennewein, Ch. Simon, H. Weinfurter, A. Zeilinger, *Phys. Rev. Lett.* **81**, 5039 (1998).

30. T. Jennewein, Ch. Simon, G. Weihs, H. Weinfurter, A. Zeilinger, *Phys. Rev. Lett.* **84**, 4729 (2000).

31. W. Tittel, J. Brendel, H. Zbinden, N. Gisin, *Phys. Rev. Lett.* **84**, 4737 (2000).

32. C. H. Bennett, G. Brassard, N. D. Mermin, *Phys. Rev. Lett.* **68**, 557 (1992).

33. A. V. Sergienko, M. Atatüre, Z. Walton, G. Jaeger, B. E. A. Saleh, M. C. Teich, *Phys. Rev. A* **60**, R2622 (1999).

34. D. S. Naik, C. G. Peterson, A. G. White, A. J. Berglund, P. G. Kwiat, *Phys. Rev. Lett.* **84**, 4733 (2000).

35. J. Brendel, N. Gisin, W. Tittel, H. Zbinden, *Phys. Rev. Lett.* **82**, 2594 (1999).

36. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).

37. N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (2000).

38. O. Haderka, J. Peřina, Jr., *12th Czech-Slovak-Polish Optical Conference*, Velké Losiny, Czech Republic, September 2000, to appear in *Proc. SPIE*.

39. A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, H. Zbinden, *J. Mod. Optics* **47**, 595 (2000); T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, A. Zeilinger, *Rev. Sci. Instr.* **71**, 1675 (2000); J. Soubusta, O. Haderka, M. Hendrych, *12th Czech-Slovak-Polish Optical Conference*, Velké Losiny, Czech Republic, September 2000, to appear in *Proc. SPIE*.

40. C. Crépeau, L. Salvail, in *Advances of Cryptology: Proc. Eurocrypt '95*, Guillon L. C. and Quisquater J. J., eds., Springer-Verlag, New York, 1995, p. 133.

41. G. Brassard, C. Crépeau, R. Jozsa, D. Langlois, *Proc. 34^{th} Ann. IEEE Symp. Found. Comp. Sci.*, 362 (1993).

42. D. Mayers, *Phys. Rev. Lett.* **78**, 3410 (1997); H.-K. Lo, H. F. Chau, *Phys. Rev. Lett.* **78**, 3410 (1997).

43. M. Dušek, O. Haderka, M. Hendrych, *Acta Phys. Slov.* **48**, 169 (1998); M. Dušek, O. Haderka, M. Hendrych, R. Myška, *Phys. Rev. A* **60**, 149 (1999).

44. H. Barnum, *Quantum secure identification using entanglement and catalysis*, Los Alamos e-print archive `quant-ph/9910072` (1999).

45. D. Ljunggren, M. Bourennane, A. Karlsson, *Phys. Rev. A* **62** 022305 (2000).

46. M. Hillery, V. Bužek, A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999); M. Hillery, V. Bužek, *Acta Phys. Slov.* **49**, 533 (1999).

47. A. Karlsson, M. Koashi, N. Imoto, *Phys. Rev. A* **59**, 162 (1999).

48. W. Tittel, H. Zbinden, N. Gisin, *Quantum secret sharing using pseudo-GHZ states*, Los Alamos e-print archive `quant-ph/9912035` (1999).

49. C. H. Bennett, G. Brassard, C. Crépeau, M.-H. Skubiszewska, in: *Advances in Cryptology: Proc. Crypto '91*, Springer-Verlag, New-York, 1992, p. 361.

50. A. Ekert, B. Huttner, G. M. Palma, A. Peres, *Phys. Rev. A* **50**, 1047 (1994).

51. H. P. Yuen, *Quantum Semiclass. Opt.* **8**, 939 (1996).

52. B. Huttner, A. K. Ekert, *J. Mod. Opt.* **41**, 2455 (1994).

53. E. Biham, T. Mor, *Phys. Rev. Lett.* **78**, 2256 (1997); E. Biham, T. Mor, *Phys. Rev. Lett.* **79**, 4034 (1997); E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor, *Security of Quantum Key Distribution Against All Collective Attacks*, Los Alamos e-print archive `quant-ph/9801022` (1998).

54. D. Mayers, in: *Advances in Cryptology – Proceedings of Crypto '96*, Springer, Berlin, 1996, p. 343, Los Alamos e-print archive `quant-ph/9606003`; D. Mayers, *Unconditional security in Quantum Cryptography*, Los Alamos e-print archive `quant-ph/9802025v4` (1998); H.-K. Lo and H. F. Chau, *Science* **283**, 2050 (1999).

55. M. Dušek, O. Haderka, and M. Hendrych, *Opt. Commun.* **169**, 103 (1999).

56. M. Dušek, M. Jahma, N. Lütkenhaus, *Phys. Rev. A* **62**, 022306 (2000).

57. H. Inamori, N. Lütkenhaus, D. Mayers, in preparation.