Physics – Uspekhi **68** (10) 963 – 986 (2025)

REVIEWS OF TOPICAL PROBLEMS

PACS numbers: 03.67.Dd, 03.67.Hk, **89.70.–a**

INTERNATIONAL YEAR OF QUANTUM SCIENCE AND TECHNOLOGY

Vernam's, Kotelnikov's, and Shannon's one-time pad and quantum cryptography

I.M. Arbekov, S.N. Molotkov

DOI: https://doi.org/10.3367/UFNe.2025.07.039972

Contents

Abstract. **Quantum cryptography — quantum key distribution (QKD) — was one of the first fields of study of quantum information theory. It reached a mature scientific level and has been implemented in commercial systems for secure quantum communications. The key distribution problem is the central issue of symmetric cryptography. Quantum cryptography solves this problem on the basis of the fundamental laws of nature: the principles of quantum mechanics. Quantum key distribution is essentially matching two independent random sequences on the transmitting and receiving sides by exchanging quantum states. Required in addition to the quantum channel is an authentic classical communication channel. Both communication channels are open and vulnerable to a perpetrator's attack. To ensure the authenticity of the classical channel at initial system startup, a seed key is required, which is used to provide information-theoretic authentication. In essence, quantum cryptography systems are mechanisms for expanding this seed key. Subsequent sessions generate a quantum key, part of which is used for authentication, while another part is employed for other cryptographic purposes, such as encryption. An issue fundamental for quantum cryptography is the number of quantum key distribution sessions that can be conducted from the initial system launch until a new system reboot, when the cryptographic properties of the quantum keys reach a critical level, after which they can no longer be used for cryptographic purposes, and a new system reboot is needed. Although a number of reviews on quantum cryptography are currently available, this issue has not been discussed in detail. It is shown that for realistic parameters of quantum cryptography systems that are currently achievable, a QKD system can operate for**

I.M. Arbekov [1,*], **S.N. Molotkov** [1,2,3,4,†]
[1] Academy of Cryptography of the Russian Federation,
119331 Moscow, PO Box 100, Russian Federation
[2] Osipyan Institute of Solid State Physics, Russian Academy of Sciences,
ul. Akademika Osipyana 2, 142432 Chernogolovka, Moscow region,
Russian Federation
[3] Lomonosov Moscow State University,
Faculty of Computational Mathematics and Cybernetics,
Leninskie gory 1, str. 52, 119991 Moscow, Russian Federation
[4] Quantum Technology Center, Lomonosov Moscow State University,
Leninskie gory 1, str. 35, 119991 Moscow, Russian Federation
E-mail: [*] arbekov53@mail.ru, [†] molotkov@issp.ac.ru

Received 13 January 2025, revised 28 July 2025
Uspekhi Fizicheskikh Nauk **195** (10) 1021 – 1046 (2025)
Translated by M.Zh. Shmatikov

virtually any length of time before the next reboot. This implies that QKD systems can implement a 'one-time pad' — a set of one-time keys using only a single seed key. A brief historical overview is also presented, outlining some facts little known to the general public. This review, which is intended for a general audience, is comprehensible to undergraduate and graduate students who have completed university courses on quantum information science. The authors hope that it will provide a deeper understanding of the cryptographic underpinnings of state-of-the-art quantum key distribution systems.

Keywords: quantum cryptography, one-time pad, secure communications, authentication

1. Introduction and brief history

About 30 years ago, the term 'cryptography' was virtually absent from the public domain. Cryptography, understood as information security, was the area of activity of specialized organizations. Today, cryptography is a part of everyday life and affects everyone, even those with little professional experience in this field. Computer passwords, PIN codes for smart cards and other electronic devices, banking transactions, cryptocurrency, digital signatures, blockchain, distributed databases, remote voting, internet technologies, and much more — all of this involves mature science related to information security. Virtually every institution of higher education offers programs for training specialists in information security.

Quantum cryptography [1], synonymous with quantum key distribution (QKD), is a rapidly developing field of quantum information science. Not only do individual experimental prototypes of QKD systems exist in this field, but entire networks with quantum key distribution have been created in various countries [2–4]. The feasibility of key distribution via a satellite has been demonstrated [2]. In Russia, a university quantum network — a quantum telephony network [4] — was launched in 2021. It is a joint development between Infotecs, a Russian IT company, and the Center for Quantum Technologies at Lomonosov Moscow State University (MSU).

To date, several reviews [5–9] have been published on various aspects of QKD systems. At its inception, quantum cryptography was positioned as a method providing unconditional security. Unconditional security refers to the secrecy of keys that is based on the fundamental laws of nature — principles of quantum physics — rather than on assumptions about the limited computational and technical capabilities of a perpetrator. This concept has been repeatedly used in both popular publications and purely scientific articles. However, the details of what lies behind this term have not yet been presented in a concentrated form within a single review. Since QKD systems are a part of today's reality, we believe that familiarizing a wider audience with the real meaning behind these concepts of secrecy requires a separate and detailed presentation in a single place.

The development of ideas in any scientific field can only be understood within the context of the logic of historical events; so, for a complete presentation, it makes sense to trace the events that led to the birth of quantum cryptography and, more broadly, quantum communications.

The history of cryptography is as ancient as the history of humanity. References to cryptography can be found as far back as the ancient Egyptians, who used tattoos on slaves' heads, hidden under their hair, to transmit secret messages.[1] Ciphers such as the Caesar cipher and the Scythala cipher of Ancient Sparta have been known since ancient times. Various historical examples of ciphers and methods for cracking them are presented in some well-known monographs [10, 11]. The history of encryption in Russia from the ancient Slavs to the mid-20th century is described in [12]. Cryptographic analysis methods, although not called such, helped decipher ancient texts written in three archaic languages on the famous Rosetta Stone, which was discovered in a well-preserved state in 1799 during Napoleon's invasion of Egypt [13].

These historical examples share a common element — an initial shared secret which is known to both the sender and recipient of the encrypted message and which ensures the protection of the transmitted message. In the Caesar cipher, such a shared secret — the secret key — is the alphabetical shift used to replace letters; in the Scytale cipher, the shared secret is the dimensions of the rod (scytale), on which a ribbon is wound to inscribe the transmitted message along the rod.

Cryptography that uses a shared secret (key) only known to the sender and receiver is commonly called symmetric cryptography. Symmetric cryptography requires that the legitimate parties to the information exchange, typically referred to as Alice and Bob, initially share a common secret — a secret key. In modern terms, a secret key is a random bit string of 0s and 1s known only to Alice and Bob. Random number generation plays a fundamental role in any cryptographic system. Quantum cryptography systems use physical quantum random number generators. A random bit string of 0s and 1s — the secret key — allows Alice to encrypt her message and Bob, using the same secret key as Alice, to decrypt the transmitted message. Speaking of terminology, people often use the term 'crack' instead of 'decrypt,' especially in various online blogs. Cracking is the decoding of a cipher; it is an illegitimate procedure performed by a perpetrator who does not know the secret key.

This raises a fundamental question about the security of a cipher. Even if the key is secret, can a perpetrator, without the secret key, crack the cipher and read the message? In other words, are there methods of encryption with a secret key that are essentially unbreakable? This is a fundamental question for cryptography, the answer to which is far from apparent.

Even great scientists have made mistakes when trying to answer this question. For example, a simple substitution cipher consists of replacing each letter of the plaintext with a symbol. This cipher is weak because the frequency of letters in the plaintext is different, and therefore the frequency of replacement symbols is preserved. The great mathematician Carl Friedrich Gauss believed that, if each letter of the plaintext were replaced with a randomly selected symbol from the cipher's alphabet, and the number of replacement symbols for each letter was proportional to the frequency of that letter, such a cipher would be unbreakable. However, this does not improve the situation, and the cipher remains weak. The delusions of geniuses are very instructive. Gauss failed to make the final step — perhaps every letter of the plaintext in each message should be replaced each time with new random symbols? It took over 100 years to bring this idea to its logical conclusion in the 20th century and make the final step —

[1] However, in modern terminology, such information concealment is referred to as steganography — the concealment of secret information among open information, for example, within individual pixels of an image.

providing an encryption system that cannot be deciphered (broken), even theoretically.

In the scientific community, it is generally accepted that G.S. Vernam, an employee of Bell Telephone Laboratories (USA), was the first to formulate this idea. A joint patent of Vernam and Major Joseph O. Mauborgne, an employee of the U.S. Army Signal Corps, is dated 1918. In his publication that appeared in 1926 [14], Vernam proposed a teletype in which plaintext letters were transformed in accordance with the Baudot code — each letter was associated with a combination of five values of 0 and 1 (bits). The bit plaintext was encrypted using a key — a random bit sequence — using the XOR operation (addition modulo 2). In the original version, the key was recorded on a closed tape, so after a certain number of text characters the key was repeated. This scheme was developed for the U.S. Army Signal Corps. A representative of the client, Mauborgne, noted that such an encryption system, due to the repetition of encryption keys, would not be completely secure, and proposed replacing the keys with an infinite running tape of random bits. He asserted [14], albeit without any mathematical justification, that encryption systems with a running random key would be completely undecipherable:

If, now, instead of using English words or sentences, we employ a key composed of letters selected absolutely at random, a cipher system is produced which is absolutely unbreakable.

New scientific ideas in any field do not arise overnight. The question of who was the first to propose the idea of the *one-time pad* — the concept of encryption with a one-time bit sequence — has haunted researchers to this day. It seems that the most recent historical study is presented in [15]. The author of this study 'dug' through archival materials, based on which it is claimed that the idea of one-time pad encryption was proposed by Frank Miller, a California banker, almost 35 years before G. Vernam's and J. Mauborgne's patent in the publication *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams.*

A banker in the West should prepare a list of irregular numbers, to be called 'shift-numbers,' such as 483, 281, 175, 892, etc.

The differences between such numbers must not be regular.

When a shift-number has been applied, or used, it must be erased from the list and not used again.

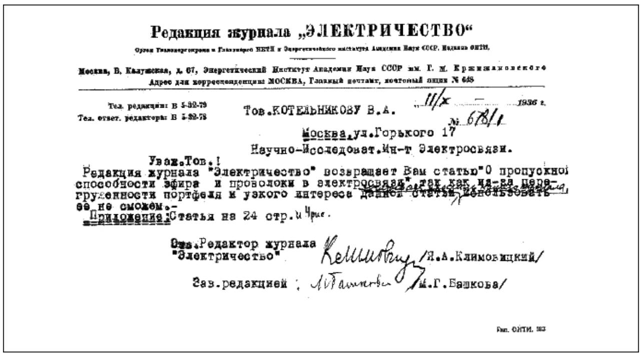
A copy of the list is to be sent to the New York banker, who prepares a different list and sends a copy thereof to the Western banker.

Miller understood that one-time use of keys was necessary.

Any system which allows a cipher word to be used twice with the same signification is open to detection. A little talk with a telegraph operator will convince one of this fact.

The aforementioned study also discusses, with reference to archival documents, the question of whether Mauborgne might have been aware of Miller's idea.

The next step, a simple proof of the absolute security of an encryption method with secret one-time keys (which can generally be understood as summation with random numbers over any modulus), was independently made by our outstanding compatriot, Academician of the USSR Academy of Sciences Vladimir Aleksandrovich Kotelnikov. The classified report, dated June 19, 1941, consisted of several pages of typewritten text [16]. Although the report was declassified more than 30 years ago, it remains unknown to the general scientific community (see details in [17]). It is important to note that Soviet cryptographers, independent of their Western colleagues, were aware of the secrecy features of this encryption method.



Редакция журнала „ЭЛЕКТРИЧЕСТВО“

Орган Главэнергопрома и Главэнерго НКТП и Энергетического института Академии Наук СССР. Издание ОНТИ.

Москва, В. Калужская, д. 67, Энергетический Институт Академии Наук СССР им. Г. М. Кржижановского
Адрес для корреспонденции: МОСКВА, Главный почтамт, почтовый ящик № 648

Тел. редакции: В 5-32-79
Тел. ответ. редактора: В 5-32-73

Тов.КОТЕЛЬНИКОВУ В.А. „11/x" 1936 г.
№ 678/1
Москва,ул.Горького 17
Научно-Исследоват.Ин-т Электросвязи.

Уваж.Тов.!
Редакция журнала "Электричество" возвращает Вам статью"О пропускной способности эфира и проволоки в электросвязи", так как из-за перегруженности портфеля и узкого интереса ~~данной статьи использовать~~ ее не сможем.-
Приложение:Статья на 24 стр. и 4 рис.

Отв.Редактор журнала
"Электричество" Климовицкий /Я.А.Климовицкий/

Зав.редакцией : /М.Г.Башкова/

Тип. ОНТИ. 383

Figure 1. Editorial board's letter rejecting V.A. Kotelnikov's paper containing proof of famous sampling theorem that marked beginning of digital era.

Report [16] should not be confused with another well-known V.A. Kotelnikov's study, "On the Bandwidth of Ether and Wire in Telecommunications," published in 1932, in which he proved the famous sampling theorem and ushered in the digital age [18]. The ideas put forward in the paper were far ahead of their time. The content of this theorem is now presented in any textbook, but it does not exist as a journal article, since it was rejected by the journal's editors as being of no scientific interest. Since historical information never disappears, it is of interest to cite the editors' response to the submitted paper (Fig. 1).

Despite this, V.A. Kotelnikov's priority in proving the sampling theorem was recognized many years later by the global scientific community [19].

The next step, with a complete mathematical proof of the secrecy of a one-time pad using methods of modern classical information theory, was made by Claude Elwood Shannon in his "Communication Theory of Secrecy Systems" [20]. The study, carried out at Bell Labs (USA) in 1945, was declassified in 1948. Some American cryptographers believe this was done in error, due to an oversight (see W. Diffie's note in the preface to Bruce Schneier's monograph, *Applied Cryptography* [21]). Following Shannon's study, this method was called 'one-time pad encryption.' Kotelnikov's and Shannon's studies provided a clear understanding of the properties a perfect cipher must satisfy, namely:

— the key must be random,

— the key length in bits must be no less than the message length,

— the key may be used only once.

The concept of *perfect secrecy* of a cryptosystem is introduced based on a probability–theoretic model that relates plaintext messages $m \in M$, keys $k \in K$, and encrypted messages $c \in C$ as a joint distribution $P(m,k,c)$. Perfect secrecy requires that the posterior probabilities of plaintext messages received after interception of a ciphertext message be equal to the prior probabilities of the same messages before interception. It is easy to verify that *perfect secrecy* holds for a cryptosystem in which:

— the plaintext message m and key k are binary sequences of length N,

— the ciphertext message $c = m \oplus k$ is the modulo-2 sum of the binary digits of the plaintext message and key,

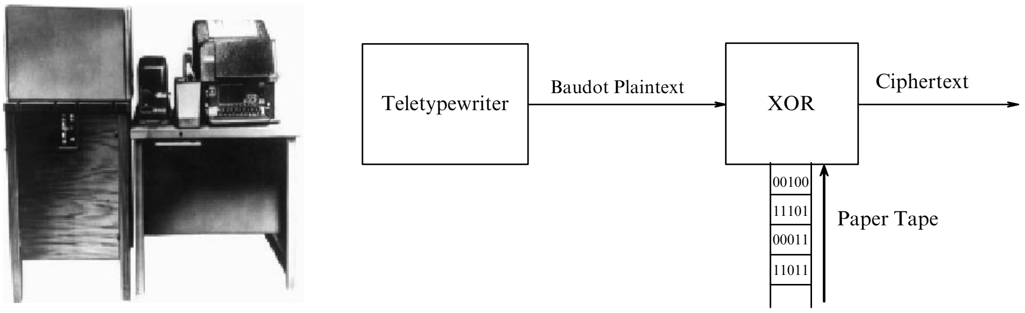
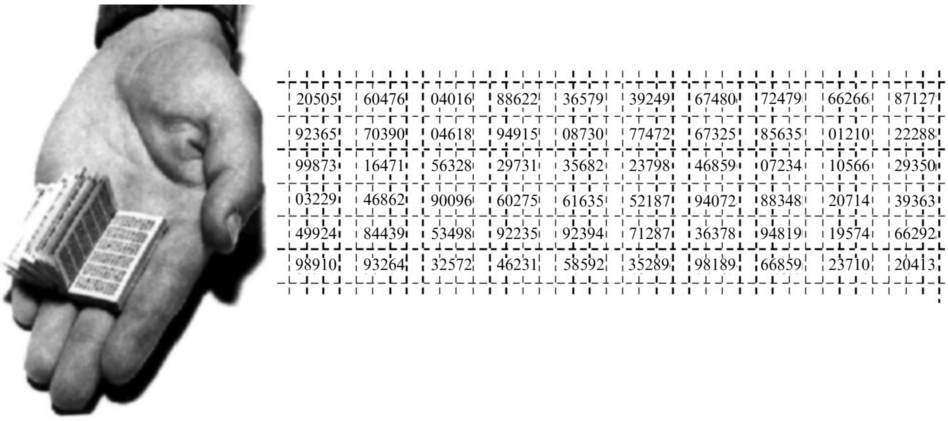


Figure 2. Vernam's polyalphabetic teletype with 'running keys.' Held by US National Security Agency [22].



20505	60476	04016	88622	36579	39249	67480	72479	66266	87127
92365	70390	04618	94915	08730	77472	67325	85635	01210	22288
99873	16471	56328	29731	35682	23798	46859	07234	10566	29350
03229	46862	90096	60275	61635	52187	94072	88348	20714	39363
49924	84439	53498	92235	92394	71287	36378	94819	19574	66292
98910	93264	32572	46231	58592	35289	98189	66859	23710	20413

Figure 3. One-time pad of famous Soviet intelligence officer Rudolf Ivanovich Abel (William Fisher), seized by FBI on June 21, 1957 as a result of treason. Pad consisted of 60 pages with five decimal digits. Held by US National Security Agency [22]. Method for generating random numbers has never been disclosed in publicly accessible reports.

— the key is chosen randomly and equiprobably from the entire space of binary sequences of length N.

Then, the conditional probability is

$$P(m|c) = \frac{P(m)P(c|m)}{P(c)} = \frac{P(m)\ \Pr\{k : m \oplus k = c\}}{\sum_{m'} P(m')\ \Pr\{k : m' \oplus k = c\}}$$

$$= \frac{P(m)2^{-N}}{2^{-N}\sum_{m'} P(m')} = P(m)\,.$$

Here, it is necessary to comment on what is meant by a 'plaintext' message. Since any language is redundant, in practice, text messages typically are compressed to bring the compressed text closer to a random bit sequence. If, for example, propagation of an external key through a quantum network encrypted with keys obtained in QKD is considered, the 'plaintext' message refers to the external key — a random bit string. The random bit string no longer requires compression.

To summarize, encryption systems that are unbreakable even theoretically do exist. What is needed to implement such systems?

(1) A shared secret key — a random bit string of 0s and 1s — is needed for Alice and Bob.

(2) The key length — the number of bit positions of 0s and 1s — must be no fewer than the number of text positions in the form of 0s and 1s (the length of the plaintext message).

(3) The key is used only once; a new key is needed for each new message.

(4) Encryption occurs by bitwise addition, modulo 2, of the text positions with the key positions, resulting in ciphertext — a bit string of 0s and 1s.

Table 1

Plaintext word	Code combination of digits
Conact	7652
...	...
endspell	1653
...	...
pay	6781
...	...
spell	5411

Decryption is similarly performed by bitwise addition, modulo 2, of the ciphertext positions with the key positions on the receiving end. For educational purposes, it's interesting to display a photo of the first device that used *running keys* (Fig. 2).

Figure 3 shows a historical example of what a one-time pad looked like in the mid-20th century.

According to [22], two-stage encryption was used.

The first stage used a codebook-dictionary, where each word in the message was assigned a group of four digits independent of the one-time pad (see Table 1, codebook-dictionary).

For example:

(1) Let the plaintext be:

konheim delivered report about rockets.

(2) Some of the 'suspicious words' (rockets) in the plaintext are replaced by other 'unsuspicious words' (grades):

teacher delivered report about grades.

For example, Julius Rosenberg and his wife Ethel were designated by the codeword LIBERAL. The atomic bomb was designated by the codeword ENORMOZ.

(3) Words in the modified plaintext were replaced with a four-digit group from the codebook dictionary:

7394 2157 1139 3872 2216.

(4) The four-digit code groups are regrouped into five-digit groups:

73942 15711 39387 22216.

(5) Six previously unused five-digit groups from the one-time pad — the one-time encryption key — are used. The first five digits from the codebook determine the order and type of message:

16471 56328 29731 35682 23798 46659.

(6) The last five digits are used by the recipient to verify the number of digit groups.

(7) Message 5 is encrypted with the one-time pad — by adding the one-time key and the modified plaintext modulo 10 without carrying to the most significant digit:

		73942	15711	39387	22216	
+ mod 10	16471	56328	29731	35682	23798	46659
	16471	25660	34442	64969	45854	46659.

(8) A group of five digits is added to the end of the message: the first three digits represent the message number, and the last two represent the date:

16471 25660 34442 64969 45854 46659 21210.

(9) Finally, all digits in the message are converted to the letters

IETWI UREEO ZTTTU ETPEP TRART TEERP UIOIO

in accordance with Table 2.

Table 2

0	1	2	3	4	5	6	7	8	9
O	*I*	*U*	*Z*	*T*	*R*	*E*	*W*	*A*	*P*

The described one-time pad encryption ensures absolute secrecy even if the codebook dictionary becomes known to an intruder. Naturally, the one-time pad must be used only once.

In the digital age, a one-time key is a bit string.

We now proceed to quantum key distribution. The basic configuration in quantum cryptography for key distribution is a point-to-point configuration. In information networks, network nodes can be connected into various structures. Moreover, the structure of a quantum network — the connection of various nodes via quantum channels through which quantum key distribution occurs — may differ from that of a classical network. In other words, not every pair of network nodes may be directly connected by a quantum communication channel through which quantum key distribution occurs. A shared key can only be distributed between nodes directly connected by a quantum channel. Transmitting secure information requires a shared secret key between any pair of network nodes. To agree on keys between any pair of nodes, the network must be connected by a quantum channel to any pair of nodes via intermediate trusted nodes.

The intermediate trusted nodes contain transmitting and receiving equipment for quantum key distribution between a given node and the nodes connected to it via a quantum communication channel. Naturally, these intermediate trusted nodes also hold multiple keys, which arise from distributing keys among different network segments.

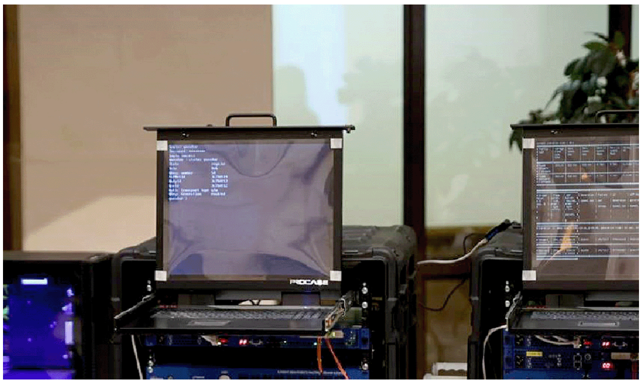


Figure 4. Quantum phone developed jointly by Infotecs, Russian IT company, and Center for Quantum Technologies at Moscow State University.

This raises the question of how to agree on keys — to obtain a shared secret key — between any pair of nodes not directly connected by a quantum communication channel. The issue of key agreement across different network segments was studied in [23].

An example of quantum network hardware, dubbed a 'quantum telephone,' is shown in Fig. 4 (see [4] for details).

1.1 Why are quantum cryptography systems — quantum seed key expansion systems — needed?

It may seem that the problem of completely secure communications has been solved. The only remaining step is a small one. A secret key must be propagated (or rather, distributed) for each message, or otherwise Alice and Bob must have a large supply of secret keys in advance for all subsequent messages, which must also be transmitted somehow and then stored to prevent an intruder from accessing them.

However, at this point, a vicious circle or, equivalently, the so-called 'chicken and egg' problem, arises — which came first? To transmit secret keys, a secure communication channel is required, which is itself implemented using secret keys, or a communication channel with couriers, the secrecy of which is based on the honesty and reliability of the couriers and technical organizational measures.

Until now, the carrier of the secret key has not been important, but it has been implicitly assumed that the carrier is a classical object — a courier, a classical signal, etc.

The question arises: what fundamentally new thing could emerge if the key carrier is a quantum object, for example, the quantum state of photons?

At this point, a transition to the quantum world occurs and it turns out that quantum mechanics breaks the vicious circle.

The original idea of using the laws of quantum mechanics to protect information was put forward by Stephen Wiesner. A year later [24], Charles H. Bennett and Gil Brassard proposed the first quantum cryptography protocol, which was named BB84 after the authors.

In what sense and in what way does the quantum nature of the microworld break this cycle?

To maintain the general logic of events, we present statements that are clarified and detailed below.

Statements.

(1) Quantum mechanics allows the secret distribution of keys through an open and modifiable quantum communica-

tion channel, accessible for eavesdropping, by transmitting quantum states that encode the bits of the future key. A standard optical fiber or atmospheric communication channel is used as a quantum communication channel, through which quantum states of light are transmitted — ideally, single-photon states or coherent radiation from a standard telecommunications laser, strongly attenuated to the quasi-single-photon level.

(2) Required in addition to the quantum communication channel is an authentic classical communication channel, which is open and accessible for eavesdropping. As shown below, the authenticity of the classical communication channel plays a fundamental role in ensuring the secrecy of the distributed keys.

Thus, quantum mechanics, using the transmission of quantum states through an open quantum communication channel and an additional open authentic classical communication channel, allows a shared secret key to be generated.

Essentially, quantum cryptography is a procedure for agreeing on two independent random sequences on the side of Alice and Bob. Agreement between independent sequences occurs through Alice sending quantum states in a certain basis, in accordance with her random sequence. On the receiving side, Bob selects measurements in his basis in accordance with his random sequence. An auxiliary authentic communication channel is used to agree on measurement bases, estimate error probabilities, correct errors, enhance secrecy, and transmit other auxiliary open classical messages (see details below).

Assuming that the shared key is somehow distributed and unknown to a third party, one-time pad encryption systems are *information-theoretically* secure, which implies that the security of the encryption is independent of the technical and computational capabilities of the eavesdropper.

There are asymmetric public-key cryptography systems [26] which do not have a pre-distributed shared secret. The shared key is obtained by the participants following a special protocol. Asymmetric cryptography systems are only *computationally secure*. Their security is based on the assumption that the technical and computational capabilities of the eavesdropper are limited. In fact, computational security is based on the belief that no one knows a fast (polynomial) classical algorithm for finding a key. However, it has not been proven that such a fast algorithm does not exist. Known algorithms require significant computational effort — the number of steps is exponentially large in the key length. For a quantum computer, such a polynomial algorithm is known: it is Shor's algorithm [25].

The fundamental difference between computational and information-theoretical security is that, with computational security, when running an algorithm (even if it is exponentially expensive in the number of computational steps), the probability of breaking the cipher is equal to one. In systems with information-theoretical security, such as a one-time pad, the probability of breaking the cipher is independent of technical and computational capabilities. For this reason, key distributions based solely on computationally secure methods (e.g., the Diffie–Hellman method [26]) are more vulnerable, since these methods are potentially unstable with respect to key discovery (breaking) during its distribution.

In the classical domain, the key distribution problem, unless computationally secure key distribution methods are used, is 'factored out,' implying that this problem is solved in each case by its own organizational and technical methods. Therefore, the secrecy of one-time keys is based on the 'security of organizational methods.' Either way, a new key is required for each message, or multiple keys for all subsequent messages, which must be stored and used as messages are generated.

A fundamental question arises: is it possible to implement one-time pad encryption using only one primary — seed — key? At first glance, even the very formulation of the question seems absurd.

In the classical domain, when the information carriers are classical signals, the answer to this question is negative.

In the quantum domain, the answer is positive. Quantum cryptography (or QKD) technology allows one, using only one pre-distributed seed key, to distribute secret keys that can be used for encryption in one-time pad mode for virtually any length of time. Moreover, the secrecy of the keys is guaranteed to be based on the fundamental laws of Nature, rather than on assumptions about the technical and computational capabilities of the eavesdropper. The fundamental difference from the classical case is that the secrecy of each key distributed in the classical case using organizational methods must be ensured. In the quantum case, it is sufficient to distribute only one short primary seed key using organizational methods. Subsequent keys are obtained through quantum distribution, and their secrecy is guaranteed by the fundamental laws of Nature — the keys are information-theoretically secure (precise definitions are given below).

To ensure information-theoretically secure authentication, a single, pre-distributed seed key is required. Subsequent keys are obtained through quantum distribution. Part of the new quantum key is used to secure the authentic communication channel in subsequent sessions, while the remainder can be used as a one-time key for encryption.

In this situation, the fundamental theorem on one-time keys [14, 16, 20] acquires a new meaning: for multiple one-time keys, distributing a single seed key is sufficient, unlike the classical case, where a key must be distributed for each message.

Authenticity of a classical channel implies ensuring the integrity (immutability) of transmitted public (accessible to everyone) classical messages. Authenticity is fundamentally important for achieving the secrecy of distributed quantum keys.

If the integrity of classical messages is compromised, an intruder can carry out a *Man-in-the-Middle* attack, which is undetectable by legitimate users (Fig. 5).

Since legitimate users only control their transmitting (Alice) and receiving (Bob) equipment and neither the quantum nor the classical communication channels, an intruder can disrupt both communication channels (see Fig. 5).

Alice will send quantum states and classical messages to the intruder. Likewise, the intruder will send their quantum states and classical messages to Bob. The intruder will not introduce errors on Bob's side. As a result, Alice and Bob will believe they are communicating with each other and share a key, although they share keys with the intruder.

Without an authentic classical communication channel, such an attack is undetectable; the intruder knows the key, or, more precisely, has the same keys as Alice and Bob, and the system does not provide the secrecy of the distributed keys. With an authentic classical communication channel, such an attack will be detected.

Since quantum cryptography, by design, must ensure unconditional security of distributed keys, based on the fundamental principles of quantum mechanics rather than on assumptions about the computational or technical capabilities of the eavesdropper, the authentication of a classical communication channel must also be information-theoretically secure.

In cryptography, classical key expansion methods are known that also require a seed key. Key expansion, promotion, and re-encryption also occur in classical information networks without quantum cryptography technology, using a primary master key and classical cryptographic methods.

A natural question is: why does one need to use quantum cryptography if classical methods exist? Below, we show that, using the fundamental laws of nature — quantum mechanics — it is possible to derive fundamental constraints on the relationship between the secrecy of quantum keys and the number of valid QKD sessions. Moreover, these fundamental constraints are independent of the technical or computational capabilities of the eavesdropper and do not depend on the presence of a quantum computer.

In quantum cryptography, it is possible to derive explicit limits on the number of one-time keys in the form of analytical formulas based solely on the fundamental laws of nature.

2. Quality of distributed keys

Informally speaking, when using one-time pad encryption, an intruder 'sees' each encrypted message in the channel as a random bit string that is statistically independent of the message [16, 20]. If a one-time key is a perfectly random bit string, where each position is equally probable and independent of the others an intruder has no choice in this situation but to guess the key. With perfect keys, the probability of guessing the true key is $1/2^n$, where n is the key/message length.

Proofs of secrecy in quantum key distribution are quite complex. Secrecy is defined in terms that differ from the requirements placed on keys in classical cryptography.

In quantum cryptography, key secrecy is formulated in terms of the distinguishability of quantum states — the density matrices ρ^{Real} and ρ^{Ideal}, corresponding to the *real* and *ideal* situations under quantum key distribution. The proximity metric of two quantum states is the trace metric.

In classical cryptography, key secrecy is understood in terms of, for example, the difficulty of a brute-force key search in the presence of side information. In quantum cryptography, the eavesdropper's side information is the entire set of key information obtained from both quantum and classical channels.

The fact that the mathematical apparatus for proving key secrecy in classical and quantum cryptography differs significantly leads to misunderstandings and heated debates [27, 28].

We now consider quantum states corresponding to various situations.

The ideal situation is one in which there is no intrusion into the quantum and classical communication channels.

In a real situation, both quantum and classical communication channels are attacked.

In quantum cryptography, keys are called ε-secret if the following relation holds:

$$D(\rho^{\text{Real}}, \rho^{\text{Ideal}}) = ||\rho^{\text{Real}} - \rho^{\text{Ideal}}||_1 \leqslant \varepsilon\,, \tag{1}$$

$$||\rho^{\text{Real}} - \rho^{\text{Ideal}}||_1 = \text{Tr}\left\{|\rho^{\text{Real}} - \rho^{\text{Ideal}}|\right\}$$

$$= \text{Tr}\left\{\sqrt{(\rho^{\text{Real}} - \rho^{\text{Ideal}})^{+}(\rho^{\text{Real}} - \rho^{\text{Ideal}})}\right\},$$

where $(...)^{+}$ is the Hermitian conjugation symbol.

Mathematically, key secrecy is formulated in terms of the distinguishability of quantum states [29]. A pair of quantum states is considered ε-indistinguishable if *no measurement* can distinguish one quantum state from the other with a success probability greater than the probability of simple guessing by more than ε.

Requirements for secret keys used in various encryption algorithms are formulated in entirely different terms. Shannon [20] introduced a criterion for the practical secrecy of a cryptosystem, which is understood as "The average amount of work to determine the key for a cryptogram... ." This criterion was not formalized, so different criteria for the average work (labor intensity) of key determination are possible depending on the situation. The very concept of labor intensity is essentially related to the enumeration (trial) of keys until the true key is determined. Moreover, the direct search can be either complete — over the entire key space — or partial — over a portion of the key space. Such a direct search can occur both in the absence and in the presence of side information about the key.

With regard to keys obtained through quantum key distribution, the eavesdropper acquires side information about the key during measurements on a quantum system correlated with the true key of legitimate users.

One should clearly understand how the seemingly completely different secrecy criteria in the quantum domain and classical cryptography are related. Without clarifying the precise relationship between the various criteria, it remains unclear how securely the keys obtained through quantum key distribution can be used for various cryptosystems.

Previously, studies [30–33] established a direct connection between a secrecy criterion based on the distinguishability of a pair of quantum states and various criteria using the concept of complexity — the difficulty of searching an exponentially large (by key length) space in classical cryptography.

In practical cryptography, an important characteristic is the average complexity Q of a partial key search for a given probability of success (finding the key) π not less than π_0 [30–33]. A brute-force search is carried out over a set of the most probable keys of strength M, for which $\pi(M) > \pi_0$.

The complexity Q — the average number of keys tried before finding the true key — is related to the ε-secrecy of the keys. The lower bound for the complexity of a partial search is the inequality

$$Q(\varepsilon, \pi_0) > \left(1 - \frac{\varepsilon}{\pi_0}\right)\left(\frac{N(1 - 4\varepsilon) + 1}{2}\right), \tag{2}$$

where $N = 2^n$ is the size of the key space.

Thus, the quality of the keys (their proximity to ideal in terms of trace distance) is directly related to the complexity of breaking the cipher — finding the true encryption key.

Suppose we manage to determine the value of ε for the first run of the system using the seed starting key for authentication. Furthermore, if we determine how the value of ε changes in subsequent sessions, this will answer the question: how many quantum key distribution sessions can be allowed before the next system restart, while the quality of the distributed keys has not yet reached a critical level at which their use becomes unacceptable?

3. Why is authentic classical communication channel needed in quantum key distribution?

Authenticity of a classical channel implies ensuring the integrity (immutability) of broadcast public (accessible to everyone) classical messages. Authenticity is fundamentally important for achieving the secrecy of distributed quantum keys. If the integrity of classical messages is compromised, a perpetrator can carry out a *Man-in-the-Middle* attack, which is undetectable by legitimate users (see Fig. 5) [34–37].

Since legitimate users only control their transmitting (Alice) and receiving (Bob) equipment and neither the quantum nor the classical communication channels, an intruder (Eve) can disrupt both communication channels (see Fig. 5).

Alice will send quantum states and classical messages to the intruder. Likewise, the intruder will send their quantum states and classical messages to Bob. The intruder will not introduce errors on Bob's side. As a result, Alice and Bob will believe they are communicating with each other and share a key, although they share keys with the intruder.

Without an authentic classical communication channel, such an attack is undetectable; the intruder knows the key, or more precisely, has the same keys as Alice and Bob, and the system does not ensure the secrecy of the distributed keys. With an authentic classical communication channel, such an attack will be detected.

Since quantum cryptography, by design, must ensure unconditional security of distributed keys, based on the fundamental laws of quantum mechanics rather than on assumptions about the computational or technical capabilities of the eavesdropper, authentication of a classical communication channel must also be information-theoretically secure.

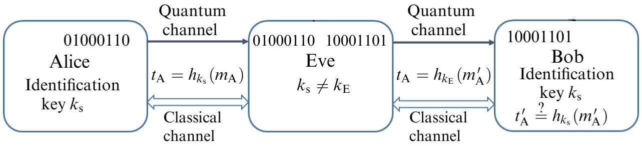


Figure 5. Illustration of *Man-in-the-Middle* attack. Intruder cracks quantum and classical communication channels and generates separate Alice–Eve and Eve–Bob keys. This attack is undetectable if classical channel does not ensure authenticity — *immutability* of plaintext classical messages. Alice and Bob share a secret authentication key k_s. Alice sends plaintext messages m and their 'digest' — hash values $t_A = h_{k_s}(m_A)$. Eve, not knowing secret key k_s, intends to substitute Alice's messages with her own pair $t'_A = h_{k_E}(m'_A)$. Eve calculates hash value t'_A of substitute m'_A using her key k_E, which, generally speaking, does not match true key k_s. Bob verifies authenticity of message and tag using key k_s. If $t'_A \neq h_{k_s}(m'_A)$, QKD session is terminated. If Eve guesses the key, authentication is accepted. Probability of such an event in information-theoretical authentication does not depend on Eve's technical or computational capabilities, but is determined solely by structure of hash functions.

The fundamental study by Wegman and Carter [38] has shown that information-theoretically secure authentication can be achieved using a class of special hash functions [39–52].

Authentication secure in information-theoretical terms ensures the detection of intrusions into a classical communication channel regardless of the technical capabilities of the eavesdropper (for example, even if the eavesdropper has a full-scale quantum computer).

Authentication secure in information-theoretical terms requires a shared secret key between Alice and Bob, so a common seed key must be provided to Alice and Bob when the system is first launched.

It follows from the above that quantum cryptography systems are essentially systems for expanding the initial seed key.

In cryptography, classical key expansion methods are available, which also require a seed key. Key expansion, propagation, and re-encryption also occur in classical information networks without quantum cryptography technology, using a primary master key and classical cryptographic methods.

A natural question is: why use quantum cryptography if classical methods exist?

The fundamental difference is that, unlike quantum cryptography, the security of classical key expansion methods is based on assumptions regarding the technical or computational capabilities of the eavesdropper. For this reason, in the classical case, it is not possible to set fundamental limits on the admissible number of key expansion sessions and their quality. In quantum cryptography, explicit limits can be derived in the form of analytical formulas based solely on the fundamental laws of nature.

4. Concept of abstract cryptography: distinguishability among quantum states

As discussed in Section 1.1, after quantum key distribution, part of the key can be used for authentication in a subsequent session, and part for encryption with a one-time pad.

This raises a fundamental question: what will the quality of the keys be in each of the subsequent processes if the quality of the input key is known? In our case, such an input key is the seed authentication key when the system is first launched.

The answer to this question is given in an approach called *abstract cryptography*.

The concept of abstract cryptography for the classical case was formulated in [53, 54] and, in the quantum field, this idea was developed in some studies [55, 56] (for a review of recent studies, see [55]).

Essentially, the concept of abstract cryptography boils down to calculating the distance in a certain metric between different situations. Each situation corresponds to a specific quantum state. A measure of the closeness of different situations — quantum states — is the trace distance [57].

A real situation is a real quantum key distribution session with a perpetrator's intrusion into the quantum communication channel and real authentication, during which message substitution is possible in a classical communication channel.

An ideal situation is an ideal quantum key distribution session without intrusion into the quantum communication channel and ideal authentication without message substitution in a classical communication channel.

Each situation corresponds to a quantum state — the density matrix of all three participants in the Alice–Bob–Eve protocol; ρ^{Real} corresponds to the real situation, ρ^{Ideal} corresponds to the ideal situation.

How can we determine which situation is taking place?

To do so, a third party (*distinguisher*) is introduced, which has access to all subsystems of the composite quantum state Alice–Bob–Eve. Recall that Alice, Bob, and Eve have access only to their own quantum subsystem. A distinguisher has conceptual access (for this reason, this approach is called abstract cryptography) to the quantum states corresponding to the real and ideal situations. The distinguisher's task is to distinguish between two situations using quantum mechanical measurements.

It turns out that, for optimal measurements — optimal in the sense of minimizing the error in distinguishing between two quantum states — the maximum probability $\Pr_{OK}$ of correctly distinguishing between two quantum states ρ^{Real} and ρ^{Ideal} is equal to

$$\Pr{}_{OK} = \frac{1}{2}\left(1 + \frac{1}{2}\,||\rho^{\text{Real}} - \rho^{\text{Ideal}}||_1\right) = \frac{1}{2}(1+\varepsilon)\,,$$

where $\frac{1}{2}||\rho^{\text{Real}} - \rho^{\text{Ideal}}||_1 \leqslant \varepsilon$. By definition, $||\rho||_1 = \operatorname{Tr}\{\sqrt{\rho^+\rho}\}$. In this case, the real and ideal situations are called ε-indistinguishable. Similarly, the keys obtained in the two situations are ε-secret.

5. Secrecy of cryptographic compositions — composable security

An abstract secrecy criterion based on a trace metric features an important and convenient property. It turns out that the secrecy criterion can be decomposed into secrecy criteria between individual elementary processes. For individual processes, the trace distance can be calculated. Then, the trace distance between the composite real and ideal processes is bounded by the sum of the trace distances between the individual processes.

In this case, the ε values from (non-ideal) sequential processes are summed. The secrecy of several processes is called composable security.

The further logic of actions is as follows. Assume that a current quantum key distribution session is underway, consisting of the following stages:

(1) transmission and measurement of quantum states;

(2) post-processing: agreement on bases, error probability estimation, error correction, and enhancement of the secrecy of cleared keys.

All post-processing procedures occur without authentication. If the session is successful, i.e., the trace distance between the real and ideal situations for the current session is less than ε, at the end of the session, the authenticity of all accumulated classical messages is verified during post-processing.

If the session is unsuccessful, i.e., the required level of key secrecy in terms of trace distance is not achieved, the current session is discarded, and a new one is conducted.

A successful session is authenticated; it is considered successful if no message substitution is detected. If message substitution is detected during authentication, the session is discarded.

For further discussion, we need quantum states that describe individual real and ideal situations. During authentication, the hash functions for the current session are chosen by selecting a portion of a non-ideal key obtained in the previous session and featuring the ε-secrecy property.

Since authentication occurs after the quantum key distribution session, due to a *Man-in-the-Middle* attack, Alice and Bob can 'see' different quantum states — density matrices — and, therefore, different keys. Until message authentication over the open communication channel is completed, an eavesdropper can break the quantum and classical communication channels and conduct separate QKD sessions with Alice and Bob. After all QKD procedures, but before authentication, Alice and Bob will have different density matrices and, therefore, different keys.

Suppose Alice and Bob have a set of, generally speaking, different classical messages after a QKD attack due to an eavesdropper attack: Alice has (m), and Bob has (m'). The eavesdropper has the same set of classical messages.

Then, Alice and Bob conduct an authentication session, which consists of Alice sending to Bob the pair $(t = h_{k_s}(m), m)$, where $h_{k_s}(m)$ is the keyed hash function and k_s is the authentication key.

The eavesdropper has access to the channel and can substitute Alice's messages $(t, m) \to (t', m')$ when forwarding them to Bob. However, the eavesdropper does not have the secret key k_s for authentication, which Alice and Bob have. Having m' and k_s, Bob verifies the equality $t' = h_{k_s}(m')$. If $t' \neq h_{k_s}(m')$ is found to be true, the authentication fails, and the session is discarded.

If authentication is successful, the session is accepted.

A similar authentication process occurs when sending classical messages from Bob to Alice. The set of messages in two-way classical message exchanges depends on the type of QKD protocol used.

For further discussion, we need quantum states describing specific *real* and *ideal* situations.

We introduce the following notation:

$\rho_{\text{ABE}}^{R_\text{A} R_\text{B} R_\text{Q}}$ is the density matrix after real quantum key distribution R_Q with an intruder in a quantum communication channel, real Alice–Bob message authentication R_A, and real Bob–Alice message authentication R_B with possible message substitution in an authentic classical communication channel;

$\rho_{\text{ABE}}^{R_\text{A} R_\text{B} I_\text{Q}}$ is the density matrix after ideal quantum key distribution I_Q without an intruder in a quantum communication channel, with real Alice–Bob message authentication R_A and real Bob–Alice message authentication R_B with possible message substitution in an authentic classical communication channel;

$\rho_{\text{ABE}}^{R_\text{A} I_\text{B} I_\text{Q}}$ is the density matrix after ideal quantum key distribution I_Q without an intruder in a quantum communication channel, with real Alice–Bob message authentication R_A with possible message substitution in an authentic classical communication channel and ideal Bob–Alice authentication I_B without message substitution in an authentic classical communication channel;

$\rho_{\text{ABE}}^{I_\text{A} I_\text{B} I_\text{Q}}$ is the density matrix after ideal quantum key distribution I_Q without an intruder in a quantum communication channel, with perfect authentication of Alice–Bob messages I_A and perfect authentication of Bob–Alice I_B without message substitution in an authentic classical communication channel.

Next, we are interested in the distance between two situations in each QKD session: the real situation with intrusion into the quantum and classical communication channels $\rho_{\text{ABE}}^{R_\text{A} R_\text{B} R_\text{Q}}$ and the ideal situation without intrusion into the quantum and classical communication channels $\rho_{\text{ABE}}^{I_\text{A} I_\text{B} I_\text{Q}}$. Let the distance between $\rho_{\text{ABE}}^{R_\text{A} R_\text{B} R_\text{Q}}$ and $\rho_{\text{ABE}}^{I_\text{A} I_\text{B} I_\text{Q}}$ be ε.

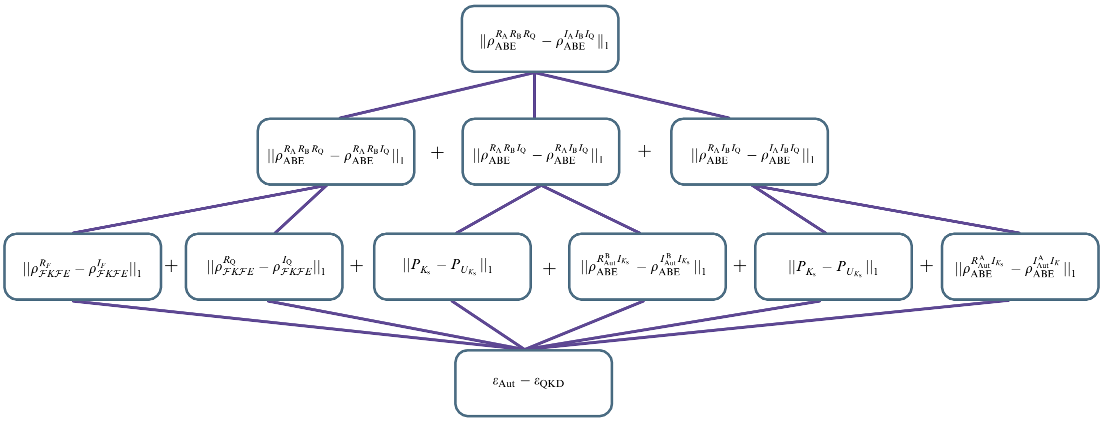

$\|\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}R_{\rm Q}} - \rho_{\rm ABE}^{I_{\rm A}I_{\rm B}I_{\rm Q}}\|_1$
$\|\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}R_{\rm Q}} - \rho_{\rm ABE}^{R_{\rm A}R_{\rm B}I_{\rm Q}}\|_1$
+
$\|\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}I_{\rm Q}} - \rho_{\rm ABE}^{R_{\rm A}I_{\rm B}I_{\rm Q}}\|_1$
+
$\|\rho_{\rm ABE}^{R_{\rm A}I_{\rm B}I_{\rm Q}} - \rho_{\rm ABE}^{I_{\rm A}I_{\rm B}I_{\rm Q}}\|_1$
$\|\rho_{\mathcal{F}K\mathcal{F}E}^{R_F} - \rho_{\mathcal{F}K\mathcal{F}E}^{I_F}\|_1$
+
$\|\rho_{\mathcal{F}K\mathcal{F}E}^{R_{\rm Q}} - \rho_{\mathcal{F}K\mathcal{F}E}^{I_{\rm Q}}\|_1$
+
$\|P_{K_{\rm s}} - P_{U_{K_{\rm s}}}\|_1$
+
$\|\rho_{\rm ABE}^{R^{\rm B}_{\rm Aut}I_{K_{\rm s}}} - \rho_{\rm ABE}^{I^{\rm B}_{\rm Aut}I_{K_{\rm s}}}\|_1$
+
$\|P_{K_{\rm s}} - P_{U_{K_{\rm s}}}\|_1$
+
$\|\rho_{\rm ABE}^{R^{\rm A}_{\rm Aut}I_{K_{\rm s}}} - \rho_{\rm ABE}^{I^{\rm A}_{\rm Aut}I_K}\|_1$
$\varepsilon_{\rm Aut} - \varepsilon_{\rm QKD}$

Figure 6. Diagram illustrating decomposition of real QKD process with information-theoretical authentication into elementary processes.

Then, the keys obtained in the real situation corresponding to the quantum state $\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}R_{\rm Q}}$ will be ε-secret. This implies that the use of real keys and the ideal keys obtained in the situation with the quantum state $\rho_{\rm ABE}^{I_{\rm A}I_{\rm B}I_{\rm Q}}$ cannot be distinguished with a probability better than ε.

Consequently, if these keys are used for encryption, the complexity of finding the keys — cracking the cipher — is determined by ε.

Our goal is to determine how the secrecy parameter depends on the QKD session number and on the quality of the seed authentication key — the closeness of the seed key to the ideal key, i.e., an equidistant one. This determines the number of sessions that can be conducted without losing the cryptographic quality of the keys employed for encryption in one-time pad mode.

For the distance between different situations (quantum states), we have:

$$\|\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}R_{\rm Q}} - \rho_{\rm ABE}^{I_{\rm A}I_{\rm B}I_{\rm Q}}\|_1 \tag{3}$$

$$\leqslant \|\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}R_{\rm Q}} - \rho_{\rm ABE}^{R_{\rm A}R_{\rm B}I_{\rm Q}}\|_1 \tag{4}$$

$$+ \|\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}I_{\rm Q}} - \rho_{\rm ABE}^{R_{\rm A}I_{\rm B}I_{\rm Q}}\|_1 \tag{5}$$

$$+ \|\rho_{\rm ABE}^{R_{\rm A}I_{\rm B}I_{\rm Q}} - \rho_{\rm ABE}^{I_{\rm A}I_{\rm B}I_{\rm Q}}\|_1\,. \tag{6}$$

In Eqns (3)–(6), the triangle inequality for trace distance [57] is used.

Trace distance (3) is majorized by the sum of the distances between individual elementary processes. It is not possible to directly calculate the distance between a complex real process and an ideal process (complex quantum states). In the paradigm of abstract cryptography, the distance between complex processes is decomposed into the sum of the distances between elementary processes (quantum states), which can be calculated explicitly.

The distance between quantum states $\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}R_{\rm Q}}$ and $\rho_{\rm ABE}^{I_{\rm A}I_{\rm B}I_{\rm Q}}$ is represented by the sum of simple states. For convenience, the decomposition of a complex process into elementary ones is shown in Fig. 6.

In subsequent sections, distances for individual processes are calculated.

5.1 Specific representations of density matrices for various processes

In this section, we calculate the trace distance. This requires density matrices for quantum states corresponding to the various situations described in the previous section.

The density matrix for process $R_{\rm A}R_{\rm B}R_{\rm Q}$ has the form

$$\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}R_{\rm Q}} = \sum_{k_{\rm A}}\sum_{k_{\rm B}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})|k_{\rm A}\rangle_{K_{\rm A}\,K_{\rm A}}\langle k_{\rm A}|$$
$$\otimes |k_{\rm B}\rangle_{K_{\rm B}\,K_{\rm B}}\langle k_{\rm B}| \otimes g^{R_{\rm A}m_{k_{\rm A}}} \otimes g^{R_{\rm B}m_{k_{\rm B}}} \otimes \rho_{\rm E}^{k_{\rm A}k_{\rm B}}\,. \tag{7}$$

The notation needs some clarification.

After QKD with possible intrusion into the quantum communication channel and authentication via a classical channel with possible substitution of classical messages and a *Man-in-the-Middle* attack, Alice and Bob have final keys $k_{\rm A}$ and $k_{\rm B}$, $P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})$ being the joint key distribution. Alice's and Bob's keys match with a probability close to one (see details below).

It is convenient to associate each key — a bit string of length ℓ — with an orthogonal quantum state:

$$k_{\rm A} = (k_{i_1{\rm A}}, k_{i_2{\rm A}}, \ldots, k_{i_\ell{\rm A}})$$
$$\to |k_{\rm A}\rangle = |k_{i_1{\rm A}}\rangle \otimes |k_{i_2{\rm A}}\rangle \otimes \ldots \otimes |k_{i_\ell{\rm A}}\rangle\,, \quad k_{i_j{\rm A}} = 0, 1\,,$$
$$k_{\rm B} = (k_{i_1{\rm B}}, k_{i_2{\rm B}}, \ldots, k_{i_\ell{\rm B}})$$
$$\to |k_{\rm B}\rangle = |k_{i_1{\rm B}}\rangle \otimes |k_{i_2{\rm B}}\rangle \otimes \ldots \otimes |k_{i_\ell{\rm B}}\rangle\,, \quad k_{i_j{\rm B}} = 0, 1\,.$$

In the general case, Eve, due to a possible *Man-in-the-Middle* attack on quantum and classical communication channels, has a quantum state $\rho_{\rm E}^{k_{\rm A}k_{\rm B}}$ at their disposal, 'linked' to each pair of keys $k_{\rm A}$ and $k_{\rm B}$, i.e., correlated with the keys.

It is also convenient to associate the set of classical messages (bit string) from Alice to Bob with possible substitution of genuine messages with orthogonal (by keys $k_{\rm A}$) quantum states $g^{R_{\rm A}m_{k_{\rm A}}}$, which are 'linked' to the keys after a QKD session, in the sense that the set of classical messages after a QKD session depends on the QKD session.

We associate the set of classical messages (bit string) from Bob to Alice with orthogonal quantum states $g^{R_{\rm B}m_{k_{\rm B}}}$.

A more detailed view of $\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}R_{\rm Q}}$ is presented below.

The density matrix for process $R_{\rm A}R_{\rm B}I_{\rm Q}$ has the form

$$\rho_{\rm ABE}^{R_{\rm A}R_{\rm B}I_{\rm Q}} = \sum_{k_{\rm A}}\sum_{k_{\rm B}} \frac{1}{|K_{\rm A}|}\,\delta_{k_{\rm A},k_{\rm B}}|k_{\rm A}\rangle_{K_{\rm A}\,K_{\rm A}}\langle k_{\rm A}| \otimes |k_{\rm B}\rangle_{K_{\rm B}\,K_{\rm B}}\langle k_{\rm B}|$$
$$\otimes g^{R_{\rm A}m_{k_{\rm A}}} \otimes g^{R_{\rm B}m_{k_{\rm B}}} \otimes \rho_{\rm E}\,, \tag{8}$$

$$\rho_{\rm E} = \sum_{k'_{\rm A}}\sum_{k'_{\rm B}} P_{K_{\rm A}K_{\rm B}}(k'_{\rm A},k'_{\rm B})\,\rho_{\rm E}^{k'_{\rm A}k'_{\rm B}}\,.$$

The difference between (7) and (8) is that the QKD process is ideal, which corresponds to index I_{Q}. Furthermore, Alice's and Bob's keys are strictly identical ($\delta_{k_{\mathrm{A}},k_{\mathrm{B}}}$ is the Kronecker symbol), i.e., they are identical with probability one and equally probable. Eve's quantum state ρ_{E} is 'untethered' from the keys, i.e., it is uncorrelated with the keys. The transmission of classical messages from Alice to Bob and from Bob to Alice occurs through a real classical communication channel with possible substitution of classical messages; $g^{R_{\mathrm{A}}m_{k_{\mathrm{A}}}}$, $g^{R_{\mathrm{B}}m_{k_{\mathrm{B}}}}$ are the corresponding quantum states.

The density matrix for process $R_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}$ has the form

$$\rho^{R_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}} = \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} \frac{1}{|K_{\mathrm{A}}|}\,\delta_{k_{\mathrm{A}},k_{\mathrm{B}}}\,|k_{\mathrm{A}}\rangle_{K_{\mathrm{A}}\,K_{\mathrm{A}}}\langle k_{\mathrm{A}}| \otimes |k_{\mathrm{B}}\rangle_{K_{\mathrm{B}}\,K_{\mathrm{B}}}\langle k_{\mathrm{B}}| \otimes g^{R_{\mathrm{A}}m_{k_{\mathrm{A}}}} \otimes g^{I_{\mathrm{B}}m_{k_{\mathrm{B}}}} \otimes \rho_{\mathrm{E}}\,. \tag{9}$$

In this QKD process, QKD occurs through an ideal quantum communication channel, similar to the previous process in (8).

The transmission of classical messages from Bob to Alice also occurs through an ideal authentic communication channel; $g^{I_{\mathrm{B}}m_{k_{\mathrm{B}}}}$ is the corresponding quantum state.

The transmission of classical messages from Alice to Bob occurs through a real communication channel with possible message substitution; $g^{R_{\mathrm{A}}m_{k_{\mathrm{A}}}}$ is the corresponding quantum state.

The density matrix for process $I_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}$ has the form

$$\rho^{I_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}} = \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} \frac{1}{|K_{\mathrm{A}}|}\,\delta_{k_{\mathrm{A}},k_{\mathrm{B}}}\,|k_{\mathrm{A}}\rangle_{K_{\mathrm{A}}\,K_{\mathrm{A}}}\langle k_{\mathrm{A}}| \otimes |k_{\mathrm{B}}\rangle_{K_{\mathrm{B}}\,K_{\mathrm{B}}}\langle k_{\mathrm{B}}| \otimes g^{I_{\mathrm{A}}m_{k_{\mathrm{A}}}} \otimes g^{I_{\mathrm{B}}m_{k_{\mathrm{B}}}} \otimes \rho_{\mathrm{E}}\,. \tag{10}$$

This quantum state corresponds to a situation where QKD passed through an ideal quantum communication channel without intrusion. The classical communication channel is also ideal; all classical messages from Alice to Bob and vice versa pass without substitution.

6. Trace distance between real and ideal quantum key distribution

We now calculate the trace distances for individual elementary processes. Since

$$\begin{aligned}
\rho^{R_{\mathrm{A}}R_{\mathrm{B}}R_{\mathrm{Q}}}_{\mathrm{ABE}} - \rho^{R_{\mathrm{A}}R_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}} &= \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} P_{K_{\mathrm{A}}K_{\mathrm{B}}}(k_{\mathrm{A}},k_{\mathrm{B}})|k_{\mathrm{A}}\rangle_{K_{\mathrm{A}}\,K_{\mathrm{A}}}\langle k_{\mathrm{A}}| \\
&\otimes |k_{\mathrm{B}}\rangle_{K_{\mathrm{B}}\,K_{\mathrm{B}}}\langle k_{\mathrm{B}}| \otimes g^{R_{\mathrm{A}}m_{k_{\mathrm{A}}}} \otimes g^{R_{\mathrm{B}}m_{k_{\mathrm{B}}}} \otimes \rho^{k_{\mathrm{A}}k_{\mathrm{B}}}_{\mathrm{E}} \\
&- \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} \frac{1}{|K_{\mathrm{A}}|}\,\delta_{k_{\mathrm{A}},k_{\mathrm{B}}}|k_{\mathrm{A}}\rangle_{K_{\mathrm{A}}\,K_{\mathrm{A}}}\langle k_{\mathrm{A}}| \otimes |k_{\mathrm{B}}\rangle_{K_{\mathrm{B}}\,K_{\mathrm{B}}}\langle k_{\mathrm{B}}| \\
&\otimes g^{R_{\mathrm{A}}m_{k_{\mathrm{A}}}} \otimes g^{R_{\mathrm{B}}m_{k_{\mathrm{B}}}} \otimes \rho_{\mathrm{E}} \\
&= \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} \big(|k_{\mathrm{A}}\rangle_{K_{\mathrm{A}}\,K_{\mathrm{A}}}\langle k_{\mathrm{A}}|\big) \otimes \big(|k_{\mathrm{B}}\rangle_{K_{\mathrm{B}}\,K_{\mathrm{B}}}\langle k_{\mathrm{B}}|\big) \\
&\otimes g^{R_{\mathrm{A}}m_{k_{\mathrm{A}}}} \otimes g^{R_{\mathrm{B}}m_{k_{\mathrm{B}}}} \\
&\otimes \left(P_{K_{\mathrm{A}}K_{\mathrm{B}}}(k_{\mathrm{A}},k_{\mathrm{B}}) \otimes \rho^{k_{\mathrm{A}}k_{\mathrm{B}}}_{\mathrm{E}} - \frac{1}{|K_{\mathrm{A}}|}\,\delta_{k_{\mathrm{A}},k_{\mathrm{B}}}\,\rho_{\mathrm{E}}\right),
\end{aligned}$$

and the quantum states $g^{R_{\mathrm{A}}m_{k_{\mathrm{A}}}}$, $g^{R_{\mathrm{B}}m_{k_{\mathrm{B}}}}$ for a fixed pair $(k_{\mathrm{A}},k_{\mathrm{B}})$ are reliably distinguishable (commutativity–orthogonality), a direct calculation shows that

$$\begin{aligned}
&||\rho^{R_{\mathrm{A}}R_{\mathrm{B}}R_{\mathrm{Q}}}_{\mathrm{ABE}} - \rho^{R_{\mathrm{A}}R_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}}||_1 \\
&\quad = \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} \mathrm{Tr}\left\{\left|P_{K_{\mathrm{A}}K_{\mathrm{B}}}(k_{\mathrm{A}},k_{\mathrm{B}})\rho^{k_{\mathrm{A}}k_{\mathrm{B}}}_{\mathrm{E}} - \delta_{k_{\mathrm{A}},k_{\mathrm{B}}}\,\frac{1}{|K_{\mathrm{A}}|}\,\rho_{\mathrm{E}}\right|\right\} \\
&\quad = ||\rho^{R_{\mathrm{Q}}}_{\mathrm{ABE}} - \rho^{I_{\mathrm{Q}}}_{\mathrm{ABE}}||_1\,.
\end{aligned} \tag{11}$$

Here,

$$\begin{aligned}
\rho^{R_{\mathrm{Q}}}_{\mathrm{ABE}} &= \mathop{\mathrm{Tr}}_{R_{\mathrm{A}}R_{\mathrm{B}}}\big(\rho^{R_{\mathrm{A}}R_{\mathrm{B}}R_{\mathrm{Q}}}_{\mathrm{ABE}}\big) = \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} P_{K_{\mathrm{A}}K_{\mathrm{B}}}(k_{\mathrm{A}},k_{\mathrm{B}}) \\
&\times \big(|k_{\mathrm{A}}\rangle_{K_{\mathrm{A}}\,K_{\mathrm{A}}}\langle k_{\mathrm{A}}|\big) \otimes \big(|k_{\mathrm{B}}\rangle_{K_{\mathrm{B}}\,K_{\mathrm{B}}}\langle k_{\mathrm{B}}|\big) \otimes \rho^{k_{\mathrm{A}}k_{\mathrm{B}}}_{\mathrm{E}}\,, \\
\rho^{I_{\mathrm{Q}}}_{\mathrm{ABE}} &= \mathop{\mathrm{Tr}}_{R_{\mathrm{A}}R_{\mathrm{B}}}\big(\rho^{R_{\mathrm{A}}R_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}}\big) \\
&= \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} \frac{1}{|K_{\mathrm{A}}|}\,\delta_{k_{\mathrm{A}},k_{\mathrm{B}}}\big(|k_{\mathrm{A}}\rangle_{K_{\mathrm{A}}\,K_{\mathrm{A}}}\langle k_{\mathrm{A}}|\big)\otimes\big(|k_{\mathrm{B}}\rangle_{K_{\mathrm{B}}\,K_{\mathrm{B}}}\langle k_{\mathrm{B}}|\big) \otimes \rho_{\mathrm{E}}\,.
\end{aligned}$$

The resulting equality is also a consequence of the density matrix having a quantum-classical structure. This implies that classical messages after a QKD session with a *Man-in-the-Middle* attack belong to different sessions of the 'regular' QKD and are therefore distinguishable.

In the language of quantum states, the resulting equality can be said to be a consequence of the reliable distinguishability (commutativity–orthogonality) of the density matrices $g^{R_{\mathrm{A}}m_{k_{\mathrm{A}}}}$, $g^{R_{\mathrm{B}}m_{k_{\mathrm{B}}}}$ for pairs $(k_{\mathrm{A}},k_{\mathrm{B}})$ from different QKD sessions.

The density matrix $\rho^{R_{\mathrm{Q}}}_{\mathrm{ABE}}$ is the final one after QKD, which is obtained from the original density matrix after error correction and security enhancement. Crucially, the final keys $(k_{\mathrm{A}},k_{\mathrm{B}})$ may differ with a given, arbitrarily small probability determined by the error correction procedure.

The QKD process consists of several stages.

After the transmission and registration of quantum states, an error correction stage occurs. A quantum state corresponding to the so-called sifted key is created.

Then, the errors in the sifted key are corrected, resulting in a clean key. The length of the clean key is the same as that of the sifted key. This situation also has its own density matrix.

Next, the identity of the clean key is verified. Alice's and Bob's clean keys match with a certain probability, which is determined by the verification procedure.

This results in a clean key that is identical (with a given probability) for Alice and Bob. Eve has partial information about the clean key, which she obtained by attacking the quantum communication channel, and classical information from the plaintext messages transmitted by Alice to Bob and by Bob to Alice during error correction.

The final stage is to enhance the clean key secrecy. This procedure results in compression of the clean key. Compression is implemented using universal second-order hash functions [38] over an open classical communication channel. This information is available to Eve. To select the hash function $f \in \mathcal{F}$, which is itself a random variable, Alice chooses a random bit string. This results in the final density matrix $\rho^{R_{\mathrm{Q}}}_{\mathrm{ABE}}$, which appears in Eqn (11).

In reality, the hash function is selected according to a distribution $\varepsilon_{\mathcal{F}}$ that is close to equiprobable. This circumstance is taken into account in Section 7.

6.1 Correctness of key distribution

Thus, the trace distance between processes is decomposed into the sum of the trace distances between the individual constituent processes in (11).

With some probability, Alice's and Bob's keys differ from each other, which is formalized by the form of the density matrix

$$\rho_{\rm ABE}^{R_{\rm Q}} = \sum_{k_{\rm A}\in\{0,1\}^{\ell}}\ \sum_{k_{\rm B}\in\{0,1\}^{\ell}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})|k_{\rm A}\rangle_{\rm A\,A}\langle k_{\rm A}| \otimes |k_{\rm B}\rangle_{\rm B\,B}\langle k_{\rm B}| \otimes \rho_{\rm E}^{k_{\rm A}k_{\rm B}}\,. \tag{12}$$

We introduce a density matrix of the following form:

$$\overline{\rho_{\rm ABE}^{R_{\rm Q}}} = \sum_{k_{\rm A}\in\{0,1\}^{\ell}}\ \sum_{k_{\rm B}\in\{0,1\}^{\ell}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})\big(|k_{\rm A}\rangle_{\rm A\,A}\langle k_{\rm A}|\big) \otimes \big(|k_{\rm A}\rangle_{\rm B\,B}\langle k_{\rm A}|\big) \otimes \rho_{\rm E}^{k_{\rm A}k_{\rm B}}\,. \tag{13}$$

Equation (13) contains identical states $|k_{\rm A}\rangle_{\rm A}$ and $|k_{\rm A}\rangle_{\rm B}$.

Using the triangle inequality for Eqn (11), we estimate the trace distance as

$$||\rho_{\rm ABE}^{R_{\rm Q}} - \rho_{\rm ABE}^{I_{\rm Q}}||_1 \leqslant ||\rho_{\rm ABE}^{R_{\rm Q}} - \overline{\rho_{\rm ABE}^{R_{\rm Q}}}||_1 + ||\overline{\rho_{\rm ABE}^{R_{\rm Q}}} - \rho_{\rm ABE}^{I_{\rm Q}}||_1\,. \tag{14}$$

The density matrix corresponding to quantum key distribution through an ideal quantum communication channel can be represented as

$$\rho_{\rm ABE}^{I_{\rm Q}} = \rho_{\rm UAB}^{I_{\rm Q}} \otimes \rho_{\rm E}\,, \tag{15}$$

$$\rho_{\rm UAB}^{I_{\rm Q}} = \frac{1}{|K_{\rm A}|}\sum_{k_{\rm A}} |k_{\rm A}\rangle_{\rm A\,A}\langle k_{\rm A}| \otimes |k_{\rm A}\rangle_{\rm B\,B}\langle k_{\rm A}|\,,$$

$$\rho_{\rm E} = \sum_{k_{\rm A}}\sum_{k_{\rm B}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})\,\rho_{\rm E}^{k_{\rm A}k_{\rm B}}\,.$$

Using the relationship between trace distance and fidelity [29, 57], we find that the trace distance

$$\begin{aligned}
&||\rho_{\rm ABE}^{R_{\rm Q}} - \overline{\rho_{\rm ABE}^{R_{\rm Q}}}||_1 \\
&= {\rm Tr}\left\{\left|\sum_{k_{\rm A}\in\{0,1\}^{\ell}}\ \sum_{k_{\rm B}\in\{0,1\}^{\ell}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})|k_{\rm A}\rangle_{\rm A\,A}\langle k_{\rm A}| \otimes \rho_{\rm E}^{k_{\rm A}k_{\rm B}} \otimes \big(|k_{\rm B}\rangle_{\rm B\,B}\langle k_{\rm B}| - |k_{\rm A}\rangle_{\rm B\,B}\langle k_{\rm A}|\big)\right|\right\} \\
&= \sum_{k_{\rm A}\in\{0,1\}^{\ell}}\ \sum_{k_{\rm B}\in\{0,1\}^{\ell}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B}) \times \frac{1}{2}\,{\rm Tr}\,\big\{\big||k_{\rm B}\rangle_{\rm B\,B}\langle k_{\rm B}| - |k_{\rm A}\rangle_{\rm B\,B}\langle k_{\rm A}|\big|\big\} \\
&= \sum_{k_{\rm A}\in\{0,1\}^{\ell}}\ \sum_{k_{\rm B}\in\{0,1\}^{\ell}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})\sqrt{1 - \big|_{\rm B}\langle k_{\rm B}|k_{\rm A}\rangle_{\rm B}\big|^2} \\
&= \sum_{k_{\rm A},k_{\rm B}\in\{0,1\}^{\ell},k_{\rm A}\neq k_{\rm B}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})\,.
\end{aligned}$$

Thus, we find that the probability that Alice's key $k_{\rm A}$ differs from Bob's key $k_{\rm B}$ is equal to

$$\Pr\,(k_{\rm A}\neq k_{\rm B}) = ||\rho_{\rm ABE}^{R_{\rm Q}} - \overline{\rho_{\rm ABE}^{R_{\rm Q}}}||_1 = \sum_{k_{\rm A},\,k_{\rm B}\in\{0,1\}^{\ell},\,k_{\rm A}\neq k_{\rm B}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B}) \leqslant \varepsilon_{\rm corr} \tag{16}$$

and does not exceed $\varepsilon_{\rm corr}$, the protocol parameter. This probability is determined by the choice of error-correcting code and the identity-checking procedure for the clean key.

In other words, Eqn (16) implies that, after error correction and identity-checking of the clean keys, Alice and Bob have identical keys with a probability of no less than $1-\varepsilon_{\rm corr}$.

In this case, the QKD protocol is said to be $\varepsilon_{\rm corr}$-correct.

Next, taking into account Eqns (13) and (15), we verify by direct calculation that

$$\begin{aligned}
&||\overline{\rho_{\rm ABE}^{R_{\rm Q}}} - \rho_{\rm ABE}^{I_{\rm Q}}||_1 \\
&= {\rm Tr}\left\{\left|\sum_{k_{\rm A}\in\{0,1\}^{\ell}}\ \sum_{k_{\rm B}\in\{0,1\}^{\ell}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})\big(|k_{\rm A}\rangle_{\rm A\,A}\langle k_{\rm A}|\big) \otimes \big(|k_{\rm A}\rangle_{\rm B\,B}\langle k_{\rm A}|\big) \otimes \rho_{\rm E}^{k_{\rm A}k_{\rm B}} - \frac{1}{|K_{\rm A}|}\sum_{k_{\rm A}} |k_{\rm A}\rangle_{\rm A\,A}\langle k_{\rm A}| \otimes |k_{\rm A}\rangle_{\rm B\,B}\langle k_{\rm A}| \otimes \rho_{\rm E}\right|\right\} \\
&= \sum_{k_{\rm A}\in\{0,1\}^{\ell}} {\rm Tr}\left\{\left|\sum_{k_{\rm B}} P_{K_{\rm A}K_{\rm B}}(k_{\rm A},k_{\rm B})\,\rho_{\rm E}^{k_{\rm A}k_{\rm B}} - \frac{1}{|K_{\rm A}|}\,\rho_{\rm E}\right|\right\} \\
&= \sum_{k_{\rm A}\in\{0,1\}^{\ell}} {\rm Tr}\left\{\left|P_{K_{\rm A}}(k_{\rm A})\,\rho_{\rm E}^{k_{\rm A}} - \frac{1}{|K_{\rm A}|}\,\rho_{\rm E}\right|\right\} \\
&= ||\overline{\rho_{\rm AE}^{R_{\rm Q}}} - \rho_{\rm AE}^{I_{\rm Q}}||_1 = ||\rho_{\rm AE}^{R_{\rm Q}} - \rho_{\rm AE}^{I_{\rm Q}}||_1 \leqslant \varepsilon_{\rm QKD}\,,
\end{aligned} \tag{17}$$

where

$$\rho_{\rm AE}^{I_{\rm Q}} = \rho_{\rm UA}\otimes\rho_{\rm E}\,,\quad \rho_{\rm UA} = \underset{\rm B}{\rm Tr}\,\{\rho_{\rm UAB}\}\,,\quad \rho_{\rm AE}^{R_{\rm Q}} = \underset{\rm B}{\rm Tr}\,\{\rho_{\rm ABE}^{R_{\rm Q}}\}\,, \tag{18}$$

and $\varepsilon_{\rm QKD}$ is the quantum key secrecy parameter, which appears in proofs of the secrecy of QKD protocols in the case of

(1) an ideal authentic classical communication channel,

(2) coincidence between the final quantum keys,

(3) an ideal choice of hash function.

Thus, the distance between the non-ideal and ideal distribution (17) allows us to exclude Bob from consideration and retain only the states of Alice and Eve.

7. Distance between density matrices after enhancing key secrecy

Now, taking into account Eqn (17), we can consider only the states of Alice's original clean key, which are the reference states. Bob's clean key matches Alice's key with a probability of at least $1-\varepsilon_{\rm corr}$.

We denote Alice's original reference bit string as $|k\rangle = |k_1\rangle\otimes|k_2\rangle\otimes\ldots\otimes|k_n\rangle$, where $k_i = 0, 1$ are the bit positions of the clean key, the number of positions in it being n.

We denote the Alice–Eve density matrix after error correction — the density matrix with the clean key, but before enhancing security of the clean key (we omit the index A below for brevity) — by

$$\rho_{K\mathrm{E}}^{R_\mathrm{Q}} = \sum_{k\in\{0,1\}^n} P_K(k)|k\rangle\langle k| \otimes \rho_\mathrm{E}^k\,; \tag{19}$$

consequently, the density matrix for the ideal situation is

$$\rho_{K\mathrm{E}}^{I_\mathrm{Q}} = \rho_\mathrm{U} \otimes \hat{\rho}_\mathrm{E}\,, \quad \rho_\mathrm{U} = \frac{1}{|\mathcal{K}|}\sum_{k\in\{0,1\}^n} |k\rangle\langle k|\,,$$
$$\hat{\rho}_\mathrm{E} = \sum_{k\in\{0,1\}^n} P_K(k)\,\rho_\mathrm{E}^k\,. \tag{20}$$

After security enhancement, the final secret key becomes smaller and contains ℓ bits. Consequently, the quantum state corresponding to the final secret key is

$$|k_\mathrm{A}\rangle_\mathrm{A} = |k_{1\mathrm{A}}\rangle_\mathrm{A} \otimes |k_{2\mathrm{A}}\rangle_\mathrm{A} \otimes \ldots \otimes |k_{\ell\mathrm{A}}\rangle_\mathrm{A}\,,$$

where $\ell < n$ is the length of the final secret key.

7.1 Second-order universal hash functions

Privacy enhancement uses second-order universal hash functions U_2 (two-universal hash functions [38]).

Ideally, the hash function $\{f\colon\{0,1\}^n \to \{0,1\}^\ell\}$ is chosen randomly and equiprobably from the corresponding set of hash functions.

Then, for any bit strings x and x', $x \neq x'$ of length n, the inequality

$$\Pr\left[f\colon f(x) = f(x')\right] \leqslant \sum_{f\colon f(x)=f(x')} \frac{1}{2^n} = \frac{1}{2^\ell} \tag{21}$$

holds.

7.1.1 Example of implementation of universal second-order hash functions.

The procedure for randomly selecting a hash function is as follows.

The bit string $x = (x_0, x_1, \ldots, x_{n-1}) \in \{0,1\}^n$ under compression is assigned a polynomial

$$P_{n-1}(y) = x_0 + x_1 y + x_2 y^2 + \ldots + x_n y^{n-1}$$

$P_{n-1}(y)$ of power $n-1$ as an element of the Galois field $GF(2^n)$.

A random bit string $z = (z_0, z_1, \ldots, z_n) \in \{0,1\}^n$ is generated, which is assigned the corresponding element of the field, the polynomial

$$R_{n-1}(y) = z_0 + z_1 y + z_2 y^2 + \ldots + z_n y^{n-1}\,.$$

The product of the polynomials $P_{n-1}(y)$ and $R_{n-1}(y)$ in the field $GF(2^n)$ is calculated as the remainder of dividing the product of the polynomials by the irreducible polynomial $IR_n(y)$:

$$\mathrm{Res}_{n-1}(y) = P_{n-1}(y)R_{n-1}(y) \bmod IR_n(y)\,.$$

We denote the coefficients of the polynomial $\mathrm{Res}_{n-1}(y)$ by $k = (k_0, k_1, \ldots, k_{n-1}) \in \{0,1\}^n$.

From this bit string, the ℓ lowest positions are retained, which represent the result of compression by the hash function:

$$\mathcal{F} = \left\{f\colon\{0,1\}^n \to \{0,1\}^\ell\right\}.$$

7.2 Trace distance after security enhancement

Since the choice of a hash function requires a random bit string that is also imperfectly random, the trace distance (17) also includes the imperfection of the random string when choosing hash functions.

The density matrix after a real QKD session and security enhancement for a real choice of hash functions according to the distribution $P_\mathcal{F}^R(f)$ is equal to

$$\rho_{\mathrm{AE}}^{R_\mathrm{Q}} = \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{R_\mathcal{F} R_\mathrm{Q}} = \sum_{f\in\mathcal{F}} P_\mathcal{F}^R(f)\,|f\rangle_{FF}\langle f| \otimes \rho_{f\mathrm{E}}\,, \tag{22}$$
$$\rho_{f\mathrm{E}} = \sum_{k_\mathrm{A}\in\{0,1\}^\ell} P_{K_\mathrm{A}}(k_\mathrm{A})|k_\mathrm{A}\rangle\langle k_\mathrm{A}| \otimes \rho_\mathrm{E}^{k_\mathrm{A}}\,,$$
$$P_{K_\mathrm{A}}(k_\mathrm{A}) = \sum_{\{k\colon k\in f^{-1}(k_\mathrm{A})\in\{0,1\}^n\}} P_K(k)\,,$$
$$k_\mathrm{A} = f(k)\,,$$
$$\rho_\mathrm{E}^{k_\mathrm{A}} = \sum_{\{k\colon k\in f^{-1}(k_\mathrm{A})\in\{0,1\}^n\}} \frac{P_K(k)}{P_{K_\mathrm{A}}(k_\mathrm{A})}\,\rho_\mathrm{E}^k\,,$$

where the set of hash functions f is associated with orthogonal quantum states $|f\rangle_F$.

The density matrix after an ideal QKD session and security enhancement for a real choice of hash functions according to the real distribution $P_\mathcal{F}^R(f)$ is of the form

$$\rho_{\mathrm{AE}}^{I_\mathrm{Q}} = \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{R_\mathcal{F} I_\mathrm{Q}} = \sum_{f\in\mathcal{F}} P_\mathcal{F}^R(f)\,|f\rangle_{FF}\langle f| \otimes \rho_{f\mathrm{U}} \otimes \overline{\rho_\mathrm{E}}\,, \tag{23}$$
$$\rho_{f\mathrm{U}} = \sum_{k_\mathrm{A}\in\{0,1\}^\ell} \left(\sum_{\{k\colon k\in f^{-1}(k_\mathrm{A})\in\{0,1\}^n\}} \frac{1}{|\mathcal{K}|}\right)|k_\mathrm{A}\rangle\langle k_\mathrm{A}|\,,$$
$$\overline{\rho_\mathrm{E}} = \sum_{k_\mathrm{A}\in\{0,1\}^\ell} P_{K_\mathrm{A}}(k_\mathrm{A})\,\rho_\mathrm{E}^{k_\mathrm{A}} = \sum_{\{k\in\{0,1\}^n\}} P_K(k)\,\rho_\mathrm{E}^k\,.$$

The density matrix after a real QKD session and security enhancement with an ideal equiprobable choice of hash functions according to the equiprobable distribution $P_\mathcal{F}^I(f) = 1/|\mathcal{F}|$ takes the form

$$\rho_{\mathrm{AE}}^{R_\mathrm{Q}} = \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} R_\mathrm{Q}} = \sum_{f\in\mathcal{F}} P_\mathcal{F}^I(f)\,|f\rangle_{FF}\langle f| \otimes \rho_{f\mathrm{E}}\,, \tag{24}$$
$$P_\mathcal{F}^I(f) = \frac{1}{|\mathcal{F}|}\,.$$

The density matrix after an ideal QKD session and security enhancement with an actual choice of hash functions according to the equiprobable distribution $P_\mathcal{F}^I(f)$ is equal to

$$\rho_{\mathrm{AE}}^{I_\mathrm{Q}} = \rho_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}^{I_\mathcal{F} I_\mathrm{Q}} = \sum_{f\in\mathcal{F}} P_\mathcal{F}^I(f)\,|f\rangle_{FF}\langle f| \otimes \rho_{f\mathrm{U}} \otimes \overline{\rho_\mathrm{E}}\,. \tag{25}$$

The imperfection in the choice of hash function is given by the trace distance between the actual $P_\mathcal{F}^R(f)$ and ideal $P_\mathcal{F}^I(f)$ distributions:

$$||P_\mathcal{F}^R - P_\mathcal{F}^I||_1 = \sum_{f\in\mathcal{F}} \left|P_\mathcal{F}^R(f) - P_\mathcal{F}^I(f)\right| \leqslant \varepsilon_F\,. \tag{26}$$

Before compression of the clean key k Eve 'sees' states ρ_E^k — each clean key has an Eve state ρ_E^k 'attached' to it. After compression of the clean key $k \in \{0,1\}^n \to k_\mathrm{A} \in \{0,1\}^\ell$, each final key k_A has an Eve state $\rho_\mathrm{E}^{k_\mathrm{A}}$ 'attached' to it in Eqn (22).

Quantum state $\rho^{R_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}$ corresponds to the situation after security enhancement, which is carried out for a real Alice–Eve density matrix with Eve's intrusion into the quantum communication channel and compression of the clean keys using a real (not strictly equiprobable) distribution when choosing hash functions.

The second state $\rho^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}$ corresponds to the ideal QKD situation without Eve's intrusions into the quantum channel, followed by compression of the clean key and selection of hash functions according to an equiprobable distribution.

Then, by direct calculation, taking into account Eqns (22)–(26), we obtain

$$\begin{aligned}
||\rho^{R_{\mathrm{Q}}}_{\mathrm{AE}} - \rho^{I_{\mathrm{Q}}}_{\mathrm{AE}}||_1 &= ||\rho^{R_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 \\
&\leqslant ||\rho^{R_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 + ||\rho^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 \\
&= ||\rho^{R_{\mathcal{F}}}_{(\mathcal{F}K)} - \rho^{I_{\mathcal{F}}}_{(\mathcal{F}K)}||_1 + ||\rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 \\
&= ||P^R_{\mathcal{F}} - P^I_{\mathcal{F}}||_1 + ||\rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 \\
&\leqslant \varepsilon_F + ||\rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 \,, \qquad (27)
\end{aligned}$$

where

$$\rho^{R_{\mathcal{F}}}_{(\mathcal{F}K)} = \operatorname*{Tr}_{R_{\mathrm{Q}}}\left\{\rho^{R_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}\right\}, \quad \rho^{I_{\mathcal{F}}}_{(\mathcal{F}K)} = \operatorname*{Tr}_{R_{\mathrm{Q}}}\left\{\rho^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}\right\},$$

$$\rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} = \operatorname*{Tr}_{I_{\mathcal{F}}}\left\{\rho^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}\right\}, \quad \rho^{I_{Q}}_{(\mathcal{F}\mathrm{E})} = \operatorname*{Tr}_{I_{\mathcal{F}}}\left\{\rho^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}\right\}.$$

To estimate the value of $||\rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1$, we need the concept of smoothed quantum min-entropy.

7.3 Smoothed quantum min-entropy and hashing residue lemma

We now define relative min-entropy [57].

Let ρ_{AB} and σ_{B} be density matrices. Then,

$$H_{\min}(\rho_{\mathrm{AB}}|\sigma_{\mathrm{B}}) = -\log\lambda\,, \qquad (28)$$

where λ is the minimum number such that the operator

$$\lambda I_{\mathrm{A}} \otimes \sigma_{\mathrm{B}} - \rho_{\mathrm{AB}} > 0\,. \qquad (29)$$

In quantum-information science problems, the exact form of the density matrices is usually unknown.

The smoothed conditional min-entropy is defined as

$$H^{\varepsilon}_{\min}(\rho_{\mathrm{AB}}|\sigma_{\mathrm{B}}) = \sup_{\tilde{\rho}_{\mathrm{AB}}} H_{\min}(\tilde{\rho}_{\mathrm{AB}}|\sigma_{\mathrm{B}})\,, \qquad (30)$$

where the upper bound is taken over quantum states such that the density matrices $\tilde{\rho}_{\mathrm{AB}}$ lie in a ball,

$$\mathcal{B}^{\varepsilon}(\rho_{\mathrm{AB}}) = \left\{\tilde{\rho}_{\mathrm{AB}} : ||\rho_{\mathrm{AB}} - \tilde{\rho}_{\mathrm{AB}}||_1 \leqslant \varepsilon\right\},$$

i.e., the estimate $\tilde{\rho}_{\mathrm{AB}}$ is close to the true density matrix ρ_{AB} in the sense that the distance $||\rho_{\mathrm{AB}} - \tilde{\rho}_{\mathrm{AB}}||_1 \leqslant \varepsilon$ is small.

Here, we study $||\rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1$, the trace distance between the actual situation under QKD (taking into account Eve's intrusion) and the ideal situation under an ideal choice of hash function.

Let, for some ε', the estimate of the true density matrix (before compression and after error correction) be

$$||\rho^{R_{\mathrm{Q}}}_{K\mathrm{E}} - \tilde{\rho}^{R_{\mathrm{Q}}}_{K\mathrm{E}}||_1 \leqslant \varepsilon'\,.$$

We introduce

$$\tilde{\rho}^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} = \operatorname*{Tr}_{I_{\mathcal{F}}}\left\{\tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}\right\}, \quad \tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} = \operatorname*{Tr}_{I_{\mathcal{F}}}\left\{\tilde{\rho}^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}\right\}.$$

The density matrix $\tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}$ belongs to a ball not exceeding ε' in size. Specifically, since any hashing is a compressive mapping, the inequality

$$\begin{aligned}
||\tilde{\rho}^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 &\leqslant ||\rho^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 \\
&\leqslant ||\rho^{R_{\mathrm{Q}}}_{K\mathrm{E}} - \tilde{\rho}^{R_{\mathrm{Q}}}_{K\mathrm{E}}||_1 \leqslant \varepsilon' \qquad (31)
\end{aligned}$$

holds.

The ball size for the matrix $\tilde{\rho}^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}$ is determined below. We introduce the density matrix

$$\rho_{\mathcal{F}(\mathrm{U}K)} = \sum_{f\in\mathcal{F}} P^I_{\mathcal{F}}(f)\,|f\rangle_{FF}\langle f| \otimes \rho_{f\mathrm{U}}\,.$$

Note that

$$\rho^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} = \rho_{\mathcal{F}(\mathrm{U}K)} \otimes \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}\,.$$

Then, using the triangle inequality and taking into account Eqn (31), we obtain

$$\begin{aligned}
||\rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 &= ||\rho^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 \\
&\leqslant ||\,\rho^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 \\
&+ ||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho_{\mathcal{F}(\mathrm{U}K)} \otimes \tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 \\
&+ ||\,\rho_{\mathcal{F}(\mathrm{U}K)} \otimes \tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathcal{F}}I_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 \\
&= ||\,\rho^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 \\
&+ ||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho_{\mathcal{F}(\mathrm{U}K)} \otimes \tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 + ||\,\tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 \\
&\leqslant \varepsilon' + ||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho_{\mathcal{F}(\mathrm{U}K)} \otimes \tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 + ||\,\tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1\,. \qquad (32)
\end{aligned}$$

We seek to obtain a minimal upper bound for $||\rho^{R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1$. Therefore, in the last inequality, we seek a minimal upper bound for $||\tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho_{\mathcal{F}(\mathrm{U}K)} \otimes \tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1$. To estimate the second term in Eqn (32), we use a quantum version of the famous *leftover hash lemma* (see [57] for details). We obtain

$$\begin{aligned}
||\,\tilde{\rho}^{I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} &- \rho_{\mathcal{F}(\mathrm{U}K)} \otimes \tilde{\rho}^{I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 \\
&\leqslant \mathbf{E}_f\left[\left|\left|\sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}} |k_{\mathrm{A}}\rangle\langle k_{\mathrm{A}}|\left(\tilde{\rho}_{f\mathrm{E}} - \frac{1}{|\mathcal{K}_{\mathrm{A}}|}\,\overline{\tilde{\rho}_{\mathrm{E}}}\right)\right|\right|_1\right] \\
&= \sum_f P^I_F(f)\left[\left|\left|\sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}} |k_{\mathrm{A}}\rangle\langle k_{\mathrm{A}}|\left(\tilde{\rho}_{f\mathrm{E}} - \frac{1}{|\mathcal{K}_{\mathrm{A}}|}\,\overline{\tilde{\rho}_{\mathrm{E}}}\right)\right|\right|_1\right] \\
&\leqslant 2^{-(1/2)\left[H_{\min}(\tilde{\rho}_{K\mathrm{E}}|\tilde{\rho}_{\mathrm{E}}C)-\ell\right]}\,, \qquad (33)
\end{aligned}$$

where the following notations are introduced:

$$\overline{\tilde{\rho}_{\mathrm{E}}} = \sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}} P_{K_{\mathrm{A}}}(k_{\mathrm{A}})\,\tilde{\rho}^{k_{\mathrm{A}}}_{\mathrm{E}} = \sum_{\{k\in\{0,1\}^n\}} P_K(k)\,\tilde{\rho}^{k}_{\mathrm{E}}\,,$$

C is the total number of bits of information transmitted by Alice and Bob through an open, authentic, classical communication channel during error correction, key validation, etc., and ℓ is the length of the final secret key after compression.

For the minimum entropy $H_{\min}(\tilde{\rho}_{K\mathrm{E}}|\tilde{\rho}_{\mathrm{E}}C)$, the following inequality holds [57]:

$$H_{\min}(\tilde{\rho}_{K\mathrm{E}}|\tilde{\rho}_{\mathrm{E}}C) \geqslant H_{\min}(\tilde{\rho}_{K\mathrm{E}}|\tilde{\rho}_{\mathrm{E}}) - C\,.$$

Since inequality (33) holds for any $\tilde{\rho}_{K\mathrm{E}}$ from a ball of radius ε', taking into account the definition of smoothed min-entropy (30), we obtain

$$\begin{aligned}
&||\,\tilde{\rho}^{\,I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \rho_{\mathcal{F}(\mathrm{U}K)} \otimes \tilde{\rho}^{\,I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 \\
&\quad \leqslant \min_{\tilde{\rho}_{K\mathrm{E}}} \left\{2^{-(1/2)[H_{\min}(\tilde{\rho}_{K\mathrm{E}}|\tilde{\rho}_{\mathrm{E}})-C-\ell]}\right\} \\
&\quad = 2^{-(1/2)\left[\max_{\tilde{\rho}_{K\mathrm{E}}} H_{\min}(\tilde{\rho}_{K\mathrm{E}}|\tilde{\rho}_{\mathrm{E}})-C-\ell\right]} \\
&\quad = 2^{-(1/2)\left[H^{\varepsilon'}_{\min}(\rho_{K\mathrm{E}}|\rho_{\mathrm{E}})-C-\ell\right]}\,. \qquad (34)
\end{aligned}$$

The notation $\mathbf{E}_f$ in Eqn (33) means finding the mathematical expectation — the average over a randomly chosen hash function in accordance with the equiprobable distribution

$$P^{I}_{F}(f) = \frac{1}{|\mathcal{F}|}\,, \quad \mathbf{E}_f(\ldots) = \sum_{f\in\mathcal{F}} \frac{1}{|\mathcal{F}|}(\ldots)\,.$$

Essentially, the smoothed conditional min-entropy $H^{\varepsilon'}_{\min}(\rho_{K\mathrm{E}}|\rho_{\mathrm{E}})$ is the definition of Eve's information *deficit* with respect to Alice's bit string, given that Eve has the quantum system ρ_{E} in their possession.

The smoothed conditional min-entropy value contains all information about Eve's attacks on the quantum communication channel, including information leakage to Eve via side channels [58].

We now proceed to estimating $||\tilde{\rho}^{\,I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{\,I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1$ in Eqn (32).

We have

$$\begin{aligned}
&||\tilde{\rho}^{\,I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{\,I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 = \left\|\sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}} P_{K_{\mathrm{A}}}(k_{\mathrm{A}})\big(\tilde{\rho}^{\,k_{\mathrm{A}}}_{\mathrm{E}} - \rho^{\,k_{\mathrm{A}}}_{\mathrm{E}}\big)\right\|_1 \\
&\quad \leqslant \sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}} ||P_{K_{\mathrm{A}}}(k_{\mathrm{A}})(\tilde{\rho}^{\,k_{\mathrm{A}}}_{\mathrm{E}} - \rho^{\,k_{\mathrm{A}}}_{\mathrm{E}})||_1 \\
&\quad = \left\|\sum_{k_{\mathrm{A}}\in\{0,1\}^{\ell}} P_{K_{\mathrm{A}}}(k_{\mathrm{A}})|k_{\mathrm{A}}\rangle\langle k_{\mathrm{A}}| \otimes (\rho^{\,k_{\mathrm{A}}}_{\mathrm{E}} - \tilde{\rho}^{\,k_{\mathrm{A}}}_{\mathrm{E}})\right\|_1 \\
&\quad = ||\rho^{\,I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})} - \tilde{\rho}^{\,I_{\mathcal{F}}R_{\mathrm{Q}}}_{(\mathcal{F}K)(\mathcal{F}\mathrm{E})}||_1 \leqslant ||\rho^{\,R_{\mathrm{Q}}}_{K\mathrm{E}} - \tilde{\rho}^{\,R_{\mathrm{Q}}}_{K\mathrm{E}}||_1 \leqslant \varepsilon'\,. \qquad (35)
\end{aligned}$$

Finally, from Eqn (32) and estimates (34), (35), we derive for $||\rho^{\,R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{\,I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1$ the inequality

$$||\rho^{\,R_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})} - \rho^{\,I_{\mathrm{Q}}}_{(\mathcal{F}\mathrm{E})}||_1 \leqslant 2\varepsilon' + 2^{-(1/2)\left[H^{\varepsilon'}_{\min}(\rho_{K\mathrm{E}}|\rho_{\mathrm{E}})-C-\ell\right]}\,.$$

The value of $H^{\varepsilon'}_{\min}(\rho_{K\mathrm{E}}|\rho_{\mathrm{E}})$ increases with the length of the clean key $k \in K$. With an appropriate choice of n, the inequality

$$2\varepsilon' + 2^{-(1/2)\left[H^{\varepsilon'}_{\min}(\rho_{K\mathrm{E}}|\rho_{\mathrm{E}})-C-\ell\right]} \leqslant \bar{\varepsilon}$$

can be fulfilled.

7.4 Calculating smoothed conditional min-entropy

The smoothed conditional min-entropy is calculated on density matrices $\tilde{\rho}^{\,R_{\mathrm{Q}}}_{K\mathrm{E}}$, ε'-close in terms of trace distance $||\rho^{\,R_{\mathrm{Q}}}_{K\mathrm{E}} - \tilde{\rho}^{\,R_{\mathrm{Q}}}_{K\mathrm{E}}||_1 < \varepsilon'$ to the density matrix $\rho^{\,R_{\mathrm{QKD}}}_{K\mathrm{E}}$.

Combining the previous results, we derive an inequality for the trace distance between a real and ideal key distribution:

$$||\rho^{\,R_{\mathrm{Q}}}_{\mathrm{ABE}} - \rho^{\,I_{\mathrm{Q}}}_{\mathrm{ABE}}||_1 \leqslant \varepsilon_{\mathrm{corr}} + \bar{\varepsilon} + \varepsilon_F = \varepsilon_{\mathrm{QKD}}\,. \qquad (36)$$

Thus, the distance $\bar{\varepsilon}$ between a quantum real key distribution with intrusion into a quantum communication channel and subsequent security enhancement increases by $\varepsilon_{\mathrm{corr}} + \varepsilon_F$, where:

— ε_F corresponds to the choice of a second-order hash function using non-ideal keys,

— $\varepsilon_{\mathrm{corr}}$ is the probability that Alice's and Bob's final keys do not match.

8. Distance between real and ideal situations during authentication

Before proceeding to calculating the distances $||\rho^{\,R_{\mathrm{A}}R_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}} - \rho^{\,R_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}}||_1$ in Eqn (5) and $||\rho^{\,R_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}} - \rho^{\,I_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}_{\mathrm{ABE}}||_1$ in Eqn (6), we present necessary information on the class of hash functions used in information-theoretic authentication [47, 49, 50]. This class consists of key hash functions that use a secret key k_{s} for authentication.

8.1 Definition of hash functions for information-theoretical secure authentication

Let m be a classical message represented by a bit string of arbitrary length. A hash function maps any string m to a bit string t of fixed length.

A hash function $h_{k_{\mathrm{s}}}(m)$ depending on a secret key k_{s} is called an ε-ASU$_2$ hash function if the following conditions hold for an equiprobable selection of keys k_{s}.

(1) For any m and t, the number of hash functions (keys k_{s}), such that $t = h_{k_{\mathrm{s}}}(m)$, is equal to

$$\frac{|\mathcal{K}_{\mathrm{s}}|}{|\mathcal{T}|}\,,$$

where $\mathcal{K}_{\mathrm{s}}$, $\mathcal{T}$ are the set of keys and the set of hash values (tags), $k_{\mathrm{s}} \in \{0,1\}^{\log|\mathcal{K}_{\mathrm{s}}|}$, $t \in \{0,1\}^{\log|\mathcal{T}|}$.

Let an intruder choose an arbitrary pair (t, m) and attempt to find a key k_{s} such that $t = h_{k_{\mathrm{s}}}(m)$. The probability of impersonation over all keys is

$$\Pr_{k_{\mathrm{s}}}\{t = h_{k_{\mathrm{s}}}(m)\} = \frac{1}{|\mathcal{T}|}\,. \qquad (37)$$

In fact, it follows from Eqn (37) that, for any (t, m) and an equally probable choice of keys k_{s}, the number of hash functions (keys k_{s}) for which the equality $t = h_{k_{\mathrm{s}}}(m)$ holds is equal to $|\mathcal{K}_{\mathrm{s}}|/|\mathcal{T}|$. Therefore, the probability of falling into this subset for an equally probable choice of keys k_{s} is represented as

$$\frac{|\mathcal{K}_{\mathrm{s}}|}{|\mathcal{T}|}\,\frac{1}{|\mathcal{K}_{\mathrm{s}}|} = \frac{1}{|\mathcal{T}|}\,.$$

(2) For any $m \neq m'$ and any t and t' (possibly equal) and an equally probable choice of keys k_{s}, the number of hash functions for which $t = h_{k_{\mathrm{s}}}(m)$ and $t' = h_{k_{\mathrm{s}}}(m')$ does not exceed $\varepsilon|\mathcal{K}_{\mathrm{s}}|/|\mathcal{T}|$.

Suppose an intruder has a legitimate pair $(t, m), t = h_{k_{\mathrm{s}}}(m)$, does not know the secret authentication key k_{s}, and wants to substitute the tag and message (t, m) with his/her own pair (t', m'). The substitution probability for all keys satisfies the inequality

$$P_{k_{\mathrm{s}}}\big[t = h_{k_{\mathrm{s}}}(m),\, t' = h_{k_{\mathrm{s}}}(m')\big] < \frac{\varepsilon}{|\mathcal{T}|}\,. \tag{38}$$

Ultimately, Eqn (38) shows that, for any (t, m), (t', m') $(m \neq m'$ and any t and $t')$ and an equally probable choice of keys k_{s}, the number of hash functions for which equalities $t = h_{k_{\mathrm{s}}}(m)$, $t' = h_{k_{\mathrm{s}}}(m')$ are simultaneously satisfied does not exceed $\varepsilon|\mathcal{K}_{\mathrm{s}}|/|\mathcal{T}|$. Therefore, the probability of falling into this subset for an equiprobable choice of keys k_{s} does not exceed

$$\varepsilon\,\frac{|\mathcal{K}_{\mathrm{s}}|}{|\mathcal{T}|}\,\frac{1}{|\mathcal{K}_{\mathrm{s}}|} = \varepsilon\,\frac{1}{|\mathcal{T}|}\,.$$

These hash functions provide information-theoretical authentication in the sense that, based on the definitions of ε-ASU$_2$ hash functions, it may be concluded that the conditional probability of substitution, given the observation of a pair (m, t), is independent of the computational capabilities of the eavesdropper, but only depends on the properties of the set of hash functions $\mathcal{K}_{\mathrm{s}}$ and does not exceed

$$P_{k_{\mathrm{s}}}\big[t' = h_{k_{\mathrm{s}}}(m') | t = h_{k_{\mathrm{s}}}(m)\big] < \varepsilon\,. \tag{39}$$

8.2 Information-theoretical authentication in quantum key distribution

Now, all the tools required for calculating the distances between authentication processes over a real classical channel with possible message substitution by a perpetrator and authentication processes over an ideal communication channel without message substitution are ready.

Auxiliary classical messages in a QKD session are transmitted both from Alice to Bob and vice versa. The trace distance between processes $\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}R_{\mathrm{B}}I_{\mathrm{Q}}}$ and $\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}$, given the quantum-classical structure of states, is equal to

$$||\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}R_{\mathrm{B}}I_{\mathrm{Q}}} - \rho_{\mathrm{ABE}}^{R_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}||_1 = ||\rho_{\mathrm{ABE}}^{R_{\mathrm{B}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{B}}}||_1\,. \tag{40}$$

Similarly, for states $\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}$ and $\rho_{\mathrm{ABE}}^{I_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}$, we find

$$||\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{A}}I_{\mathrm{B}}I_{\mathrm{Q}}}||_1 = ||\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{A}}}||_1\,. \tag{41}$$

The problem essentially reduces to calculating the distance only between a process transmitting messages through a classical channel with information-theoretical authentication with possible state substitution and a process transmitting messages through a channel without message substitution.

It is shown below that, with information-theoretical authentication, the following inequalities hold for trace distances:

$$||\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{A}}}||_1 \leqslant \varepsilon_{\mathrm{Aut}}, \quad ||\rho_{\mathrm{ABE}}^{R_{\mathrm{B}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{B}}}||_1 \leqslant \varepsilon_{\mathrm{Aut}}\,, \tag{42}$$

where $\varepsilon_{\mathrm{Aut}}$ is the authentication secrecy parameter, an explicit expression for which is presented below.

In Eqn (42), it is sufficient to estimate only the first trace distance, while the second is estimated similarly.

As already noted, information-theoretical authentication requires a seed secret key k_{s}, which, generally speaking, is not ideal — strictly equiprobable — but only $\varepsilon_{k_{\mathrm{s}}}$-close to ideal in terms of trace distance:

$$||P_{K_{\mathrm{s}}} - P_{U_{K_{\mathrm{s}}}}||_1 = \sum_{k_{\mathrm{s}} \in \mathcal{K}_{\mathrm{s}}} \big|P_{K_{\mathrm{s}}}(k_{\mathrm{s}}) - P_{U_{K_{\mathrm{s}}}}(k_{\mathrm{s}})\big| \leqslant \varepsilon_{k_{\mathrm{s}}}\,, \quad P_{U_{K_{\mathrm{s}}}} = \frac{1}{|\mathcal{K}_{\mathrm{s}}|}\,, \tag{43}$$

where the parameter $\varepsilon_{k_{\mathrm{s}}}$ of the authentication key imperfection is determined by the random number generator that generates the initial authentication key.

We introduce the notation $\rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}R_{K_{\mathrm{s}}}} = \rho_{\mathrm{ABE}}^{R_{\mathrm{A}}}$, which is the density matrix after authenticating Alice's messages in a real channel with real authentication keys, and $\rho_{\mathrm{ABE}}^{I^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}} = \rho_{\mathrm{ABE}}^{I_{\mathrm{A}}}$, which is the density matrix after authenticating Alice's messages in an ideal channel with ideal authentication keys. To estimate the first trace distance in (42), we need another quantum state, which we denote by $\rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}}$, the density matrix after authenticating Alice's messages in a real channel with ideal authentication keys. Below, we show that $||\rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}} - \rho_{\mathrm{ABE}}^{I^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}}||_1 < \varepsilon$, the parameter contained in the definition of the ε-ASU$_2$ hash function.

Then, the first trace distance in Eqn (42), taking into account Eqn (43), is estimated as

$$\begin{aligned}
&||\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}} - \rho_{\mathrm{ABE}}^{I_{\mathrm{A}}}||_1 \\
&\quad \leqslant ||\rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}R_{K_{\mathrm{s}}}} - \rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}}||_1 + ||\rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}} - \rho_{\mathrm{ABE}}^{I^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}}||_1 \\
&\quad = ||P_{K_{\mathrm{s}}} - P_{U_{K_{\mathrm{s}}}}||_1 + ||\rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}} - \rho_{\mathrm{ABE}}^{I^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}}||_1 \\
&\quad \leqslant \varepsilon_{k_{\mathrm{s}}} + \varepsilon = \varepsilon_{\mathrm{Aut}}\,.
\end{aligned} \tag{44}$$

Thus, the security of information-theoretical authentication is determined by the security parameter $\varepsilon_{\mathrm{Aut}}$, which includes both the ε-ASU$_2$ hash function parameter and the imperfection of the authentication key.

Using the representation

$$\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}R_{\mathrm{B}}R_{\mathrm{Q}}} = \sum_{k_{\mathrm{A}}}\sum_{k_{\mathrm{B}}} P_{K_{\mathrm{A}}K_{\mathrm{B}}}(k_{\mathrm{A}}, k_{\mathrm{B}})|k_{\mathrm{A}}\rangle_{K_{\mathrm{A}}\,K_{\mathrm{A}}}\langle k_{\mathrm{A}}| \otimes |k_{\mathrm{B}}\rangle_{K_{\mathrm{B}}\,K_{\mathrm{B}}}\langle k_{\mathrm{B}}| \otimes g^{R_{\mathrm{A}}R_{K_{\mathrm{s}}}m_{k_{\mathrm{A}}}} \otimes g^{R_{\mathrm{B}}R_{K_{\mathrm{s}}}m_{k_{\mathrm{B}}}} \otimes \rho_{\mathrm{E}}^{k_{\mathrm{A}}k_{\mathrm{B}}}\,,$$

we find that

$$\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}} = \rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}R_{K_{\mathrm{s}}}} = \operatorname*{Tr}_{R_{\mathrm{B}}R_{\mathrm{Q}}}\big\{\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}R_{\mathrm{B}}R_{\mathrm{Q}}}\big\} = \sum_{k_{\mathrm{A}}} P_{K_{\mathrm{A}}}(k_{\mathrm{A}})g^{R_{\mathrm{A}}R_{K_{\mathrm{s}}}m_{k_{\mathrm{A}}}}\,.$$

Similarly, we can write

$$\rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}} = \sum_{k_{\mathrm{A}}} P_{K_{\mathrm{A}}}(k_{\mathrm{A}})g^{R_{\mathrm{A}}I_{K_{\mathrm{s}}}m_{k_{\mathrm{A}}}}\,,$$

$$\rho_{\mathrm{ABE}}^{I^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}} = \sum_{k_{\mathrm{A}}} P_{K_{\mathrm{A}}}(k_{\mathrm{A}})g^{I_{\mathrm{A}}I_{K_{\mathrm{s}}}m_{k_{\mathrm{A}}}}\,.$$

These density matrix data have a transparent statistical interpretation and meaning. We discuss these features using the example of $\rho_{\mathrm{ABE}}^{R^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}}$ and similarly for state $\rho_{\mathrm{ABE}}^{I^{\mathrm{A}}_{\mathrm{Aut}}I_{K_{\mathrm{s}}}}$.

We assume that many QKD sessions are conducted. After each one, Alice has a key k_{A}, which occurs with probability $P_{K_{\mathrm{A}}}(k_{\mathrm{A}})$ in each session.

Each key in a session is 'associated' with a set of classical messages, which corresponds to a density matrix $g^{R_{\mathrm{A}} I_{K_{\mathrm{s}}} m_{k_{\mathrm{A}}}}$. In each session, the classical messages and their tags from Alice to Bob (m, t) and the substituted messages (m', t') from Eve to Bob are set by a joint conditional probability distribution $P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t' \,|\, k_{\mathrm{A}})$ (see the following formula), given the key k_{A} in each session.

It is shown below that the trace distance is independent of the specific type of probability distribution, which is a consequence of the use of ε-ASU$_2$ hash functions in authentication.

Given this, the density matrix $g^{R_{\mathrm{A}} I_{K_{\mathrm{s}}} m_{k_{\mathrm{A}}}}$ for messages in the authentication channel can be represented as

$$g^{R_{\mathrm{A}} I_{K_{\mathrm{s}}} m_{k_{\mathrm{A}}}} = \sum_{k_{\mathrm{s}}} \frac{1}{|\mathcal{K}_{\mathrm{s}}|} |k_{\mathrm{s}}\rangle_{K_{\mathrm{s}}\,K_{\mathrm{s}}}\langle k_{\mathrm{s}}| \otimes \sum_{((m,t),(m',t')) \in ((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t' \,|\, k_{\mathrm{A}}) \, |m\rangle_{M\,M}\langle m| \otimes |t\rangle_{T\,T}\langle t| \otimes |m'\rangle_{M'M'}\langle m'| \otimes |t'\rangle_{T'\,T'}\langle t'|$$

and, therefore,

$$\rho^{R^{\mathrm{A}}_{\mathrm{Aut}} I_{K_{\mathrm{s}}}}_{\mathrm{ABE}} = \sum_{k_{\mathrm{s}}} \frac{1}{|\mathcal{K}_{\mathrm{s}}|} |k_{\mathrm{s}}\rangle_{K_{\mathrm{s}}\,K_{\mathrm{s}}}\langle k_{\mathrm{s}}| \otimes \sum_{((m,t),(m',t')) \in ((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t') \, |m\rangle_{M\,M}\langle m| \otimes |t\rangle_{T\,T}\langle t| \otimes |m'\rangle_{M'\,M'}\langle m'| \otimes |t'\rangle_{T'\,T'}\langle t'| \,, \tag{45}$$

where

$$P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t') = \sum_{k_{\mathrm{A}}} P_{K_{\mathrm{A}}}(k_{\mathrm{A}}) P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t' \,|\, k_{\mathrm{A}}) .$$

The superscript $R_{\mathrm{A}} I_{K_{\mathrm{s}}}$ in the probability distribution $P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t')$ corresponds to the situation of a real authentication channel with substitution using ideal authentication keys.

The density matrix is presented in a similar way:

$$\rho^{I^{\mathrm{A}}_{\mathrm{Aut}} I_{K_{\mathrm{s}}}}_{\mathrm{ABE}} = \sum_{k_{\mathrm{s}}} \frac{1}{|\mathcal{K}_{\mathrm{s}}|} |k_{\mathrm{s}}\rangle_{K_{\mathrm{s}}\,K_{\mathrm{s}}}\langle k_{\mathrm{s}}| \otimes \sum_{((m,t),(m',t')) \in ((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} P^{I_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t') \, |m\rangle_{M\,M}\langle m| \otimes |t\rangle_{T\,T}\langle t| \otimes |m'\rangle_{M'\,M'}\langle m'| \otimes |t'\rangle_{T'\,T'}\langle t'| \,. \tag{46}$$

The superscript $I_{\mathrm{A}} I_{K_{\mathrm{s}}}$ in the probability distribution $P^{I_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t')$ corresponds to the situation of an ideal authentication channel without substitution using ideal authentication keys.

Taking into account Eqns (45) and (46), we obtain for the trace distance

$$||\rho^{R_{\mathrm{A}}}_{\mathrm{ABE}} - \rho^{I_{\mathrm{A}}}_{\mathrm{ABE}}||_1 = ||\rho^{R^{\mathrm{A}}_{\mathrm{Aut}} I_{K_{\mathrm{s}}}}_{\mathrm{ABE}} - \rho^{I^{\mathrm{A}}_{\mathrm{Aut}} I_{K_{\mathrm{s}}}}_{\mathrm{ABE}}||_1 \tag{47}$$

$$= \Bigg\|\sum_{k_{\mathrm{s}}} \frac{1}{|\mathcal{K}_{\mathrm{s}}|} |k_{\mathrm{s}}\rangle_{K_{\mathrm{s}}\,K_{\mathrm{s}}}\langle k_{\mathrm{s}}| \otimes \sum_{((m,t),(m',t')) \in ((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} \Big(P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t') - P^{I_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t')\Big) \, |m\rangle_{M\,M}\langle m| \otimes |t\rangle_{T\,T}\langle t| \otimes |m'\rangle_{M'\,M'}\langle m'| \otimes |t'\rangle_{T'\,T'}\langle t'|\Bigg\|_1$$

$$= \sum_{k_{\mathrm{s}}} \frac{1}{|\mathcal{K}_{\mathrm{s}}|} \sum_{((m,t),(m',t')) \in ((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} \Big| P_{MT}(m, t) \times \Big(P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{M'T'|MT}(m', t'|m, t) - P^{I_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{M'T'|MT}(m', t'|m, t)\Big)\Big|$$

$$\leqslant \sum_{k_{\mathrm{s}}} \frac{1}{|\mathcal{K}_{\mathrm{s}}|} \sum_{(m' \neq m),((m,t),(m',t')) \in ((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t') . \tag{48}$$

The transition to the last inequality takes advantage of the fact that the distributions for the ideal and real situations coincide when $m' = m$ (no substitution); $P_{MT}(m, t)$ is the probability distribution of plaintext messages and tags (m, t) arriving in the classical communication channel from a legitimate user.

In Eqns (45)–(48), the summation index

$$((m, t), (m', t')) \in ((\mathcal{M}\mathcal{T}), (\mathcal{M}'\mathcal{T}'))_{OK}$$

means summation over elements $(m, t), (m', t')$ of the set $(\mathcal{M}\mathcal{T}), (\mathcal{M}'\mathcal{T}')$, where $t = h_{k_{\mathrm{s}}}(m)$, $t' = h_{k_{\mathrm{s}}}(m')$.

In other words, the summation is carried out over a set of messages and their tags that correspond to passing the authentication check.

When estimating the trace distance, the probabilities of events (outcomes) that fail to pass the authentication check are not taken into account.

Then, for brevity, we replace the superscript $R_{\mathrm{A}} I_{K_{\mathrm{s}}}$ with k_{s}, keeping in mind the dependence of the probability $P^{R_{\mathrm{A}} I_{K_{\mathrm{s}}}}_{MTM'T'}(m, t, m', t')$ on the authentication key.

Next, similar to [35], it is convenient to replace the variables m, t, m', t' with the new variables m, m', $y = (m, t)$, and $y' = (m', t')$ for a fixed authentication key k_{s}.

The probability in Eqn (48) can be rewritten in an equivalent form taking into account the new variables:

$$\begin{aligned} P^{k_{\mathrm{s}}}_{MTM'T'}(m, t, m', t') &= P^{k_{\mathrm{s}}}_{MT}(m, t) P^{k_{\mathrm{s}}}_{MT|M'T'}(m', t'|m, t) \\ &= P^{k_{\mathrm{s}}}_{MYM'Y'}\big(m, (m, t), m', (m', t')\big) \\ &= P_M(m) P^{k_{\mathrm{s}}}_{Y|M}\big((m, t)|m\big) P^{k_{\mathrm{s}}}_{Y'|MY}\big((m', t')|m, (m, t)\big) \\ &\quad P^{k_{\mathrm{s}}}_{M'|MYY'}\big(m'|m, (m, t), (m't')\big) \,. \end{aligned} \tag{49}$$

The conditional probabilities in Eqn (49) depend on the type of hash functions employed. For a fixed value of k_{s}, the conditional probabilities in Eqn (49) can be represented in an equivalent form:

$$P^{k_{\mathrm{s}}}_{Y|M}\big((m, t)|m\big) = P^{k_{\mathrm{s}}}_{T|M}(t|m) = P^{k_{\mathrm{s}}}\big[t = h_{k_{\mathrm{s}}}(m)\big] \,, \tag{50}$$

$$P^{k_{\mathrm{s}}}_{Y'|MY}\big((m', t')|m, (m, t)\big) = P^{k_{\mathrm{s}}}_{M'T'|MT}(m', t'|m, t) \,, \tag{51}$$

$$P^{k_{\mathrm{s}}}_{M'|MYY'}\big(m'|m, (m, t), (m', t')\big) = P^{k_{\mathrm{s}}}\big[t' = h_{k_{\mathrm{s}}}(m')|t = h_{k_{\mathrm{s}}}(m)\big] \,. \tag{52}$$

The probabilities $P^{k_{\mathrm{s}}}[t = h_{k_{\mathrm{s}}}(m)] \neq 0$, since, when summing over $(m, t), (m', t')$, nonzero terms only appear for the indices $((m, t), (m', t')) \in ((\mathcal{M}\mathcal{T}), (\mathcal{M}'\mathcal{T}'))_{OK}$.

Calculating the trace distance according to Eqns (47) and (48) using Eqns (49)–(52) and the definition of the ε-ASU$_2$

hash function yields

$$||\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}}-\rho_{\mathrm{ABE}}^{I_{\mathrm{A}}}||_1$$

$$=\sum_{k_{\mathrm{s}}}\frac{1}{|\mathcal{K}_{\mathrm{s}}|}\sum_{(m'\neq m),((m,t),(m',t'))\in((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} P_{MTM'T'}^{k_{\mathrm{s}}}(m,t,m',t')$$

$$=\sum_{m,t,m'\neq m,t'} P_M(m)P_{M'T'|MT}(m',t'|m,t)$$

$$\times\left(\sum_{k_{\mathrm{s}}}\frac{1}{|\mathcal{K}_{\mathrm{s}}|}\,P^{k_{\mathrm{s}}}\left[t=h_{k_{\mathrm{s}}}(m)\right]P^{k_{\mathrm{s}}}\left[t'=h_{k_{\mathrm{s}}}(m')|t=h_{k_{\mathrm{s}}}(m)\right]\right)$$

$$=\sum_{(m'\neq m),((m,t),(m',t'))\in((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} P_M(m)P_{M'T'|MT}(m',t'|m,t)$$

$$\times\left(\sum_{k}\frac{1}{|\mathcal{K}_{\mathrm{s}}|}\,P^{k_{\mathrm{s}}}\left[t'=h_{k_{\mathrm{s}}}(m'),t=h_{k_{\mathrm{s}}}(m)\right]\right)$$

$$=\sum_{(m'\neq m),((m,t),(m',t'))\in((\mathcal{M}\mathcal{T}),(\mathcal{M}'\mathcal{T}'))_{OK}} P_M(m)P_{M'T'|MT}(m',t'|m,t)$$

$$\times P_{K_{\mathrm{s}}}\left[t'=h_{k_{\mathrm{s}}}(m'),t=h_{k_{\mathrm{s}}}(m)\right]<\ldots\,. \tag{53}$$

For ε-ASU$_2$ hash functions, according to Eqn (38), we have

$$P_{K_{\mathrm{s}}}\left[t'=h_{k_{\mathrm{s}}}(m'),t=h_{k_{\mathrm{s}}}(m)\right]<\frac{\varepsilon}{|\mathcal{T}|}\,; \tag{54}$$

then, continuing (53), we obtain

$$\ldots<\sum_{t}\sum_{m}P_M(m)\sum_{m',t'}P_{M'T'|MT}(m',t'|m,t)\,\frac{\varepsilon}{|\mathcal{T}|}$$

$$=\sum_{t}\frac{\varepsilon}{|\mathcal{T}|}=|\mathcal{T}|\,\frac{\varepsilon}{|\mathcal{T}|}=\varepsilon\,. \tag{55}$$

Equation (55) takes into account the normalization of probability distributions

$$\sum_{m}P_M(m)=1\,,\quad\sum_{m',t'}P_{M'T'|MT}(m',t'|m,t)=1\,.$$

Putting together Eqns (43), (44), and (55), we obtain

$$||\rho_{\mathrm{ABE}}^{R_{\mathrm{A}}}-\rho_{\mathrm{ABE}}^{I_{\mathrm{A}}}||_1=||\rho_{\mathrm{ABE}}^{R_{\mathrm{Aut}}^{\mathrm{A}}R_{K_{\mathrm{s}}}}-\rho_{\mathrm{ABE}}^{I_{\mathrm{Aut}}^{\mathrm{A}}I_{K_{\mathrm{s}}}}||_1\leqslant\varepsilon_{k_{\mathrm{s}}}+\varepsilon=\varepsilon_{\mathrm{Aut}}\,. \tag{56}$$

Similarly, we obtain

$$||\rho_{\mathrm{ABE}}^{R_{\mathrm{B}}}-\rho_{\mathrm{ABE}}^{I_{\mathrm{B}}}||_1=||\rho_{\mathrm{ABE}}^{R_{\mathrm{Aut}}^{\mathrm{B}}R_{K_{\mathrm{s}}}}-\rho_{\mathrm{ABE}}^{I_{\mathrm{Aut}}^{\mathrm{B}}I_{K_{\mathrm{s}}}}||_1\leqslant\varepsilon_{k_{\mathrm{s}}}+\varepsilon=\varepsilon_{\mathrm{Aut}}\,. \tag{57}$$

Thus, the distance between real ε-secure information-theoretical authentication with possible message substitution, using real $\varepsilon_{k_{\mathrm{s}}}$-secret keys, and ideal authentication without message substitution, using ideal — strictly equiprobable keys — does not exceed $\varepsilon_{k_{\mathrm{s}}}+\varepsilon=\varepsilon_{\mathrm{Aut}}$ (56), (57).

8.3 Example of implementing information-theoretical secure authentication

To conserve a one-time authentication key, the ε-ASU$_2$ hash function can be implemented as a composition of the ε-AXU$_2$ function with a reused key to obtain the *intermediate* tag and an XOR operation to obtain the *final* tag.

The hash function $t=h_k(m)$, $t\in\{0,1\}^{\log(|\mathcal{T}|)}$ is an ε-AXU$_2$ hash function if, for any $m\neq m'$ and $c\in\{0,1\}^{\log(|\mathcal{T}|)}$, the inequality

$$\Pr_{k}\left[h_k(m)\oplus h_k(m')=c\right]\leqslant\varepsilon$$

holds.

For $\varepsilon=1/|\mathcal{T}|$, the ε-AXU$_2$ hash function becomes (is called) the ε-XU$_2$ hash function.

In turn, the ε-AXU$_2$ function is implemented as a composition of the ε_1-AU$_2$ hash function $h_{k_1}^{(1)}(...)$ and the ε_2-XU$_2$ hash function $h_{k_2}^{(2)}(...)$ with the intermediate tag $t^{(1,2)}=h_{k_2}^{(2)}(h_{k_1}^{(1)}(m))$ and the reused key (k_1,k_2) (see definition below).

A hash function $t=h_{k_1}(m)$, $t\in\{0,1\}^{\log(|\mathcal{T}_1|)}$ is an ε_1-AU$_2$ hash function if, for any $m\neq m'$, the inequality

$$\Pr_{k_1}\left[h_{k_1}(m)=h_{k_1}(m')\right]\leqslant\varepsilon_1$$

holds.

For $\varepsilon_1=1/|\mathcal{T}_1|$, the ε_1-AU$_2$ hash function becomes the U$_2$ hash function — a universal second-order hash function (see Section 7.1).

The composition of two ε_2-XU$_2$ and ε_1-AU$_2$ hash functions yields a $(\varepsilon_1+\varepsilon_2)$-AXU$_2$ hash function with an intermediate tag $t^{(1,2)}$.

As shown below, this procedure leads to fairly 'mild' estimates of the length of a binary one-time key for information-theoretical authentication.

8.3.1 Implementation of ε-ASU$_2$ hash function via composition of ε-AXU$_2$ hash function with XOR operation. The ε-AXU$_2$ hash function uses the same key for all authentication sessions. The key for encrypting the intermediate tag is used as a one-time key in each authentication session.

It has been proven in [52] that, after encryption with a one-time key k_{s} — applying the XOR operation to the intermediate tag $t^{(1,2)}$, namely,

$$t=t^{(1,2)}\oplus k_{\mathrm{s}}=h_{k_2}^{(2)}(h_{k_1}^{(1)}(m))\oplus k_{\mathrm{s}}\,,$$

the hash function $t=h_{k_{\mathrm{s}}}(m)=h_{k_2}^{(2)}(h_{k_1}^{(1)}(m))\oplus k_{\mathrm{s}}$ is an ε-ASU$_2$ hash function.

It follows that, for an equally probable choice of keys k_{s}, the following inequality holds:

$$\Pr_{k_{\mathrm{s}},k_2,k_1}\left[t'=h_{k_2}^{(2)}(h_{k_1}^{(1)}(m'))\oplus k_{\mathrm{s}}\,,t=h_{k_2}^{(2)}(h_{k_1}^{(1)}(m))\oplus k_{\mathrm{s}}\right]<\frac{\varepsilon}{|\mathcal{T}|}\,. \tag{58}$$

The keys (k_1,k_2) are the same in all sessions, and the key k_{s} is a one-time key that alters in each session.

Consequently, the conditional probability for hashing with the ε-ASU$_2$ hash function, by definition, satisfies the inequality

$$\Pr_{k_{\mathrm{s}},k_2,k_1}\left[t'=h_{k_2}^{(2)}(h_{k_1}^{(1)}(m'))\oplus k_{\mathrm{s}}|t=h_{k_2}^{(2)}(h_{k_1}^{(1)}(m))\oplus k_{\mathrm{s}}\right]<\varepsilon\,. \tag{59}$$

8.3.2 Example of constructing ε-ASU$_2$ hash function as composition of ε-AU$_2$ and ε-XU$_2$ functions and XOR operation.

(1) Implementation of $h_{k_1}^{(1)}(...)$ as an ε_1-AU$_2$ function.

We use PolyCW polynomial hashing [44, 50].

Let the message be a bit string of length M and the reused key be k_1 bits long.

If the message length M is not a power of two, the message is padded so that

$$\frac{(M||1||0^m)}{k_1} = n_1 + 1 \tag{60}$$

is an integer.

For simplicity, we assume that M is evenly divisible by k_1.

We obtain as a result a sequence of bit blocks $(m_0, m_1, \ldots, m_n)$, each k_1 bits long.

Each pair of blocks (k_1, m_i) is associated with a polynomial of degree $k_1 - 1$ according to the following rule:

— take an irreducible polynomial $IP(2^{k_1})$ in field $GF(2^{k_1})$,

— calculate

$$y = (m_0 k_1^n + m_1 k_1^{n-1} + \ldots + m_n k_1^0) \bmod IP_1(2^{k_1})\,. \tag{61}$$

All these operations described are performed in field $GF(2^{k_1})$, where each bit string is assigned a polynomial in this field.

This results in a bit string y, the number of bit positions being k_1.

This procedure implements the hash function ε_1-AU$_2$ with parameter

$$\varepsilon_1 = \frac{n_1}{2^{k_1}}\,, \tag{62}$$

where n_1 is defined in Eqn (60).

(2) Implementation of $h_{k_2}^{(2)}(\ldots)$ as an ε_2-XU$_2$ hash function.

To reduce the length of the one-time key k_s, y bits of length k_1 are compressed to a length of k_s bits, which are then encrypted using the XOR operation on the one-time key k_s.

We construct the hash function $h_{k_2}^{(2)}(\ldots)$.

Let the lengths $k_2 = k_1$. Take an irreducible polynomial $IP_2(2^{k_1})$ in field $GF(2^{k_1})$.

Randomly choose a polynomial $RP_2(2^{k_1})$ in field $GF(2^{k_1})$ of power $k_1 - 1$. Calculate

$$z = y\, RP_2(2^{k_1}) \bmod IP_2(2^{k_1})\,. \tag{63}$$

From the resulting bit string z of k_1-bit length, we retain the k_s least significant bit positions — the bit string z_{k_s}. This bit string of k_s-bit length is encrypted with the one-time key k_s, yielding the tag t,

$$t = z_{k_\mathrm{s}} \oplus k_\mathrm{s}\,.$$

The result is an implementation of the function ε-ASU$_2$ = $(\varepsilon_1 + \varepsilon_2)$-ASU$_2$, where

$$\varepsilon = \varepsilon_1 + \varepsilon_2 = \frac{n_1}{2^{k_1}} + \frac{1}{2^{k_\mathrm{s}}} = \frac{n_1}{2^{k_1}} + \frac{1}{|\mathcal{T}|}\,. \tag{64}$$

The total length of the authentication key is

$$k_\mathrm{Aut} = 2k_1 + k_\mathrm{s}\,, \tag{65}$$

where (k_1, k_2) is the reused key of length $2k_1$, and k_s is the one-time key in each session. Here, we assume that $k_1 = k_2$.

Thus, the probability of message substitution (65) is determined by the authentication key (65), which consists of two keys: the permanent key (k_1, k_2) — this key is the same in all sessions — and the one-time key k_s, which alters in each QKD session and is taken as part of the key obtained in the previous QKD session.

9. How many quantum key distribution sessions can be conducted with single seed authentication key?

A chicken is not a bird, and a logarithm is not infinity.
Biographers attribute this aphorism to Albert Einstein.

Combining the results of the previous sections, we find that, after the first QKD session, the trace distance between (1) a real QKD situation with an intrusion into a quantum communication channel, along with real information-theoretical authentication with possible substitution of classical messages, and (2) the corresponding ideal situation, satisfies the inequality

$$||\rho_\mathrm{ABE}^{R^\mathrm{A}_\mathrm{Aut} R^\mathrm{B}_\mathrm{Aut} R^\mathrm{AB}_\mathrm{QKD}} - \rho_\mathrm{ABE}^{I^\mathrm{A}_\mathrm{Aut} I^\mathrm{B}_\mathrm{Aut} I^\mathrm{AB}_\mathrm{QKD}}||_1 \leqslant 2(\varepsilon_{k_\mathrm{s}} + \varepsilon) + \varepsilon_\mathrm{QKD} = \varepsilon_\mathrm{Aut} + \varepsilon_\mathrm{QKD}\,. \tag{66}$$

The quantity $\varepsilon_\mathrm{Aut} = 2(\varepsilon_{k_\mathrm{s}} + \varepsilon)$ arises from the imperfections of one-time $\varepsilon_{k_\mathrm{s}}$-secret authentication keys. The parameter ε determines the properties of ε-ASU$_2$ hash functions and is independent of the secret key. The coefficient 2 arises from the exchange of classical messages from Alice to Bob and from Bob to Alice.

The quantity $\varepsilon_\mathrm{QKD} = \varepsilon_\mathrm{corr} + \varepsilon_F + \bar{\varepsilon}$ accounts for all imperfections in quantum key distribution under ideal authentication.

Next, we introduce the notation $\bar{\varepsilon}_{k_\mathrm{s}} = 2\varepsilon_{k_\mathrm{s}}$, $\varepsilon_\Sigma = 2\varepsilon + \varepsilon_\mathrm{QKD}$.

After the first run of the QKD system, we obtain an $\varepsilon(1)$-secret quantum key, where

$$\varepsilon(1) = \bar{\varepsilon}_{k_\mathrm{s}} + \varepsilon_\Sigma\,.$$

In the second QKD session, a portion of the $\varepsilon(1)$-secret quantum key from the first session is used for authentication. It is important to note that any part of the $\varepsilon(1)$-secret quantum key also features the $\varepsilon(1)$-secret property.

After the second QKD session, we obtain an $\varepsilon(2)$-secret quantum key, where

$$\varepsilon(2) = \varepsilon(1) + \varepsilon_\Sigma = \bar{\varepsilon}_{k_\mathrm{s}} + 2\varepsilon_\Sigma\,.$$

Similarly, after the Nth QKD session, we obtain an $\varepsilon(N)$-secret quantum key, where

$$\varepsilon(N) = \bar{\varepsilon}_{k_\mathrm{s}} + N\varepsilon_\Sigma = \bar{\varepsilon}_{k_\mathrm{s}} + N\varepsilon_\mathrm{corr} + N\varepsilon_F + N2\varepsilon + N\bar{\varepsilon}\,.$$

This key incorporates the imperfections of all QKD processes.

Thus, the 'quality' of the quantum key degrades with an increasing number of QKD sessions, since the secrecy parameter increases linearly with N.

Our goal is to ensure that a given, sufficiently large number N of QKD sessions is conducted in such a way that the key secrecy parameter in the final session does not exceed a given critical value $\varepsilon_\mathrm{crit}$.

The admissible number of sessions is found from the equality

$$\bar{\varepsilon}_{k_\mathrm{s}} + N\varepsilon_\mathrm{corr} + N\varepsilon_F + N2\varepsilon + N\bar{\varepsilon} = \varepsilon_\mathrm{crit}\,. \tag{67}$$

How can this be accomplished?

The terms on the left-hand side of equality (67) affect the QKD mechanism in ensuring final secrecy $\varepsilon_{\text{crit}}$ in a different way.

The quantity $\overline{\varepsilon}_{k_s} = 2\varepsilon_{k_s}$ appears in the sum only once. The quantity ε_{k_s} accounts for the imperfection of the seed authentication key — the (unequal probability) of the choice of bit strings that are the coefficients of the polynomials used to construct ε-ASU$_2$ authentication hash functions. It is essentially determined by the properties of the random number generator (RNG), i.e., by external factors not directly related to QKD. We assume that it is always possible to achieve the condition $\overline{\varepsilon}_{k_s} \ll \varepsilon_{\text{crit}}$ and not consider the value $\overline{\varepsilon}_{k_s}$ when calculating N.

Then, taking these conditions into account, we represent equality (67) as

$$\varepsilon_{\text{corr}} + \varepsilon_F + 2\varepsilon + \overline{\varepsilon} = \frac{\varepsilon_{\text{crit}}}{N} .$$

Next, we set the value N and, for specificity, assign each of the four terms $\varepsilon_{\text{corr}}$, ε_F, 2ε, $\overline{\varepsilon}$ the same contribution equal to $\varepsilon_{\text{crit}}/4N$ to the total sum $\varepsilon_{\text{crit}}/N$.

We now consider the terms separately.

(1) The quantity $\varepsilon_{\text{corr}}$.

The correctness parameter — the probability of a mismatch between Alice's and Bob's keys — is determined by the relation $\varepsilon_{\text{corr}} = 2^{-v}$, where v is the number of parity bits calculated from Alice's and Bob's bit strings.

Using the equality $\varepsilon_{\text{corr}} = \varepsilon_{\text{crit}}/4N$, we obtain the relation

$$v = \log \frac{4N}{\varepsilon_{\text{crit}}} .$$

(2) The quantity ε_F.

The parameter ε_F is responsible for the imperfection (unequal probability) of the choice of the bit string — the coefficients of the U$_2$ polynomial of the hash function f of the security-enhancing procedure. The parameter ε_F is determined by the properties of the RNG, i.e., external factors not directly related to QKD. We assume that the equality $\varepsilon_F = \varepsilon_{\text{crit}}/4N$ can be ensured for any reasonable values of $\varepsilon_{\text{crit}}$ and N.

(3) The quantity 2ε.

The parameter ε specifies the ε-ASU$_2$ property of authentication hash functions with an equiprobable choice of bit strings — the coefficients of the polynomials employed to construct the hash functions, with

$$\varepsilon = \frac{n_1}{2^{k_1}} + \frac{1}{2^{k_s}} ,$$

where n_1 is the number of blocks in a message of length k_1; k_1 is the length of the reused authentication key; and k_s is the length of the one-time authentication key, $k_s < k_1$.

The length of the reused authentication key k_1 can be chosen sufficiently large so that $\varepsilon \approx 1/2^{k_s}$. Then, using the relation $2\varepsilon = \varepsilon_{\text{crit}}/4N$, we obtain the minimum required length of the one-time authentication key:

$$k_s = \log \frac{8N}{\varepsilon_{\text{crit}}} .$$

The value k_s (in bits) is the additive factor to the quantum key of length ℓ_{cip} used for encryption. The total quantum key to be generated during QKD must have a length of no less than $\ell = \ell_{\text{cip}} + k_s$.

(4) The quantity $\overline{\varepsilon}$.

The value of $\overline{\varepsilon}$ estimates the distance between the quantum real and ideal key distributions after security enhancement:

$$||\rho^{R_Q}_{(\mathcal{F}\text{E})} - \rho^{I_Q}_{(\mathcal{F}\text{E})}||_1 \leqslant 2\varepsilon' + 2^{-(1/2)\left[H^{\varepsilon'}_{\min}(\rho_{K\text{E}}|\rho_\text{E}) - C - \ell\right]} = \overline{\varepsilon} . \qquad (68)$$

To solve our problem, the condition $\overline{\varepsilon} = \varepsilon_{\text{crit}}/4N$ must be satisfied.

The smallness of $\overline{\varepsilon}$ is determined by the compression ratio (the ratio between n and ℓ) of the security-enhancing hash function

$$f \colon \{0,1\}^n \to \{0,1\}^\ell .$$

The required value of n is calculated using the lower bound for the smoothed min-entropy, which contains all data about the information leakage to the perpetrator through the quantum communication channel and side leakage channels. The smoothed min-entropy for the tensor product $\rho^{n\otimes}_{K\text{E}}$ can be assessed using the conditional von Neumann entropy.

According to [57], we have

$$H^{\varepsilon'}_{\min}(\rho_{K\text{E}}|\rho_\text{E}) \geqslant nH(\rho_{K\text{E}}|\rho_\text{E}) - \log(5)\sqrt{n \log\left(\frac{1}{\varepsilon'}\right)} , \qquad (69)$$

where n is the number of recorded quantum state transmissions on Bob's receiving side,

$$H(\rho_{K\text{E}}|\rho_\text{E}) = H(\rho_{K\text{E}}) - H(\rho_\text{E}) ,$$

and $H(\rho_{K\text{E}})$, $H(\rho_\text{E})$ are the von Neumann entropies.

We set $\varepsilon' = \overline{\varepsilon}/3 = \varepsilon_{\text{crit}}/12N$ in Eqn (68).

Then, solving the equation

$$2^{-(1/2)\left[nH(\rho_{K\text{E}}|\rho_\text{E}) - C - \log(5)\sqrt{n\log(12N/\varepsilon_{\text{crit}})} - \ell\right]} = \frac{\varepsilon_{\text{crit}}}{12N} \qquad (70)$$

with respect to n yields the minimum number of recorded quantum state transmissions at the receiving end needed to ensure the required level of quantum key secrecy.

Here,

$C = \text{leak} + v = n \cdot \text{leak} + \log(4N/\varepsilon_{\text{crit}})$ is the total number of bits of information transmitted by Alice and Bob over an open, authentic classical communication channel during error correction and key validation, and

$\ell = \ell_{\text{cip}} + k_s$, ℓ_{cip} is the fraction of the quantum key length used for encryption, and $k_s = \log(8N/\varepsilon_{\text{crit}})$ is the fraction of the quantum key length used for authentication.

Taking the logarithm of (70), we obtain

$$n\Delta H - \log(5)\sqrt{n \log \frac{12N}{\varepsilon_{\text{crit}}}} - \left(2\log\frac{12N}{\varepsilon_{\text{crit}}} + \log\frac{8N}{\varepsilon_{\text{crit}}} + \log\frac{4N}{\varepsilon_{\text{crit}}} + \ell_{\text{cip}}\right) = 0 , \qquad (71)$$

$$\Delta H = H(\rho_{K\text{E}}|\rho_\text{E}) - \text{leak} .$$

We derive from Eqn (70) $n(\Delta H, N, \varepsilon_{\text{crit}}, \ell)$, the number of transmissions recorded at the receiving side that is needed to ensure the required level of key secrecy (to reach the value of

$\varepsilon_{\text{crit}}$) after N quantum key distribution sessions:

$$n(\Delta H, N, \varepsilon_{\text{crit}}, \ell_{\text{cip}}) = \left\{ \frac{1}{2\Delta H} \left[\log(5) \sqrt{\log \frac{12N}{\varepsilon_{\text{crit}}}} + \left(\log^2(5) \log \frac{12N}{\varepsilon_{\text{crit}}} + 4\Delta H \left(2 \log \frac{12N}{\varepsilon_{\text{crit}}} + \log \frac{8N}{\varepsilon_{\text{crit}}} + \log \frac{4N}{\varepsilon_{\text{crit}}} + \ell_{\text{cip}} \right) \right)^{1/2} \right] \right\}^2 . \tag{72}$$

It is of importance to note here that the dependence of the minimum required number of recorded quantum state transmissions n on the receiving side on the number of sessions $N \gg 1$ for a given critical secrecy parameter $\varepsilon_{\text{crit}} \ll 1$ is weak — logarithmic:

$$n \propto \log \left(\frac{12N}{\varepsilon_{\text{crit}}} \right) \propto \log(N) + \log \left(\frac{1}{\varepsilon_{\text{crit}}} \right) . \tag{73}$$

The aphorism presented at the beginning of this section perfectly reflects the actual situation. Informally speaking, the number of physical resources — the number of quantum states sent by Alice to Bob — depends logarithmically on the required number of QKD sessions and the key secrecy level up to the last session.

After N QKD sessions, the entire QKD system must be relaunched, i.e., a new seed authentication key for the next series of QKD sessions must be pre-distributed between Alice and Bob (by organizational, technical, or other means).

10. Long one-time key — one-time pad

In Section 9, we considered the situation where N QKD sessions are conducted, each distributing a one-time key that is $\varepsilon_{\text{crit}}$-secret until the last session. We now consider the situation where we need to generate a single long one-time key from all sessions.

Assume QKD sessions are conducted. Each one produces a quantum key ℓ_{cip}-bit long. We assume that, in the first QKD session, the quantum key is $2\varepsilon_{\text{crit}}/N^2$-secret. These keys are concatenated into a single quantum key of length $\ell_N = N\ell_{\text{cip}}$. From the triangle inequality for trace distance, it follows that the composite key of length ℓ_N is $\varepsilon_{\text{crit}}(1 + 1/N)$, since the key secrecy parameters when concatenated add up to

$$1 \cdot \frac{2\varepsilon_{\text{crit}}}{N^2} + 2 \cdot \frac{2\varepsilon_{\text{crit}}}{N^2} + \ldots + N \cdot \frac{2\varepsilon_{\text{crit}}}{N^2} = \varepsilon_{\text{crit}} \left(1 + \frac{1}{N} \right) \approx \varepsilon_{\text{crit}} .$$

Thus, to obtain a quantum key of length $\ell_N = N\ell_{\text{cip}}$, it is sufficient for the quantum key in the first QKD session to be $2\varepsilon_{\text{crit}}/N^2$-secret. Using (73), it is easy to deduce that, to ensure such a secrecy parameter, it is necessary to record

$$n \propto \log \left(\frac{12N^2}{\varepsilon_{\text{crit}}/2} \right) \propto \log(N) + \log \left(\frac{1}{\varepsilon_{\text{crit}}} \right)$$

quantum state transmissions. We see that, in this case, the number of quantum states sent by Alice to Bob also depends logarithmically on the required key length $\ell_N = N\ell_{\text{cip}}$ and the secrecy parameter $\varepsilon_{\text{crit}}$ of the composite one-time key.

11. Some numerical examples

In this section, we present examples of calculations that demonstrate, from a practical standpoint, the feasibility of generating a given large number N of quantum keys of length ℓ_{cip} used for encryption and having a given quality, with a secrecy parameter no worse than $\varepsilon_{\text{crit}}$.

In fact, by specifying a sufficiently large value of N (the number of QKD sessions) and a sufficiently small value of $\varepsilon_{\text{crit}}$ (the quantum key secrecy parameter) and using Eqn (71), we estimate a practically significant value of n: the number of quantum state transmissions actually required to implement QKD.

We set the length of quantum encryption keys $\ell_{\text{cip}} = 10^3$ and consider somewhat extreme cases where

— $N = 10^6$, $\varepsilon_{\text{crit}} = 10^{-6}$, $\ell_{\text{cip}} = 10^3$;

— $N = 10^9$, $\varepsilon_{\text{crit}} = 10^{-9}$, $\ell_{\text{cip}} = 10^3$.

Calculations using Eqn (72) are entirely correct provided that, when estimating the parameter

$$\varepsilon = \frac{n_1}{2^{k_1}} + \frac{1}{2^{k_s}} , \tag{74}$$

the first term of the authentication hash function can be disregarded. Here, n_1 is the number of blocks of length k_1 in the message, k_1 is the length of the reused authentication key, and $k_s = \log(8N/\varepsilon_{\text{crit}})$ is the length of the one-time authentication key.

For the cases under consideration, the length $k_s = 42-63$. By choosing the length of the reused authentication key $k_1 = 128$, it is easy to see that the first term in Eqn (74) can be neglected for the number of blocks $n_1 \leqslant 2^{64}$ or the limitation on the length of plaintext classical messages $M \leqslant 2^{64} \cdot 128$ bits. This length is more than sufficient for assessing the length of plaintext messages in a QKD session.

The value ΔH represents the deficit of the intruder's information, in bits, per recorded position after a QKD session, error correction, and security enhancement.

It is crucial to note here that the value ΔH is calculated based on the fundamental laws of quantum theory and is independent of assumptions about the technical and computational capabilities of the intruder (see details, e.g., in [57, 58]).

Typical values for the length of a quantum communication fiber line $L = 100$ km are $\Delta H \approx 0.1$–0.5 bits.

The dependences of the required number of registered states $n(\Delta H, N, \varepsilon_{\text{crit}}, \ell_{\text{cip}})$ in each QKD session are displayed in Fig. 7.

As follows from Fig. 7, the number of registered quantum states on Bob's receiving end weakly (logarithmically) depends on the final $\varepsilon_{\text{crit}}$ (critical value of the secrecy parameter) and on the magnitude of Eve's information deficit (ΔH) relative to Alice's key. This implies that, after initialization of the QKD system, secret keys can be distributed for virtually any length of time, and they are guaranteed to be ε-secret with $\varepsilon \leqslant \varepsilon_{\text{crit}}$. Consequently, the complexity of a brute-force attack to crack the cipher is also guaranteed to be no less than a critical value.

We now provide estimates of the quantum state transmission time.

For the length of a fiber optic communication line $L = 100$ km with a standard loss coefficient $\delta = 0.2$ dB km^{-1}, taking into account channel losses ($T(L) = 10^{-\delta L/10}$ is the coefficient of transmission through a communication line of length L), the quantum efficiency of the detectors ($\eta \approx 0.1$), the average number of photons in information states ($\mu \approx 0.2-0.5$), and losses in the system itself ($\alpha \approx 0.1$), the protocol efficiency is eff $= \alpha\eta\mu T^{-1}(L) \approx 10^{-5}$.

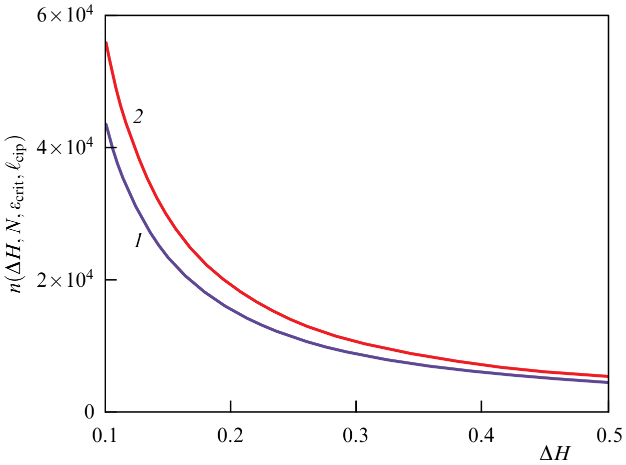


Figure 7. Required number of recorded states $n(\Delta H, N, \varepsilon_{\text{crit}}, \ell_{\text{cip}})$ in each QKD session as a function of intruder's information deficiency (ΔH) for given security level ($\varepsilon_{\text{crit}}$), number of sessions ($N$), and key length in a session (ℓ_{cip}). Parameters: curve *1* (blue) $N = 10^6$, $\varepsilon_{\text{crit}} = 10^{-6}$, $\ell_{\text{cip}} = 10^3$; curve *2* (red) $N = 10^9$, $\varepsilon_{\text{crit}} = 10^{-9}$, $\ell_{\text{cip}} = 10^3$.

It follows that, to obtain the number of recorded states $n \approx 10^5$ (see Fig. 7), $n/\text{eff} \approx 10^{10}$ quantum states must be transmitted by Alice.

At a clock rate of 100 MHz (10^8 Hz), each session requires $10^{10}/10^8 = 10^2$ s. Consequently, at a frequency of 10 MHz (10^7 Hz), the time required is $10^{10}/10^7 = 10^3$ s, i.e., approximately 1 hour per session. At a frequency of 1 GHz (10^9 Hz), transmitting 10^{10} states requires $10^{10}/10^9 = 10$ s. This implies that, every 10 s, a one-time 1000-bit-long key of a given quality can be obtained. The number of such keys — QKD sessions — is 10^6; of course, these estimates only provide orders of magnitude.

12. Conclusions

This review addresses a fundamental issue of quantum cryptography: the number of quantum key distribution sessions that can be conducted from the moment the system is launched before a new system restart until the cryptographic properties of the quantum keys reach a critical level, after which they can no longer be used for cryptographic purposes.

Quantum cryptography systems are essentially those for expanding the seed starting key, which is required at system startup to ensure information-theoretical, secure message authentication in a classical communication channel. In the current session, a quantum key is generated, part of which is used for authentication in the next session.

Derived is an explicit formula for the number of recorded messages in each quantum key distribution session required to ensure that, after N sessions, the secrecy parameter of the distributed keys is no worse than a specified level. The admissible number of sessions N and the final secrecy parameter ε_c chosen by legitimate users determine the choice of ε-ASU$_2$ hash function for information-theoretical authentication, the length of the authentication key, and the initial secrecy parameter of the seed key for system initialization. After N quantum key distribution sessions, the system must be restarted to maintain the required level of key quality.

The technology of quantum cryptography — quantum key distribution — allows the distribution of secret keys for virtually any length of time using only one pre-distributed seed key. These secret keys can be used for encryption in one-time pad mode, with the guarantee that the key secrecy is based on the fundamental laws of nature, rather than on assumptions regarding the technical and computational capabilities of an eavesdropper, including a full-scale quantum computer.

The fundamental difference from the classical case is that, in the classical case, the secrecy of each key distributed by organizational methods must be ensured. In QKD systems, it is sufficient to only distribute one short primary seed key using organizational methods. Subsequent keys are obtained through quantum distribution, and their secrecy is guaranteed by the fundamental laws of nature.

To achieve information-theoretical security in QKD systems, random bit sequences are required, which must be obtained as a result of the operation of quantum random number generators [61]. Issues related to obtaining provably random bit sequences are discussed in [62–64].

It should be noted that the issue of the number of admissible segments also arises in quantum key distribution networks with key distribution through trusted nodes [23, 59, 60]. The results presented above can be used to estimate the admissible number of segments in a quantum network. In this case, the number of quantum key distribution sessions N should be understood as the admissible number of network segments.

The obtained results show that, for experimentally achievable values of the secrecy parameter $\varepsilon_c \approx 10^{-9}$ for quantum key distribution, the length of the one-time key k_s during authentication in each session turns out to be quite 'mild.' The length of the reused key also turns out to be small.

The admissible number of QKD sessions $N = 10^9$ effectively implies that, after initialization, the QKD system can operate 'infinitely long.' For example, let each QKD session last 1 s (which is a very optimistic estimate). Then, over 100 years of operation, $N = 10^9$ sessions will be conducted, which in practice implies 'infinitely long' operation of the system after initialization.

One of the conclusions from the above discussion is that the trace distance, on which the concept of abstract cryptography is based and which sets the degree of distinguishability of a pair of quantum states corresponding to a real and ideal situation, is an adequate and sufficient characteristic for finding lower bounds on the complexity of a brute-force search — finding actual encryption keys in various situations of their use [30].

In conclusion, it is necessary to make a fundamentally important remark for quantum key distribution systems.

Quantum mechanics is not only correct, in the sense that it correctly describes phenomena in the microworld, but also a complete theory [65–70]. Of importance for quantum cryptography is not only the correctness of quantum mechanics, but also its completeness.

Quantum mechanics is the theory most profoundly verified in experiments. Over 100 years of testing a vast number of quantum theory's predictions, no disagreements with experiment have been revealed.

As applied to quantum cryptography, the laws of quantum mechanics provide a fundamental upper bound on information leakage to an intruder, given an observable perturbation of the quantum states detected at the receiver.

The completeness of quantum mechanics is fundamentally important for the secrecy of keys in quantum cryptography. Briefly and informally, the completeness of quantum mechanics implies that it is not possible to improve the probabilistic predictions of the theory that follow from the description of quantum systems using a wave function — a state vector or a density matrix. This implies that an eavesdropper has no additional resources — hidden parameters — that could improve his/her measurement results and, consequently, increase the leakage of information about distributed keys given the same observable perturbation of quantum states, compared to those that follow from the description of quantum systems using a wave function and, more generally, a density matrix [68].

Acknowledgments

We are grateful to S.P. Kulik, V.A. Kiryukhin, and the staff of the Center for Quantum Technologies at Moscow State University and colleagues from Infotecs and the SFB Laboratory for their interest in this work and numerous discussions.

References

1. Bennett C H, Brassard H "Quantum cryptography: Public key distribution and coin tossing", in *Proc. of the IEEE Intern. Conf. on Computers, Systems, and Signal Processing, Bangalore, India, 10–12 December 1984* (Piscataway, NJ: IEEE, 1984) p. 175; *Theor. Comput. Sci.* **560** 7 (2014); arXiv:2003.06557
2. Zhang Q et al. *Opt. Express* **26** 24260 (2018)
3. Sasaki M et al. *Opt. Express* **19** 10387 (2011)
4. "The University's quantum network is launched. A video overview of the grand opening at Moscow State University" 21.02.2022. InfoTeCS, https://www.youtube.com/watch?v=0WAuDcYhKbo; https://rutube.ru/video/74c8fa47de0f5d111f1eb04bc532bb60/?r=wd
5. Scarani V et al. *Rev. Mod. Phys.* **81** 1301 (2009)
6. Xu F et al. *Rev. Mod. Phys.* **92** 025002 (2020)
7. Portmann Ch, Renner R *Rev. Mod. Phys.* **94** 025008 (2022)
8. Lu C-Y et al. *Rev. Mod. Phys.* **94** 035001 (2022)
9. Azuma K et al. *Rev. Mod. Phys.* **95** 045006 (2023)
10. Kahn D *The Codebreakers*: *The Story of Secret Writing* (New York: McMillan, 1967)
11. Bauer F L *Decrypted Secrets*: *Methods and Maxims of Cryptology* 3rd ed. rev. and updated (Berlin: Springer-Verlag, 2002)
12. Soboleva T A *Istoriya Shifroval'nogo Dela v Rossii* (The History of Encryption in Russia) (Moscow: OLMA-PRESS, 2002)
13. Champollion J-F *O Egipetskom Ieroglificheskom Alfavite* (On the Egyptian Hieroglyphic Alphabet) (Ser. "Classics of Science," Translation, Editing, and Commentary by I.G. Livshits) (Moscow–Leningrad: Izd. AN SSSR, 1950)
14. Vernam G S *J. Am. IEE* **45** 109 (1926); Reprint Bell Telephone Laboratories B-198, June 1926
15. Bellovin G S *Cryptologia* **35** 203 (2011)
16. Kotel'nikov V A "Osnovnye polozheniya avtomaticheskoi shifrovki" ("Basic provisions of automatic encryption"), Report of June 19, 1941; published in: Kotel'nikov V A *Sobranie Trudov* (Collected Works) Vol. 1 *Radiofizika, Informatika, Telekommunikatsii* (Radiophysics, Informatics, Telecommunications) (Moscow: Fizmatlit, 2008) p. 153
17. Nauchnaya sessiya Otdeleniya fizicheskikh nauk Rossiiskoi Akademii nauk, posvyashchennaya pamyati akademika Vladimira Aleksandrovicha Kotel'nikova (22 fevralya 2006 g.) (Scientific session of the Division of Physical Sciences of the Russian Academy of Sciences, in commemoration of Academician Vladimir Aleksandrovich Kotel'nikov (22 February 2006)): Gulyaev Yu V *Phys. Usp.* **49** 725 (2006); *Usp. Fiz. Nauk* **176** 751 (2006); Kotel'nikova N V *Phys. Usp.* **49** 727 (2006); *Usp. Fiz. Nauk* **176** 753 (2006); Armand N A *Phys. Usp.* **49** 744 (2006); *Usp. Fiz. Nauk* **176** 770 (2006); Sachkov V N *Phys. Usp.* **49** 748 (2006); *Usp. Fiz. Nauk* **176** 775 (2006); Molotkov S N *Phys. Usp.* **49** 750 (2006); *Usp. Fiz. Nauk* **176** 777 (2006); Chertok B E *Phys. Usp.* **49** 761 (2006); *Usp. Fiz. Nauk* **176** 788 (2006)
18. Kotel'nikov V A "O propusknoi sposobnosti 'efira' i provoloki v elektrosvyazi" ("On the transmission capacity of 'ether' and wire in electric communications"), in *Vsesoyuznyi Energeticheskii Komitet. Materialy k I Vsesoyuz. S'ezdu po Voprosam Tekhnicheskoi Rekonstruktsii Dela Svyazi i Razvitiya Slabotochnoi Promyshlennosti, 1932, Moskva* (All-Union Energy Committee. Materials for the 1st All-Union Congress on Technical Reconstruction of Communications and Development of the Low-Current Industry, 1932, Moscow) (Moscow: Upravlenie Svyazi RKKA, 1933) p. 1; reprinted in: Kotel'nikov V A *O Propusknoi Sposobnosti 'Efira' i Provoloki v Elektrosvyazi* (On the Transmission Capacity of 'Ether' and Wire in Electric Communications) (Moscow: Inst. Radiotekhniki i Elektroniki MEI (TU), 2003); Kotel'nikov V A *Phys. Usp.* **49** 736 (2006); *Usp. Fiz. Nauk* **176** 762 (2006)
19. Bissell Ch *IEEE Commun. Mag.* **47** (10) 24 (2009)
20. Shannon C E "A mathematical theory of cryptography", Bell System Technical Memo MM 45-110-02, dated Sept. 1 1945, p. 86, Part III of original document; https://www.iacr.org/museum/shannon/shannon45.pdf
21. Schneier B *Applied Cryptography. Protocols, Algorithms, and Source Code in C* (New York: John Wiley and Sons, 1996); Translated into Russian: *Prikladnaya Kriptografiya. Protokoly, Algoritmy, Iskhodnye Teksty na Yazyke Si* (Moscow: Triumf, 2012)
22. Konheim A G *Computer Security and Cryptography* (Hoboken, NJ: John Wiley and Sons, 2007)
23. Arbekov I M, Molotkov S N *Matem. Voprosy Kriptografii* **14** (3) 9 (2023)
24. Wiesner S "Conjugate Coding" (manuscript circa 1970); subsequently published in *ACM SIGACT News* **15** (1) 78 (1983)
25. Shor P W "Algorithms for quantum computation: discrete logarithms and factoring//, in *Proc. of the 35th Annual Symp. on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994* (Ed. S Goldwasser) (Piscataway, NJ: IEEE Computer Society Press, 1994) p. 124, DOI: 10.1109/SFCS.1994.365700
26. Diffie W, Hellman M *IEEE Trans. Inform. Theory* **22** 644 (1976)
27. Yuen H P, arXiv:1109.2675
28. Renner R, arXiv:1209.2423
29. Wilde M M, arXiv:1106.1445v6, corrected version of 2 Dec. 2015
30. Arbekov I M, Molotkov S N *J. Exp. Theor. Phys.* **125** 50 (2017); *Zh. Eksp. Teor. Fiz.* **152** 62 (2017)
31. Arbekov I M *Matem. Voprosy Kriptografii* **7** (1) 39 (2016)
32. Molotkov S N *J. Exp. Theor. Phys.* **123** 784 (2016); *Zh. Eksp. Teor. Fiz.* **150** 903 (2016)
33. Arbekov I M *Elementarnaya Kvantovaya Kriptografiya*: *dlya Kriptografov, ne Znakomykh s Kvantovoi Mekhanikoi* (Elementary Quantum Cryptography: for Cryptographers Unfamiliar with Quantum Mechanics) (Basics of Information Security, No. 23) (Moscow: URSS. LENAND, 2022)
34. Cederlöf J, Larsson J-A *IEEE Trans. Inform. Theory* **54** 1735 (2008)
35. Abidin A, Larsson J-A *Int. J. Quantum Inform.* **7** 1047 (2009)
36. Peev M et al. *Int. J. Quantum Inform.* **7** 1401 (2009)
37. Pacher C et al. *Quantum Inform. Process.* **15** 327 (2016)
38. Wegman M N, Carter J L *J. Comput. Syst. Sci.* **22** 265 (1981)
39. Simmons G J *Proc. IEEE* **76** 603 (1988)
40. Atici M, Stinson D R "Universal hashing and multiple authentication", in *Advances in Cryptology, CRYPTO'96. 16th Annual Intern. Cryptology Conf., Santa Barbara, California, USA, August 18–22, 1996, Proc.* (Lecture Notes in Computer Science, Vol. 1109, Ed. N Koblitz) (Berlin: Springer-Verlag, 1996) p. 16, DOI: 10.1007/3-540-68697-5_2
41. Bierbrauer J et al. "On families of hash functions via geometric codes and concatenation", in *Advances in Cryptology, CRYPTO'93. 13th Annual Intern. Cryptology Conf., Santa Barbara, California, USA, August 22–26, 1993, Proc.* (Lecture Notes in Computer Science, Vol. 773, Ed. D R Stinson) (Berlin: Springer-Verlag, 1994) p. 331, DOI: 10.1007/3-540-48329-2_28
42. den Boer B *J. Comput. Security* **2** 65 (1993)
43. Krawczyk H "LFSR-based hashing and authentication", in *Advances in Cryptology, CRYPTO'94. 14th Annual Intern. Cryptology Conf., Santa Barbara, California, USA, August 21–25, 1994, Proc.* (Lecture Notes in Computer Science, Vol. 839, Ed. Y G Desmedt)

(Berlin: Springer-Verlag, 1994) p. 129, DOI: 10.1007/3-540-48658-5_15

44. Krawczyk H "New hash functions for message authentication", in *Advances in Cryptology, EUROCRYPT'95. Intern. Conf. on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 21–25, 1995. Proc.* (Lecture Notes in Computer Science, Vol. 921, Eds L C Guillou, J-J Quisquater) (Berlin: Springer-Verlag, 1995) p. 301, DOI: 10.1007/3-540-49264-X_24
45. Stinson D R "Universal hashing and authentication codes", in *Advances in Cryptology, CRYPTO'91. Proc.* (Lecture Notes in Computer Science, Vol. 576 , Ed. J Feigenbaum) (Berlin: Springer, 1992) p. 74, DOI: 10.1007/3-540-46766-1_5
46. Stinson D R *J. Comput. Syst. Sci.* **48** 337 (1994)
47. Stinson D R *Congressus Numerantium* **114** 7 (1996)
48. Stinson D R *J. Combin. Math. Combin. Comput.* **42** 3 (2002)
49. Abidin A, Larsson J-Å "New universal hash functions", in *Research in Cryptology. 4th Western European Workshop, WEWoRC 2011, Weimar, Germany, July 20–22, 2011, Revised Selected Papers* (Lecture Notes in Computer Science, Vol. 7242, Eds F Armknecht, S Lucks) (Berlin: Springer, 2012) p. 99, DOI: 10.1007/978-3-642-34159-5_7
50. Rogaway P *J. Cryptology* **12** 91 (1999)
51. Abidin A, Larsson J-Å *Quantum Inform. Process.* **13** 2155 (2014)
52. Portmann Ch *IEEE Trans. Inform. Theory* **60** 4383 (2014)
53. Canetti R "Universally composable security: a new paradigm for cryptographic protocols", in *Proc. 42nd IEEE Symp. on Foundations of Computer Science, 08–11 October 2001, Newport Beach, CA, USA* (Piscataway, NJ: IEEE, 2001) p. 136, DOI: 10.1109/SFCS.2001.959888
54. Canetti R et al. "Universally composable security with global setup", in *Theory of Cryptography. 4th Theory of Cryptography Conf., TCC 2007, Amsterdam, The Netherlands, February 21–24, 2007, Proc.* (Lecture Notes in Computer Science, Vol. 4392, Ed. S P Vadhan) (Berlin: Springer, 2007) p. 61, DOI: 10.1007/978-3-540-70936-7_4
55. Müller-Quade J, Renner R *New J. Phys.* **11** 085006 (2009)
56. Maurer U, Renner R "Abstract cryptography", in *Proc. of the Second Symp. on Innovations in Computer Science, ICS 2011, Beijing, China* (Beijing: Tsinghua Univ. Press, 2011) p. 1
57. Renner R "Security of quantum key distribution," PhD Thesis (Zürich: ETH, 2005)
58. Molotkov S N *J. Exp. Theor. Phys.* **133** 272 (2021); *Zh. Eksp. Teor. Fiz.* **160** 327 (2021)
59. Molotkov S N *Laser Phys. Lett.* **19** 045201 (2022)
60. Molotkov S N *Laser Phys.* **34** 045202 (2024)
61. Herrero-Collantes M, Garcia-Escartin J C *Rev. Mod. Phys.* **89** 015004 (2017)
62. Arbekov I M, Molotkov S N *Phys. Usp.* **64** 617 (2021); *Usp. Fiz. Nauk* **191** 651 (2021)
63. Arbekov I M, Molotkov S N *Phys. Usp.* **67** 919 (2024); *Usp. Fiz. Nauk* **194** 974 (2024)
64. Balygin K A, Kulik S P, Molotkov S N *JETP Lett.* **119** 538 (2024); *Pis'ma Zh. Eksp. Teor. Fiz.* **119** 533 (2024)
65. Einstein A, Podolsky B, Rosen N *Phys. Rev.* **47** 777 (1935)
66. Bell J S *Physics* **1** 195 (1964)
67. Bell J S *Rev. Mod. Phys.* **38** 447 (1966)
68. Bell J S (Introduction by Aspect A) "Free variables and local causality", in *Speakable and Unspeakable in Quantum Mechanics: Collected Papers on Quantum Philosophy* 2nd ed. (Cambridge: Cambridge Univ. Press, 2004) pp. 100–104, Ch. 12
69. Kochen S, Specker E P *J. Math. Mech.* **17** 59 (1967) DOI: 10.1512/iumj.1968.17.17004
70. Colbeck R, Renner R *Nat. Commun.* **2** 411 (2011)