ISSN 0021-3640, JETP Letters, 2025, Vol. 121, No. 6, pp. 481–489. © The Author(s), 2025. This article is an open access publication.
Russian Text © The Author(s), 2025, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2025, Vol. 121, No. 6, pp. 503–512.

QUANTUM INFORMATICS

# On the Key Search Complexity in Quantum Cryptography with Strong Information-Theoretic Authentication

**S. P. Kulik[a] and S. N. Molotkov[b,*]**

[a]*Center for Quantum Technologies, Moscow State University, Moscow, 119991 Russia*
[b]*Osipyan Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, 142432 Russia*
**e-mail: sergei.molotkov@gmail.com*

Received December 26, 2024; revised February 10, 2025; accepted February 10, 2025

The stability of quantum key distribution systems is based not only on the detection of attacks on quantum states, which is guaranteed by the fundamental quantum theory laws, but also on ensuring the integrity of classical messages transmitted through an auxiliary classical communication channel. To detect attacks on the classic communication channel, the authentication procedure is used. Information-theoretic authentication guarantees the detection of attacks on the classical communication channel regardless of the computational and technical capabilities of an eavesdropper, including the quantum computer. The fundamental quantum cryptographic relationship between the abstract criterion of the robustness of quantum key distribution systems with theoretical-information authentication and the quantum key search complexity has been determined for the first time using simple means.

**DOI:** 10.1134/S002136402460544X

## INTRODUCTION

Quantum cryptography involves two open communication channels accessible for eavesdropping [1]. A quantum channel is available for attacks and modification of transmitted quantum states. A classical channel is open, but must be authentic and is used to transmit auxiliary messages between Alice and Bob. The authenticity of the classical channel means ensuring the integrity, i.e., the robustness of the transmitted public classical messages.

The final product of quantum key distribution (QKD) is a "quantum" key, which does not even explicitly appear in the strength criterion based on the distinguishability of quantum states. A key is called $\varepsilon$-secure if the trace distance between the quantum state describing a real QKD session and the state for the ideal situation does not exceed $\varepsilon$.

The real quantum key distribution session allows an eavesdropping attack on the quantum communication channel, and authentication in the classical communication channel, in which message substitution is possible.

The ideal situation is a quantum key distribution session without any attack on the quantum communication channel, and authentication without message substitution in the classical communication channel.

The strength criterion based on the trace distance is rather abstract.

When using a quantum key for cryptographic purposes, the decisive parameter is the used in further applications, for example, in encryption rather than the smallness of the trace distance itself.

The dependence of the quantum key search complexity on the trace distance is fundamental for quantum cryptography. This dependence remained unknown for a long time, which led to emotional discussions in the scientific community [2–6].

This dependence was determined for the first time in works [7–9], which presented explicit analytical relations between the trace distance and the key search complexity, i.e., the number of brute-force steps required to determine the quantum key.

It was assumed in [7–9] that the classical authentic channel is ideal: an eavesdropper does not attack the channel and does not replace classical messages. In a real situation, authentication is not perfect, and the eavesdropper can replace classic messages, which can violate the integrity of transmitted messages.

The eavesdropper can perform a man-in-the-middle attack (see Fig. 1) [10–12]. Without attacks on the classical communication channel, the eavesdropper can only attack states in the quantum channel. If the eavesdropper can also replace classical messages, the range of attacks expands. It is extremely difficult to establish an $\varepsilon$ security criterion for a complex composite process. The abstract security criterion based on the trace method has an important convenient property: it can be decomposed into the security criteria between individual elementary processes. The trace distances can be calculated for individual processes;

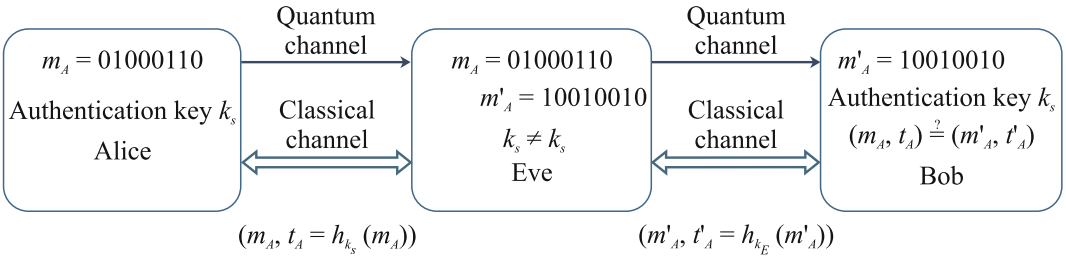


**Fig. 1.** Illustration of the man-in-the-middle attack. The eavesdropper breaks the quantum and classical communication channels and generates separate Alice–Eve and Eve–Bob keys. Such an attack is not detected if the classical channel does not provide authenticity, i.e., the constancy of public classical messages.

then, the trace distance between composite real and ideal processes is limited by the sum of the trace distances between individual processes [13].

According to the original design [1, 14], the QKD should provide the unconditional security of the distributed keys, which is based on the fundamental laws of quantum mechanics rather than on the limited computational or technical capabilities of the eavesdropper. Consequently, authentication should be information-theoretically robust, and guarantee the detection of attacks on the classical communication channel, regardless of the technical and computational limitations of the eavesdropper.

Information-theoretic authentication was first proposed by Simmons in [15]. Wegman and Carter in their fundamental work [16] showed that information-theoretic authentication can be achieved using a class of special hash functions [16–28].

Information-theoretic authentication *guarantees* the detection of attacks on the classical communication channel, regardless of the technical capabilities of the eavesdropper, even if he has a full-scale quantum computer.

*Information-theoretic authentication requires a shared key $k_s$ between Alice and Bob. Therefore, the shared start key $k_s$ must be delivered to Alice and Bob at the first initiation of the system.* Information-theoretic authentication was studied in [16–28].

As shown in [13], after the initiation of the system using the shared start key, an almost arbitrarily long quantum key distribution is possible, until the next restart of the system.

## COMPLEXITY IN QUANTUM KEY DISTRIBUTION WITH INFORMATION-THEORETIC AUTHENTICATION

It is still unclear how eavesdropping attacks on both quantum and classical communication channels change the quantum key search complexity for the complete trace criterion of the QKD security.

The answer to this question is fundamental both for understanding the theoretical robustness of QKD systems and for practical applications of quantum cryptography.

As shown in [13], the total strength parameter $\varepsilon$ for QKD with information-theoretic authentication is limited from above by the sum of two trace distances: (i) the distance $\varepsilon_{QKD}$ is between the quantum states of the real and ideal QRC sessions, but with perfect authentication without attacks on the classical communication channel and (ii) the distance $\varepsilon_{Aut}$ between the real and ideal situations in the transmission of classical messages, but without attacks on quantum states in the quantum communication channel.

**What is the fundamental difference between situations (i) and (ii)?** A naïve point of view is that the total $\varepsilon$-security parameter in the complexity in the case of attacks on both quantum and classical communication channels, as well as combined attacks, is equal to the sum $\varepsilon = \varepsilon_{QKD} + \varepsilon_{Aut}$.

However, a more detailed consideration immediately leads to doubts.

In situation (i), the eavesdropper has a quantum system $\rho_E^k$ correlated with the key $k$, which is a bit string distributed at the end of the QKD session with Alice and Bob. The eavesdropper makes measurements on the quantum system $\rho_E^k$ and receives a "copy" of the key used by Alice and Bob, which is a bit string $y$ correlated with the key $k$. The degree of correlation is determined by the joint probability distribution $P_{KY}(k, y)$, as well as by the conditional probability distributions $P_{K|Y}(k|y)$ and $P_{Y|K}(y|k)$.

Then, having the probability distribution, the eavesdropper begins to test the keys according to a posteriori distribution, starting with the most probable key. The number of testing steps determines the key search complexity (see details in [7]).

We emphasize that this way for the eavesdropping attack and the calculation of the complexity works because the quantum system $\rho_E^k$ and the bit string $y$ are "direct" side variables for the eavesdropper, which are **directly dependent on the key** $k$. This situation is characteristic of only the case of attacks on the quantum communication channel.

We recall that the classical channel is open; i.e., all information transmitted here is available to the eavesdropper. Messages contain information about the coordination of bases, estimate of the probability of errors, error correction, and strengthening the security of cleared keys.

However, there is a fundamental difference between classical and quantum side information. Classical messages are only **indirectly correlated with the key** $k$.

It is far from obvious how to determine the key search complexity in such a situation. In view of the importance of the issue, relations should be strictly derived on the basis of the careful consideration rather than on heuristic qualitative reasons.

A direct relationship will be established below between the robustness criterion based on the trace distance between the state $\rho_{\mathrm{ABE}}^{R^A_{\mathrm{Aut}}R^B_{\mathrm{Aut}}R^{AB}_{\mathrm{QKD}}}$ corresponding to the real quantum key distribution and the real classical channel with possible message substitution and the state $\rho_{\mathrm{ABE}}^{I^A_{\mathrm{Aut}}I^B_{\mathrm{Aut}}I^{AB}_{\mathrm{QKD}}}$ corresponding to the ideal quantum key distribution without the eavesdropper and the ideal authentication of messages in the classical channel without message substitution by the eavesdropper.

**Almost ε strongly universal (ε-ASU$_2$) hash functions.** We give information on hash functions, which are used in information-theoretic authentication, necessary for further consideration [16–28]. Information-theoretic authentication allows Alice and Bob to ensure the integrity of information transmitted through the open communication channel. At authentication, the transmission of the open message $m \in \mathcal{M} = \{0, 1\}^{\mu}$ is accompanied by the transmission of its shorter hash value (hereinafter, tag) $t = h_{k_s}(m) \in \mathcal{T} = \{0, 1\}^{\tau}$ ($|\mathcal{T}| \ll |\mathcal{M}|$).

Information-theoretic authentication requires the shared secret key between two users. A hash function is randomly selected from the set of hash functions $\mathcal{H} = \{h_{k_s}\}_{k_s \in \mathcal{K}_s}$, depending on the equiprobably chosen key $k_s \in \mathcal{K}_s = \{0,1\}^{\kappa_s}$.

Information-theoretic authentication is understood as authentication in which the probability of message substitution (impersonation) without knowing the key $k_s$, i.e., the determination of *a valid pair* ($t$, $m$) and an equiprobable choice of keys $k_s$, does not exceed the value $\Pr_{k_s}\{t = h_{k_s}(m)\} = \dfrac{1}{|\mathcal{T}|}$.

Further, the probability of message substitution without knowing the key $k_s$, i.e., the replacement of the true message after observing the pair ($t$, $m$) with another pair ($t'$, $m'$), does not exceed $P_{k_s}[t = h_{k_s}(m), t' = h_{k_s}(m')] < \dfrac{\varepsilon}{|\mathcal{T}|}$.

From the definitions of ε-ASU$_2$ hash functions, it follows that the probability of substitution $(m, t) \to (m', t')$, more precisely the conditional probability, without knowing the key, and when observing the pair $(m, t)$, *does not depend on the computational capabilities of the eavesdropper, but depends only on the properties of the set of hash functions* $\mathcal{H}_s$ and does not exceed $P_{k_s}[t' = h_{k_s}(m') \mid t = h_{k_s}(m)] < \varepsilon$.

The family of ε-ASU$_2$ functions can be implemented in various ways. With regard to information-theoretic authentication in quantum cryptography, it is necessary to minimize the number of authentication keys, i.e., the set $|\mathcal{H}_s|$. For the family of ε-ASU$_2$ hash functions, the relations between the parameters ε, $|\mathcal{H}_s|$, and $|\mathcal{T}|$ [29] are known, which impose restrictions on the size of the set of keys $|\mathcal{H}_s|$ at given ε and $|\mathcal{T}|$ values.

To save authentication keys, the ε-ASU$_2$ functions are implemented based on the composition of the ε-AXU$_2$ hash functions and the encryption of the hash value with a one-time pad (see details in [13, 29]). For the ε-AXU$_2$ functions, the same key is used during all authentication sessions. The key for the encryption of the tag is used as one-time in each authentication session.

## TRACE DISTANCE BETWEEN QUANTUM STATES (SITUATIONS)

It was previously shown in [13] that the distance between the two situations after the QKD with information-theoretic authentication is no more than

$$\|\rho_{\mathrm{ABE}}^{R^A_{\mathrm{Aut}}R^B_{\mathrm{Aut}}R^{AB}_{\mathrm{QKD}}} - \rho_{\mathrm{ABE}}^{I^A_{\mathrm{Aut}}I^B_{\mathrm{Aut}}I^{AB}_{\mathrm{QKD}}}\|_1 \le \varepsilon_{\mathrm{Aut}} + \varepsilon_{\mathrm{QKD}}, \qquad (1)$$

where the parameters $\varepsilon_{\mathrm{Aut}} + \varepsilon_{\mathrm{QKD}}$ include all the imperfections of individual processes [13]. The parameter $\varepsilon_{\mathrm{QKD}} = \varepsilon_F + \varepsilon_{\mathrm{corr}} + \varepsilon_{\mathrm{sec}}$ describes the QKD process under perfect authentication, where $\varepsilon_F$ is responsible for the imperfection of the choice of hash functions $F$ when strengthening security in the QKD, $1 - \varepsilon_{\mathrm{corr}}$ determines the probability of the QKD protocol being correct, i.e., the key match for Alice and Bob, and $\varepsilon_{\mathrm{sec}}$ is the security parameter of the QKD session (see details in [14]).

Next, we need density matrices for real and ideal QKD situations, which have the quantum–classical form

$$\rho_{\mathrm{ABE}}^{R^A_{\mathrm{Aut}}R^B_{\mathrm{Aut}}R^{AB}_{\mathrm{QKD}}} = \sum_{k_s \in \mathcal{K}_s} P_{K_s}(k_s) |k_s\rangle_{K_s K_s} \langle k_s|$$
$$\times \sum_{k_A \in \{0,1\}^{\ell}} \sum_{k_B \in \{0,1\}^{\ell}} P_{K_A K_B}(k_A, k_B) \rho_E^{k_A k_B}$$
$$\otimes |k_A\rangle_{AA}\langle k_A| \otimes |k_B\rangle_{BB}\langle k_B| \otimes \rho^{R^A_{\mathrm{Aut}}}(k_A, k_s)$$
$$\otimes \rho^{R^B_{\mathrm{Aut}}}(k_B, k_s).$$

Here, $\ell$ is the length of the secret key; $|k_A\rangle_A = |k_{1A}\rangle_A|k_{2A}\rangle_A...|k_{\ell A}\rangle_A$ and $|k_B\rangle_B = |k_{1B}\rangle_B|k_{2B}\rangle_B...|k_{\ell B}\rangle_B$ are the quantum states corresponding to keys of Alice and Bob, respectively, which can, generally speaking, differ at the end of the QKD session due to the eavesdropping attack; $P_{K_s}(k_s)$ is the distribution function of the initial authentication key; $P_{K_AK_B}(k_A,k_B)$ is the distribution function of the final keys of Alice and Bob; $\rho_E^{k_Ak_B}$ is Eve's quantum state correlated with the keys $(k_A, k_B)$; $\rho^{R^A_{Aut}}(k_A,k_s)$ and $\rho^{R^B_{Aut}}(k_B,k_s)$ are the quantum states associated with classical messages from Alice to Bob and from Bob to Alice, respectively, when authenticating at the end of the session; and open messages depend on the QKD session (final key).

As in [13], we assume that the integrity of messages is checked at the end of the QKD session. First, Alice and Bob conduct the QKD session, including the exchange of open classic messages, and all the accumulated open messages $m$ along with their hash values $(m,t = h_{k_s}(m)$, which can be replaced by the eavesdropper $(m,t = h_{k_s}(m)) \to (m',t')$ are then resent at the end of the session.

The density matrices $\rho^{R^A_{Aut}}(k_A,k_s)$ and $\rho^{R^B_{Aut}}(k_B,k_s)$ in the basis $|m\rangle_A|t\rangle_A|m'\rangle_E|t'\rangle_E$ $(m \neq m', t \neq t')$ have off-diagonal matrix elements:

$$\rho^{R^A_{Aut}}(k_A,k_s) = \sum_{((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M}'\mathcal{T}'))_{OK}} P^{R_A}_{MTM'T'}(m,t,m',t'|k_A) \times |m\rangle_{MM}\langle m| \otimes |t\rangle_{TT}\langle t| \otimes |m'\rangle_{M'M'}\langle m'| \otimes |t'\rangle_{T'T'}\langle t'|. \quad (2)$$

The symbolic notation $((m, t), (m', t')) \in ((\mathcal{MT}),(\mathcal{M}'\mathcal{T}'))_{OK}$ means that summation occurs only over the substituted messages that have been checked on the receiving end. Messages that have not passed the check are discarded. The density matrix $\rho^{R^A_{Aut}}(k_B,k_s)$ that describes the transmission of classical messages from Bob to Alice has a similar form. Next, the quantum state for the ideal QKD situation and the ideal classical channel without message substitution has the form

$$\rho^{I^A_{Aut}I^B_{Aut}I^{AB}_{QKD}}_{ABE} = \sum_{k_s\in\mathcal{K}_s}\frac{1}{|\mathcal{K}_s|}|k_s\rangle_{K_sK_s}\langle k_s| \times \sum_{k_A\in\{0,1\}^\ell}\sum_{k_B\in\{0,1\}^\ell}\frac{\delta_{k_A,k_B}}{|\mathcal{K}_A|}|k_A\rangle_{AA}\langle k_A| \otimes |k_B\rangle_{BB} \times \langle k_B| \otimes \rho^{I^A_{Aut}}(k_A,k_s) \otimes \rho^{I^B_{Aut}}(k_B,k_s) \otimes \rho_E, \quad (3)$$

$$\rho^{I^A_{Aut}}(k_A,k_s) = \sum_{((m,t),(m',t'))\in((\mathcal{MT}),(\mathcal{M}'\mathcal{T}'))_{OK}} P^{I_A}_{MTM'T'}(m,t,m',t' \mid k_A) \times |m\rangle_{MM}\langle m| \otimes |t\rangle_{TT}\langle t| \otimes |m'\rangle_{M'M'}\langle m'| \otimes |t'\rangle_{T'T'}\langle t'|, \quad (4)$$

where the probability distribution $P^{I_A}_{MTM'T'}(m,t,m',t'|k_A)$ for the ideal classical channel without message substitution is diagonal over $(m,t,m',t')$, i.e., $P^{I_A}_{MTM'T'}(m,t,m',t'|k_A) \propto \delta_{m,m'}\delta_{t,t'}$. Note that the sums in Eqs. (2) and (4) include only the terms and $((m_B, t_B = h_{k_s}(m_B)),(m'_B,t'_B = h_{k_s}(m'_B)))$, which means that the authentication test was passed, although substitution was possible. The density matrix $\rho^{I^B_{Aut}}(k_B,k_s)$ describing the transmission of classical messages from Bob to Alice for the ideal classical communication channel without message substitution has the form similar to Eq. (4).

The quantum system of Eve is given by the expression

$$\rho_E = \sum_{k_A\in\{0,1\}^\ell}\sum_{k_A\in\{0,1\}^\ell} P_{K_AK_B}(k_A,k_B)\rho_E^{k_Ak_B}.$$

Here, $\rho^{I^A_{Aut}}(k_A)$ and $\rho^{I^B_{Aut}}(k_B)$ are the density matrices that correspond to a set of classical messages and their tags transmitted through an ideal classical channel with authentication without message substitution by Eve from Alice to Bob and from Bob to Alice, respectively. The key distribution function of Alice and Bob corresponds to an equiprobable distribution of keys, the keys of Alice and Bob are the same $\left(\frac{\delta_{k_A,k_B}}{|\mathcal{K}_A|}\right)$, the distribution of initial keys is also equiprobable, and the quantum system of Eve $\rho_E$ is uncorrelated with keys. The density matrices $\rho^{I^A_{Aut}}(k_A,k_s)$ and $\rho^{I^B_{Aut}}(k_B,k_s)$ associated with classical messages have a diagonal structure [13], since there is no message substitution.

## AVERAGE KEY GUESSING PROBABILITY

The trace criterion given by Eq. (1) does not explicitly contain keys that are used for various cryptographic purposes after the QKD. The ultimate goal of the eavesdropper is to determine the key that appears as a result of the QKD.

The eavesdropper makes measurements over his *quantum state obtained by attacking Alice's quantum states directly correlated with the key.* As a result, the eavesdropper has the side variables $(y_A, y_B)$, i.e., bit strings *directly* correlated with the keys $(k_A, k_B)$, as well as all open messages and their tags, which are only *indirectly* related to the key.

We first determine the average probability of guessing by keys. For the sake of brevity, we introduce the notation

$$\begin{gathered}(K, K_s, M, T, Y)\\ \leftrightarrow (k_A, k_B, k_s, m_A, t_A, m'_A, t'_A, m_B, t_B, m'_B, t'_B, y_A, y_B),\\ (K \mid K_s, M, T, Y)\\ \leftrightarrow (k_A, k_B \mid k_s, m_A, t_A, m'_A, t'_A, m_B, t_B, m'_B, t'_B, y_A, y_B),\end{gathered} \tag{5}$$

where $m_A$ ($t_A$) and $m_B$ ($t_B$) are the original messages (their tags) from Alice to Bob and from Bob to Alice, respectively, and $m'_A, t'_A, m'_B, t'_B$ are the corresponding substituted messages and their tags. Side variables ($y_A$, $y_B$) are bit strings that are obtained in eavesdropper's measurement of the quantum system $\rho_E^{k_A,k_B}$. Having a set of side variables, the eavesdropper tries to determine the keys ($k_A$, $k_B$) according to some decisive rule. Since Bob's key is bound to Alice's key and coincides with Alice's key with a probability of at least $1 - \varepsilon_{corr}$, the set of ($k_A$, $k_B$) values is $|\mathcal{K}_A|$.

Since the density matrices given by Eqs. (2)–(4) have a quantum–classical form, it is natural to choose measurements that also have a quantum–classical structure, although this is not essential for further conclusions. We consider a complete measurement over the entire Alice–Eve–Bob quantum system, which is given by operator-valued measures

$$\begin{aligned}&\mathcal{F}(K, K_s, M, T, Y)\\ &= |k_s\rangle_{K_s K_s}\langle k_s| \otimes |k_A\rangle_{K_A K_A}\langle k_A| \otimes |k_B\rangle_{K_B K_B}\langle k_B|\\ &\otimes |m_A\rangle_{M_A M_A}\langle m_A| \otimes |t_A\rangle_{T_A T_A}\langle t_A|\\ &\otimes |m'_A\rangle_{M'_A M'_A}\langle m'_A| \otimes |t'_A\rangle_{T'_A T'_A}\langle t'_A|\\ &\otimes |m_B\rangle_{M_B M_B}\langle m_B| \otimes |t_B\rangle_{T_B T_B}\langle t_B|\\ &\otimes |m'_B\rangle_{M'_B M'_B}\langle m'_B| \otimes |t'_B\rangle_{T'_B T'_B}\langle t'_B| \otimes \mathcal{M}_E^{y_A y_B}.\end{aligned} \tag{6}$$

Operator-valued measures implement the decomposition of the unit, which is a formal description of the measurement

$$\begin{aligned}&I_{K_s} \otimes I_{K_A} \otimes I_{K_B} \otimes I_M \otimes I_T \otimes I_{M'} \otimes I_{T'} \otimes I_E\\ &= \sum_{K, K_s, M, T, Y} \mathcal{F}(K, K_s, M, T, Y).\end{aligned} \tag{7}$$

We use the following well-known relationship between the trace distance and the distribution function of measurement results [30]:

$$\begin{aligned}&\left\|\rho_{ABE}^{R_{Aut}^A R_{Aut}^B R_{QKD}^{AB}} - \rho_{ABE}^{I_{Aut}^A I_{Aut}^B I_{QKD}^{AB}}\right\|_1\\ &= \max_{\mathcal{F}} \sum_{K, K_s, M, T, Y} \left|\mathrm{Tr}\left\{\mathcal{F}(K, K_s, M, T, Y)\rho_{ABE}^{R_{Aut}^A R_{Aut}^B R_{QKD}^{AB}}\right\}\right.\\ &\left. - \mathrm{Tr}\left\{\mathcal{F}(K, K_s, M, T, Y)\rho_{ABE}^{I_{Aut}^A I_{Aut}^B I_{QKD}^{AB}}\right\}\right|.\end{aligned} \tag{8}$$

This limit is achievable [30]; i.e., there are optimal measurements for which this equality is implemented. For further calculations, it is sufficient that the trace distance on the right-hand side of Eq. (8) at arbitrary measurements does not exceed the trace distance for the density matrices.

Measurement leads to the probability distribution for real and ideal situations

$$\begin{aligned}&P^R(K, K_s, M, T, Y)\\ &= \mathrm{Tr}\left\{\mathcal{F}(K, K_s, M, T, Y)\rho_{ABE}^{R_{Aut}^A R_{Aut}^B R_{QKD}^{AB}}\right\},\end{aligned} \tag{9}$$

$$\begin{aligned}&P^I(K, K_s, M, T, Y)\\ &= \mathrm{Tr}\left\{\mathcal{F}(K, K_s, M, T, Y)\rho_{ABE}^{I_{Aut}^A I_{Aut}^B I_{QKD}^{AB}}\right\}.\end{aligned} \tag{10}$$

After the QKD session, legitimate users have keys ($k_A$, $k_B$) and the shared authentication key $k_s$, which are not available to the eavesdropper. After the measurements, the eavesdropper has a set of the side variables $M$, $T$, and $Y$ that are correlated with the keys of legitimate users.

The goal of the eavesdropper, having side variables and applying some decisive rule $\mathcal{G}$, is to determine the true keys of Alice and Bob or to "guess" ($k_A$, $k_B$); i.e., having the side variables $M$, $T$, and $Y$, the eavesdropper makes a decision about the real keys $(\hat{k}_A, \hat{k}_B) = \mathcal{G}(M, T, Y)$. If $(\hat{k}_A, \hat{k}_B) = (k_A, k_B)$, the decision of the eavesdropper is successful. This solution is implemented by authentication with the key $k_s$, which is unknown to the eavesdropper.

To calculate the average probability of guessing on all keys, it is necessary to sum over all random implementations of the key $k_s$. Since the side variables are also random variables, it is also necessary to average only those values of side variables at which the guessing was successful. As a result, we get

$$\begin{aligned}\Pr_{Guess} &= \sum_{K_s} \sum_{(M,T,Y):\mathcal{G}(M,T,Y)=(k_A,k_B)} P^R(K_s, M, T, Y)\\ &\times P^R(K \mid K_s, M, T, Y)\\ &= \sum_{K_s} \sum_{(M,T,Y):\mathcal{G}(M,T,Y)=(k_A,k_B)} P^R(K, K_s, M, T, Y),\end{aligned} \tag{11}$$

where $P^R(K_s, M, T, Y)$ is the distribution function of $K_s$, $M$, $T$, and $Y$; $P^R(K|K_s, M, T, Y)$ is the conditional distribution function; and $P^R(K, K_s, M, T, Y) = P^R(K_s, M, T, Y)P^R(K|K_s, M, T, Y)$. *The sum includes only the estimates for a pair of keys whose estimates coincide with the true keys* $(\hat{k}_a, \hat{k}_B) = (k_A, k_B)$. As will be seen below, to calculate the upper limit of the probability of correctly guessing the keys $\Pr_{Guess}$, *an explicit form of the decisive rule is not required. We obtain*

$$\sum_{K_s}\sum_{(M,T,Y):\mathcal{G}(M,T,Y)=(k_A,k_B)}\left(P^R(K,K_s,M,T,Y)-P^I(K,K_s,M,T,Y)\right) \tag{12}$$

$$\le\sum_{K_s}\sum_{\substack{(M,T,Y):\mathcal{G}(M,T,Y)=(k_A,k_B)\\ \left(P^R(K,K_s,M,T,Y)-P^I(K,K_s,M,T,Y)\right)>0}}\left(P^R(K,K_s,M,T,Y)-P^I(K,K_s,M,T,Y)\right)$$

$$\le\sum_{\substack{K,K_s,M,T,Y\\ \left(P^R(K,K_s,M,T,Y)-P^I(K,K_s,M,T,Y)\right)>0}}\left(P^R(K,K_s,M,T,Y)-P^I(K,K_s,M,T,Y)\right)$$

$$=\sum_{K,K_s,M,T,Y}\frac{1}{2}|P^R(K,K_s,M,T,Y)-P^I(K,K_s,M,T,Y)|$$

$$\le\|\rho_{ABE}^{R_{Aut}^A R_{Aut}^B R_{QKD}^{AB}}-\rho_{ABE}^{I_{AutAut}^{A\ B}I_{QKD}^{AB}}\|_1\le\varepsilon_{Aut}+\varepsilon_{QKD}. \tag{13}$$

In Eq. (12), we used the following relation between the probability distributions $P_1(x)$ and $P_2(x)$ [31]:

$$\frac{1}{2}\sum_x|P_1(x)-P_2(x)|=\sum_{x:(P_1(x)-P_2(x))>0}(P_1(x)-P_2(x)). \tag{14}$$

Measurements for the ideal quantum state give

$$P^I(K,K_s,M,T,Y)=\mathrm{Tr}\left\{\mathcal{F}(K,K_s,M,T,Y)\rho_{ABE}^{I_{Aut}^A I_{Aut}^B I_{QKD}^{AB}}\right\}$$
$$=\frac{1}{|\mathcal{K}_s|}\frac{1}{|\mathcal{K}_A|}P_{M_A}(m_A)P_{M_B}(m_B)\delta_{k_A,k_B}\delta_{m_A',m_A}\delta_{m_B',m_B}\delta_{t_A',t_A}\delta_{t_B',t_B}\delta_{t_A,h_{k_s}(m_A)}\delta_{t_B,h_{k_s}(m_B)}P_{Y_AY_B}(y_A,y_B), \tag{15}$$

$$P_{Y_AY_B}(y_A,y_B)=\sum_{k_A,k_B}P_{K_AK_B}(k_A,k_B)\mathrm{Tr}_E\left\{M_E^{y_Ay_B}\rho_E\right\}=\sum_{k_A,k_B}P_{K_AK_B}(k_A,k_B)P_{Y_AY_B|K_AK_B}(y_A,y_B\mid k_A,k_B), \tag{16}$$

$$\sum_{y_A,y_B}P_{Y_AY_B}(y_A,y_B)=1.$$

Taking into account Eqs. (12)–(16), we reduce Eq. (11) to the form

$$\Pr_{Guess}=\sum_{K_s}\sum_{(M,T,Y):\mathcal{G}(M,T,Y)=(k_A,k_B)}P^I(K,K_s,M,T,Y)+\|\rho_{ABE}^{R_{Aut}^A R_{Aut}^B R_{QKD}^{AB}}-\rho_{ABE}^{I_{Aut}^A I_{Aut}^B I_{QKD}^{AB}}\|_1$$
$$\le\sum_{K,K_s,M,T,Y}P^I(K,K_s,M,T,Y)+\|\rho_{ABE}^{R_{Aut}^A R_{Aut}^B R_{QKD}^{AB}}-\rho_{ABE}^{I_{Aut}^A I_{Aut}^B I_{QKD}^{AB}}\|_1 \tag{17}$$
$$\le\frac{1}{|\mathcal{K}_A|}+\|\rho_{ABE}^{R_{Aut}^A R_{Aut}^B R_{QKD}^{AB}}-\rho_{ABE}^{I_{Aut}^A I_{Aut}^B I_{QKD}^{AB}}\|_1\le\frac{1}{|\mathcal{K}_A|}+\varepsilon_{Aut}+\varepsilon_{QKD}.$$

Thus, the probability of guessing the keys after QKD with information-theoretic authentication exceeds the simple guessing probability $\frac{1}{|\mathcal{K}_A|}=\frac{1}{2^\ell}$ by no more than $\varepsilon_{Aut}+\varepsilon_{QKD}$.

## KEY SEARCH COMPLEXITY AT A GIVEN PROBABILITY OF SUCCESS AFTER A QUANTUM KEY DISTRIBUTION SESSION WITH INFORMATION-THEORETIC AUTHENTICATION

The average probability of guessing by keys is a rather rough characteristic, because it does not provide information about the complexity, i.e., the number of steps to determine the true key. A more important characteristic is the number of encrypted messages before the first read. Let each message be encrypted with its own key received in the QKD.

Let the eavesdropper have a readability criterion in his favor; i.e., if the eavesdropper has found the correct key by testing the keys, the message is considered read. It is of interest what is the key search complexity, i.e., the number of testing steps necessary to determine the true key if only a brute-force set of keys and the probability of success being the probability that the key falls within the brute-force set are specified.

Let the eavesdropper, not knowing the authentication key $k_s$, but having a set of side variables $s_i=(M,T,Y)_i=(m_A,m_A',t_A,t_A',m_B,m_B',t_B,t_B',y_A,y_B)_i$, *some*

*of which are directly and some indirectly* related to the true keys ($k_A$, $k_B$), test the first $1 \le N \le |\mathcal{K}_A|$ most probable keys for each encrypted message.

In favor of the eavesdropper, we assume that he knows the probability distributions themselves. The eavesdropper orders the first $N$ keys in descending order of conditional probabilities for given values of side variables $s_i$. In addition, the probability of success $\pi_0$ is specified (see below). Let conditional posterior probabilities at *given* $s_i$ be ordered as

$$P^R(k_{1(s_i)} \mid s_i) \ge P^R(k_{2(s_i)} \mid s_i) \ldots \ge P^R(k_{N(s_i)} \mid s_i), \quad (18)$$

where $P^R(k_{\ell(s_i)} \mid s_i) = \sum_{k_s} P^R(k_{\ell(s_i)} \mid k_s, s_i)$ ($l = 1, 2, \ldots, N$) is the probability averaged over all values of the authentication key, $k_{m(s_i)} = (k_A, k_B)_{m(s_i)}$, and $1(s_i)$, $2(s_i)$, ..., $|\mathcal{K}_A|(s_i)$ is the permutation of the ordinal numbers of the original keys $m(s_i)$, which depend on $s_i$ when the probabilities are ordered.

The task is to calculate the average number of tests until the first successful crack of the cipher, i.e., the determination of the true key. For the first message, the first $N$ most probable keys from the full set of keys $|\mathcal{K}_A|$ are tested, if the key is found, then the process is successfully completed. If the key is not found after $N$ trials, the testing stops, and the second message is expected, and so on until the true key is determined. Let the sequence of the side variable of the eavesdropper in series of tests is

$$\mathbf{s} = (s_1, s_2 \ldots s_i \ldots), \quad s_i \in S. \quad (19)$$

Here, the index $i$ enumerates the messages and the side variables $s_i$, which arise for the eavesdropper for this message, and $S$ is the set of *all possible values of the side variables*, which they take after measurements by the eavesdropper.

Let the corresponding sequence of brute force sets of the first $N$ most probable keys attributed to each set of side variables $s_1$, $s_2$, ..., $s_{|\mathcal{K}_A|}$ be

$$\mathbf{K} = (\mathcal{K}_1, \mathcal{K}_2, \ldots \mathcal{K}_i \ldots). \quad (20)$$

Here, each set $\mathcal{K}_i$ depends on $s_i$: $\mathcal{K}_i = \{k_{1(s_i)}, k_{2(s_i)} \ldots k_{N(s_i)}\}$.

The probability obeying the geometric distribution for the sequences with the length $j$ for given side variables to the first determination of the key is

$$P(j) = \pi(N, s_{j+1}) \prod_{i=0}^{j} (1 - \pi(N, s_i))$$
$$\text{where} \quad \pi(N, s_i) = \sum_{\{k_{m(s_i)} \in \mathcal{K}_i\}} P^R(k_{m(s_i)} \mid s_i). \quad (21)$$

Formula (21) gives the probability of determining the key in the $j$ step, provided that the key was not found in the previous $j - 1$ steps.

Further, let

$$\mathcal{K}_i = \{k_{m(s_i)} : P(k_{1(s_i)} \mid s_i) \ge P(k_{2(s_i)} \mid s_i) \ldots \ge P(k_{M(s_i)} \mid s_i); \quad m(s_i) = 1 \ldots N\}, \quad (22)$$

i.e., ordering in $\mathcal{K}_i$ depends uniquely on the side variable $s_i$. In other words, the arrangement of the indices $m(s_i)$ and conditional probabilities in the set $\mathcal{K}$ of all possible key values is given by the side variable $s_i$, and the sets $\mathcal{K}_i$ and $\mathcal{K}$ are the same or, more precisely, differ only in the permutation of the keys.

The average complexity $G(N, K|\mathbf{s})$, where the symbol $S$ indicates only that the average complexity depends on the set of observed side variables, for all observations of all side variables, which are independent for different $j$ values, i.e., the average number of trail steps within the test set, has the form

$$G(N, K \mid S) = \mathbf{E}\big(G(N, K \mid \mathbf{s})\big)$$
$$= \mathbf{E}\left( N \sum_{j=0}^{\infty} \left( j\pi(N, s_{j+1}) \prod_{i=0}^{j} (1 - \pi(N, s_i)) \right) \right. \quad (23)$$
$$\left. + \sum_{j=0}^{\infty} \sum_{m=1}^{N} \left( m \frac{P(k_{m(s_{j+1})} \mid s_{j+1})}{\pi(N, s_{j+1})} \pi(N, s_{j+1}) \prod_{i=0}^{j} (1 - \pi(N, s_i)) \right) \right)$$

$$= \frac{(1 - \pi(N))N}{\pi(N)} + \frac{1}{\pi(N)} \sum_{m=1}^{N} mp(m). \quad (24)$$

Here, $G(N, K|\mathbf{s})$ is the complexity for a specific observed set of side variables (see Eq. (19)),

$$\mathbf{E}(\ldots) = \sum_{s_1 \in S} P^R(s_1) \sum_{s_2 \in S} P^R(s_2) \ldots \sum_{s_i \in S} P^R(s_i) \ldots (\ldots) \quad (25)$$

is the average of all independent implementations of side variables $s_i$,

$$p(m) = \sum_{s_i \in S} P^R(s_i) P^R(k_{m(s_i)} \mid s_i),$$
$$\pi(N) = \sum_{m=1}^{N} p(m) = \sum_{m=1}^{N} \sum_{s_i \in S} P^R(s_i) P^R(k_{m(s_i)} \mid s_i). \quad (26)$$

Here, $\pi(N)$ is the average probability of success (the determination of the encryption key), i.e., the probability that a random key $k_1$ enters into the test set of the most likely keys.

The index $m(s_j)$ determines the key test step and takes the values $m(s_j) = 1(s_j)$, $2(s_j)$, …, and $N(s_j)$ at a fixed $s_j$ value. This representation indicates that the keys at the given $s_j$ value are permuted in such a way that the conditional probability is maximum $k_{2(s_j)}$ for the first key $k_{1(s_j)}$ and decreases with increasing ordinal number of the keys, i.e., $P^R(k_{1(s_j)} \mid s_j) \ge P^R(k_{2(s_j)} \mid s_j) \ge \ldots$. The

probability depends only on the ordinal number of the test step. Taking into account Eqs. (26), we find

$$\sum_{m=1}^{N} m \sum_{s_i \in S} P^{\mathrm{R}}(s_i) P^{\mathrm{R}}(k_{m(s_i)} \mid s_i) = \sum_{m=1}^{N} m \cdot p(m). \qquad (27)$$

*To estimate the lower limit of complexity in Eqs.* (23) *and* (24), *it is necessary to have a lower estimate of the parameter* $\sum_{m=1}^{N} mp(m)$, *which appears in the numerator of Eq.* (24) *and both the lower and upper estimates for the parameter* $\pi(N)$, *which enters into both the numerator and the denominator of Eq.* (24).

Since the sets $\mathcal{H}_i$ and $\mathcal{H}$ differ only in the permutation of the keys and the testing step $m$ and the testing key $k(m)$ at the given side variables $s$ are uniquely related by virtue of Eq. (22), taking into account the right-hand sides of Eqs. (21), (26), and (27), we directly obtain a chain of relations

$$\begin{aligned}
\pi(N) &= \sum_{s\in S} P^{\mathrm{R}}(s)\pi(N,s) = \sum_{s\in S}\sum_{k(m)\in\mathcal{H}} P^{\mathrm{R}}(s)P^{\mathrm{R}}(k(m)|s) \\
&= \sum_{s\in S}\sum_{m=1}^{N}(P^{\mathrm{R}}(k(m),s) - P^{\mathrm{I}}(k(m),s)) + \sum_{s\in S}\sum_{m=1}^{N} P^{\mathrm{I}}(k(m),s) \\
&= \frac{N}{|\mathcal{H}_{\mathrm{A}}|} + \sum_{s\in S}\sum_{m=1}^{N}\left(P^{\mathrm{R}}(k(m),s) - P^{\mathrm{I}}(k(m),s)\right) \\
&\le \frac{N}{|\mathcal{H}_{\mathrm{A}}|} + \frac{1}{2}\sum_{s\in S}\sum_{m=1}^{N}\left|P^{\mathrm{R}}(k(m),s) - P^{\mathrm{I}}(k(m),s)\right| \\
&\le \frac{N}{|\mathcal{H}_{\mathrm{A}}|} + \left\|\rho_{\mathrm{ABE}}^{R_{\mathrm{Aut}}^{\mathrm{A}} R_{\mathrm{Aut}}^{\mathrm{B}} R_{\mathrm{QKD}}^{\mathrm{AB}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{Aut}}^{\mathrm{A}} I_{\mathrm{Aut}}^{\mathrm{B}} I_{\mathrm{QKD}}^{\mathrm{AB}}}\right\|_1 \\
&\le \frac{N}{|\mathcal{H}_{\mathrm{A}}|} + \varepsilon_{\mathrm{Aut}} + \varepsilon_{\mathrm{QKD}}.
\end{aligned} \qquad (28)$$

To estimate the lower bound by with similar calculations, as in Eq. (28), we get

$$\begin{aligned}
\pi(N) &= \sum_{s\in S} P^{\mathrm{R}}(s)\pi(N,s) \ge \frac{N}{|\mathcal{H}_{\mathrm{A}}|} \\
&- \left\|\rho_{\mathrm{ABE}}^{R_{\mathrm{Aut}}^{\mathrm{A}} R_{\mathrm{Aut}}^{\mathrm{B}} R_{\mathrm{QKD}}^{\mathrm{AB}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{Aut}}^{\mathrm{A}} I_{\mathrm{Aut}}^{\mathrm{B}} I_{\mathrm{QKD}}^{\mathrm{AB}}}\right\|_1 \ge \frac{N}{|\mathcal{H}_{\mathrm{A}}|} - (\varepsilon_{\mathrm{Aut}} + \varepsilon_{\mathrm{QKD}}).
\end{aligned} \qquad (29)$$

Next, we obtain

$$\begin{aligned}
&\sum_{s\in S}\sum_{m=1}^{N} mP^{\mathrm{R}}(s)P^{\mathrm{R}}(k(m) \mid s) \\
&= \frac{N(N+1)}{2|\mathcal{H}_{\mathrm{A}}|} + \sum_{s\in S}\sum_{m=1}^{N} m\left(P^{\mathrm{R}}(k(m),s) - P^{\mathrm{I}}(k(m),s)\right) \\
&\ge \frac{N(N+1)}{2|\mathcal{H}_{\mathrm{A}}|} - \sum_{s\in S}\sum_{k\in\mathcal{H}}^{|\mathcal{H}_{\mathrm{A}}|}\frac{1}{2}\left|m\left(P^{\mathrm{R}}(k,s) - P^{\mathrm{I}}(k,s)\right)\right| \\
&\ge \frac{N(N+1)}{2|\mathcal{H}_{\mathrm{A}}|} - N\sum_{s\in S}\sum_{k\in\mathcal{H}}\frac{1}{2}\left|\left(P^{\mathrm{R}}(k,s) - P^{\mathrm{I}}(k,s)\right)\right| \\
&\ge \frac{N(N+1)}{2N} - (\varepsilon_{\mathrm{Aut}} + \varepsilon_{\mathrm{QKD}}).
\end{aligned} \qquad (30)$$

To obtain Eq. (30), we used the equality

$$\begin{aligned}
\sum_{s\in S}\sum_{m=1}^{N} mP^{\mathrm{I}}(k(m),s) &= \sum_{s\in S} P^{\mathrm{I}}(s)\sum_{m=1}^{N} mP^{\mathrm{I}}(k(m) \mid s) \\
&= \sum_{s\in S} P^{\mathrm{I}}(s)\frac{1}{|\mathcal{H}_A|}\sum_{m=1}^{N} m\frac{N(N+1)}{2|\mathcal{H}_A|}.
\end{aligned}$$

Here, it is taken into account that the transition probability $P^{\mathrm{I}}(k(m) \mid s) = \frac{1}{|\mathcal{H}_A|}$ in the ideal case does not depend on the side variables $s$, and $\sum_{m=1}^{N} m = \frac{N(N+1)}{2}$ is the sum of the arithmetic progression, and the normalization condition $\sum_{s\in S} P^{\mathrm{I}}(s) = 1$ for the probabilities.

Taking into account the estimates given by Eqs. (28)–(30), we obtain the result

$$\begin{aligned}
Q(K \mid S, \pi_0) &= \min_{\{N:\pi(N)\ge\pi_0\}} G(K \mid S, N) \\
&\ge \left(1 - \frac{\varepsilon_{\mathrm{Aut}} + \varepsilon_{\mathrm{QKD}}}{\pi_0}\right)\left(\frac{|\mathcal{H}_A|(1 - 4(\varepsilon_{\mathrm{Aut}} + \varepsilon_{\mathrm{QKD}})) + 1}{2}\right).
\end{aligned} \qquad (31)$$

Thus, the complexity of partial brute-force after a QKD session with information-theoretic authentication is explicitly expressed in terms of the trace distance (1).

It is important to note that the answer to the question posed at the beginning of the work is based on strict calculations rather than on qualitative intuitive considerations and it can thereby be reliably used in further research and applications of QKD systems.

## CONCLUSIONS

It is interesting to make some estimates. Let the given probability of success be $\pi_0 = 1/2$. For real systems, $\varepsilon_{\mathrm{QKD}} \approx 10^{-9}$–$10^{-7}$ and $\varepsilon_{\mathrm{Aut}} \approx 10^{-9}$–$10^{-7}$ are achievable. The number of trial steps to the first read of a message, i.e., to the true key determination, is about $2^l(1 - 16(10^{-9}–10^{-7})/4$. At a key length of $l = 256$ bits, the number of brute-force steps is almost equal to the number of brute-force steps across the entire key space about $2^{254} \approx 10^{76}$.

## ACKNOWLEDGMENTS

We are grateful to I.M. Arbekov, to the staff of InfoTeks, and SFB Laboratory, and to colleagues from the Academy of Cryptography of the Russian Federation for their interest in the work, numerous discussions, advice, and support.

## FUNDING

This work was supported by ongoing institutional funding for the Center for Quantum Technologies, Moscow State University (S.P. Kulik) and the Osipyan Institute of Solid State Physics, Russian Academy of Sciences

(S.N. Molotkov). No additional grants to carry out or direct this particular research were obtained.

## CONFLICT OF INTEREST

The authors of this work declare that they have no conflicts of interest.

## OPEN ACCESS



## REFERENCES

1. C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers 7, Systems and Signal Processing, Bangalore, India* (1984), p. 175.
2. H. P. Yuen, Phys. Rev. A **82**, 062304 (2010).
3. H. P. Yuen, arXiv: 1109.1051 [quant-ph].
4. H. P. Yuen, arXiv: 1109.2675 [quant-ph].
5. H. P. Yuen, arXiv: 1109.1066 [quant-ph].
6. R. Renner, arXiv: 1209.2423 [quant-ph].
7. I. M. Arbekov and S. N. Molotkov, J. Exp. Theor. Phys. **125**, 50 (2017).
8. I. M. Arbekov, Mat. Vopr. Kriptogr. **7** (1), 39 (2016).
9. S. N. Molotkov, J. Exp. Theor. Phys. **123**, 784 (2016).
10. A. Abidin and J.-Å. Larsson, Int. J. Quantum Inform. **7**, 1047 (2009).
11. M. Peev, C. Pacher, T. Lorünser, M. Nölle, A. Poppe, O. Maurhart, M. Suda, A. Fedrizzi, R. Ursin, and A. Zeilinger, Int. J. Quantum Inform. **7**, 1401 (2009).
12. C. Pacher, A. Abidin, T. Lornser, M. Peev, R. Ursin, A. Zeilinger, and J.-Å. Larsson, Quantum Inform. Process. **15**, 327 (2012); arXiv: 1209.0365.
13. S. N. Molotkov, Laser Phys. **34**, 045202 (2024).
14. R. Renner, PhD Thesis (ETH, Zürich, 2005).
15. G. Simmons, Proc. IEEE **76**, 603 (1988).
16. M. N. Wegman and J. L. Carter, J. Comput. Syst. Sci. **22**, 265 (1981).
17. M. Atici and D. R. Stinson, in *Proceedings of the CRYP-TO 96,* Ed. by N. Koblitz, Lect. Notes Comput. Sci. **1109**, 16 (1996).
18. J. Bierbrauer, T. Johansson, G. Kabatianskii, and B. Smeets, in *Proceedings of the CRYPTO'93,* Ed. by D. Stinson, Lect. Notes Comput. Sci. **773**, 331 (1994).
19. B. den Boer, J. Comput. Secur. **2**, 65 (1993).
20. H. Krawczyk, in *Proceedings of the CRYPTO 94,* Ed. by Y. Desmedt, Lect. Notes Comput. Sci. **839**, 129 (1994).
21. H. Krawczyk, in *Proceedings of the EUROCRYPT 95,* Ed. by L. C. Guillou and J. J. Quisquater, Lect. Notes Comput. Sci. **921**, 301 (1995).
22. D. R. Stinson, in *Proceedings of the CRYPTO 91,* Ed. by J. Feigenbaum, Lect. Notes Comput. Sci. **576**, 74 (1992).
23. D. R. Stinson, J. Comput. Syst. Sci. **48**, 337 (1994).
24. D. R. Stinson, Congr. Numer. **114**, 7 (1996).
25. D. R. Stinson, J. Combin. Math. Combin. Comput. **42**, 3 (2002).
26. A. Abidin and J.-Å. Larsson, in *Proceedings of the WEWoRC 2011,* Ed. by S. Lucks and F. Armknecht, Lect. Notes Comput. Sci. **7242**, 99 (2012).
27. P. Rogaway, J. Cryptol. **12**, 91 (1999).
28. A. Abidin and J.-Å. Larsson, Quantum Inf. Process. **13**, 2155 (2014).
29. Ch. Portmann, IEEE Trans. Inform. Theory **60**, 4383 (2014).
30. M. M. Wilde, arXiv: 1106.1445v6 [quant-ph] (2015).
31. T. M. Cover and J. A. Thomas, *Elements of Information Theory,* 2nd ed. (Wiley, Hoboken, NJ, 2006).

*Translated by R. Tyapaev*

**Publisher's Note.** Pleiades Publishing remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
AI tools may have been used in the translation or editing of this article.