ISSN 0021-3640, JETP Letters, 2013, Vol. 97, No. 10, pp. 604–610. © Pleiades Publishing, Inc., 2013.
Original Russian Text © S.N. Molotkov, 2013, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2013, Vol. 97, No. 10, pp. 693–699.

On the Quantum-Mechanical Bound on the Loss of Information through Side Channels in Quantum Cryptography

S. N. Molotkov

Academy of Cryptography of the Russian Federation, Moscow, 121552 Russia
Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, 142432 Russia
Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow, 119991 Russia

Received March 11, 2013; in final form, April 15, 2013

The security of cryptographic keys in quantum cryptography systems is guaranteed by fundamental quantum mechanical exclusion principles. A quantum channel through which quantum states are transferred is not controlled and an eavesdropper can perform any modifications with it. The security of quantum key distribution protocols has already been proved [M. Tomamichel et al., Nature Commun. **3**, 634 (2011); S. N. Molotkov, J. Exp. Theor. Phys. **115**, 969 (2012)], including the realistic case of a finite length of transmitted sequences. It is always assumed that the eavesdropper has neither direct nor indirect access to the transmitting and receiving equipment. The real situation is somewhat different. The preparation and detection of quantum states occur according to random sequences that are generated on the transmitter and receiver sides. Detecting electromagnetic radiation generated in these processes, the eavesdropper can obtain additional information on a key. The upper quantum-mechanical bound on the amount of information of the eavesdropper on the key that can be obtained through a side channel has been determined.

DOI: 10.1134/S002136401310007X

INTRODUCTION

Side leakage channels are efficient sources of unauthorized acquisition of information [1]. A source of information can be a certain physical device (source of acoustic, mechanical, optical, or electromagnetic signals). The side channel associated with the emission of an electromagnetic field in the process of generation of random numbers in quantum cryptography will be considered below. As far as I know, this problem has not yet been discussed in this context.

To reduce information that can be obtained through the side channel, an initial signal is weakened and/or made noisy. Therefore, any weak desired signal can be efficiently amplified and separated from noise. For this reason, there is no upper bound on the leakage of information. Information that can be obtained by the eavesdropper depends on the technical properties of his detection equipment. Such a situation is fundamentally unsatisfactory. Nobody can be sure that the eavesdropper does not have equipment with characteristics better than those initially assumed.

The main questions are as follows. (i) Does an upper bound on the leakage of information that with certainty cannot be increased by the eavesdropper with the further development of technologies exist at given parameters (e.g., attenuation of the initial signal)? (ii) How does the upper bound depend on the signal attenuation controlled by legitimate users and can it be decreased to any preset small value?

The fundamental difference of the eavesdropping of states in the quantum communication channel from the detection of radiation states in the side channel is as follows.

(a) Information states sent to the quantum communication channel are controllably weakened so that quantum states with known properties are sent to the communication channel on the receiver side. (b) Quantum states are measured on the receiver side in order to, first, obtain information on the transmitted bit and, second, estimate the degree of distortion of quantum states in the process of transmission from the observed errors and, then, relate the upper bound of the eavesdropper's information on transmitted states to their observed distortions. (c) Further, the degree of distortion (upper bound of eavesdropper's information) makes it possible to determine the degree of compression of the key cleaned from errors to the final secret key.

(a) If states are not controlled (this is usually not discussed), states with uncontrolled intensities escape to the side channel. Further, legitimate users do not follow the detection and distortions of these states. For this reason, states should be immediately weakened to the level such that information on the key that can be obtained by the eavesdropper will be as small as is wished; i.e., the classical side channel should be transformed to a quantum one. It is fundamentally important that the complete screening of states in the side channel is not required in practice because this cannot

be ensured. The level of the signal in the side channel makes it possible to choose the degree of key compression at which the eavesdropper cannot obtain information on the key from the side channel.

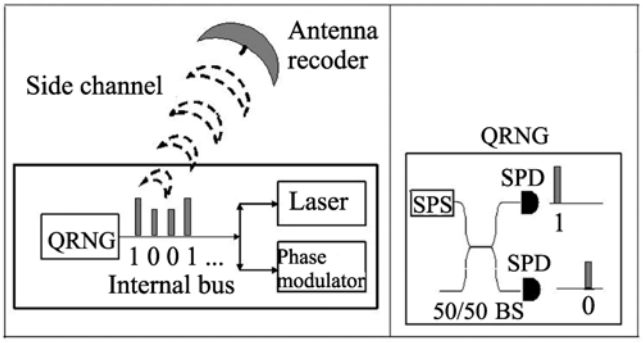
The aim of the eavesdropper in the first case is to obtain maximum information on the key from the quantum channel and to minimally distort transmitted states. The aim of the eavesdropper in the second case is to obtain maximum information on the states from the side channel without taking care of introduced distortions. Universal hashing is used to eliminate information in both cases. Such a hashing in the case of the side channel has not yet been discussed and used.

INFORMAL FORMULATION OF THE PROBLEM

The problem will be formulated more accurately in this section in application to quantum key distribution systems. Independent random number generators for 0 and 1 on the transmitter and receiver sides are one of the main elements in quantum cryptography systems. According to these random sequences, quantum states are prepared on the transmitter side and measurements are chosen on the receiver side. It is always implied that random number sequences are *completely unavailable* to the eavesdropper. The eavesdropper cannot directly read the sequences by cracking equipment, but can have certain access to these sequences through the side channel.

There are numerous different physical methods for obtaining random numbers. Many methods are reduced to the digitization of a certain classical noise signal (e.g., current noise in the channel of a field-effect transistor). However, the detailed analysis indicates that the real physical reason for the appearance of classical noise has a quantum nature. True randomness is absent in classical physics, because the evolution of any system in classical physics is described by differential equations and the state of the system is unambiguously determined by initial conditions. The situation in quantum physics is fundamentally different. Even upon the same preparation of the initial state and subsequent evolution, which is also described by differential equations, a quantum-mechanical measurement provides an unpredictable result. In this sense, any true randomness has a quantum origin.

To understand the reason for side radiation, we consider the generation of a random sequence. One of the methods of the generation of a random sequence of 0 and 1 involves the detection of single-photon states (really quasi-single-photon, but this is unimportant now) at one of the exits of a fiber beam splitter (see figure). In this method, the fundamental uncertainty of a quantum-mechanical measurement outcome is explicitly used. If a single-photon packet propagates through two different paths, detection occurs randomly and unpredictably only in one path. An outcome in one arm of the beam splitter is interpreted as logical 0, whereas an outcome in the other arm is treated as logical 1. In the case of the strictly single-photon packet, measurement outcomes, as well as the resulting sequence of 0 and 1, are actually random and uniformly distributed. The detection of a photon leads to a current pulse in one of the single-photon detectors; this pulse after necessary amplification is transmitted through an internal bus to other control devices (see figure). Thus, random numbers appear *only at the time of detection (measurement) of a photon* (flow of a current pulse in a photodetector). Until this time, random numbers are not generated.



Scheme of the generation and transmission of random numbers on the transmitter side: QRNG is the quantum random number generator, SPS is the source of single-photon or quasi-single-photon states, and SPD is the photodetector.

Radiation appears already when a current flows through the photodetector. However, this is not the main side radiation channel. Random bits 0 or 1 (current pulses after the detection of a photon in the corresponding photodetector) are transferred through the internal bus to other devices (laser control, phase modulator, etc.). Different voltages correspond to logical 0 and 1 when pulses are transferred through the bus. Transfer through the conductors of the internal bus is responsible for intense side electromagnetic radiation, which can be detected by the eavesdropper.

QUANTUM STATES OF RADIATION IN THE SIDE CHANNEL

A decrease in the intensity of classical fields is inevitably accompanied by an increase in the fraction of the vacuum component; this increase should lead to an increase in the error of distinguishing between two states of the field. The maximally weakened field mainly consists of the vacuum component. According to quantum mechanics, even "classical" quantum states with a macroscopically large average number of photons are not ideally distinguishable in view of the presence of the vacuum component. However, the probability of an error when distinguishing between such states is negligibly small. Two quantum observ-

ables (density matrices) are certainly distinguishable if their supports are in orthogonal subspaces, i.e., they do not overlap: $\mathrm{supp}(\rho_0) \cap \mathrm{supp}(\rho_1) = \emptyset$. The minimum error of distinguishing between two quantum states ρ_0 and ρ_1 is given by the expression (for details, see [4])

$$Q_{\min} = \pi_0 + \sum_{\lambda_j < 0} \lambda_j . \quad (1)$$

Here, λ_j are the eigenvalues of the operator $\pi_1\rho_1 - \pi_0\rho_0$, where π_0 and π_1 are the probabilities of the preparation of the density matrices ρ_0 and ρ_1, respectively. According to Eq. (1), if the supports of the density matrices do not overlap, the distinguishing error is zero. An attenuation-induced increase in the vacuum component inevitably leads to a decrease in the distinguishability of two states in measurements.

Since only the power of the signal is fixed when generating random numbers, the radiation state is not a pure state, but is described by the density matrix. The density matrices of the electromagnetic radiation, which can be detected within the entire range of solid angles, that correspond to 0 and 1 can be represented in the form (see, e.g., [5])

$$\rho^{(0,1)} = \sum_{\omega} \left(\sum_{m_\omega = 0}^{N_\omega^{(0,1)}} p_{m_\omega}^{(0,1)} |m_\omega\rangle\langle m_\omega| \right), \quad \langle m_\omega | n_{\omega'} \rangle = \delta_{m_\omega, n_{\omega'}}, \quad (2)$$

where $|n_{\omega'}\rangle$ is the Fock state with the number of photons n_ω with the frequency ω. The normalization condition for the density matrices has the form $\sum_\omega (\sum_{m_\omega = 0}^{N_\omega^{(0,1)}} p_{m_\omega}^{(0,1)}) = 1$. Here, $N_\omega^{(0,1)}$ is the minimum number of photons in the spectral model with the frequency ω for states corresponding to 0 and 1, and $p_{m_\omega}^{(0,1)}$ is the probability (the fraction of photons in the spectral component with the frequency ω). The vacuum component of the field corresponds to the coefficients $p_{m_\omega}^{(0,1)}$ with zero Fock occupation numbers $m_\omega = 0$.

The particular structure of the density matrix of radiation appearing when transmitting voltage pulses corresponding to 0 or 1 through the data bus or interunit connections is determined by the type of cable, etc. It can be obtained from the solution of the corresponding electrodynamic problem for a given device, which gives particular numerical coefficients $p_{m_\omega}^{(0,1)}$ of the density matrix. These coefficients are assumed to be known. Their explicit form will not be required for the general answer.

The initial unweakened quantum states of radiation are related to a random bit string $X = \{0, 1\}^{N_{\mathrm{key}}}$ (N_{key} is the length of the string),

$$(|x\rangle \otimes \rho^{(x)})^{\otimes N_{\mathrm{key}}} = (|x_{i_1}\rangle \otimes \rho^{(x_{i_1})}) \otimes (|x_{i_2}\rangle) \otimes \rho^{(x_{i_2})} \otimes \ldots \otimes (|x_{N_{\mathrm{key}}}\rangle \otimes \rho^{(x_{N_{\mathrm{key}}})}). \quad (3)$$

Below, it is convenient to make a correspondence of classical bits $x = 0, 1$ to orthogonal certainly distinguishable quantum states $|x\rangle$ *available only to the legitimate users*.

Let T_ω be the attenuation coefficient of the spectral component owing to the screening of equipment. The joint state of the initial radiation and equipment before absorption is a united quantum state. The equipment of legitimate users in which attenuation occurs has a macroscopically large number of degrees of freedom over which averaging is performed. For this reason, the radiation state after absorption is described by the density matrix. Screening transforms each side channel as follows (see, e.g., [6]):

$$|m_\omega\rangle\langle m_\omega| \longrightarrow \sum_{k_\omega = 0}^{m_\omega} C_{k_\omega}^{m_\omega} T_\omega^{k_\omega} (1 - T_\omega)^{m_\omega - k_\omega} |k_\omega\rangle\langle k_\omega|. \quad (4)$$

The density matrix available to the eavesdropper has the form

$$\rho_E^{(0,1)} = \sum_\omega \left[\sum_{m_\omega = 0}^{N_\omega^{(0,1)}} p_{m_\omega}^{(0,1)} \times \sum_{k_\omega = 0}^{m_\omega} C_{k_\omega}^{m_\omega} T_\omega^{k_\omega} (1 - T_\omega)^{m_\omega - k_\omega} |k_\omega\rangle\langle k_\omega| \right]. \quad (5)$$

This means that the fraction T_ω of each side channel is absorbed as a result of screening and becomes unavailable to the eavesdropper and the fraction $1 - T_\omega$ leaves equipment and becomes available to the eavesdropper. In the presence of the strong damping in the system, $\max_\omega\{N_\omega^{(0,1)} T_\omega\} \ll 1$, up to the terms linear in T_ω, we obtain

$$|m_\omega\rangle_{AA}\langle m_\omega| \longrightarrow (1 - T_\omega)^{m_\omega} (|\mathrm{vac}\rangle\langle \mathrm{vac}| + m_\omega T_\omega |1_\omega\rangle_{EE}\langle 1_\omega|), \quad (6)$$

where $|\mathrm{vac}\rangle$ is the vector of the vacuum state of the field common for all ω values. In the limit of small occupation numbers, density matrix (5) becomes

$$\rho_E^{(0,1)} = \left[(1 - \overline{N}^{(0,1)}) |\mathrm{vac}\rangle\langle \mathrm{vac}| + \sum_\omega \overline{N}_\omega^{(0,1)} |1_\omega\rangle\langle 1_\omega| \right], \quad (7)$$

where $\overline{N}_\omega^{(0,1)} = \sum_{m_\omega}^{N_\omega^{(0,1)}} p_{m_\omega}^{(0,1)} m_\omega T_\omega \ll 1$ is the average occupation number over the frequency modes and $\overline{N}^{(0,1)} = \sum_\omega \overline{N}_\omega^{(0,1)}$. The correlation between a random bit string with the length N_{key} and the eavesdropper's quantum states in the side channel is given by the tensor product similar to Eq. (3), where $\rho_{XE} = \sum_{x=0,1} |x\rangle\langle x| \otimes \rho_E^{(x)}$ is the density matrix.

INDIVIDUAL MEASUREMENTS

The aim of the eavesdropper is reduced to distinguish between two density matrices $\rho_E^{(0)}$ and $\rho_E^{(1)}$. Taking into account Eq. (7), the minimum distinguishing error in individual measurements of the radiation state in each position in the case of the uniform distribution of 0 and 1 on a random number generator ($\pi_0 = \pi_1 = 1/2$) is

$$Q_{\min} = (1-q)/2. \tag{8}$$

Here, q is determined by negative eigenvalues of $\rho_E^{(0)} - \rho_E^{(1)}$. Taking into account Eq. (7), $q = \left|(1-\overline{N}^{(0)}) - (1-\overline{N}^{(1)})\right|$. Since the density matrices are normalized to unity, $(1-\overline{N}^{(0)}) - (1-\overline{N}^{(1)}) = -[(\sum_\omega \overline{N}_\omega^{(0)}|1_\omega) - (\sum_\omega \overline{N}_\omega^{(1)}|1_\omega)]$. In individual measurements of the state of side radiation in each individual position, the eavesdropper and legitimate users are in the situation of a classical binary symmetric channel with the error probability $Q_{\min}$. The average number $I(A; E)$ of information bits per position (mutual information) between the legitimate users (A) and eavesdropper (E) that the eavesdropper can obtain is limited by the classical transmission capacity [7], is determined only by the error $Q_{\min}$, and does not exceed

$$\begin{aligned} I(A;E) &< C_{\text{cl}}(Q_{\min}) \\ &= -Q_{\min}\log Q_{\min} - (1-Q_{\min})\log(1-Q_{\min}), \end{aligned} \tag{9}$$

$I(A; E)$ tends to unity in the limit $Q_{\min} \longrightarrow 0$.

COLLECTIVE MEASUREMENTS

Bound (9) is not an upper bound of information in quantum mechanics because the eavesdropper is not restricted to individual measurements. Quantum mechanics allows more efficient collective measurements. In this case, the eavesdropper performs measurements immediately over the entire sequence of radiation quantum states, using quantum memory, and, then, performing measurements with the sequence as a united quantum state. The aim of the eavesdropper is reduced to distinguishing between entire sequences of quantum states. In this case, the legitimate users and eavesdropper are in the situation of a quantum–classical communication channel. The upper bound of information that the eavesdropper can extract from these measurements is limited by the fundamental Holeveo value $\chi(\rho_{\text{E}}^{(0,1)})$ [4]. This value is achievable in collective measurements and gives an upper bound for classical information that can be obtained from the ensemble of quantum states [4]. As a result,

$$\begin{aligned} I(A;E) &< \chi(\rho_{\text{E}}^{(0,1)}) = \overline{C} \\ &= H[(\rho_{\text{E}}^{(0)} + \rho_{\text{E}}^{(1)})/2] - [H(\rho_{\text{E}}^{(0)}) + H(\rho_{\text{E}}^{(1)})]/2, \end{aligned} \tag{10}$$

where $H(\rho) = -\text{Tr}\{\rho\log\rho\}$ is the von Neumann entropy. Fundamental bound (10) is dictated only by quantum-mechanical laws. It is noteworthy that value (10) coincides with the *classical transmission capacity of the quantum–classical communication channel.* As was mentioned in [8], in contrast to classical channels, quantum channels allow an infinite set of transmission capacities $\overline{C}_n$ ($n = 1, 2, ...$) such that $\overline{C}_1 \le \overline{C}_2 \le ... \le \overline{C}$. This set differs in measurements. The value $\overline{C}_1$ appears if the eavesdropper performs only individual measurements at each position, which gives the transmission capacity in one shot $\overline{C}_1 = C_{\text{cl}}(Q_{\min})$. The value $\overline{C}_2$ appears if the eavesdropper performs measurements at two positions simultaneously, etc. The value $\overline{C}$ is determined by measurements with the entire sequence and gives the upper bound of information available to the eavesdropper.

At the same time, the smallness of mutual information does not generally guarantee that the eavesdropper does not know individual bits with certainty, which is unacceptable for keys. This effect is purely quantum mechanical and is called information locking [9]. As a result, additional removal of residual information is in any case necessary even after the attenuation of side radiation to a certain level. To this end, a finer quantity than mutual information is required. Such a tool is provided by the remarkable theorem on hashing residual [10].

REMOVAL OF EAVESDROPPER'S INFORMATION FROM THE SIDE CHANNEL

After the measurement of the radiation state in the side channel, the eavesdropper has a bit string, which partially correlates with the bit string of the legitimate users. The idea is that the legitimate users compress (hash) the initial bit string, on which the eavesdropper has partial information, and obtain a shorter bit string, on which the eavesdropper has no information (more precisely, this information can be arbitrarily reduced by the legitimate users). *It is fundamentally important that this compression is open; i.e., it is thought that the eavesdropper knows all steps of this procedure and the*

hash function itself. After that, the distance to the ideal situation is exponentially small in the parameter chosen by the legitimate users themselves.

After the eavesdropper's measurements of the quantum state of the field, the degree of correlation between the bit sequence $(|x\rangle\langle x|)^{\otimes n}$ and the sequence is described by the density matrix $\rho_{XE}^{\otimes n}$. If correlation is absent (ideal situation), the joint matrix is separated into the tensor product $\rho_X^{\otimes n} \otimes \rho_E^{\otimes n}$. It is convenient to describe the degree of correlation by the trace distance to the ideal situation (see, e.g., [11]):

$$d_1(\rho_{XE}^{\otimes n}, \rho_X^{\otimes n} \otimes \rho_E^{\otimes n}) = \frac{1}{2}\left\|\rho_{XE}^{\otimes n} - \rho_X^{\otimes n} \otimes \rho_E^{\otimes n}\right\|_1. \quad (11)$$

Here, $\|A\|_1 = \mathrm{Tr}\{\sqrt{AA^+}\}$, where A is a Hermitian operator. In the situation under consideration, $\rho_X^{\otimes n} = \frac{1}{2^{N_{\mathrm{key}}}}\sum_x (|x\rangle\langle x|)^{\otimes n}$ corresponds to a uniform distribution and $\rho_E^{\otimes n} = \mathrm{Tr}_X\{\rho_{XE}^{\otimes n}\}$. It is important that any manipulations with the sequence $(|x\rangle\langle x|)^{\otimes n}$ cannot increase the trace distance; any transformations of the binary string $(|x\rangle\langle x|)^{\otimes n}$ only reduce the degree of correlation.

Correlations can be reduced by compression (hashing) of the bit string $\{x\}_{\mathrm{key}}^N((|x\rangle\langle x|)^{\otimes N_{\mathrm{key}}})$ to the bit string $\{z\}^{N_{\mathrm{sec}}}$ $((|z\rangle\langle z|)^{\otimes N_{\mathrm{sec}}}$, $z = 0, 1)$ with the smaller length N_{sec}. This compression is described by mapping with random universal hash functions of the second order introduced in [12]:

$$f:\ X = \{0, 1\}_{\mathrm{key}}^N \longrightarrow Z = \{0, 1\}^{N_{\mathrm{sec}}}, \quad (12)$$

where $f \in F$ is a hash function, which is a random variable chosen openly, randomly, and equiprobably from the set F. *Thus, the eavesdropper knows the chosen function*. These hash functions of the second order have the property

$$\Pr_f[f(\hat{x}) = f(x)] \le \frac{1}{|Z|} = 2^{-N_{\mathrm{sec}}}, \quad \hat{x} \ne x, \quad (13)$$

i.e., Eq. (13) provides an upper bound of the probability that the hash value is the same for different arguments. In other words, the probability that different initial bit strings $\{x\}^{N_{\mathrm{key}}}$ and $\{\hat{x}\}^{N_{\mathrm{key}}}$ are transformed to the same bit string $\{z\}^{N_{\mathrm{sec}}}$ does not exceed the value given in Eq. (13). *The degree of compression is determined by smooth min-entropy*. The min-entropy is defined as (for details, see [11])

$$H_{\min}(X|E) = -\sup_{\sigma_E}\log\lambda, \quad (14)$$

where λ is the minimum number at which $\lambda I_X \otimes \sigma_E - \rho_{XE} > 0$. Here, σ_E and ρ_{XE} are the density matrices acting in $\mathcal{H}_E$ and $\mathcal{H}_X \otimes \mathcal{H}_E$, respectively, and I_X is the identity operator in $\mathcal{H}_X$. By definition [11], the quantum smooth min-entropy is

$$H_{\min}^{\varepsilon}(X|E) = \sup_{\bar{\rho}_{XE} \in \mathcal{B}^{\varepsilon}(\rho_{XE})} H_{\min}(X|E)_{\bar{\rho}_{XE}}, \quad (15)$$

where the exact upper and lower bounds are taken over all density matrices $\bar{\rho}_{XE}$ in the ball $\mathcal{B}^{\varepsilon}(\rho_{XE})$ with the radius ε with the center at ρ_{XE}: $\mathcal{B}^{\varepsilon}(\rho_{XE}) = \{\bar{\rho}_{XE}: \|\rho_{XE} - \bar{\rho}_{XE}\|_1 \le \mathrm{Tr}\{\bar{\rho}_{XE}\}\varepsilon\}$. *The indicated entropy has a clear operational meaning (for details, see [13]): if one of the subsystems, e.g., X is a classical bit string and $\varepsilon \longrightarrow 0$, then $H_{\min}^{\varepsilon}(X|E)$ is the number of random uniformly distributed bits that can be obtained from the string X and do not now correlate with the quantum subsystem E*. According to the Leftover Hash Theorem [10], the distance to the ideal situation after compression becomes

$$d_1(\rho_{ZE_z}, \rho_Z \otimes \rho_{E_z}) = \frac{1}{2}\left\|\rho_{ZE_z} - \rho_Z \otimes \rho_{E_z}\right\|_1 < \varepsilon + \frac{1}{2}\sqrt{2^{N_{\mathrm{sec}} - H_{\min}^{\varepsilon}\left(\rho_{XE}^{\otimes N_{\mathrm{key}}}\middle|\rho_E^{\otimes N_{\mathrm{key}}}\right)}}, \quad (16)$$

where the density matrix after hashing has the form

$$\rho_{ZE_z} = \sum_f\sum_z p_f|f\rangle\langle f| \otimes |z\rangle\langle z| \otimes \rho_E^z, \quad (17)$$

where

$$\rho_{E_z}^z = \sum_{x:\,f^{-1}(x) = z} \rho_E^x,$$

$$p_f = \frac{1}{|F|}, \quad \rho_{E_z}^z = \sum_{x,\,x = f^{-1}(z)} \rho_E^x.$$

Here, $\rho_{E_z} = \mathrm{Tr}\{\rho_{ZE_z}\}$ is the eavesdropper's density matrix after hashing and ρ_Z is the density matrix corresponding to the uniform distribution Z, which is similar to ρ_X. For convenience, orthogonal quantum states $|f\rangle$ corresponding to a particular hash function f are introduced into Eq. (17). One of the methods for implementation of the hash function, although being not the most computationally optimal (see [14]), is the modulo 2 multiplication of a bit string with the length N_{key} by a $N_{\mathrm{sec}} \times N_{\mathrm{key}}$ openly chosen random matrix consisting of 0 and 1. As a result, a bit string with the length N_{sec} appears. It is intuitively quite obvious that, since approximately $2^{N_{\mathrm{key}}}/2^{N_{\mathrm{sec}}}$ strings, which are only partially known to the eavesdropper, are transferred to

the new string, the eavesdropper's information on the shorter new string can only decrease. If the length of the new compressed bit string does not exceed

$$N_{\text{sec}} \le H_{\min}^{\varepsilon}(\rho_{XE}^{\otimes N_{\text{key}}} \| \rho_E^{\otimes N_{\text{key}}}) - 2\log\frac{1}{2\varepsilon}, \quad (18)$$

the distance to the ideal situation is no more than

$$d_1(\rho_{ZE_z}, \rho_Z \otimes \rho_{E_z}) = \frac{1}{2}\|\rho_{ZE_z} - \rho_Z \otimes \rho_{E_z}\|_1 \le 2\varepsilon. \quad (19)$$

For particular calculations, smooth min-entropy should be estimated. According to [11],

$$\frac{1}{N_{\text{key}}} H_{\min}^{\varepsilon}(\rho_{XE}^{\otimes N_{\text{key}}} \| \rho_E^{\otimes N_{\text{key}}}) \ge H(\rho_{XE}) - H(\rho_E) - \delta. \quad (20)$$

Here, $\delta = [2H_{\max}(\rho_X) + 3]\sqrt{\frac{\log 1/\varepsilon}{N_{\text{key}}} + 1}$, where $H_{\max}(\rho_X) = \log\text{rank}(\rho_X)$. Von Neumann entropies in Eq. (20) can be calculated. Taking into account that $\pi_0 = \pi_1 = 1/2$, $H(\rho_{XE}) = 1$ and

$$\rho_{XE} = \sum_{x=0,1} \pi_x |x\rangle\langle x| \otimes \rho_E^{(x)}$$

$$= \frac{1}{2}(|0\rangle\langle 0| \otimes \rho_E^{(0)} + |1\rangle\langle 1| \otimes \rho_E^{(1)}), \quad (21)$$

$$\rho_E = \text{Tr}_X\{\rho_{XE}\} = \frac{1}{2}(\rho_E^{(0)} + \rho_E^{(0)}),$$

$$H(\rho_E) = -\lambda_{\text{vac}}\log\lambda_{\text{vac}} - \sum_{\omega}\lambda_{\omega}\log\lambda_{\omega},$$

$$\lambda_{\text{vac}} = 1 - (\overline{N}^{(0)} + \overline{N}^{(1)})/2, \quad (22)$$

$$\lambda_{\omega} = (\overline{N}_{\omega}^{(0)} + \overline{N}_{\omega}^{(1)})/2.$$

Since the space $\mathcal{H}_X$ is two-dimensional, $\log\text{rank}(\rho_X) = 1$. Relations (20)–(22) relate the degree of compression of the initial sequence N_{key} to N_{sec} to the parameters of side radiation. The distance ε to the ideal situation can be made arbitrarily small. Owing to compression, the probability that the eavesdropper knows the compressed string is larger than the guessing probability by no more than the arbitrarily small value 2ε.

SOME EXAMPLES

Let radiation states in the side channel be pure. This example is idealized, but allows a physically clear interpretation of the results. Pure states can be written in the form $\rho_E^{(0,1)} = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|$, where $|\varphi_{0,1}\rangle = \lambda_{\text{vac}}^{(0)}|\text{vac}\rangle + \sum_{n_\omega}\lambda_{n_\omega}^{(0,1)}|n_\omega\rangle\langle n_\omega|$. In this case, the only significant parameter is the scalar product of states that determines the measure of nonorthogonality (reliable indistinguishability) of states, $\zeta = |\langle\varphi_0|\varphi_1\rangle| = \left|\lambda_{\text{vac}}^{(0)}\lambda_{\text{vac}}^{(1)} + \sum_{n_\omega}\lambda_{n_\omega}^{(0)}\lambda_{n_\omega}^{(1)}\right|$. In this case, formulas for the eavesdropper's information have a simple form.

For individual measurements, mutual information in Eq. (9) has the form $I(A, E) \le C_{\text{cl}} = \frac{1}{2}[(1 + \sqrt{1-\zeta^2})\log(1 + \sqrt{1-\zeta^2}) + (1 - \sqrt{1-\zeta^2}) \times \log(1 - \sqrt{1-\zeta^2})]$. *For collective measurements*, $I(A, E) \le \chi = \bar{C} = -\left[\left(\frac{1-\zeta}{2}\right)\log\left(\frac{1-\zeta}{2}\right) + \left(\frac{1+\zeta}{2}\right)\log\left(\frac{1+\zeta}{2}\right)\right]$. In this case, $\bar{C} \ge C_{\text{cl}}$.

Min-entropy. In this case, min-entropy in Eq. (20) is $\frac{1}{N_{\text{key}}} H_{\min}^{\varepsilon}(\rho_{XE}^{\otimes N_{\text{key}}} \| \rho_E^{\otimes N_{\text{key}}}) \ge 1 - \bar{C} - \delta$. Thus, in the case of pure states, all quantities are determined by the single quantity $\bar{C}$, which is the classical transmission capacity of the quantum channel $(x, |x\rangle \longrightarrow \rho_E^x)$ between the source of random numbers and the eavesdropper, which coincides with the Holeveo value [4].

CONCLUSIONS

To summarize, the quantity $\bar{C}$ determines an upper bound of information that is determined by fundamental laws of quantum mechanics and can be extracted from a quantum ensemble. If the length of a random classical sequence is $X - N_{\text{key}}(X = \{0, 1\}^{N_{\text{key}}})$, the eavesdropper *knows* no more than $N_{\text{key}}\bar{C}$ bits in this sequence on average and *does not know* $N_{\text{key}}(1 - \bar{C})$ bits. After the compression of this sequence to the length $N_{\text{sec}} \le N_{\text{key}}(1 - \bar{C})$, which does not exceed the number of bits unknown to the eavesdropper, the distance to the ideal situation (complete absence of correlation between the sequence of legitimate users and the eavesdropper's sequence) in Eq. (16) becomes exponentially small in the parameter $2^{-N_{\text{key}}[l_{\text{sec}} - (1-\bar{C})]}$. *In other words, a secret string cannot be longer than the number $N_{\text{key}}(1 - \bar{C})$ of bits unknown to the eavesdropper. This number is determined only by the characteristics of side radiation given by Eqs. (5) and (7) and is independent of any assumptions on the technical capabilities of the eavesdropper.*

The main conclusion of this work is that the existing proofs of the security of quantum cryptography protocols should be supplemented by the additional compression of keys in order to remove information on the key that the eavesdropper can obtain from the side channel. The additional compression of keys is dictated by fundamental exclusions of quantum

mechanics and is determined only by the intensities of the spectral components of the field.

I am grateful to my colleagues at the Academy of Cryptography of the Russian Federation for ongoing support.

REFERENCES

1. M. G. Kuhn, Technical Report, UCAM-CL-TR-577, No. 577 (Cambridge Univ., 2003).
2. M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Commun. **3**, 634 (2011).
3. S. N. Molotkov, J. Exp. Theor. Phys. **115**, 969 (2012).
4. A. S. Holevo, *Introduction to Quantum Theory of Information*, Ser. Modern Mathem. Physics, No. 5 (MTsNMO, Moscow, 2002); Usp. Mat. Nauk **53**, 193 (1998).
5. R. Loudon, *The Quantum Theory of Light* (Clarendon, Oxford, 1973).
6. L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Cambridge Univ. Press, Cambridge, 1995; Fizmatlit, Moscow, 2000).
7. R. G. Gallager, *Information Theory and Reliable Communication* (Wiley, New York, 1968; Sov. Radio, Moscow, 1974).
8. P. Shor, arXiv:quant-ph/0304102.
9. R. König, R. Renner, A. Dariska, and U. Maurer, Phys. Rev. Lett. **98**, 140502-1 (2007).
10. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner, arXiv/quant-ph: 10022436.
11. R. Renner, arXiv/quant-ph: 0512258.
12. J. L. Carter and M. N. Wegman, J. Comput. Syst. Sci. **18**, 143 (1979).
13. R. König, R. Renner, and C. Schaffner, arXiv/quant-ph: 08071338.
14. C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

Translated by R. Tyapaev