International Journal of Quantum Information
Vol. 6, No. 2 (2008) 347–367

ON STANDARDS AND SPECIFICATIONS IN QUANTUM CRYPTOGRAPHY

A. S. TRUSHECHKIN

*Department of Cybernetics, Moscow Engineering Physics Institute,
Kashirskoe sh. 31, Moscow, 115409, Russian Federation
trushechkin@mail.ru*

I. V. VOLOVICH

*Department of Mathematical Physics, Steklov Mathematical Institute,
Russian Academy of Sciences, Gubkin st. 8,
Moscow, 119991, Russian Federation
volovich@mi.ras.ru*

Received 29 August 2007

Quantum cryptography is used to find practical and useful applications. Recently, some first quantum cryptographic solutions became available on the market. For clients, it is important to be able to compare the quality and properties of the proposed products. To this end, one needs to elaborate on specifications and standards of solutions in quantum cryptography. We propose and discuss a list of characteristics for the specification, which includes numerical evaluations of the security of solution and can be considered as a standard for quantum key distribution solutions. The list is based on the average time of key generation, depending on some parameters. In the simplest case for the user, the list includes three characteristics: the security degree, the length of keys and the key refresh rate.

Keywords: Quantum cryptography; quantum key distribution; product specification.

1. Introduction

Bennett and Brassard[1] proposed the first quantum key distribution (QKD) protocol, which was named BB84 later, and on which many of the present-day practical realizations of QKD are based.[2–7] Eckert proposed a QKD protocol of another type (based on quantum entanglement)[8] which is called E91. There are also practical realizations of this type of protocol.[9]

Recently,[3,4] the first commercial QKD system became available on the market. Some commercial, military and security institutions were interested in this new technology. In this connection, the questions about the concept of the security of QKD protocols and keys generated by them are crucial.

As with any product, the problem of elaborating on some standards and specifications of QKD systems arises: What kind of characteristics does a producer have to include in the specification? The necessity of the elaboration of some standards for the widespread deployment of quantum cryptography has already been pointed out in Ref. 10.

In this paper, we propose and discuss a list of characteristics for the specification, which includes a numerical evaluation of the security of the solution, and which can be considered as a standard for quantum key distribution solutions. The list is based on the average time of key generation depending on some parameters.

In the simplest case for the user, the list includes three characteristics: the security degree ε, the length of keys m and the key refresh rate R.

The paper is organized as follows. In Sec. 2, we recall some features of QKD. We give a comparison of the computational and information-theoretic (unconditional) approaches to cryptography, the notions of QKD protocol and key security, a classification of the adversary's attacks and some specific features of QKD. In Sec. 3, we discuss the problem of specification of QKD systems and propose a list of characteristics of these systems, which can be taken as a standard and which a producer has to indicate in the specification.

For a review on quantum cryptography see, e.g. Refs. 11 and 12.

2. Features of QKD

In this section, we discuss various properties of QKD which are relevant to specifications.

2.1. *Computational and information-theoretic approaches*

Two approaches depending on the nature of the assumptions about the adversary are distinguished in cryptography.[13,14]

- *The Computational approach* is proposed in Ref. 15, and is based on the complexity of solving some computational problems (such as, for example, factorization of the whole numbers or discretely taking the logarithm) and on the assumption that the adversary's computational power is bounded. However, as the adversary with the unbounded computational power can solve any such problem as quickly as he wishes and hence, break the cryptographic system, computational security is always conditional. The risk that such a system will be broken always exists due to the progress in computer engineering (for example, in quantum computer engineering).
- *The Information-theoretic approach* originates in Ref. 16 and is based on the assumption that the information of the adversary is bounded. In quantum cryptography, the adversary's information is bounded due to the uncertainty relations in the quantum world. As there are no assumptions on the adversary's computational power, information-theoretic security is called *unconditional* and is more

desirable. Theoretically, the adversary has no way to break an unconditionally-secure cryptographic system, even using infinite computing power.

Most of the present-day cryptographic protocols (for example, RSA) are based on the computational approach, namely, on the lack of effective algorithms for the solution of NP-problems at present. Besides the weaknesses of the computational approach pointed out above, the fact that the impossibility to effectively solve the NP-problems has not been proved, is considered to be one more weakness of the present-day cryptosystems. If effective algorithms for solving NP-problems are found, most of the present-day cryptosystems will lose their security.

2.2. *Security of pair of keys*

The problem of key distribution is an important problem in cryptography. Two legal parties, Alice and Bob, want to get a pair of keys[a] (one key for Alice and another one for Bob) using communication channels. A realization of a certain random variable on a finite set $\mathcal{K}$, or this random variable itself is regarded as a key. A pair of keys is called *perfectly secure* if

(i) they are uniformly distributed,
(ii) they are identical, and
(iii) a potential adversary (Eve) has no information about them.

Accordingly, the adversary Eve aims, firstly, to get as much information about the keys as possible and, secondly, to make Alice's and Bob's keys different.

It is necessary to evaluate the security of the pair of keys. It is natural to define the insecurity of the pair of keys as the distance from the ideal pair of keys which is perfectly secure.[17,18] Since the definition must be applicable to quantum cryptography, it must be given in terms of quantum states. Classical state (probability distribution) is a particular case of the quantum state. Let $P_{K_A K_B}$ be a joint distribution of Alice's key K_A and Bob's key K_B. Let ρ be a quantum state which includes both the keys K_A and K_B, and Eve's (in general, quantum) information about these keys. Let ρ_{ideal} be the state which corresponds to the ideal pair of keys. Then, the pair of keys (K_A, K_B) is called ε-*secure* where $\varepsilon \in [0, 1]$, if

$$\delta(\rho, \rho_{\text{ideal}}) \leq 1 - \varepsilon. \tag{1}$$

We will call the number ε the *security degree* of the pair of keys. Here $\delta(\cdot, \cdot) \in [0, 1]$ is the distance measured between two quantum states. Hence, a pair of keys is as secure as ε is closer to one. A one-secure pair of keys is perfectly secure. Note that this security is information-theoretic (unconditional), because there are no assumptions about Eve's computational power.

[a] In a number of papers, only one key has been discussed, but we will discuss two keys in order to emphasize that formally, there are two different random values and, in general, Alice's and Bob's keys do not coincide with each other.

See the Appendix for the formal definition of the security degree of a pair of keys. Here we give some important properties of this definition.

- This definition of security is *universally composable* in the sense of Ref. 19, which is important for the modern cryptographic protocols.
- If the pair of keys is ε-secure, then the probability P_{guess} that the adversary guesses the keys (*success probability*) is bounded by (see Refs. 20 and 18)

  $$P_{\text{guess}} \leq \frac{1}{|\mathcal{K}|} + 1 - \varepsilon, \tag{2}$$

  where $|\mathcal{K}|$ is the number of elements in the set of keys $\mathcal{K}$. For example, the success probability of the ε-secure n-bit pair of keys is bounded by $2^{-n} + 1 - \varepsilon$. If the pair of keys is perfectly secure, then the success probability is $1/|\mathcal{K}|$, i.e. the adversary has no information and can only perform the completely random guessing from $|\mathcal{K}|$ elements.
- The fact that the pair of keys is ε-secure can be interpreted as that the pair is perfectly secure with the probability ε.

  Hence, this definition is useful because it is universally composable, and obviously, because it is related to the adversary's success probability and the probability that the pair is perfectly secure.
- If the pair of keys $(K_A^1 K_A^2, K_B^1 K_B^2)$ which is detained by concatenation of two pairs (K_A^1, K_B^1) and (K_A^2, K_B^2) is ε-secure, then both the pairs (K_A^1, K_B^1) and (K_A^2, K_B^2) are also ε-secure. The same holds for the concatenation of an arbitrary number of pairs of keys. Therefore, we can divide pairs of keys into shorter pairs of keys with the same degree of security.

2.3. *QKD protocol*

A practical quantum cryptography system with two legal parties (Alice and Bob) is a pair of hardware devices (Alice's hardware device and Bob's one). These devices are connected to each other by a quantum channel (mostly by optical fiber) and a classical channel (e.g. Ethernet or optical fiber), and each of the devices is attached to the corresponding (Alice's or Bob's) computer. It is clear that for operation of these devices, the software is necessary.

Hence, in the most general case, a quantum cryptography protocol (with two legal parties) is a pair of programs (algorithms) for a pair of computers which interact with each other by quantum and classical channels using special hardware devices. Besides the commands of a usual programming language, these programs must contain the additional commands for the hardware devices (lasers, detectors etc.) management.

Key distribution is one of the problems which can be solved by quantum cryptography. Besides the legal parties, there is also the adversary Eve in QKD. She also has a computer with an attached hardware device, which allows Eve to eavesdrop the channels and to change the messages transmitting over them. Therefore, in essence, the adversary's attack is a program for her computer with a special hardware. For a more formal discussion, see, e.g. Refs. 21 and 22.

The QKD protocols usually include the following steps.

(i) Photon transmission. Alice transmits to Bob a certain number of photons over the quantum channel in the states that she randomly chooses from a certain set. Her choices are unknown to Eve. Eve can perform different operations on the transmitted photons. Bob measures these photons in the bases that he also randomly chooses from a certain set. His choices are also unknown to Eve.

(ii) Test. Using the public classical channel, Alice and Bob analyze the data transmitted and received through the quantum channel and estimate a certain measure of Eve's interference. For BB84-type protocols, the *quantum bit error rate* (*QBER*) plays the role of the measure of Eve's interference. In E91-type protocols, the level of violation of Bell's inequality plays the role of this measure. Using the estimated value of this measure, they estimate Eve's information about the data. If the estimation of Eve's information exceeds a certain bound, then Alice and Bob go to step (iii). If not, they go to step (iv). This analysis is based on the property of the quantum world: the measurement of the quantum system changes the state of this system, so it is impossible for Eve to get information by measuring the transmitted photons without introducing the noise in them.

(iii) Decision abut the further course of the protocol. The negative result on step (ii) may be caused by both Eve's influence and statistical deviations. Alice and Bob may end the execution of the protocol, or return to step (i) and run the cycle once again.

(iv) Classical postprocessing of the quantum data. Alice and Bob perform certain classical procedures by communicating over the classical (public) channel which allows them to correct errors, to reduce Eve's information and so, to get a pair of keys with the desirable security degree.

During steps (ii)–(iv), Eve taps the classical channel and, maybe (see the next subsection), actively intercept the classical communication of Alice and Bob.

In this way, one gets the quantum state ρ which includes Alice's and Bob's keys K_A and K_B, and Eve's information about them. See the previous subsection.

In some cases, steps (iii) and (iv) can be omitted. For example, another approach to quantum cryptography is proposed in Ref. 23. But there is also the same sequence: a photon transmission, then a test.

Note the following features of QKD protocols:

- The Probability that Eve guesses all Alice's and Bob's choices during the photon transmission step is negligibly small, but not zero. In this case, Eve will have full information about the keys. On the other hand, privacy amplification procedure on step (iv) can reduce Eve's information to an arbitrary small amount, but not to zero. Hence, a pair of keys generated by a QKD system cannot be perfectly secure.

- It is possible that either Alice or Bob, or both of them can retract the key distribution [see step (iii)]. This is possible even in the case of no eavesdropping, but noisy quantum channel: if there are too many errors due to the natural noise in the quantum channel (this can happen with some non-zero probability), Alice and Bob could think that there is an eavesdropper and retract the key distribution. In order to reduce this probability (i.e. to reduce the statistical fluctuations), Alice has to send more photons to Bob, which has an effect on the time of key generation (see Sec. 3.4).

2.4. *Classification of the adversary's attacks*

When we speak about the security degree of the pair of keys which is generated by the key distribution protocol, we must specify our assumptions about the adversary's attacks relative to which the pair of keys has been declared the security degree. We consider the following classification.

(i) By the degree of mastering of quantum technologies by the adversary.

  (a) *Incomplete mastering of quantum technologies.* Besides the laws of quantum mechanics, there are other restrictions on the adversary's operations on the photons transmitted over the quantum channel. For example, the adversary can perform only individual attacks, or the adversary cannot perform the beam-splitting attack.[11]

  (b) *Complete mastering of quantum technologies.* During the photons transmission, the adversary can perform any operations that are allowed by quantum mechanics with these photons.

(ii) By the authenticity of the classical channel.

  (a) *Authentic classical channel.* The adversary can freely tap the classical channel, but cannot change and interrupt the messages sent by the legal parties, and send other messages. Hence, the adversary has read access, but does not have write access to the classical channel. In the case of this assumption, the authenticity of the channel must be provided by technology.

  (b) *Unauthentic classical channel.* The adversary cannot only freely tap the classical channel, but can also change and interrupt the messages sent by the legal parties, and send her messages to Alice and Bob. Hence, the adversary has read and write access to the classical channel. In this case, the authenticity of the channel in the protocol must be provided by mathematics.

  Generally speaking, it is more preferable if the classical channel is not assumed to be authentic, but the technological methods of providing with the authenticity can be, in some cases, more effective from the viewpoint of other parameters of the QKD system (e.g. one can avoid the key degradation problem — see Secs. 2.5, 3.4, and 3.5).

(iii) By the adversary's computing power.
   (a) *Adversary has limited computing power.*
   (b) *Adversary has unlimited computing power.*
   We should make a remark about the limitation of the computing power. Assumption about the adversary's computing power can be applied for using the public-key methods (e.g. digital signatures) as a mathematical method of authentication of the classical channel. In this case, the security of the pair of keys generated by the protocol, generally speaking, is not unconditional. But there is an advantage over the public-key cryptosystems, which is noticed in Ref. 24. In public-key cryptosystems, even if the adversary has not enough computing power now, she can calculate the secret key using the public key and so, break the cryptosystem in future, when enough computing power will probably be available. In the case of the use of public-key methods for authentication in the QKD protocol, if the adversary does not have enough computing power now, it is useless to have unlimited computing power later. Therefore, one can say that, in general, such a pair of keys is unconditionally-secure against future attacks.

Accordingly, the most general class of attacks is the case when the adversary has complete mastering of quantum technologies and unlimited computing power, and the classical channel is unauthentic.

This classification is rather rough, more precise classifications, e.g. specifications of adversary's mastering of quantum technologies (if it is incomplete) and computing power (if it is limited) are possible. The intermediate authenticity degrees of the classical channel, e.g. the case when the adversary can send her messages, but cannot change and interrupt other messages (it is realistic in radio communication), are also possible.

2.5. *Key degradation problem*

One more significant problem in quantum cryptography is the key degradation problem, which is considered in Ref. 17.

In the case of unauthentic classical channel and Eve's unlimited computing power, Alice and Bob have to use the unconditional message authentication codes (MAC), and for that they have to have a common key, or, as shown in Ref. 25, at least correlated random variables about which Eve does not have complete information. A portion of each of the generated keys must be kept for the next session, where it will be used as the initial key (for authentication). However, the obtained pair of keys is not perfectly secure. Hence, with every run of a QKD protocol, Alice and Bob obtain less and less secure keys.

Hence, after a number of runs of a QKD protocol, Alice and Bob need to obtain a new pair of keys not by a QKD protocol. We will call these keys and the source that generates them and deliver them to Alice and Bob *external*. Therefore, in this case, Alice and Bob need to have an external source of keys.

If the classical channel is authentic, then it is not necessary to have an external pair of keys. If the channel is unauthentic, but Eve's computing power is limited, then Alice and Bob can use public-key methods for authentication, e.g. digital signatures. In this case, they need to have an external initial key only at the beginning for the announcement of the first public key. Then a portion of public and secret keys is used for the authentication of the current message, and another portion, for the authentication of the announcement of the next public key. In this case, we have no problem of key degradation.

Note that the initial pair of keys cannot be used only for authentication.[23]

3. Specifications of QKD Systems

3.1. *Questions to the producers of QKD systems*

At present, first commercial QKD systems come into the market.[3,4] They provide specifications which include physical, environmental, and some other characteristics of the QKD systems. Note that for the commercial QKD systems, the length of keys m and the key refresh rate R are indicated ($m = 256$ bits, $R = 100$ times/s).[3,4] In specifications and descriptions of these systems, some important information from a practical point of view is lacking. One asks the following questions:

(i) How secure can a pair of keys that the user obtains using these systems be?
(ii) Against which class of attacks are these systems secure?
(iii) Is the key degradation problem taken into account?

Concerning the security, it is claimed that the keys generated by the commercial QKD systems are absolutely secure. It is not clear what this means. As we have said above, the security degree ε of the pair of keys generated by the QKD protocol cannot be equal to one, i.e. the pair of keys cannot be perfectly secure in this sense. We suggest that such an important characteristic as the security degree of the pair of keys should be indicated in the specification.

These questions are important since one of the declared advantages of quantum cryptography over the conventional one is the availability of rigorous proofs and estimations (see also the discussion in Ref. 23). Hence, the lack of the rigorous numerical estimations of the security is a retreat from the original idea of quantum cryptography. Certainly, any security estimation is relative: the adversary can perform an attack which is not concerned directly with the operations on the transmitted photons, i.e. which was not taken into account by the mathematical formalism (the examples of such attacks see, e.g. in Ref. 11). However, in our opinion, the rigorous numerical security estimations in the assumption that the adversary's operations satisfy the declared class of attacks are necessary. The estimation of the real security can be obtained only when numerous various attacks on the practical

QKD systems are carried out. Therefore, we need an army of "quantum hackers" (see Ref. 10).

Besides, the following general principle of cryptography is known[26,27]: any statement about the security of a cryptographic scheme demands the precise specification of values of all of its parameters, and often even a small deviation from the established values completely destroys the security of the system.

3.2. *Maximal measure of Eve's interference and success probability in case of no eavesdropping*

In Sec. 2.3, we mentioned the measure of Eve's interference (QBER for BB84-type protocols and the level of violation of Bell's inequality for E91-type protocols). This measure is denoted by M.

In Ref. 28, the notion of secrecy capacity of the classical broadcast channel was introduced. This is an analog of Shannon's channel capacity for the case with the presence of an eavesdropper: besides the required transmission rate, it is demanded in the definition of secrecy capacity that the eavesdropper has a negligibly small amount of information. In Ref. 29, these ideas were extended for the case when, in addition to the broadcast channel, Alice and Bob can also communicate through the public channel. The notion of secret key rate was introduced there.

A quantum channel with classical input (Alice's coding of classical bits into the quantum states) and classical output (Bob's and Eve's measurements) can be considered as a classical broadcast channel. Hence, in quantum cryptography, we can also use the notion of the secret key rate. But, in contrast to the classical models, in the quantum case, the secret key rate S depends on Eve's activity. Alice and Bob can estimate it by estimating the measure of Eve's interference M, i.e. $S = S(M)$.

And there is a maximal value $M_{\max}$ of the measure M such that $S(M) = 0$, if $M \geq M_{\max}$, and $S(M) > 0$, if $M < M_{\max}$. For example, the maximal QBER for the BB84 protocol is known to be 11%.[30]

This value $M_{\max}$ is often used to characterize and compare different QKD protocols. A larger value of $M_{\max}$ for a protocol means that this protocol is more robust against the natural noise (i.e. the noise when there is no eavesdropping) in the quantum channel. If $M_{\max}$ is such that due to the natural noise, the value of M estimated by Alice and Bob is more than $M_{\max}$ with high probability, then this protocol cannot operate, since Alice and Bob would think that they cannot generate a secret key due to the eavesdropping, whereas in fact there is no eavesdropping.

Of course, $M_{\max}$ is an important characteristic of a QKD protocol, but, in our opinion, it has the following drawbacks for the specification of QKD systems:

- Secret key rate, as well as secrecy capacity and usually Shannon's channel capacity, is an asymptotic characteristic: it guarantees that it is possible to get a pair of keys with security degree arbitrarily close to one *only for a sufficiently large number of transmitted photons.* But Alice and Bob only have a finite number of transmitted photons on the step of the test (see Sec. 2.3). If they determine that this number is not enough to achieve the desired security degree with the given secret key rate, Alice can transmit more photons to Bob. But Eve can change her strategy of interception of the quantum channel and, hence, change the value of the secret key rate during this second transmission. Therefore, the satisfaction of the condition $M < M_{\max}$ does not mean that the distribution of the pair of keys with the desired security degree is possible.

- $M_{\max}$ is not a universal characteristic of a QKD protocol, since the different measures of Eve's interference are used in the different protocols.
- $M_{\max}$ is a rather internal characteristic of a QKD protocol. It is of the interest of the engineer who develops the QKD solution, but not of the engineer who develops further applications using the QKD solution, or of the end-user.

$M_{\max}$ is not a measure of robustness of the protocol against Eve's attacks: if Eve wants to break the communication between Alice and Bob, she can always do it by making M greater than $M_{\max}$. $M_{\max}$ is only a measure of robustness of the protocol against the natural noise. But then we can use the probability

$$\gamma = \Pr[M < M_{\max} \,|\, \text{no eavesdropping}], \tag{3}$$

instead of $M_{\max}$. γ is the probability that both Alice and Bob do not retract the key distribution in the case of no eavesdropping. This parameter is both universal and suitable for users. We will call γ the *success probability in the case of no eavesdropping.*

In fact, γ depends on the number n of transmitted photons: Alice can send more photons in order to decrease the statistical fluctuations and, hence, to increase γ. But we do not write this dependence [like $\gamma(n)$], because we consider γ as an external parameter, which is set by the user (or it may be fixed — see Sec. 3.4), and the number of photons n as an internal parameter of the current operation of the QKD system, which is not of interest to the user. Therefore, the number of photons n depends on γ, and the computer program of the QKD system determines the required number of photons $n(\gamma)$ for the given γ.

3.3. *The simplest specification of QKD parameters*

We propose to use the following three characteristics for the specification of QKD parameters of the system in the simplest case:

- security degree ε,
- length of keys m, and
- key refresh rate R.

The security degree ε is considered in Sec. 2.2. In principle, the security degree depends on the practical implementation of the QKD system and it is assesed after the installation for each deployment. However, it is a general problem that for many manufactured goods, their specification has a conditional applicability, since it assumes rather restrictive conditions on the environment. Normally, the producer indicates the results of his own testing and in spite of its conditional character, this information is useful for the user.

Here, it is assumed that the security degree and the length of keys in the QKD system are fixed and in this sense, this is the simplest case. If the user can vary ε and m, then $R = R(m, \varepsilon)$ is a function depending on these parameters. A pair of keys which is longer or more secure requires more time for its generation, i.e. the smaller key refresh rate.

But ε and m are fixed for an individual launch of the QKD system. Therefore, in all cases, these parameters characterize the individual launch of the QKD system.

Here, it is also assumed that there is no key degradation problem, i.e. the users do not have external keys.

3.4. *Functional engineering characteristics of QKD systems*

In this subsection, we introduce the functional characteristics of the QKD systems suitable for detailed specifications.

3.4.1. *Average time of key generation*

For the functional description of the QKD system, we propose to use the average time of key generation T, if the QKD parameters (security degree, length of keys etc.) are fixed. The average time T describes the quality of the QKD system. Higher security requires the longer time of key generation. Note that the time T includes the times required for both photon transmission and classical computations. We suppose that the time depends on the following parameters:

(i) The desirable length of keys m.
(ii) The desirable security degree of keys ε, $0 < \varepsilon \leq 1$.
(iii) The desirable success probability (i.e. probability that both Alice and Bob do not retract key distribution — see the end of Sec. 2.3), γ, $0 < \gamma \leq 1$.
(iv) The length of the initial pair of keys m_0, $m_0 < m$.
(v) The security degree of the initial pair of keys. ε_0, $0 < \varepsilon_0 \leq 1$.

Hence, the average time T is a function $T = T(m, \varepsilon, \gamma, m_0, \varepsilon_0)$. The average time T increases as m, ε or γ increase, or m_0 or ε_0 decrease. $T(m, \varepsilon, \gamma, m_0, \varepsilon_0) = \infty$ is interpreted as an impossibility of key generation with the given parameters. Here, it is assumed that the distance of the QKD system functioning is fixed.

3.4.2. *Key refresh rate and key generation rate*

The average time T describes the QKD system in detail, but it depends on too many arguments. It is necessary to introduce functions which describe the QKD system in a less detailed way but have fewer parameters. One of these characteristics is the *key generation rate.* In order to define the key generation rate properly, we must analyze what information is needed for the user.

In the following, we fix γ, say, $\gamma = 0,99$, and do not consider the dependance of the functional characteristics below on γ. Furthermore, we first consider the simple case when $m_0 = 0$ (no key degradation). Hence, the average time T depends only on two arguments: the desirable length of keys m and the desirable security degree of the pair of keys ε. We will write $T(m, \varepsilon)$.

The user is interested in the pair of values (m, ε), i.e. he wants to generate a pair of keys (only once or continuously) with the length m bits and the security degree ε. Also, he wants to know the time $T(m, \varepsilon)$ (measured, e.g. in seconds) during which he can generate it, or, equivalently, he wants to know the *key refresh rate*,

$$R(m, \varepsilon) = \frac{1}{T(m, \varepsilon)}, \tag{4}$$

measured in times/second, which is more common in specifications of key distribution systems. We must give a definition of the key generation rate so that the user, knowing the key generation rate and the desirable parameters (m, ε), could find (may be approximately) the key refresh rate. It is natural to define the key generation rate as

$$\tilde{V}(m, \varepsilon) = \frac{m}{T(m, \varepsilon)} = mR(m, \varepsilon), \tag{5}$$

measured in bits/second. But we want to eliminate the length m from the arguments of the key generation rate, because it is natural to define the key generation rate which depends on the security degree but not on the length. We define the key generation rate as

$$V(\varepsilon) = \lim_{m \to \infty} \frac{m}{T(m, \varepsilon)}. \tag{6}$$

It is assumed that the limit, which may be infinite, exists.

Let us explain the introduced definition. Let (m, ε) be the desired pair of parameters.

$$V(\varepsilon) \approx \frac{m_\infty}{T(m_\infty, \varepsilon)}, \tag{7}$$

where m_∞ is a large number. Let $m_\infty = mn$ where n is some natural number. We divide the pair of keys with the length m_∞ into n pairs of keys with the length m. The security of each of these shorter pairs is also ε (see the properties of the security degree at the end of Sec. 2.2). Hence, n pairs of keys with the length m and the security degree ε are generated during the time $T(m_\infty, \varepsilon) \approx m_\infty / V(\varepsilon)$. The key refresh rate is $R(m, \varepsilon) = n/T(m_\infty, \varepsilon) \approx V(\varepsilon)/m$. Thus, the user knowing (m, ε) and $V(\varepsilon)$ can calculate the key refresh rate by the formula,

$$R(m, \varepsilon) \approx \frac{V(\varepsilon)}{m}. \tag{8}$$

It is possible that in concrete QKD systems, there are faster ways for generating keys with the parameters (m, ε) than generating much longer keys with the same security degree. But the value $V(\varepsilon)/m$ gives the guaranteed key refresh rate.

If $V(\varepsilon) = \infty$, then arbitrarily large key refresh rates are achievable by the proper (large enough) choice of m_∞.

Now we consider the general case where $T = T(m, \varepsilon, \gamma, m_0, \varepsilon_0)$ (γ is fixed, as before). Now Alice and Bob must have an external pair of keys in order to generate a pair of longer keys. Hence, the key refresh rate

$$R(m, \varepsilon, m_0) = \frac{1}{T(m, \varepsilon, \gamma, m_0, 1)} \tag{9}$$

has an additional parameter: the length of initial (external) keys m_0, i.e. the length of the perfectly secure keys that Alice and Bob must have before the QKD session, in order to generate the keys with the length m and the security degree ε. Smaller m_0 is more desirable, but it can decrease the key generation rate. For example, some security degrees becomes unavailable (i.e. the key refresh rate falls to zero) when the length of the external pair of keys becomes too small, or more rounds in the authentication protocol,[31] which require additional time, are needed in order to generate keys with the same security degree, but having the external pair of keys with a shorter length.

Therefore, $R(m, \varepsilon, m_0) = r$ times/s means that Alice and Bob using the QKD system can refresh r times per second their keys with the length m and security degree ε, and before each refreshing, they must have for that at the average m_0 bits of the perfectly secure external keys (if the external keys are not perfectly secure, then they must be longer than m_0).

Now, in order to define the key generation rate, we should take $m \to \infty$ and $m_0 \to \infty$ so that $m_0/m = D =$ const. We will call the amount D the *external key consumption rate*. Thus, in this case, the key generation rate depends on two parameters: the security degree ε and the external key consumption rate D. Since $m_0 = [Dm]$, where $[x]$ denotes the floor of the real number x, i.e. the integer nearest to x from below, we define the key generation rate as

$$V(\varepsilon, D) = \lim_{m \to \infty} \frac{m}{T(m, \varepsilon, \gamma, [Dm], 1)}. \tag{10}$$

Knowing m, m_0 and $V(\varepsilon, \frac{m_0}{m})$ one can calculate $R(m, \varepsilon, m_0)$ by the formula,

$$R(m, \varepsilon, m_0) \approx \frac{V(\varepsilon, \frac{m_0}{m})}{m}. \tag{11}$$

Of course, it makes no sense to decrease the security degree to zero, or to increase the external key consumption rate to one or greater (in the first case, the optimal way for Alice and Bob is to generate two keys independently, in the latter case the optimal way is to use the external pair of keys for the direct purpose instead of generating a pair with shorter lengths). Hence, the domain of the function $V(\varepsilon, D)$ is $0 < \varepsilon \leq 1$, $0 \leq D < 1$.

It is reasonable to suppose that V is a continuous function on its domain, a non-increasing function of ε and a non-decreasing function of D.

Note that the concept of secret key rate has been introduced in Ref. 29. This is the limit of the ratio of the number of key bits to the whole number of the transmitted bits. This concept is important in the information-theoretic sense, but not so useful for practice, because it considers neither the time of computation nor the technical aspects such as the transmission time.

In contrast, our concept of key generation rate is rather engineering-inclined, because it is derived from the full time of the key generation process, i.e. exactly what the user wants to know.

3.4.3. *Upper bound of security degrees*

One more important functional characteristic of the QKD system is the upper bound of the security degrees which can be achieved with the given external key consumption rate. It cannot decrease as the external key consumption rate D increases. We define this function $\varepsilon_{\max}(D)$ of D, $0 < \varepsilon \leq 1$, with the following formula:

$$\varepsilon_{\max}(D) = \min\{\varepsilon | V(\varepsilon, D) = 0\}. \tag{12}$$

By implication, $\varepsilon_{\max}$ is a continuous function on its domain and a non-decreasing function of D.

Since there is the security degree among the arguments of the functions T and V, it is necessary to point out the class of attacks (see Sec. 2.4) relative to which the keys have the declared security.

In view of the key degradation problem (see Sec. 2.5), we will distinguish the systems with *one-time* and *permanent external key consumption*. Formally, we will say that the system needs the maximum one-time external key consumption (no key degradation problem), if $V(\varepsilon, D) = \text{const.}$ when ε is fixed (hence, $\varepsilon_{\max}(D) = \text{const}$). Otherwise, we will say that the system needs permanent external key consumption.

3.5. *Numeric engineering and end-user characteristics of QKD systems*

Thus, for engineering description of the QKD system, we have proposed the functions $T = T(m, \varepsilon, \gamma, m_0, \varepsilon_0)$, $V(\varepsilon, D)$, and $\varepsilon_{\max}(D)$.

It is worthwhile to simplify these functional characteristics to a set of numerical characteristics for QKD systems which may be useful both for engineers and end-users. Hence, there is a problem of choosing a set of numbers which describes the functions well.

3.5.1. *No key degradation case*

At first, we consider the simple case of the one-time external key consumption rate, i.e. $V(\varepsilon, D) = V(\varepsilon, 0) = V(\varepsilon)$ and $\varepsilon_{\max}(D) = \text{MAXS} = \text{const}$.

It is clear that we are interested in the generation of keys with the most achievable security degrees. We are not interested in the behavior of the function $V(\varepsilon)$ in the area where ε is close to zero. Hence, we must choose some numerical characteristic of the function $V(\varepsilon)$ which concerns the interesting area.

Firstly, we are interested in the upper bound MAXS of the achievable security degrees. By continuity of the function V, $V(\text{MAXS}) = 0$, we can generate keys only at rates smaller than MAXS. But there is a difference how fast this increases the rate as the security degree decreases from MAXS. In order to characterize this, we approximate the function $V(\varepsilon)$ by its tangent at the point MAXS and introduce the *marginal increment of the key generation rate* (MIR),

$$\text{MIR} = -\left.\frac{dV(\varepsilon)}{d\varepsilon}\right|_{\varepsilon=\text{MAXS}}, \tag{13}$$

where the derivative is left-sided (since $V(\varepsilon)$ hits zero in MAXS, this point may be salient). Since $V(\varepsilon)$ is a non-increasing function, $dV(\varepsilon)/d\varepsilon \leq 0$ and $\text{MIR} \geq 0$. Hence, the key generation rate with the desirable security degree of the pair of keys ε is approximately calculated by

$$V(\varepsilon) \approx \text{MIR}(\text{MAXS} - \varepsilon). \tag{14}$$

Vice versa, the security degree of the pair of keys generated at a given rate V is calculated by

$$\varepsilon(V) \approx \text{MAXS} - \frac{V}{\text{MIR}}. \tag{15}$$

Hence, in this simple (but practical) case, we only need two numbers in order to approximately characterize a QKD system: the *marginal security degree* MAXS, $0 < \text{MAXS} \leq 1$, and the marginal increment of key generation rate MIR, $0 \leq \text{MIR} < \infty$. If a QKD system has greater MAXS and MIR than another one, then the first QKD system is better because it allows us to generate more secure keys at higher rates.

3.5.2. *The general case*

Now we consider the general case. We are interested in the key generation with the maximal security degree and the minimal external key consumption rate, i.e. in the area where ε is close to one and D is close to zero. But the difficulty is that $\varepsilon(0)$ can be far from one and this is an unacceptable variant. Hence, the user has to find compromise values of ε and D.

The value that characterizes the quality of the QKD system is the minimal achievable distance of the curve $\varepsilon_{\max}(D)$, $0 \leq D < 1$, to the point $(\varepsilon = 1, D = 0)$:

$$\text{DIST} = \min_{0 \leq D < 1} \sqrt{a(\varepsilon_{\max}(D) - 1)^2 + bD^2}, \tag{16}$$

where $a > 0$ and $b > 0$, $a + b = 1$, are some fixed coefficients. For example, one can take $a = b = 0.5$. But it may be useful to set a and b so that $a > b$, because the security degree and the external key consumption rate are not equivalent amounts. For example, $D = 0,1$ (i.e. on each 10 bits of the new keys, one has to spend 1 bit of the external keys) may be acceptable, but the security degree $\varepsilon = 1 - 0,1 = 0,9$ may be too small. If $a > b$, one pays a larger penalty for the distance ε from one than for the distance D from zero. Optimal values of D and ε with respect to this distance we denote by D^* and $\varepsilon^* = \varepsilon_{\max}(D^*)$. These values can also be used as a characteristic of the QKD system. These are the parameters at which key generation is optimal.

But $V(\varepsilon^*, D^*) = 0$ by definition of the function $\varepsilon_{\max}(D)$ and continuity of the function $V(\varepsilon, D)$. As in the case $D = 0$, we have to introduce a characteristic showing how fast the key generation rate increases when ε decreases from ε^* and D remains constant. We define the marginal increment (MIR) of the key generation rate as

$$\mathrm{MIR} = -\left.\frac{\partial V(\varepsilon, D)}{\partial \varepsilon}\right|_{(\varepsilon^*, D^*)}, \tag{17}$$

where the derivative is left-sided.

We are also interested in the ends of the function $\varepsilon_{\max}(D)$. Consider the right end. There are two possibilities for either $\varepsilon_{\max}(0) > 0$ or $\varepsilon_{\max}(0) = 0$. In the latter case, define

$$D_{\min} = \inf\{D | \varepsilon_{\max}(D) > 0\}. \tag{18}$$

Of course, the first case is more preferable than the second one. In the first case, it is possible to generate pairs of keys with some security degree without external key consumption. In the second case, the external key consumption rate cannot be smaller than $D_{\min}$ even if we want to generate a pair of keys with very small security degree. We define the quantity

$$\mathrm{SOC} = \begin{cases} -D_{\min}, & \text{if } D_{\min} > 0 \\ \varepsilon_{\max}(0), & \text{if } D_{\min} = 0 \end{cases}, \tag{19}$$

which we will call the *security degree of the pair of keys without the external key consumption*. Negative SWE corresponds to the second case where the external key consumption rate cannot be smaller than some value (−SWE).

Similarly, we analyze the right end of the function $\varepsilon_{\max}(D)$, i.e.

$$\varepsilon_{\max}(1) \overset{\text{def}}{=} \lim_{D \to 1} \varepsilon_{\max}(D). \tag{20}$$

There are also two possibilities: $\varepsilon_{\max}(1) = 1$ or $\varepsilon_{\max}(1) < 1$. In the first case, define

$$D_{\max} = \min\{D | \varepsilon_{\max}(1) = 1\}. \tag{21}$$

The first case is more preferable than the second one. In the first case, it is possible to generate keys with the security arbitrarily close to perfect with the external key consumption rate less than the amount $D_{\max} \leq 1$. In the second case, the security degree cannot be larger since $\varepsilon_{\max}(1) < 1$ even if the external key consumption rate is very close to one. We define the quantity

$$\mathrm{GMC} = \begin{cases} -(1 - \varepsilon_{\max}(1)), & \text{if } \varepsilon_{\max}(1) < 1 \\ 1 - D_{\max}, & \text{if } \varepsilon_{\max}(1) = 1 \end{cases}, \tag{22}$$

which we will call the *gain at the maximal external key consumption.*

Thus, we obtain six characteristics of the QKD system with the external key consumption: $DIST$, ε^*, D^*, MIR, SOC and GMC.

Approximately, the key generation rate at a point (ε, D), $\varepsilon \leq \varepsilon_{\max}(D)$ is given by

$$V(\varepsilon, D) \approx \mathrm{MIR}(\varepsilon_{\max}(D) - \varepsilon). \tag{23}$$

It is assumed that the user generates the keys with the parameters near the optimal point (ε^*, D^*), so, $\varepsilon_{\max}(D) \approx \varepsilon_{\max}(D^*) = \varepsilon^*$. Also, the user, knowing the above numeric characteristics, can approximately (rather roughly) calculate the key generation rate at a point (ε, D), $\varepsilon \leq \varepsilon_{\max}(D)$, by the formula

$$V(\varepsilon, D) \approx \mathrm{MIR}(\varepsilon^* - \varepsilon). \tag{24}$$

Vice versa, the security degree of the pair of keys generated at a given rate V and external key consumption rate D is calculated by

$$\varepsilon(V, D) \approx \varepsilon^* - \frac{V}{\mathrm{MIR}}. \tag{25}$$

D^* is an approximate value of the external key consumption rate, if the user generates the keys at a point near the optimum. SOC and GMC do not participate in these approximations, but they characterize the potential abilities of a QKD system. Also, DIST is a characteristic of the quality of a system.

Consider the simple case with no external key consumption from the point of view of the general case. It was said before that $V(\varepsilon, D) = \text{const.}$, when ε is fixed, and $\varepsilon_{\max}(D) = \text{const.} = \mathrm{MAXS}$. Evidently, $D^* = 0$, $\varepsilon^* = \mathrm{MAXS} = \mathrm{SOC}$ and $\mathrm{DIST} = 1 - \mathrm{MAXS}$. $\mathrm{GMC} = -(1 - \mathrm{MAXS})$, if $\mathrm{MAXS} < 1$, and $\mathrm{GMC} = 1$, if $\mathrm{MAXS} = 1$. The quantity MIR coincides with the same quantity that we defined for the simple case. Thus, one can use these characteristics for both the general and simple cases.

3.6. *The list of characteristics for the specification*

Of course, besides these numeric characteristics, the user must have knowledge about the assumptions of the adversary and the distance within which these characteristics are valid. Finally, we propose the following list of qualitative and quantitative characteristics which can be included in the specification:

(i) The assumed degree of the adversary's mastering of quantum technologies: incomplete/complete.

(ii) Method of providing with the authenticity of the classical channel: technological/mathematical.

(iii) The assumed adversary's computing power: limited/unlimited.

(iv) Distance from the ideal DIST (variation interval is $[0,1)$, dimensionless value).

(v) The optimal security degree ε^* (variation interval is $(0,1]$, dimensionless value).

(vi) The optimal external key consumption rate D^* (variation interval is $[0,1)$, dimensionless value).

(vii) Marginal increment of the key generation rate MIR (variation interval is $(0,\infty)$, bits/s).

(viii) Security degree of the pair of keys without the external key consumption SOC (variation interval is $(-1,1]$, dimensionless value).

(ix) Gain at the maximal external key consumption GMC (variation interval is $(-1,1]$, dimensionless value).

(x) The distance within which these characteristics are valid (km).

A larger value of each of the numeric characteristics [except (iv)] is preferable. In the first three (qualitative) characteristics, the second value is preferable.

It is assumed that the producer of the QKD system has to give to the engineer the functions T, V, $\varepsilon_{\max}$ (analytical formulas or graphics) and characteristics 1–10. To the end-user, the producer has to give characteristics 1–10.

The present-day commercial quantum cryptography solutions have the encryption systems (e.g. AES and 3DES) attached to the QKD systems. The security of these encryption protocols when the keys are perfectly secure is a problem of conventional cryptography, but the above (or similar) characteristics about the security of keys and key generation must be given.

In Sec. 3.3, we have introduced three characteristics for the simplest case: security degree ε, length of keys m and key refresh rate R. Length of keys m drops out since m is not a constant any more. In the general case the user can choose any m. Security degree ε is also not a constant any more, but some information about the values that ε can have is given in characteristics (iv) and (v) (in the case with no key degradation problem, these characteristics are equal). $R(m,\varepsilon)$ as a function of m and ε, which specifies the user, can be calculated from formulas (11) and (24).

For the end-user, ten characteristics may be too many and it is necessary to reduce the number of characteristics. Firstly, some of the above characteristics may be equal for all or for a very wide class of the QKD systems and will be eliminated. Secondly, some of these characteristics may be for engineers rather then for end-users. In our opinion, characteristics (i)–(iv), (vii) and (x) (i.e. three qualitative and three quantitative characteristics) are the most important for the user.

Acknowledgments

This work was partially supported by the Russian Foundation of Basic Research (project 05-01-00884), the grant of the President of the Russian Federation (project

NSh-1542.2003.1) and the program "Modern problems of theoretical mathematics" of the Mathematical Sciences Department of the Russian Academy of Sciences.

Appendix. Definition of the security degree of pair of keys

Definition 1 (see Refs. 17 and 18). Let $\mathcal{K}$ be a finite or a countable set, K_A, K_B be a pair of random variables (keys) on $\mathcal{K}$ with a joint distribution P_{K_A,K_B}. Let, further, $\mathcal{H}_{AB}, \mathcal{H}_E$ be Hilbert spaces, $\dim \mathcal{H}_{AB} = |\mathcal{K}|^2$, $\{|k_A, k_B\rangle\}_{k_A,k_B\in\mathcal{K}}$ be an orthonormal base of $\mathcal{H}_{AB}$. The pair of keys (K_A, K_B) is called *ε-secure* relative to the joint (with the adversary) quantum state

$$\rho = \sum_{k_A,k_B\in\mathcal{K}} P_{K_AK_B}(k_A,k_B)|k_A,k_B\rangle\langle k_A,k_B| \otimes \rho^E_{k_A,k_B} \in \mathcal{S}(\mathcal{H}_{AB}\otimes\mathcal{H}_E), \quad \text{(A.1)}$$

where

$$\rho^E_{k_A,k_B} \in \mathcal{S}(\mathcal{H}_E), \quad k_A, k_B \in \mathcal{K}, \quad \text{(A.2)}$$

if

$$\delta(\rho, \rho_{\text{ideal}}) \le 1 - \varepsilon, \quad \text{(A.3)}$$

where

$$\rho_{\text{ideal}} = \left(\sum_{k\in\mathcal{K}} \frac{1}{|\mathcal{K}|}|k,k\rangle\langle k,k|\right) \otimes \left(\sum_{k_A,k_B\in\mathcal{K}} P_{K_AK_B}(k_A,k_B)\rho^E_{k_A,k_B}\right). \quad \text{(A.4)}$$

Here $\delta(\cdot,\cdot)$ is the distance between two quantum states. For arbitrary $\sigma, \eta \in \mathcal{S}(\mathcal{H})$ where $\mathcal{H}$ is a Hilbert space,

$$\delta(\sigma,\eta) = \|\sigma - \eta\|_1 \overset{\text{def}}{=} \sum_{\lambda\in\,\text{spec}(\sigma-\eta)} |\lambda|. \quad \text{(A.5)}$$

Let $\mathcal{X}$ be a finite set. The *variational distance* between two probability distributions (classical states) P and Q on this set

$$\delta(P,Q) = \frac{1}{2}\sum_{x\in\mathcal{X}} |P(x) - Q(x)|, \quad \text{(A.6)}$$

is the classical analog and a particular case of the above distance between quantum states.

For the distance $\delta(\cdot,\cdot)$, the following properties are satisfied. $\mathcal{H}, \mathcal{H}'$ are arbitrary Hilbert spaces and $\sigma, \eta \in \mathcal{S}(\mathcal{H})$, $\sigma', \eta' \in \mathcal{S}(\mathcal{H}')$ are arbitrary states.

(i) $$\delta(\sigma\otimes\sigma', \eta\otimes\eta') \le \delta(\sigma,\eta) + \delta(\sigma',\eta'), \quad \text{(A.7)}$$
with equality if $\sigma' = \eta'$.

(ii) For arbitrary function (quantum operation) $\mathcal{E}$ on $\mathcal{S}(\mathcal{H})$,

$$\delta(\mathcal{E}(\sigma), \mathcal{E}(\eta)) \leq \delta(\sigma, \eta). \tag{A.8}$$

In a particular case, if $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$, $\sigma = \sigma_1 \otimes \sigma_2$, $\eta = \eta_1 \otimes \eta_2$, $\sigma_1, \eta_1 \in \mathcal{H}_1$, $\sigma_2, \eta_2 \in \mathcal{H}_2$ and $\mathcal{E}(\sigma_1 \otimes \sigma_2) = \sigma_1$, $\mathcal{E}(\eta_1 \otimes \eta_2) = \eta_1$, then

$$\delta(\sigma_1, \eta_1) \leq \delta(\sigma_1 \otimes \sigma_2, \eta_1 \otimes \eta_2). \tag{A.9}$$

It implies that we can divide the pairs of keys into shorter pairs of keys with the same degree of security (see Sec. 2.2).

(iii) Consider the probability distributions P and Q of the outcomes when the same measurements to σ and η, respectively, is applied. Then

$$\delta(P, Q) \leq \delta(\sigma, \eta). \tag{A.10}$$

References

1. C. H. Bennett and G. Brassard, in *Proc. IEEE Int. Conf. Computers, Systems, and Signal Processing*, Bangalore, India, 1984, pp. 175–179.
2. BBN Technologies, Cambridge, USA [http://www.bbn.com/].
3. id Quantique SA, Geneva, Switzerland [http://www.idquantique.com/].
4. MagiQ Technologies, New York, USA [http://www.magiqtech.com/].
5. NEC Corporation, Tokyo, Japan [http://www.nec.com/].
6. QinetiQ, Farnborough, UK [http://www.qinetiq.com/].
7. Toshiba Research Europe, Cambridge, UK [http://www.toshiba-europe.com/].
8. A. K. Ekert, *Phys. Rev. Lett.* **67**(6) (1991) 661–663.
9. A. Poppe *et al.*, Practical quantum key distribution with polarization entangled photons [quant-ph/0404115].
10. H.-K. Lo, Will quantum cryptography ever become a successful technology in the marketplace? [quant-ph/9912011].
11. N. Gisin *et al.*, Quantum cryptography [quant-ph/0101098].
12. I. V. Volovich and Ya. I. Volovich, On classical and quantum cryptography [quant-ph/0108133].
13. U. M. Maurer, in *Proc. 4th IMA Conf. Cryptography and Coding*, The Institute of Mathematics and Its Applications, Southend-on-Sea, England (1993), pp. 49–71.
14. B. Schneier, *Applied Cryptography*: *Protocols, Algorithms and Source Code in C* (John Wiley and Sons, Inc., New York, 1996).
15. W. Diffie and M. E. Hellman, *IEEE Trans. Inform. Theory* **22**(6) (1976) 644–654.
16. C. E. Shannon, *Bell Syst. Tech. J.* **28** (1948) 656–715.
17. M. Ben-Or *et al.*, The universal composable security of quantum key distribution [quant-ph/0409078].
18. R. Renner and R. König, in *Second Theory of Cryptography Conference*, TCC 2005, Lecture Notes in Computer Science, Vol. 3378 (Springer, 2005), pp. 407–425.
19. M. Ben-Or and D. Mayers, General security definition and composability for quantum and classical protocols [quant-ph/0409062].
20. R. König *et al.*, On the power of quantum memory [quant-ph/0305154].
21. M. Christandl, R. Renner and A. Ekert, A generic security proof for quantum key distribution [quant-ph/0402131].
22. A. S. Trushechkin and I. V. Volovich, General model of quantum key distribution [quant-ph/0504156].

23. H. P. Yuen, KCQ: A new approach to quantum cryptography. I. General principles and key generation [quant-ph/0311061].
24. K. G. Paterson *et al.*, Why quantum cryptography? [quant-ph/0406147].
25. R. Renner and S. Wolf, in *Advances in Cryptology — EUROCRYPT '04*, Lecture Notes in Computer Science, Vol. 3027 (Springer-Verlag, 2004), pp. 109–125.
26. V. V. Yashchenko *et al.*, *Introduction to Cryptography* (Piter, Saint-Petersburg, 2001) (in Russian).
27. B. Schneier, *IEEE Comput.* **21**(9) (1998) 29–33.
28. I. Csiszár and J. Körner, *IEEE Trans. Inform. Theory* **24**(3) (1978) 339–348.
29. U. M. Maurer, *IEEE Trans. Inform. Theory* **39**(3) (1993) 733–742.
30. P. W. Shor and J. Preskill, *Phys. Rev. Lett.* **85** (2000) 441–444.
31. P. Gemmel and M. Naor, in *Advances in Cryptology — Proc. Crypto '93*, Lecture Notes in Computer Science, Vol. 773 (Springer-Verlag, Berlin, 1994), pp. 355–367.