ISSN 0021-3640, JETP Letters, 2017, Vol. 105, No. 12, pp. 801–805. © Pleiades Publishing, Inc., 2017.
Original Russian Text © S.N. Molotkov, 2017, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2017, Vol. 105, No. 12, pp. 763–767.

QUANTUM INFORMATICS

Quantum Entanglement and Composite Keys in Quantum Cryptography

S. N. Molotkov*

Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, 142432 Russia
Academy of Cryptography of the Russian Federation, Moscow, 121552 Russia
Faculty of Computational Mathematics and Cybernetics, Moscow State University, Moscow, 119991 Russia
** e-mail: sergei.molotkov@gmail.ru*

Received March 9, 2017; in final form, May 10, 2017

The security of quantum cryptography protocols after a quantum key distribution (QKD) session is formulated in terms of proximity between two situations: quantum states corresponding to real and ideal situations after QKD. The measure of proximity is the trace distance. It is more reasonable to formulate security directly in terms of the smallness of probability of successive guessing of keys by an eavesdropper after an arbitrary number of QKD sessions. There is a fundamental question the answer to which is a priori very unobvious: Is the security criterion in terms of the proximity of the real and ideal situations for a single QKD session sufficient to guarantee the security of keys in terms of the smallness of probability of guessing of keys by the eavesdropper after an arbitrary number of QKD sessions? It has been shown that the answer to this question is positive.

DOI: 10.1134/S0021364017120098

INTRODUCTION

Many fundamental problems of transmission and processing of information in quantum informatics are reduced to problems of distinguishing quantum states [1]. The probability of distinguishing quantum states appears in measurements. There are several measures in terms of which the probability of success of distinguishing quantum states is expressed. Such measures are the trace distance [1] and Holevo quantity [2–4].

The trace distance appears in the problem of distinguishing *a pair of quantum states. The measurement has two outcomes.* Measurements are performed for one of the states ρ and σ. One outcome of measurements is treated as the state ρ, whereas the second outcome is interpreted as σ. For a pair of the quantum states ρ and σ, there is an exact solution for the maximum probability of successive guessing, which is expressed in terms of the trace distance between the density matrices $\|\rho - \sigma\|_1$ (see below).

The Holevo quantity $\chi(\mathscr{E})$ appears in the problem of distinguishing the maximum possible number of sequences of quantum states ρ^x emitted by a source according to the probability distribution $P_X(x)$. Here, $\mathscr{E} = \{P_X(x), \rho^x\}$ is the quantum ensemble and $x \in X = \{0,1\}^n$ is accepted for definiteness. Let a classical source generate classical alphabetic symbols $x \in X = (x_1, x_2, \ldots x_n)$ according to the probability distribution $P_X(x)$. Further, each classical symbol is assigned a quantum state ρ^x, which is presented for measurements. A series of independent states $M - \rho^{x_{i_1}} \otimes \rho^{x_{i_2}} \otimes \ldots \rho^{x_{i_M}}$ with the length M are generated. The aim of measurements is to distinguish between sequences of states. *A measurement has* 2^{Mn} outcomes. The Holevo quantity gives a fundamental bound for the maximum number of sequences $2^{M\chi(\mathscr{E})}$ that can be distinguished from the total number 2^{Mn} of all possible sequences.

Quantum mechanics allows collective measurements with the use of entangled states. Such measurements are reduced to the measurement of the entire sequence. One of the fundamental results of quantum theory of information is that classical information extracted in such measurements is larger than the sum of amounts of information in individual measurement. The Holevo bound is reached in such measurements [2–4].

Quantum cryptography is possibly the only field of quantum theory of information that is developed to real applications. The aim of quantum cryptography is secret key distribution over quantum communication channels open for eavesdropping. *The proven criterion of security of quantum cryptography protocols is formulated in terms of distinguishability of a pair of quantum states corresponding to the real and ideal situations*

rather than in terms of distinguishability of keys themselves [5–7]. Furthermore, the criterion of security of a quantum cryptography protocol is formulated for a single quantum key distribution (QKD) session. In this case, there are fundamental problems concerning composite protocols and composite keys [6, 7].

It would be more reasonable to formulate the criterion of security directly for the probability of successive guessing of keys that are available to the legitimate users and eavesdropper after his measurements of his quantum system correlated with keys of legitimate users. In this case, the probability of success in guessing could be obtained immediately for an arbitrary number of QKD sessions with allowance for collective measurements by the eavesdropper. However, to formulate the criterion of security in terms of the probability of guessing of keys by the eavesdropper, it is necessary to know quantum states. In this case, the fundamental Holevo bound, as well as the probability of success of guessing of keys by the eavesdropper, could be calculated. However, eavesdropper's quantum states are unknown; it is only known that they are ε close in sense of the trace distance to states for the ideal situation. There is a fundamental question: Is the trace distance, which determines the probability of distinguishing between a pair of states or situations in a single session, sufficient to guarantee the smallness of probability of guessing of keys in an arbitrary number of QKD sessions? This question is discussed in this work.

CRITERION OF SECURITY IN QUANTUM CRYPTOGRAPHY BASED ON THE TRACE DISTANCE

We consider the criterion of security of a protocol based on the trace distance [5–7]. We again emphasize that *this criterion refers to the distinguishability of a pair of quantum states describing the real and ideal situations after a QKD session rather than to the criterion of distinguishability of keys themselves.* After the QKD session, the legitimate users have a common key $x \in X = \{0,1\}^n$ with the length n and probability $P_X(x)$. The eavesdropper has the quantum system ρ_E^x correlated with this key, which can be stored in quantum memory. The real situation after the QKD session is described by the density matrix ρ_{XE}. The ideal situation corresponds to the state $\rho_U \otimes \rho_E$. Keys in the ideal situation $x \in X = \{0,1\}^n$ are uniformly distributed and uncorrelated with eavesdropper's quantum system. The density matrices describing both situations have the form

$$\rho_{XE} = \sum_{x\in X} P_X(x)|x\rangle\langle x| \otimes \rho_E^x,$$
$$\rho_U = \frac{1}{N}\sum_{x\in X}|x\rangle\langle x|, \qquad (1)$$
$$\rho_E = \sum_{x\in X} P_X(x)\rho_E^x, \quad N = 2^n.$$

The criterion of security proposed in [5, 6] is formulated in abstract terms of distinguishability of *a pair of quantum states*, i.e., the smallness of the trace distance between two situations or quantum states:

$$\|\rho_{XE} - \rho_U \otimes \rho_E\|_1 = \frac{1}{2}\mathrm{Tr}\{|\rho_{XE} - \rho_U \otimes \rho_E|\} < \varepsilon.$$

It is often stated that keys obtained in such a protocol are ε-secret [5, 6], which can result in confusion. It is more correct to state that the real situation after the protocol is ε-secret. The parameter of security ε is chosen by the legitimate users "administratively." A given ε value is reached by the compression of cleaned keys to the final key x with the necessary length. Cleaned keys appear after the transmission of quantum states, measurements of them, and correction of errors in the initial bit sequence. The smaller the ε value, the longer the necessary cleaned key and, correspondingly, the larger the number of initially transmitted quantum states. *From the operational point of view, the criterion of security proposed in* [5, 6], *which is based on the trace distance, hardly refers to keys themselves, but more likely to the distinguishability of the real and ideal situations. This criterion gives the probability of successful distinguishing of two situations.* This means that, if the eavesdropper performs measurements with two outcomes after QKD in order to distinguish the situation in which he is—in the situation with the real density matrix ρ_{XE} or in the ideal situation with the density matrix $\rho_U \otimes \rho_E$—then the maximum probability of success in distinguishing these two situations is larger than the probability of simple guessing by no more than $\varepsilon/2$:

$$\Pr_{\mathrm{Guess}}(\rho_{XE}, \rho_U \otimes \rho_E)$$
$$= \frac{1}{2} + \frac{1}{2}\|\rho_{XE} - \rho_U \otimes \rho_E\|_1 < \frac{1}{2} + \frac{1}{2}\varepsilon. \qquad (2)$$

CRITERION OF SECURITY BASED ON THE PROBABILITY OF GUESSING OF KEYS FOR AN ARBITRARY NUMBER OF QKD SESSIONS

Any measurement in quantum mechanics is described by the decomposition of unity. We again emphasize that a measurement that gives the probability of success in the distinguishing of two states or situations ρ_{XE} and $\rho_U \otimes \rho_E$ can give two outcomes. In this case, the decomposition of unity has the form

$$I_{XE} = \mathcal{P}_0 + \mathcal{P}_1, \quad 0 \to \rho_{XE}, \quad 1 \to \rho_U \otimes \rho_E, \quad (3)$$

where $\mathcal{P}_0$ and $\mathcal{P}_1$ are the positive operator-valued measures and I_{XE} is the identity operator for the space of states in a single QKD session; the corresponding operator for M sessions is $I_{XE}^{\otimes M}$.

It is more reasonable to use the criterion of security directly for the probability of guessing of keys at an arbitrary number of sessions. Let M sessions be performed, providing the keys x_{i_1}, x_{i_2}, ..., x_{i_M}; $x_{i_k} \in X = \{0,1\}^n$, $k = 1, 2, \ldots M$. The eavesdropper has a sequence of quantum states correlated with these keys $\rho_E^{x_{i_1}}, \rho_E^{x_{i_2}}, \ldots, \rho_E^{x_{i_M}}$ and can perform collective measurements simultaneously of the entire sequence. As a result of measurements of the entire sequence, the eavesdropper obtains a united bit sequence $(\hat{x}_{i_1}, \hat{x}_{i_2}, \ldots, \hat{x}_{i_M}) \in Y^M = \{\{0,1\}^n\}^M$. The probability that this sequence coincides with keys obtained in all sessions is

$$\overline{\mathrm{Pr}}_{\mathrm{Guess}}(M) = \sum_{x_i=\hat{x}_i\in(X,Y),i=1,2,\ldots M} P_{X^M Y^M}(x_1, x_2, \ldots x_M, \hat{x}_1, \hat{x}_2, \ldots \hat{x}_M). \quad (4)$$

The measurement that allows the eavesdropper to distinguish the sequence of quantum states correlated with keys is described by the decomposition of unity in the form

$$I_{XE}^{\otimes M} = \sum_{\hat{i}\in(i_1,i_2,\ldots i_M)} \mathcal{M}_{\hat{i}}, \quad \hat{i} = 1, 2, \ldots 2^{Mn}, \quad i_k = 1, 2, \ldots 2^n, \quad k = 1, 2, \ldots n, \quad (5)$$

where $\mathcal{M}_{\hat{i}}$ are the positive operator-valued measures different from measures in Eq. (3). The measurements have 2^n outcomes for a single session and 2^{Mn} outcomes for M sessions. *It is unobvious a priori that the smallness of the probability of distinguishing of keys themselves follows from the smallness of the probability of success in distinguishing two states* ρ_{XE} and $\rho_U \otimes \rho_E$.

The next aim is to find the upper bound for guessing of keys from all possible measurements. As will be shown below, the upper bound from collective measurements of the entire sequence of quantum states with the length M simultaneously for all QKD sessions is expressed in terms of the Holevo fundamental quantity, which can be majorized by the trace distance for a single QKD session.

ENTANGLED COLLECTIVE MEASUREMENTS AND HOLEVO BOUND FOR M QKD SESSIONS

In this section, we obtain an upper bound for the probability of guessing of keys for an arbitrary number of sessions with allowance for the eavesdropper's collective measurements. To calculate the Holevo quantity, it is necessary to know the eavesdropper's quantum states in each message. However, these states are unknown, and only their closeness in the trace metric to states for the ideal situation is guaranteed. It is unobvious a priori that this is sufficient. It will be shown that the Holevo quantity giving the probability of success of guessing of keys in an arbitrary number of sessions can be bounded from above by the trace distance in a single session.

There are 2^{Mn} sequences associated with sequences of quantum states. Each key appears with the probability $P_X(x)$. Let a certain random code table be chosen. This informally means that each bit sequence is attributed to quantum states: $\hat{x}^l = (x_{i_1}^l, x_{i_2}^l, \ldots x_{i_M}^l) \to (\rho_E^{x_{i_1}^l}, \rho_E^{x_{i_2}^l}, \ldots \rho_E^{x_{i_M}^l})$. The error owing to collective entangled measurements for all code words in this table is determined as

$$\overline{\mathrm{Pr}}_{\mathrm{Guess}}(M, l) = 1 - \frac{1}{2^{Mn}} \sum_{j=1}^{2^{Mn}} \mathrm{Tr}\{\rho_{\hat{E}}^{\hat{x}^l} \mathcal{M}_j^l\}, \quad \hat{x}^l = (x_{i_1}^l, x_{i_2}^l, \ldots x_{i_M}^l), \quad (6)$$

where the measurement is described by the decomposition of unity specified by Eq. (5). The average error over all random code tables generated according to the probability distribution $P_X(x)$ is given by the expression (for details, see [2–4, 8–10]; the idea of calculation of error is based on works [9, 10] for classical channels; then, the idea was applied to quantum channels [2–4, 8]):

$$\overline{\mathrm{Pr}}_{\mathrm{Guess}}(M) = \mathbf{E}\left(\overline{\mathrm{Pr}}_{\mathrm{Guess}}(M, l)\right), \quad \mathbf{E}(\ldots) = \sum_{x_{i_1}\in X} \sum_{x_{i_2}\in X} \ldots \sum_{x_{i_M}\in X} P_X(x_{i_1}) P_X(x_{i_2}) \ldots P_X(x_{i_M})(\ldots), \quad (7)$$

where averaging is performed over the probability distribution $P_X(x)$. The following inequality, which is a strong converse of the coding theorem, can be obtained (for details, see [8, 10]):

$$\overline{\mathrm{Pr}}_{\mathrm{Guess}}(M) > 1 - \exp\{-M(-s \cdot n + E_0(s, P_X))\}, \quad (8)$$

$$E_0(s, P_X) = -\log\left(\mathrm{Tr}\left(\sum_{x\in X} P_X(x)(\rho_E^x)^{\frac{1}{s+1}}\right)^{s+1}\right),$$

where s is an arbitrary number in the range $-1 < s < 0$. According to Eq. (8),

$$E_0(0, P_X) = 0, \quad \frac{\partial E_0(s, P_X)}{\partial s}\Big|_{s=0} = S(\bar{\rho}_E) - \sum_{x\in X} P_X(x) S(\rho_E^x) = \chi(\mathscr{E}), \quad (9)$$

where $S(\rho) = -\mathrm{Tr}\{\rho\log(\rho)\}$ is the von Neumann entropy and $\chi(\mathscr{E})$ is the Holevo quantity for the quantum ensemble $\mathscr{E} = \{P_X(x), \rho_E^x\}$. According to Eq. (9), the error will be exponentially small at $-sn + \chi(\mathscr{E}) > 0$ (for $-1 < s < 0$). Further, it is necessary to establish a relation between the trace distance and Holevo bound $\chi(\mathscr{E})$.

SECURITY FOR DISTINGUISHING A PAIR OF STATES

Security in terms of the trace distance for distinguishing a pair of states in a single session guarantees security in terms of the smallness of the probability of success in guessing keys for any number of QKD sessions. We now show that the criterion of security in terms of the trace distance for a single QKD session is sufficient for an arbitrary number of QKD sessions. We show that the trace distance majorizes the Holevo information, $\chi(\mathscr{E}) < 2\varepsilon n$. Consequently, the eavesdropper can distinguish no more than $2^{Mn2\varepsilon}$ bit sequences, i.e., only an exponentially small fraction $2^{-Mn(1-2\varepsilon)}$ of the total number of sequences 2^{Mn}. To show this, several auxiliary quantities associated with the asymmetric relative quantum entropy are required (for details, see [11–13]]). Mapping for positive operators $\Lambda_\rho(\sigma)$ is defined as

$$\begin{aligned}&\Lambda_\rho(\sigma)\frac{d}{dt}\log(\rho+\sigma t)\,|_{t=0}\\ &=\int_0^\infty ds(\rho+sI)^{-1}\sigma(\rho+sI)^{-1},\quad \Lambda_\rho(\rho)=I,\end{aligned}\tag{10}$$

where the derivative is treated as a Fréchet derivative. Then, we introduce a sesquilinear form, which can be considered as a metric:

$$M_\rho(\sigma,\tau) = \mathrm{Tr}\{\sigma\Lambda_\rho(\tau)\},\quad M_\rho(\sigma,\sigma)\geq 0.\tag{11}$$

The differential of the asymmetric relative entropy has the form

$$\begin{aligned}D_\alpha(\rho\|\sigma) &= \alpha\mathrm{Tr}\{\rho\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho-\sigma)\}\\ &= -\alpha\frac{d}{d\alpha}S(\rho\|\alpha\rho+(1-\alpha)\sigma),\end{aligned}\tag{12}$$

where $S(\rho\|\sigma)$ and $S_\alpha(\rho\|\sigma)$ are the relative and asymmetric entropies given by the expressions

$$\begin{aligned}S(\rho\|\sigma) &= \mathrm{Tr}\{\rho(\log(\rho)-\log(\sigma))\},\\ S_\alpha(\rho\|\sigma) &= -\frac{1}{\log(\alpha)}S(\rho\|\alpha\rho+(1-\alpha)\sigma).\end{aligned}\tag{13}$$

In contrast to the relative entropy, the asymmetric entropy is continuous and is related to the differential as

$$S_\alpha(\rho\|\sigma) = -\frac{1}{\log(\alpha)}\int_0^{-\log(\alpha)} D_\alpha(\rho\|\sigma)d(-\log(\alpha')).\tag{14}$$

In view of Eqs. (10)–(14), the differential entropy is explicitly bounded from above by the trace distance

$$\begin{aligned}D_\alpha(\rho\|\sigma) &= \alpha\mathrm{Tr}\{\rho\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho-\sigma)\}\\ &= \alpha\mathrm{Tr}\{(\rho-\sigma)\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho)\}\\ &\leq \alpha\mathrm{Tr}\{(\rho-\sigma)_+\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\rho)\}\\ &\leq \alpha\mathrm{Tr}\{(\rho-\sigma)_+\Lambda_{\alpha\rho+(1-\alpha)\sigma}(\alpha\rho+(1-\alpha)\sigma)\}\\ &= \mathrm{Tr}\{(\rho-\sigma)_+\} = \delta(\rho,\sigma),\end{aligned}\tag{15}$$

where $(\rho-\sigma)_+$ is the projection on the subspace corresponding to positive eigenvalues.

Finally, it is necessary to relate the Holevo quantity to the relative entropy and the relative entropy to the differential entropy, which is bounded by the trace distance. By definition [2–4], the Holevo quantity has the form

$$\begin{aligned}\chi(\mathscr{E}) &= S(\overline{\rho}_E) - \sum_{x\in X}P_X(x)S(\rho_E^x),\\ \overline{\rho}_E &= \sum_{x\in X}P_X(x)\rho_E^x.\end{aligned}\tag{16}$$

The Holevo quantity is expressed in terms of the relative entropy

$$\begin{aligned}\chi(\mathscr{E}) &= \sum_{x\in X}P_X(x)S(\rho_E^x\|\overline{\rho}_E)\\ &= -\sum_{x\in X}P_X(x)\log(P_X(x))S_{P_X(x)}(\rho_E^x\|\overline{\rho}_E^x)\\ &\leq -\sum_{x\in X}P_X(x)\log(P_X(x))\delta(\rho_E^x,\overline{\rho}_E^x)\\ &\leq -\sum_{x\in X}P_X(x)\log(P_X(x))\\ &\quad\times\sum_{x\neq x'\in X}\frac{P_X(x')}{1-P_X(x)}\delta(\rho_E^x,\rho_E^{x'}).\end{aligned}\tag{17}$$

The last term in the set of inequalities (17) is majorized by the trace distance:

$$\begin{aligned}&\frac{1}{2}\sum_{x\neq x'\in X}\frac{P_X(x')}{1-P_X(x)}|\rho_E^x-\rho_E^{x'}|\\ &\leq\frac{1}{2}\sum_{x\neq x'\in X}\frac{1}{1-P_X(x)}\\ &\times\left(|P_X(x')\rho_E^{x'}-P_X(x)\rho_E^x|+|\rho_E^x(P_X(x')-P_X(x))|\right)\\ &\leq\frac{1}{2}\sum_{x\in X}\frac{2}{1-P_X(x)}\\ &\times\left(|\frac{\overline{\rho}_E}{N}-P_X(x)\rho_E^x|+|\rho_E^x||P_X(x)-\frac{1}{N}|\right).\end{aligned}\tag{18}$$

Calculating the trace of Eq. (18) and taking into account that the maximum probability is no more than $\max_{x\in X} P_X(x) < \frac{1}{N} + \varepsilon$, we obtain

$$\frac{1}{1-\left(\frac{1}{N}+\varepsilon\right)} \times \left(\sum_{x\in X} \mathrm{Tr}\left\{\left|\frac{\overline{\rho}_E}{N} - P_X(x)\rho_E^x\right|\right\} + \left\|P_X - \frac{1}{N}\right\|_1\right) < \frac{2\varepsilon}{1-2\varepsilon}. \quad (19)$$

The Holevo quantity satisfies the inequality $\chi(\mathscr{E}) < H(X)\frac{2\varepsilon}{1-2\varepsilon} \approx 2\varepsilon H(X) < 2\varepsilon n$. Since $0 < |s^*| < 1$ in Eq. (8), the probability of success in guessing satisfies the inequality

$$\Pr_{\mathrm{Guess}}(M) < \frac{1}{2^{Mn(1-2\varepsilon)}}. \quad (20)$$

CONCLUSIONS

Formula (20) can be interpreted as follows. In the ideal case, where keys are strictly uniformly distributed and the eavesdropper can only guess them, the probability is $\Pr_{\mathrm{Guess}}(M) = \frac{1}{2^{Mn}}$, which is the inverse of the dimension of the key space. In a real situation, probability (20) of success of distinguishing of keys in M sessions with allowance for collective measurements has a similar form and it can be believed that the probabilities of success for individual QKD sessions are multiplied. It is important that this result cannot be obtained by multiplying probabilities calculated for individual QKD sessions because the eavesdropper uses collective measurements with the projection of the entire sequence of quantum states on entangled measuring states for all sessions.

Thus, if the protocol in a single QKD session is ε-secret in terms of distinguishing of two situations, it has this property for an arbitrary number of QKD sessions; i.e., the smallness of probability of guessing of keys is guaranteed. In this case, keys from different sessions can be concatenated into a unified key without loss of cryptographic security.

I am grateful to I.M. Arbekov, A.N. Klimov, and S.P. Kulik for numerous discussions and to my colleagues at the Academy of Cryptography of the Russian Federation for permanent support and discussions. This work was supported by the Russian Science Foundation (project no. 16-12-00015).

REFERENCES

1. M. M. Wilde, arXiv: 1106.1445 [quant-ph].
2. A. S. Holevo, Probl. Inform. Transm. **9**, 177 (1973).
3. A. S. Holevo, Russ. Math. Surv. **53**, 1295 (1998).
4. A. S. Holevo, *Introduction to Quantum Information Theory,* Vol. 5 of *Modern Mathematical Physics* (MTsNMO, Moscow, 2002) [in Russian].
5. R. Renner, PhD Thesis (ETH Zürich, 2005); arXiv/quant-ph:0512258.
6. C. Portmann and R. Renner, arXiv: 1409.3525 [quant-ph].
7. J. Müller-Quade and R. Renner, arXiv: 1006.2215 [quant-ph].
8. T. Ogawa and H. Nagaoka, IEEE Trans. Inform. Theory **45**, 2486 (1999).
9. R. G. Gallager, IEEE Trans. Inform. Theory **11**, 3 (1965).
10. S. Arimoto, IEEE Trans. Inform. Theory **19**, 357 (1973).
11. W. Roga, M. Fannes, and K. Zyczkowski, Phys. Rev. Lett. **105**, 040505 (2010).
12. K. M. R. Audenaert, J. Math. Phys. **54**, 073506 (2013).
13. K. M. R. Audenaert, J. Math, Phys. **55**, 112202 (2014).

Translated by R. Tyapaev