PACS numbers: 03.67.Dd, **89.70.+c**
DOI: 10.1070/PU2006v049n07ABEH006050

Quantum cryptography and V A Kotel'nikov's one-time key and sampling theorems

S N Molotkov

Quantum cryptography constitutes a new avenue in the development of the means of confidential information transmission. To be more precise, quantum cryptographic systems are systems for secret key distribution between spatially separated (remote) legitimate users. Affording secret key distribution over such users is of crucial importance in cryptography. If there existed a way of distributing (transferring) secret keys from one legitimate user to another via a public (nonsecret) communication channel with an assurance that the keys would remain unknown to the eavesdropper in the course of transfer, it would be possible to transfer messages ciphered with the aid of these keys, which in principle cannot be deciphered (broken) by a third person. Suchlike fundamentally nondecipherable systems are referred to as absolutely unbreakable, or cipher systems in a one-time pad mode. More recently, these ciphers have come to be known as perfect.

First we briefly touch upon the history of the problem.

The first rigorous substantiation of the fact that one-time key cipher systems are absolutely unbreakable was given in Vladimir Aleksandrovich Kotel'nikov's work. This work, which had been completed a few days before the Soviet Union entered the Great Patriotic war, was part of a classified report [1] and has never been published in the open press.

At the same time, the problems of theoretical cipher immunity were independently studied by C Shannon. The findings of his investigations were presented in the classified report "A mathematical theory of cryptography", which dates to 1 September 1946. Following the war this report was declassified[1] and published in 1949 as the paper "Communication theory of secrecy systems" [2], which became a well-known classic work on theoretical cryptography.

An idea quite close to the idea of the one-time pad cipher mode was advanced in G S Vernam's work "Cipher printing telegraph systems for secret wire and radio telegraphic communication" [3] back in 1926. He stated, although without any mathematical reasoning, that running key ciphers would be perfectly secure: "If, now, instead of using

[1] Here, there is good reason to mention the opinion of W Diffie, one of the founders of public-key cryptography. In his view, Shannon's work might conceivably have been declassified by mistake [see the preface to B Schneier's monograph *Applied Cryptography* (John Wiley & Sons, Inc., 1996)].

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

Thanks to Kotel'nikov's and Shannon's research, there emerged a clear and rigorous understanding as to what criteria an absolutely unbreakable cipher should satisfy.

Informally, a cipher is absolutely unbreakable when:

(i) the key is secret — is known to only the legitimate users;

(ii) the key length in bits is no shorter than the message length;

(iii) the key is random, and

(iv) the key is employed only once.

In this case, the message in cipher is statistically independent of the initial message.

The fundamental problem in the realization of one-time key cryptosystems consists in the transfer (distribution) of secret keys to remote legitimate users.

The key has to be transferred to such users by way of some physical signal via a public (i.e., accessible to eavesdropping) communication channel. From the standpoint of classical physics, in this case there is no prohibition against measuring the transmitted signal without its perturbing. That is why it is in principle impossible to guarantee the secrecy of the key in its distribution.

The situation is radically different and more interesting when the key transfer is effected by means of quantum states. Quantum cryptography, based on the basic prohibitions imposed by quantum mechanics, opens the door to key transfer with the aid of quantum states, the secrecy being ensured by the basic laws of nature. Quantum cryptography therefore makes it possible to realize absolutely unbreakable cipher systems with one-time keys, which can be traced to the works of Vernam, Kotel'nikov, and Shannon. Properly speaking, the idea of quantum cryptography is aimed precisely at solving the central cryptographic problem — the problem of secret key distribution.

The idea of invoking quantum mechanics for information protection was first stated by S Wiesner in 1973 (the idea of 'quantum' money) but published [4] only a decade later. Interestingly, the ideas of applying quantum mechanics to information protection were conceived earlier than classical public-key cryptography [5, 6].

The advent of quantum cryptography is associated with the publication of a remarkable paper by Bennett and Brassard in 1984, who came up with the first cryptographic protocol BB84 which later became classic [7].

Quantum cryptography, or secret key distribution, permits, in principle, realizing absolutely unbreakable (not decipherable by an eavesdropper even theoretically) one-time key cipher systems. The secrecy of keys in quantum cryptography relies on the fundamental quantum-mechanical prohibitions: (i) an unknown quantum state cannot be cloned (the no-cloning theorem [8]); (ii) a pair of observables to which there correspond noncommuting Hermitian operators cannot be simultaneously distinguished with confidence, which stems from the Heisenberg uncertainty relation [9], or, to be more formal, noncommuting operators cannot posses common eigenvectors. The density matrices of the information states corresponding to the classical 0 and 1 bits fulfill the function of observables in quantum cryptography. For pure states, the simultaneous unobservability (certain indistinguishability) of the density matrices is equivalent to the nonorthogonality of information quantum states [9]. The aforesaid signifies that there are no measurements which allow distinguishing one of the pair of nonorthogonal states with the probability 1 and in doing this retain the initial (unperturbed) state of the system.

Therefore, any measurement that yields information about the transmitted states is bound to disturb them, which permits detecting any attempts at eavesdropping in the communication channel. In other words, the eavesdropping (accordingly, the perturbation of the transmitted states) cannot help but change the statistics of measurement data at the receiving end in comparison with the statistics of the measurement data covering unperturbed states. A quantum state distortion takes place in a nonideal quantum channel, which is also responsible for a change in the statistics of measurement data. In quantum cryptography it is in principle impossible to distinguish whether the data statistics change in comparison with that in the ideal case due to noise in the channel or due to the actions of an eavesdropper, and therefore any changes in statistics are to be attributed to an eavesdropper's action.

If the laws of quantum mechanics allowed revealing merely the very fact of perturbation of transmitted states, this would be of little interest for the purposes of cryptography, more specifically for the transfer of keys. *Quantum mechanics permits not only detecting the state perturbation, but also relating the change in measurement data statistics to the amount of information which might be obtained by an eavesdropper for the observed change in counting statistics in comparison with the statistics in the ideal case*.

Apart from a quantum communication channel (in real conditions, this is either optical fiber or open space) employed for transferring quantum states in quantum cryptography, also required is a public, classical communication channel. The latter is required by legitimate users to reveal the changes in counting statistics and error correction in the primary key transmitted via the quantum communication channel.

The only requirement imposed on the classical communication channel is that the classical information transmitted openly and accessible to anyone, including an eavesdropper, cannot be altered by the eavesdropper, thus being intact (the so-called unjammable channel) [7]. This unjammable channel is, of course, a mathematical idealization. In real conditions, to retain the integrity of the publicly transmitted classical data advantage should be taken of data authenticity and integrity verification procedures. These procedures, in turn, require a secret key. When use is made, for instance, of the Internet as the unjammable channel, the Hellman – Diffie key generation scheme [5] may be employed for authenticity verification purposes. However, when the unjammable channel makes use of the same optical fiber line as for the quantum channel, the Hellman – Diffie key generation scheme for authenticity verification obviously turns out to be unacceptable due to the so-called 'man in the middle' attack.

In this situation, a small start-up key is required once during the first communication session. In the succeeding sessions this key is discarded, and a part of the key generated via the quantum channel during the previous exchange session is employed to verify the authenticity and integrity of data transmitted via the classical channel. The remaining greater part of the key obtained via the quantum channel is intended for transmitted information ciphering itself. When use is made of GOST R 34.11-94 procedures [10] to verify the authenticity and to retain integrity of the data, the start-up key length equals 256 bits. In this case, a new secret key (much longer than the initial one) may be

transferred during several seconds of exchange via the quantum channel.

Of course, the start-up key may be used for ciphering a new key and transferring it to the second legitimate user. However, in doing this the absolute secrecy of the new key is guaranteed only when its length does not exceed the length of the key employed to cipher the new key, i.e., there is no way of obtaining a longer key than the initial one. In quantum cryptography, the start-up key is not employed directly to transfer a new key, which is generated via the quantum communication channel. In this case, the number of open information bits transferred via the unjammable channel per one bit of the new secret key can be made smaller than unity, and a key expansion is therefore possible.

The approach involving a small start-up key is preferable to the approaches relying on asymmetric public-key cryptography algorithms, because it permits minimizing the number of sessions of exchange via the public communication channel in the course of key privacy amplification and 'purification'.

The main task of the theory reduces to elucidating the length of the secret key which can be obtained for observed changes in the statistics of the measurement data at the receiving end in comparison with the statistics covering unperturbed states. As a rule, the quantity which characterizes the departure of the measurement statistics from the ideal ones is the observed error probability at the receiving end, or more precisely, the probability that the transferred 0 bit was recorded as 1, and vice versa. This situation takes place in the widely used BB84 protocol, although other criteria of a statistics change are possible, which employ several parameters. Prior to error probability elucidation, via a public channel there occurs a comparison of the bases at the receiving and transmitting sides (for the BB84 protocol [7]) or disclosing the positions at the receiving side, where measurements yielded an indefinite result (for the B92 protocol [9]). The error probability is evaluated by comparing, via the public communication channel, a part of the sequence obtained via the quantum information channel with the corresponding part of the initial one; the disclosed part is subsequently discarded.

The next step of any quantum cryptographic key-distribution protocol consists in error correction in the undisclosed part of the sequence for legitimate users by way of information exchange via the public information channel. Legitimate users are commonly given the names Alice and Bob, while the eavesdropper is referred to as Eve. As a result of error correction, Alice and Bob retain bit sequences of shorter length that are already similar. In this context, 'similar' signifies that the sequences coincide with a probability arbitrarily close to unity: $1 - 2^{v}$ (for instance, $1 - 2^{-200} \sim 1 - 10^{-70}$; we recall that the number of atoms in the Universe is estimated at 10^{77}). The parameter v is selected by legitimate users.

Upon 'purifying' the primary key, the eavesdropper has a string of bits or a register of quantum memory with the states, or both. The last step in obtaining the final secret key consists in privacy amplification [11] — in the compression of the 'purified' key with the aid of the so-called 2-universal hash function [12], which is a random function by itself for the already similar sequences with Alice and Bob. The randomly selected hash function is openly conveyed by one of legitimate users via the public communication channel and is considered to be known to all, including the eavesdropper. For legitimate users, the compressed bit sequence is the common secret key, with the assurance that the eavesdropper has an arbitrarily small amount of information about the key according to some secrecy parameter prescribed by Alice and Bob.

The natural requirement imposed on the error correction and key privacy amplification procedures is that the number of bits conserved in the final key should be as large as possible. Yet another requirement consists in the minimization of the number of exchange sessions involving the public communication channel in terms of one bit in the final secret key.

In the error correction in the primary key, the task of the legitimate users is not only to correct the errors, but also to estimate the upper limit of the amount of information which the eavesdropper can gain from exchanges via the public communication channel. To correct errors, advantage can be taken of different procedures, including the well-elaborated classical error-correcting codes.

We now turn our attention to the discussion of experimental realizations of quantum cryptographic systems.

Research in the area of quantum cryptography and realization of different quantum cryptosystems is pursued in many universities in all developed countries and nearly all leading telecommunication companies. During the last five years, quantum cryptography has walked its way from purely theoretical investigations to their practical realization and the fabrication of the first commercial prototypes.

The existing prototypes of quantum cryptosystems employ primarily the following principles of coding classical information into the states of quantum systems.

(1) Coding the information about the key into polarization degrees of freedom [13].

(2) Phase coding with the aid of a Mach – Zehnder interferometer, in which the information is coded into the phase difference between the receiving and transmitting interferometer arms [14, 15].

(3) Coding on the basis of frequency modulation of the carrier frequency [16].

(4) Quantum cryptography on coherent states employing homodyne detection at the receiving end [17].

The greatest progress has been achieved in cryptosystems with phase coding and self-compensation [18] employing Faraday reflectors. The first laboratory prototype of a quantum cryptosystem was made in the IBM Research Center in 1989, and the length of its quantum communication channel measured 1 m [19]. Laboratory versions of a cryptosystem based on a time division Mach – Zehnder interferometer were implemented using a 30-km long optical fiber communication line in the research laboratory of British Telecom in 1995 [20] and optical fiber communication lines of total length 48 km in the Los Alamos Laboratory [21]. These schemes relied on the principle of phase coding. The NEC research laboratory extended the range to 100 km in 2003 [21], and to 150 km in 2004 [22]. These schemes exhibit a sophisticated development of the idea of phase coding with self-compensation by the use of Faraday reflectors. The aforementioned cryptosystems, particularly the schemes with phase coding and self-compensation, are rather complicated to realize. The theoretical research of a group at Geneva University resulted in the implementation of a quantum cryptosystem with a 23-km long optical fiber cable laid on the bottom of Lake Geneva between the cities of Nyon and Geneva. The line, which has been lengthened to 67 km to date, constitutes a complex optical-fiber interferometer with phase coding and self-compensation employing Faraday reflectors [18] (the first so-called plug&play quantum cryptographic

system). Active research is being pursued at the IBM research laboratory (Almaden) [23, 24]. The first local quantum cryptographic network in Boston has been approbated, which is intended for distributing secret keys between users spaced at 10 km (the project is being carried out under the auspices of the Defense Advanced Research Projects Agency) [25].

The MagiQ innovative company recently announced the first commercial version of a quantum fiber cryptosystem operating within a 120-km range, which relies on the phase coding principle. The scheme realizes the BB84 quantum cryptographic protocol.

In the opinion of experts of QinetiQ and Toshiba Research Europe (Great Britain), within three years a start will be made on the wide use of quantum cryptosystems, first and foremost by governmental institutions and banks.

There are known realizations of the prototypes of quantum cryptosystems that transfer secret keys via open space [26–28]. Judging by the published data [28], the record-long range amounts to 23.4 km, both in the daytime and night-time. Suchlike quantum cryptosystems are intended for the generation and transfer of secret keys between ground-based objects and low-orbit satellites (up to altitudes of 1000 km) or between ground-based objects via satellites. In the view of a project leader of QinetiQ, experiments are planned on the transfer of cryptographic keys to low-orbit satellites and with their aid it will be possible to convey secret keys to any point of the planet within seven years or so.

The following parameters of quantum cryptographic optical fiber communication lines are predicted for the near future:

(1) The number of errors not exceeding several percent for an effective rate of information transfer via an optical fiber quantum channel.

(2) A length of about 100–150 km for a quantum optical-fiber communication channel.

(3) 8–16 subchannels in the wavelength multiplexing.

Despite the impressive progress in the understanding of the cryptographic unbreakability (secrecy) of quantum cryptosystems, as well as in their implementation, these systems contain rather sophisticated optical-fiber, electronic, and software components, and operating them at the present time is more like conducting a subtle scientific experiment and demonstrating experimental skill rather than a practical activity involving conventional equipment in general use. Another significant circumstance which now limits the wide acceptance of quantum cryptosystems on the basis of phase coding is that the quantum cryptosystems so far are hardly compatible with standardized optical-fiber telecommunication technologies because they contain specific components (interferometers) requiring fine adjustments. Lastly, the fundamental point is that every quantum cryptographic protocol for secret key distribution in fact necessitates 'dark' optical fiber lines (vacant lines).

There are three basic protocols for secret key transfer, which are briefly termed BB84 [7], B92 [9], and BB84$(4+2)$ [29]. The BB84 protocol makes use of four quantum states: two orthogonal states for 0 and 1 in one basis, and two orthogonal states for 0 and 1 in the other. Between the bases, the states are nonorthogonal in pairs, which is needed to ensure secrecy. The B92 protocol makes use of a pair of any nonorthogonal quantum states corresponding to 0 and 1. The BB84$(4+2)$ protocol is a derivative of BB84 and differs from the latter in that the states inside the bases are also made nonorthogonal. Clearly, different exchange protocols necessitate different physical devices to produce the quantum states at the transmitting end and, accordingly, different devices to make quantum-mechanical measurements at the receiving end.

The cryptographic unbreakability (secrecy) of these protocols has been investigated in sufficient detail [29–36]. When account is taken of real parameters — the nonstrict single-photon nature of the source, the nonideality of avalanche photodetectors, and the optical-fiber communication line attenuation, the above protocols ensure the secrecy of key distribution up to a certain critical length of the optical-fiber communication line [29]. The B92 protocol is minimal in terms of the number of states involved and measurements but ensures secrecy up to distances of only $\sim 15-20$ km [33]. The most thoroughly studied BB84 protocol, which uses four quantum states, is more complicated in realization and maintains secrecy up to distances of ~ 50 km [29]. Finally, the BB84$(4+2)$ protocol makes use of four states nonorthogonal in pairs. This protocol is still more complex in realization and optical-fiber interferometer adjustment, but 'survives' up to distances of ~ 150 km from the viewpoint of secrecy [29].

Experimental realization of quantum cryptosystems calls for single-photon sources. We emphasize that from the standpoint of theory it is not necessary that the quantum states used for key transfer be single-photon states. In a multiphoton case, however, quantum-mechanical measurements taken at the receiving end to detect attempts at eavesdropping and changing the quantum states should formally be realized as projectors on the corresponding vectors of multiphoton quantum states. Such measuring devices so far do not exist, although there are no theoretical prohibitions against the realization of these quantum-mechanical measurements. That is, the use of precisely single-photon quantum states is caused by the existing detectors (actual detectors are gated avalanche photodetectors with Peltier cooling).

It is pertinent to note that superconductor-based photodetectors have already been devised; these, unlike heterostructure-based avalanche photodetectors, distinguish states with a different number of photons.

Single-photon (more precisely, quasi-single-photon) quantum states are obtained by way of strong attenuation of a coherent state — laser radiation, which contains multiphoton components even after arbitrary attenuation.

The nonstrict single-photon nature of the source in combination with the attenuation in the quantum communication channel have the effect that the distributed-key secrecy is guaranteed only when the channel length does not exceed some critical value.

The negative role of attenuation (for a nonstrictly single-photon source) in the quantum communication channel consists in the fact that, beginning with some degree of attenuation, it is no longer possible to guarantee the transferred-key secrecy (which is most important) rather than that the attenuation evidently lowers the rate of key transfer, because not all photons reach the receiving end. The attenuation in optical-fiber communication lines depends on the length of the communication channel. However, the critical length up to which the system retains secrecy is still not strictly known. Its estimates range from dozens of kilometers to 150 km [29].

Efforts are underway to employ radiation sources in quantum cryptography, which are built, for instance, around diamond nanoparticles that approach single-photon sources by their parameters [37].

When the main quantum cryptographic protocols and the proofs of their secrecy in a channel with attenuation are analyzed (BB84 and B92 are the main protocols, while the remaining ones are their derivatives of one kind or another), it becomes evident that *a priori* information is required (and employed explicitly or implicitly) about the error stream (Quantum Bit Error Rate, QBER) arising from the attenuation. For instance, if the attenuation in the communication channel varies during the key transfer protocol, the error stream also changes (even in the absence of an eavesdropper). Moreover, if the protocol implies the QBER constancy, no secrecy of the key transfer may be assured whatsoever. While the attenuation in optical-fiber quantum cryptosystems may be treated as being constant (for a single-mode optical fiber it is equal to $0.17-0.25$ dB km^{-1} at a wavelength of 1550 nm), in the transfer via open space this is clearly not so, because the state of the atmosphere is impossible to control. It is therefore desirable to have key distribution protocols that are immune to and guarantee key secrecy under variations of attenuation in the communication channel during the protocol time and whose secrecy would be independent of the *a priori* knowledge of attenuation strength. This problem, in our view, is serious enough and calls for a solution, because otherwise the absolute secrecy of quantum cryptography (the secrecy which is fully ensured by the fundamental quantum-mechanical prohibitions rather than by the technically limited capabilities of the eavesdropper) may be thrown into doubt.

All the aforementioned difficulties are related to the fact that the protocol secrecy is actually based only on the geometric properties of the state vectors of a quantum system in the Hilbert space $\mathcal{H}$. More precisely, on the impossibility of cloning (the no-cloning theorem [8]) an unknown quantum state and the principal certain indistinguishability of nonorthogonal quantum states (the Bennett theorem [9]). Roughly speaking, these protocols are formulated in the Hilbert space $\mathcal{H}$. The fact that all measurements and the distribution of quantum states occur in space – time is in no way used explicitly. In the distribution of a quantum state, attenuation takes place in space – time rather than in the Hilbert space. That is why to eliminate the problem of attenuation-caused secrecy loss requires involving other additional *basic* limitations that stem from the properties of quantum states and gaining information about them in space – time. The limitations stemming from only the geometric properties of quantum states in the Hilbert space have supposedly been exhausted with relation to the construction of quantum cryptographic protocols.

These additional basic and natural limitations are dictated by the special relativity theory. Furthermore, photons represent truly relativistic massless particles (the massless quantized field states) which travel at a maximum permissible speed. That is why in the development and realization of quantum cryptography in open space it would be unnatural to take no advantage of the additional possibilities offered by nature.

Below we briefly discuss quantum cryptosystems for key transfer via open space, which take advantage of the additional prohibitions stemming from special relativity, in addition to the limitations on the measurability of quantum states, stemming from quantum mechanics.

Since the fact of distribution of quantum states (*the key*) *in space – time is explicitly taken into account in the quantum cryptosystems discussed below, it is required to know beforehand the length of the quantum communication channel between the transmitting and receiving parts.*

Relativistic quantum cryptosystems retain secrecy for any attenuation in the communication channel. The magnitude of attenuation lowers only the key transfer rate but has no effect on its secrecy. Moreover, the key secrecy is guaranteed even for non-single-photon states. The scheme remains secret for an arbitrary average number of photons in the quantum state. According to calculations (for details, see Ref. [38]), the highest efficiency is achieved when the average number of photons is small, viz. $\mu = 1-3$. For these average occupation numbers, idle sendings are virtually absent (the vacuum component fraction in the coherent state is low). This signifies that the key generation rate is at least an order of magnitude higher than in schemes entirely based on the geometric properties of quantum states, which require attenuating laser radiation down to $\mu = 0.1-0.3$. An additional increase in the rate arises from the fact that the limitations from the side of the special relativity theory permit us to employ even orthogonal states, which does not require verifying the reconciliation of measurement bases, as in the BB84 protocol. Furthermore, since all actions of participants (both of the legitimate ones and the eavesdropper) are effected in space – time and the states are orthogonal, collective measurements of the eavesdropper do not offer him any advantages in comparison with individual measurements in every sending. Lastly, the system guarantees key secrecy even for an error level close to 50% in the received binary sequence (for details, see Ref. [38]). It is pertinent to note that the secrecy, for instance, for the BB84 protocol is ensured up to an error level of only 11% [30, 32].

Recall that error-free information transfer, actually error correction in the limit of asymptotically long sequences in a classical binary symmetric channel, is theoretically possible when the error probability does not exceed 50%. *In relativistic quantum cryptography, for an error level close to* 50% *it is possible not only to correct errors, but also to guarantee the secrecy of information* (*keys*) *transmitted by means of quantum states via open space.*

The only additional requirement imposed on relativistic quantum cryptosystems in comparison with nonrelativistic quantum cryptosystems based on nonorthogonal states is the knowledge of the length of the quantum communication channel, which, in our opinion, is a small penalty for those advantages which may be offered by relativistic quantum cryptography.

In quantum cryptosystems, the revelation of any attempts at eavesdropping is guaranteed by the following two basic, closely related quantum-mechanical prohibitions.

(1) Impossibility of the process

$$\begin{aligned} &|\varphi_0\rangle \otimes |A\rangle \mapsto |\varphi_0\rangle \otimes |\varphi_0\rangle \otimes |A_0\rangle\,, \\ &\qquad\qquad\qquad\qquad \langle\varphi_0|\varphi_1\rangle \neq 0\,. \\ &|\varphi_1\rangle \otimes |A\rangle \mapsto |\varphi_1\rangle \otimes |\varphi_1\rangle \otimes |A_1\rangle\,, \end{aligned} \qquad (1)$$

This prohibition against cloning an unknown quantum state is termed the no-cloning theorem.

(2) Impossibility of gaining information about one of the nonorthogonal states without their perturbation, i.e., forbid-

ding of the following process:

$$|\varphi_0\rangle \otimes |A\rangle \mapsto U\bigl(|\varphi_0\rangle \otimes |A\rangle\bigr) = |\varphi_0\rangle \otimes |A_0\rangle\,,$$
$$|A_0\rangle \neq |A_1\rangle, \quad (2)$$
$$|\varphi_1\rangle \otimes |A\rangle \mapsto U\bigl(|\varphi_1\rangle \otimes |A\rangle\bigr) = |\varphi_1\rangle \otimes |A_1\rangle\,,$$

where $|A\rangle$ is the state of the observer's device, and U is some unitary operator which describes the joint evolution of the state under investigation and the state of the device. These prohibitions are in essence one of the manifestations of the basic Heisenberg uncertainty principle relating to the impossibility of simultaneously measuring the observables to which there correspond noncommuting operators.

For orthogonal states, there are no prohibitions on their cloning or information extraction without their perturbation. In the framework of nonrelativistic quantum mechanics, to the observables $\rho_0 = |\varphi_0\rangle\langle\varphi_0|$ and $\rho_1 = |\varphi_1\rangle\langle\varphi_1|$ there correspond commutative measuring operators, which are orthogonal projectors $\mathcal{P}_{0,1} = |\varphi_{0,1}\rangle\langle\varphi_{0,1}|$ ($[\mathcal{P}_0, \mathcal{P}_1] = 0$). Restrictions (1) and (2) are in essence the geometric property of the state vectors $|\varphi_{0,1}\rangle$ of the quantum system in the Hilbert space of states. Unless some additional basic restrictions on the measurability of orthogonal quantum states are employed, they cannot be used for the purposes of quantum cryptography owing to certain distinguishability. The restrictions on the measurability of quantum states imposed by special relativity represent such additional basic restrictions.

For orthogonal states, there is no prohibition against certain distinguishing without their perturbation [9], or to be more precise, the theorem [9] states nothing about it. The statement that an orthogonal state 'passes' through an auxiliary system $|A\rangle$, interacts with it during the passage, and changes its state, which is frequently made in the interpretation of this theorem, does not correspond to the contents of the theorem. The theorem contains nothing of the kind, in the sense that it is purely geometric in nature and states that the state vector of the auxiliary system $|A\rangle$ may be unitarily turned, depending on the input vector $|\varphi_{0,1}\rangle$, and transferred to a new state $|A_0\rangle$ or $|A_1\rangle$ with no change of the input vector. In this case, it is implicitly assumed that the input vector $|\varphi_{0,1}\rangle$ is accessible as an integral object — that is, to perform the unitary transformation U requires having access to the entire space $\mathcal{H}_{\varphi_{0,1}}$ of states, in which the state carrier is nonzero, otherwise the transformation will not be unitary. The fact that in the proof there appears only the state vector as an integral object $|\varphi_{0,1}\rangle$ without inner coordinate 'filling' just means that the state vector participates 'as a whole' in the transformation.

For any real physical system, the Hilbert space $\mathcal{H}_{\varphi_{0,1}}$ is inevitably attached to the Minkowski space–time, in which a state possesses amplitude (the smoothing wave function). Therefore, access to the Hilbert space of states implies access to that domain of space–time, in which the state amplitude (the wave function) is nonzero. If only a part of such a domain is accessible, then even orthogonal states are impossible to reliably clone or distinguish. This is more or less obvious, since no process, including cloning or distinguishing, may have a higher outcome probability than the fraction of state normalization, which is gathered within the accessible spatio-temporal domain and thereby automatically in the accessible part of the Hilbert space. Roughly speaking, to clone with certainty and distinguish orthogonal states, they are required entirely and at once.

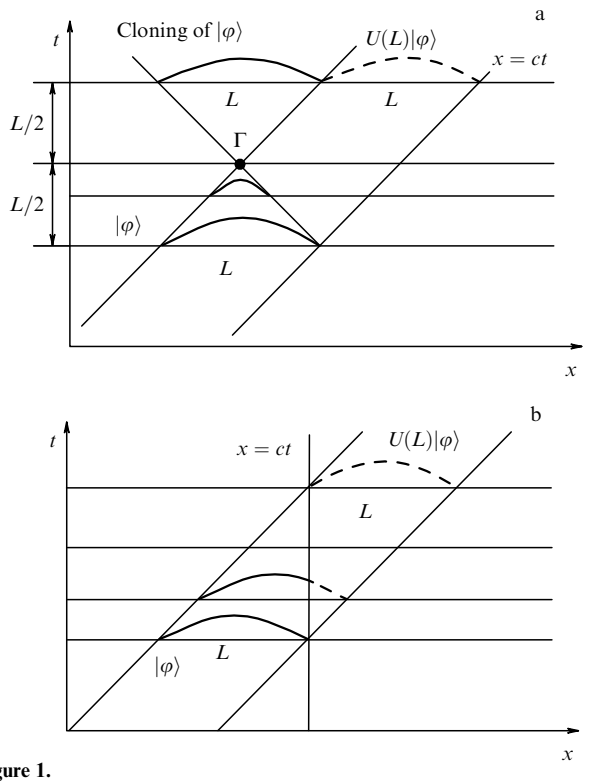

Figure 1.

So, when the amplitude of a state is nonzero in some finite domain of space–time, the words that the state is entirely accessible signify access to this domain. In nonrelativistic quantum mechanics, which imposes no restrictions on the limiting speed, access to any finite domain may be instantly obtained. In quantum field theory, which imposes restrictions on a limiting speed, access to the state as a whole may be obtained only when the lengthy state is preliminarily unitarily transformed to a state with an amplitude which is nonzero in only an arbitrarily small spatial domain. After that, advantage can be taken of the theorem [9]. According to the relativistic causality principle [39], this unitary transformation of the state defined in a finite spatio-temporal domain to a state localized in an arbitrarily small spatial domain may be effected in a finite time only. The minimum requisite time is determined from the condition that a part of the light cone relevant to the 'past' covers the initial spatial domain in which the state amplitude was nonzero (Fig. 1a). The vertex of a light cone resides in an arbitrarily strongly localized domain (at a point) to which the initial state amplitude is unitarily transformed. Each of the pairs of orthogonal states unitarily transformed to ('collected in') a localized domain may thereafter be cloned with certainty or distinguished. Since we are dealing with massless states of a quantized field (photons), which propagate at the maximum allowable speed, this unitary transformation and the subsequent cloning will result in a shift (delay) of the states in space–time relative to those in the case of their free evolution (propagation). This circumstance makes it possible to detect any attempts at eavesdropping. It is pertinent to note that the restrictions imposed on measurements in the relativistic domain were first investigated by L D Landau and R Peierls [40] and subsequently by Niels Bohr and L Rosenfeld [41].[2]

[2] The problem of state localization in the relativistic domain is of significance (in this connection see Refs [42–47]).

In other words, for orthogonal states of the massless quantized field, the no-cloning theorem looks like this. Orthogonal states may be cloned with a probability arbitrarily close to unity. The cloning results in production of states with amplitudes of the same form but being shifted (translated in space – time). That is, a weaker process than in the nonrelativistic case is allowed in expression (1). Therefore, we have

$$\begin{aligned} &|\varphi_0\rangle \mapsto \big(U_L|\varphi_0\rangle\big) \otimes \big(U_L|\varphi_0\rangle\big)\,, \\ &|\varphi_1\rangle \mapsto \big(U_L|\varphi_1\rangle\big) \otimes \big(U_L|\varphi_1\rangle\big)\,. \end{aligned} \tag{3}$$

Here, U_L is the translation operator along the branch of the light cone in space – time, $L = \Delta(x - t)$ is the dimension of the domain in which the state amplitude is nonzero [for brevity we assume that both states are nonzero in the same spatio-temporal domain but differ in amplitude form $\varphi_{0,1}(x - t)$].

Similarly modified is the theorem of Ref. [9] about distinguishing orthogonal states — only a weaker process in comparison with that in the nonrelativistic case (2) is allowed:

$$\begin{aligned} &|\varphi_0\rangle \otimes |A\rangle \mapsto \big(U_L|\varphi_0\rangle\big) \otimes |A_0\rangle\,, \\ &|\varphi_1\rangle \otimes |A\rangle \mapsto \big(U_L|\varphi_1\rangle\big) \otimes |A_1\rangle\,, \end{aligned} \qquad |A_0\rangle \neq |A_1\rangle\,. \tag{4}$$

The aforesaid is conveniently exemplified by the diagrams given in Fig. 1.

Since the amplitude of massless quantized field states propagating in one direction of the x-axis depends only on the difference $x - t$, it is possible to fix the time and treat the coordinate as a variable, or vice versa. We consider both cases. These two cases exhaust all the situations. Assume that one of the orthogonal states with an amplitude $\varphi(x - t)$ is given, and they propagate at the speed of light ($c = 1$; the subscript standing for the state 0 or 1 is for the moment omitted for brevity). Let the state be concentrated in the domain L in the sense that $\int_L \big|\varphi(x - t_0)\big|^2 \,\mathrm{d}x \approx 1$, where $\varphi_{0,1}(x - t_0)$ is the amplitude at the time section t_0.

To obtain *at once all values of the state amplitude for all x at a point in time t_0* in the domain where it is nonzero requires effecting a unitary transformation of the whole state at once. Let the unitary transformation of the state amplitude be $U\varphi_{0,1}(x - t_0) = \tilde{\varphi}_{0,1}(x' - t)$ $(t > t_0)$, then the new state amplitude $\tilde{\varphi}(x' - t)$ may be nonzero in a smaller spatial domain. The minimal domain dimension in x' by the point in time t is dictated, in essence, by the relativistic causality principle which was formulated in its final form by N N Bogolyubov [39]. The matrix elements of the unitary operator are nonzero only when the points (x, t_0) and (x', t) lie within the 'past' part of the light cone emanating from the point Γ and covering the domain in which the state amplitude is nonzero at the point in time t_0. By a point in time no earlier than L, the amplitude of the initial state may be unitarily transformed to a state with an amplitude arbitrarily strongly localized about Γ. It is basically significant that this will be *another* state, a state different from the initial one $\varphi(x - t_0)$. Accessible by the point in time Γ are the values of state amplitude for all x at once (instantaneously). It is now possible to instantaneously obtain the measurement outcome and have complete (with the probability 1) information about the state. If the pair of initial states is orthogonal, by means of a unitary transformation it is possible to obtain also a pair of orthogonal states by the point in time Γ and, therefore, reliably distinguish one from the other (it is now possible to take advantage of the theorem of Ref. [9] about the certain distinguishability of orthogonal states). We emphasize once again that these orthogonal states are *different* from the initial ones. The 'recovery' or cloning of the state may also be realized through the inverse unitary transformation 'directed' forward in time. The state with an amplitude of the same form as the initial one may be obtained by a point in time no earlier than the point defined by relativistic causality. The amplitude of the state with the same form as the initial one is located in the forward part of the light cone emanating from the point Γ. The resultant state is also *different* from the initial one in the sense that it is retarded in time relative to the initial state, which would have travelled forward along x by the point in time L by precisely the value of L had there been no attempts to clone it or obtain information about it (see Fig. 1a). So far we have been dealing with gaining information with the probability 1 about states in the channel. The same reasoning applies to gaining information with a probability lower than unity. The delay will be shorter than L in this case (see Fig. 1).

Similar reasoning also applies to the nonrelativistic case. If the restrictions of the special theory of relativity are neglected, in the previous consideration one should discard that part which appeals to the light cone. In this case, the unitary transformations may formally be effected instantaneously, and even the explicit presence of a coordinate can be eliminated from consideration, retaining implicitly only the fact that the states are entirely accessible under a unitary transformation (the entire spatial region is instantaneously accessible).

Similar reasoning may be employed when a state is unitarily transformed to the state of an auxiliary localized system. An example of such a unitary transformation is provided by the 'stopping' of light [48]. This unitary transformation transfers the photon field state to a vacuum state due to its masslessness and the impossibility of possessing the zero propagation velocity, while the state of an atomic system is transformed to some new state. Being unitary, the transformation also requires access to all values of the photon packet amplitude at the point of atomic system localization. This access is achieved in the natural way during propagation of the wave packet at the speed of light and its arrival at the localized atomic system ('entry' of the whole packet into the atomic system). Where obtaining a result with the probability 1 is involved, this process also requires a time L (the single-photon packet should completely 'enter' the atomic system). As this takes place, the photon field finds itself in a *different — vacuum — state*, while the auxiliary system finds itself in a new state, depending on the input photon state. By the point in time L with the probability 1 it is possible to find out what state it is and prepare the same one with a delay L, which is inevitable in this case, unlike the case of free propagation of the initial wave packet (see Fig. 1b).

Therefore, any acquisition of information about one of the orthogonal states inevitably leads to their modification — translation in space – time (*delay*).

For the subsequent discussion it is significant that no evolution of a massless quantized field interacting with the environment (other quantum and classical degrees of freedom in the communication channel) can result in state 'squeezing' in the sense that the state normalization would be accumulated in a spatial domain going beyond the light cone and being smaller than that in the free propagation (see Fig. 2). As

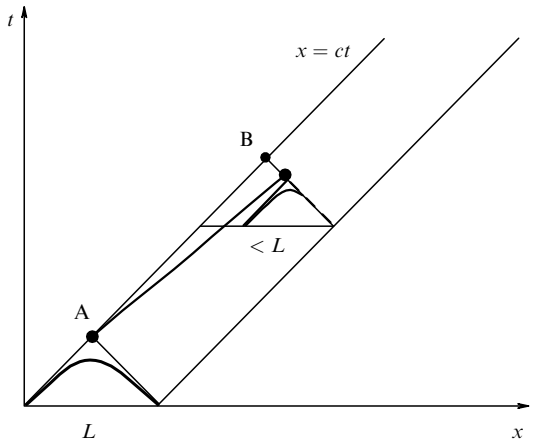

Figure 2.

a rule, this interaction will have the effect that the state will be mixed, but the carrier of the density matrix in space–time cannot be 'squeezed' and drawn out of the light cone (see Fig. 2). Otherwise, that would allow conveying of information by means of quantum states at a supraluminal speed. Indeed, let there be one of a pair of orthogonal quantum states (see Fig. 2). Participant A may extract classical information from the quantum state no earlier than at the point in time defined by the constraint that a part of the light cone relevant to the 'past' covers the state amplitude. After that he can transmit the now-classical information to participant B. This transmission cannot be effected faster than the speed of light [the observers are connected by a branch of the light cone (see Fig. 2)]. Were the quantum state in the channel able to 'squeeze' in the course of its evolution in such a way that, on covering the state by a part of the light cone relevant to the 'past', the vertex of a cone found itself in the domain spatially like to the light cone with a vertex at point A, with one of the cone branches passing through point B, then the observer at point B would be able to extract classical information from the quantum state earlier than participant A could transmit it with the speed of light, because the vertex of a light cone covering the 'squeezed' quantum state went out into a spacelike domain.

From the standpoint of cryptography, the aforesaid signifies that the noise in the channel does not permit the eavesdropper to either clone or gain information about the state earlier than it is dictated by the restrictions imposed by relativistic causality and quantum mechanics (*actually, the quantum field theory*).

Invoking new fundamental physical principles in quantum cryptography enables formulation of a new approach to assuring key transfer secrecy, which eliminates the difficulties encountered in nonrelativistic quantum cryptography (for details, see Ref. [38]). Suchlike quantum cryptosystems would naturally be termed relativistic ones.

We briefly consider here the theoretical limit of the secret key generation rate attainable in quantum cryptography [3] via a quantum communication channel with a finite transmission bandwidth W.

[3] As of now, the key distribution rate in quantum cryptography is determined not by fundamental limitations but by the technology level, or more specifically, by the time it takes an avalanche photodiode to revert to the initial state upon recording a photon, and by effects.

In the classical case, when a signal is described by a time function $x(t)$, the number of information bits transferable via a channel with a finite frequency bandwidth is, according to the famous Kotel'nikov sampling theorem proven in 1933 [49] (see the Supplement to N V Kotel'nikova's report in this issue), determined by the number of independent degrees of freedom of the signal, in whose value it is possible to encode the information transmitted. In our digital age, the sampling theory 'operates' in any facility that processes or transmits information in a digital form.

A classical signal with a finite frequency band is described by a time function $x(t)$. In a finite time interval $(-T, T)$, the signal $x(t)$ is, as first shown by Kotel'nikov [49], defined by $2WT$ degrees of freedom in the sense that in the expansion in terms of the orthogonal system of functions:

$$x(t) = \sum_n x_n \theta_n(t)\,, \tag{5}$$

it would suffice to restrict the series to $2WT$ terms, for which

$$\int_{-T}^{T} \theta_n(t)\,\theta_m(t)\,\mathrm{d}t = \delta_{nm}\lambda_n(WT), \quad \lambda_n(WT) \approx 1\,. \tag{6}$$

For basis functions $\theta_n(t)$, Kotel'nikov employed the so-called reference functions [49]

$$\theta_n(t) = \frac{\sin W(t - n\pi/W)}{W(t - n\pi/W)}\,. \tag{7}$$

The basis of reference functions possesses a remarkable property: the expansion coefficients x_n in terms of this basis are equal to the values of the signal $x(t)$ itself at the reference points in time. This has the following implication: to describe a continuous signal at any point in time it would suffice to know its values at only $2WT$ points in time.

Below we will conveniently employ other basis functions. The number of these functions localized primarily in the window $(-T, T)$ remains the same in this case. Moreover, these functions also emerge in the quantum case, where they play the part of single-particle amplitudes (wave functions) for photons which are most strongly localized in the time window $(-T, T)$.

The orthogonality of basis functions with the carrier in a finite frequency band W leads to the condition

$$\begin{aligned}
&\int_{-T}^{T} \theta_n(t)\,\theta_m(t)\,\mathrm{d}t \\
&\quad = \frac{1}{\pi}\int_{k\leqslant|W|}\int_{k'\leqslant|W|} \theta_n(k)\,\frac{\sin(k-k')T}{k-k'}\,\theta_m(k')\,\mathrm{d}k\,\mathrm{d}k', \\
&\theta_n(k) = \frac{1}{2\pi}\int_{-\infty}^{\infty} \theta_n(t)\exp(-\mathrm{i}kt)\,\mathrm{d}t\,.
\end{aligned} \tag{8}$$

The basis functions are orthogonal if they satisfy the following integral equation

$$\lambda_n(WT)\,\theta_n(k) = \frac{1}{\pi}\int_{k\leqslant|W|} \frac{\sin(k-k')T}{k-k'}\,\theta_n(k')\,\mathrm{d}k'\,. \tag{9}$$

The eigenvalues depend only on the product WT and form an infinite series

$$1 > \lambda_1(WT) > \lambda_2(WT) > \ldots > 0\,.$$

The degree of localization of the nth function squared in the time window $(-T, T)$ is determined by the eigenvalue

$$\int_{-T}^{T} \theta_n^2(t)\,\mathrm{d}t = \lambda_n(WT)\,. \tag{10}$$

The integral equation (9) defines the so-called prolate spheroidal functions [50]. The eigenvalues possess the remarkable property that for large WT ($WT \gg 1$) they break up into two groups: one with numbers $n < 2WT$, for which $\lambda_n(WT) \approx 1$, and the other with numbers $n > 2WT$, for which $\lambda_n(WT) \approx 0$. The passage from one behavior to the other occupies a domain which measures $\approx \ln(4\pi WT)$ in number, i.e., for any $\varepsilon > 0$, one has

$$\lim_{WT\to\infty} \lambda_{2WT(1-\varepsilon)}(WT) = 1\,, \qquad \lim_{WT\to\infty} \lambda_{2WT(1+\varepsilon)}(WT) = 0\,. \tag{11}$$

This signifies that for large WT there exist no more than $2WT(1-\varepsilon)$ orthogonal (distinguishable) functions whose contribution to the temporal window $(-T, T)$ tends to unity. When use is made of more than $2WT(1+\varepsilon)$ degrees of freedom, among them there will be states which make a vanishingly small contribution to the temporal window $(-T, T)$. For large WT, the signal $x(t)$ in a finite frequency band is described on a finite time interval by no more than $2WT$ independent (orthogonal and distinguishable) degrees of freedom and may by defined by $2WT$ independent expansion coefficients x_n.

When a classical source with a finite frequency band W generates signals localized in the time window $(-T, T)$ in such a way that the expansion coefficients are prescribed in accordance with a given probability distribution $p(x_n)$ on the set of these coefficients x_n (the values of signal amplitudes), the source entropy is defined by the quantity

$$\begin{aligned} &I\bigl(WT, p(x_n)\bigr) = 2WTH\bigl(p(x_n)\bigr)\,,\\ &H\bigl(p(x_n)\bigr) = -\sum_n p(x_n)\log p(x_n)\,. \end{aligned} \tag{12}$$

Furthermore, when these signals are transmitted via a perfect (noise-free) physical communication channel, for instance, having the same transmission frequency band W, the source entropy (12) coincides in essence with the mutual information between the input and output of this communication channel. Then, the transmission capacity per unit time (source + physical communication channel + receiver) is defined as

$$C = \lim_{T\to\infty} \frac{1}{2T} \max_{\{p(x_n)\}} I\bigl(WT, p(x_n)\bigr) = W \max_{\{p(x_n)\}} H\bigl(p(x_n)\bigr)\,. \tag{13}$$

We will need the following qualitative considerations to compare the classical and quantum cases. In the framework of classical physics there are no formal prohibitions against variations in the expansion coefficients x_n [the amplitudes of orthogonal basis functions $\theta_n(t)$] with an arbitrarily small discreteness (continuously). Since the classical signal intensity x_n^2, for instance, for an electromagnetic field, in every separate mode $\theta_n(t)$ is, correct to a factor $\approx \hbar W$, the number of photons in this mode, changes in signal level may take place with a finite discreteness. To encode information into x_n values requires at least two values ($x_n^2 \propto N_{\max}$, $N_{\max}$ is the highest number of possible x_n^2 values). The total number of different values for all modes equals $(\sqrt{N_{\max}})^{2WT}$. If every value is selected with equal probability, the source entropy (12) is given by

$$I\bigl(WT, p(x_n)\bigr) = 2WT\log\bigl(\sqrt{N_{\max}}\bigr)\,. \tag{14}$$

The transmission capacity (8) per unit time for the lowest signal level ($N_{\max} = 2$) is defined as

$$C = W\,. \tag{15}$$

Formula (15), *which is in essence an alternative representation of Kotel'nikov's sampling theorem, defines the amount of information in bits per one degree of freedom that can be transmitted per unit time*.

Strictly speaking, the formulas are inapplicable when the mode occupation numbers are small.

In the subsequent discussion our concern will be with the transmission capacity in the single-photon regime (the mode occupation numbers are equal to unity). It is precisely this quantity that will define the key generation rate in quantum cryptography via a channel with a finite frequency band W.

The above reasoning was needed to qualitatively compare the classical and quantum cases. Our task will actually reduce to calculating for a source with a finite frequency band W the number of possible orthogonal multiphoton states localized in the time window $(-T, T)$. First we consider single-photon states at the source output, which then travel in one direction ($k > 0$) and have a carrier in a finite frequency band W ($k \in [0, W]$). The polarization degrees of freedom will be ignored in the encoding into different forms of state amplitudes, again for the sake of a closer analogy with the classical case. For simplicity of calculations we put $c = \hbar = 1$. Then we have

$$|\varphi^e\rangle = \int_0^W \frac{\mathrm{d}k}{k}\,\varphi\bigl(k, k_0 = |k|\bigr)\,a^+(k)|0\rangle = \int_{-\infty}^{\infty} \mathrm{d}\tau\,\varphi(\tau)|\tau\rangle\,, \tag{16}$$

where $\varphi(k, k)$ ($k > 0$) and $\varphi(\tau)$ are the respective amplitudes of a single-photon packet in the momentum and spatio-temporal representations:

$$\begin{aligned} &\varphi(\tau) = \frac{1}{2\pi}\int_0^W \frac{\mathrm{d}k}{\sqrt{k}}\exp(-\mathrm{i}k\tau)\,\varphi(k, k)\,,\\ &|\tau\rangle = \int_0^W \frac{\mathrm{d}k}{\sqrt{k}}\exp(\mathrm{i}k\tau)\,|k\rangle\,, \qquad |k\rangle = a^+(k)|0\rangle\,. \end{aligned} \tag{17}$$

For a massless field, $\tau = x - t$ depends only on the difference between the coordinate and time; and so if a measurement result was obtained in the neighborhood of a point x at an instant of time t, the same result may be obtained at a point x' at the instant of time $t' = t + (x' - x)$. Below, when mentioning a time window, we will bear in mind that $(-T, T)$ signifies $[-(x-t), (x-t)]$.

We have to select the amplitude (wave function) of a single-photon packet with a carrier in a finite frequency band W in such a way as to maximize its normalization in the spatio-temporal domain, namely, in the $(-T, T)$ window. Formally, the degree of localization is described by the measurement in this window. Any measurement on the single-photon packet made in the temporal window is described by expansion of unity in the single-particle sub-

space, which is of the form

$$I^{(1)} = \int_0^W \frac{\mathrm{d}k}{k}\,|k\rangle\langle k| = I^{(1)}(T) + I^{(1)}(\overline{T}) = \int_{-T}^{T} \frac{\mathrm{d}\tau}{2\pi}\,|\tau\rangle\langle\tau| + \int_{-(\infty,\infty)/(-T,T)} \frac{\mathrm{d}\tau}{2\pi}\,|\tau\rangle\langle\tau|\,. \tag{18}$$

In view of expressions (12) and (13), the operator corresponding to the temporal window $(-T, T)$ is represented as

$$I^{(1)}(T) = \sum_{n=1}^{\infty} \lambda_n(WT)|\theta_n\rangle\langle\theta_n|\,, \qquad |\theta_n\rangle = \int_0^W \frac{\mathrm{d}k}{k}\,\theta_n(k)|k\rangle\,. \tag{19}$$

The functions $\theta_n(k)$ themselves are the eigenfunctions of an integral equation which differs from Eqn (9) only in that the integration is performed over the segment $[0, W]$. The number of functions localized in the temporal window $(-T, T)$ will equal WT. The vectors $|\theta_n\rangle$ are in essence the eigenvectors of the operator $I^{(1)}(T)$ — the operator is diagonal in the basis of these vectors. Any measurement on the initial state, when the outcomes in only the temporal window are accessible, is equivalent to measurements on the effective density matrix:

$$\rho(T) = \sum_{n,n'} \lambda_n(WT)\,\lambda_{n'}(WT)|\theta_n\rangle\langle\theta_n|\varphi\rangle\langle\varphi|\theta_{n'}\rangle\langle\theta_{n'}| + \mathrm{Tr}\left\{I^{(1)}(\overline{T})|\varphi\rangle\langle\varphi|\right\}|?\rangle\langle?|\,. \tag{20}$$

Here, we introduced the formal state $|?\rangle$ which is orthogonal to all states and describes the outcomes beyond the temporal window. These outcomes correspond to a situation wherein the equipment did not actuate inside the window whatsoever. Taking into account these outcomes, to which an inconclusive result should be assigned, the effective density matrix possesses a unit spur. For large WT, it is possible to select one of WT orthogonal (distinguishable) single-photon states, which is localized in the $(-T, T)$ window with a probability arbitrarily close to unity [$\lambda_n(WT) \approx 1$] and which possesses in this window the effective density matrix

$$\rho_n(T) = \lambda_n(WT)|\theta_n\rangle\langle\theta_n| + \big(1 - \lambda_n(WT)\big)|?\rangle\langle?|\,, \qquad 1 \leqslant n \leqslant WT\,. \tag{21}$$

Let the source generate in the working temporal window the $(N = WT)$-photon states of the form

$$|\theta_{n_1};\ldots;\theta_{n_N}\rangle = \int_0^W \ldots \int_0^W \frac{\mathrm{d}k_1}{k_1}\ldots\frac{\mathrm{d}k_N}{k_N}\,\theta_{n_1}(k_1)\ldots\theta_{n_N}(k_N)|k_1,\ldots,k_N\rangle\,,$$
$$|k_1,\ldots,k_N\rangle = a^+(k_1)\ldots a^+(k_N)|0\rangle\,, \tag{22}$$

where the generalized basis vectors are completely symmetric with respect to particle permutations:

$$|k_1,\ldots,k_N\rangle = \sqrt{\frac{k_1 k_2\ldots k_N}{N!}}\sum_{\{j\}}\delta(k_1 - q_{j_1})\ldots\delta(k_N - q_{j_N})\,, \tag{23}$$

where the symbol $\{j\}$ implies that summation is performed over all permutations. Let us now construct the $(N = WT)$-photon density matrices. In this case, the occupation number of each single-particle mode is equal to unity. The set of vectors in expression (17) with different indices is made up of the eigenvectors of the operator $I^{(N)}(T)$ in the $(N = WT)$-photon subspace, similarly to the single-photon case. We have

$$I^{(N)} = \int_0^W \ldots \int_0^W \frac{\mathrm{d}k_1}{k_1}\ldots\frac{\mathrm{d}k_N}{k_N}|k_1,\ldots,k_N\rangle\langle k_1,\ldots,k_N| = I^{(N)}(T) + I^{(N)}(\overline{T}), \tag{24}$$

$$I^{(N)}(T) = \int_{-T}^{T} \ldots \int_{-T}^{T} \frac{\mathrm{d}\tau_1}{2\pi}\ldots\frac{\mathrm{d}\tau_N}{2\pi}|\tau_1;\ldots;\tau_N\rangle\langle\tau_1;\ldots;\tau_N| = \sum_{n_1,\ldots,n_N=1}^{\infty} \lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)|\theta_{n_1};\ldots;\theta_{n_N}\rangle\langle\theta_{n_1};\ldots;\theta_{n_N}|\,. \tag{25}$$

Let us calculate the number of orthogonal $(N = WT)$-photon states. Were $N = WT$ photons distinguishable, the number of orthogonal $(N = WT)$-photon vectors in the time window $(-T, T)$, localized in it with a nearly unit probability, would be equal to N^N (neglecting the polarization degrees of freedom). By the boson (photon) identity principle, the number of such vectors, which is conveniently denoted as $2^{M(WT)}$, is equal to the number of distributions of $N = WT$ identical particles over $N = WT$ states. Therefore, we arrive at [51]

$$2^{M(WT)} = \frac{(N + N - 1)!}{(N-1)!N!}\,, \qquad N = WT, \tag{26}$$

and for large N, in view of the Stirling formula ($N! \approx (N/e)^N\sqrt{2\pi N}$), we obtain

$$\log 2^{M(WT)} = 2N\log 2 = 2WT\,. \tag{27}$$

Let the source generate with equal probability one of the $2^{M(WT)}$ orthogonal $(N = WT)$-photon states in every working time window. If the source operates for a sufficiently long time, the statistical ensemble, into which classical information may be encoded, is described by the density matrix

$$\rho\big(M(WT)\big) = \frac{1}{2^{M(WT)}}\sum_{n_1,\ldots,n_N}|\theta_{n_1};\ldots;\theta_{n_N}\rangle\langle\theta_{n_1};\ldots;\theta_{n_N}|\,. \tag{28}$$

The von Neumann ensemble entropy is highest for an equiprobable sampling of vectors. The information in the finite time window $(-T, T)$ is extracted from the effective density matrix

$$\rho(T) = \frac{1}{2^{M(WT)}} \times \sum_{n_1,\ldots,n_N}\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)|\theta_{n_1};\ldots;\theta_{n_N}\rangle\langle\theta_{n_1};\ldots;\theta_{n_N}| + \frac{1}{2^{M(WT)}}\sum_{n_1,\ldots,n_N}\big(1 - \lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)\big)|?\rangle\langle?|\,. \tag{29}$$

For large WT, it is impossible to construct a statistical ensemble comprising more than $2^{M(WT)}$ orthogonal $(N = WT)$-photon states. The classical information which may be encoded into the ensemble $\rho\big(M(WT)\big)$ and extracted from $\rho(T)$ (29) is given by the quantity $\chi\big(\rho(T)\big)$ which follows from the fundamental inequality first derived by A S Kholevo (for details, see Ref. [52]). Since the states $|\theta_{n_1};\ldots;\theta_{n_N}\rangle$ and $|?\rangle$ are pure, $\chi\big(\rho(T)\big)$ coincides with the von Neumann entropy

for $\rho(T)$, we find that

$$\begin{aligned}\chi\bigl(\rho(T)\bigr) &= -\mathrm{Tr}\left\{\rho(T)\log\rho(T)\right\}\\ &= -\sum_{n_1,\ldots,n_N}\frac{\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)}{2^{M(WT)}}\\ &\quad\times\log\left(\frac{\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)}{2^{M(WT)}}\right)\\ &\quad-\sum_{n_1,\ldots,n_N}\left(\frac{1-\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)}{2^{M(WT)}}\right)\\ &\quad\times\log\left(\frac{1-\lambda_{n_1}(WT)\ldots\lambda_{n_N}(WT)}{2^{M(WT)}}\right). \qquad (30)\end{aligned}$$

The transmission capacity per unit time is defined by the limit similar to formula (15) applied in the classical case. Taking into account that the contribution of the second sum in expression (30) tends to zero, we obtain

$$C=\lim_{T\to\infty}C_T,\qquad C_T=\frac{\log\left(2^{M(WT)}\right)}{2T}=\frac{M(WT)}{2T}=W. \quad (31)$$

During the time window, the source generates $(N=WT)$-photon states in such a way that the number of photons at the source output per unit time equals $\sim W$, and the energy per photon $\sim\hbar W$. Accordingly, the number of photons in the time window $(-T,T)$ is equal to WT (precisely the number and not the average number of photons, because the states $|\theta_{n_1};\ldots;\theta_{n_N}\rangle$ in expression (22) are the eigenvectors of the operator of the number of photons that correspond to the particle eigenvalue $N=WT$).[4] The power at the source output is constant and proportional to $(\hbar W)W$. The source minimality in the quantum case signifies that the number of orthogonal single-particle amplitudes $\theta_n(t)$, which make up the particle-permutation symmetric $(N=WT)$-photon amplitude, amount to WT, and the number of photons are WT, i.e., the occupation number in terms of an individual single-particle amplitude is equal to 1.

In the classical case, information is encoded into the values of the amplitudes (roughly, into the number of photons) in orthogonal modes, and in the quantum case into different orthogonal multiphoton states [53]. The latter are, by virtue of photon identity, fundamentally entangled inside every temporal window $2T$. This quantum source coding may be regarded as the quantum analog of Kotel'nikov's sampling theorem, when the single-particle mode occupation numbers are brought to the single-photon level.

The surprising thing is that the transmission capacity per unit time per one degree of freedom in the classical case (15), which follows from Kotel'nikov's sampling theorem, 'literally' coincides with the similar transmission capacity in the quantum case (31). However, the ways of encoding turn out to be different in the classical and quantum cases.

In summary, it is pertinent to note that the emergence of new avenues in the realm of confidential information transmission is a natural, logical development of the ideas conceived by the founders of this realm.

References

1. Kotel'nikov V A, Classified Report (1941)
2. Shannon C E "Communication theory of secrecy systems" *Bell Syst. Technol. J.* **28** 656 (1949)
3. Vernam G S "Cipher printing telegraph systems for secret wire and radio telegraphic communications" *J. Am. Inst. Elect. Eng.* **55** 109 (1926)
4. Wiesner S *SIGACT News* **15** (1) 78 (1983)
5. Diffie W, Hellman M "New directions in cryptography" *IEEE Trans. Inform. Theory* **IT-22** 644 (1976)
6. Rivest R L, Shamir A, Adleman L "A method for obtaining digital signatures and public-key cryptosystems" *Commun. ACM* **21** 120 (1978)
7. Bennett C H, Brassard G "Quantum cryptography: public-key distribution and coin tossing", in *Proc. of IEEE Intern. Conf. on Computers Systems, and Signal Processing, Bangalore, India, December 1984* (New York: IEEE Press, 1984) p. 175
8. Wootters W K, Zurek W H "A single quantum cannot be cloned" *Nature* **299** 802 (1982)
9. Bennett C H *Phys. Rev. Lett.* **68** 3121 (1992); Bennett C H, Brassard G, Mermin N D *Phys. Rev. Lett.* **68** 557 (1992)
10. "Informatsionnaya tekhnologiya. Kriptograficheskaya zashchita informatsii. Funktsiya kheshirovaniya" ("Information technology. Cryptographic information protection. Hash function"), Gosudarstvennyi Standart Rossiiskoi Federatsii (State Standard of the Russian Federation), GOST R 34.11-94 (Introduced 01.01.95)
11. Bennett C H, Brassard G, Crépeau C, Maurer U M "Generalized privacy amplification" *IEEE Trans. Inform. Theory* **41** 1915 (1995)
12. Carter J L, Wegman M N "Universal classes of hash functions" *J. Comput. Syst. Sci.* **18** 143 (1979)
13. Muller A, Breguet J, Gisin N *Europhys. Lett.* **23** 383 (1993); Muller A, Zbinden H, Gisin N *Nature* **378** 449 (1995); *Europhys. Lett.* **33** 335 (1996)
14. Marand Ch, Townsend P D *Opt. Lett.* **20** 1695 (1995); Townsend P D *Nature* **385** 47 (1997); *IEEE Photon. Technol. Lett.* **10** 1048 (1998)
15. Hughes R J et al., in *Advances in Cryptology — CRYPTO'96: 16th Annual Intern. Cryptology Conf., Santa Barbara, Calif., USA, August 1996. Proceedings* (Lecture Notes in Comput. Sci., Vol. 1109, Ed. N Koblitz) (Heidelberg: Springer-Verlag, 1996) p. 329; Hughes R J, Morgan G L, Peterson C G *J. Mod. Opt.* **47** 533 (2000)
16. Sun P C, Mazurenko Y, Fainman Y *Opt. Lett.* **20** 1062 (1995); Mazurenko Yu T, Giust R, Goedgebuer J P *Opt. Commun.* **133** 87 (1997); Molotkov S N *Zh. Eksp. Teor. Fiz.* **114** 526 (1998) [*JETP* **87** 288 (1998)]
17. Grosshans F et al. *Nature* **421** 238 (2003)
18. Stucki D et al. *New J. Phys.* **4** 41 (2002); quant-ph/0203118
19. Bennett C H et al. *J. Cryptology* **5** 3 (1992)
20. Hughes R J, Morgan G L, Peterson C G *J. Mod. Opt.* **47** 533 (2000)
21. Kosaka H et al. *Electron. Lett.* **39** 1199 (2003); quant-ph/0306066
22. Kimura T et al. *Jpn. J. Appl. Phys.* **43** L1217 (2004); quant-ph/0403104
23. Bethune D S, Risk W P *New J. Phys.* **4** 42 (2002)
24. Bethune D S, Navarro M, Risk W P *Appl. Opt.* **41** 1640 (2002); quant-ph/0104089
25. Elliott C, Pearson D, Troxel G, quant-ph/0307049
26. Rarity J G et al. *New J. Phys.* **4** 82 (2002)
27. Hughes R J et al. *New J. Phys.* **4** 43 (2002); quant-ph/0206092
28. Kurtsiefer C et al. *Proc. SPIE* **4917** 25 (2002)
29. Acín A, Gisin N, Scarani V *Phys. Rev. A* **69** 012309 (2004); quant-ph/0302037
30. Mayers D, Yao A, quant-ph/9802025
31. Biham E et al., quant-ph/9912053
32. Shor P W, Preskill J *Phys. Rev. Lett.* **85** 441 (2000); quant-ph/0003004
33. Tamaki K, Koashi M, Imoto N *Phys. Rev. A* **67** 032310 (2003); quant-ph/0212161
34. Lütkenhaus N *Phys. Rev. A* **61** 052304 (2000)
35. Brassard G et al. *Phys. Rev. Lett.* **85** 1330 (2000)
36. Gilbert G, Hamrick M "Practical quantum cryptography: a comprehensive analysis (Part I)", Mitre Technical Report, MTR00W0000052 (McLean, VA: Mitre Corporation, 2000); quant-ph/0009027
37. Beveratos A et al. *Phys. Rev. Lett.* **89** 187901 (2002); quant-ph/0206136
38. Molotkov S N *Zh. Eksp. Teor. Fiz.* **126** 771 (2004) [*JETP* **99** 669 (2004)]

[4] Strictly speaking, by WT is everywhere meant its integral part $[WT]$.

39. Bogolyubov N N, Shirkov D V *Vvedenie v Teoriyu Kvantovannykh Polei* (Introduction to the Theory of Quantized Fields) (Moscow: Nauka, 1973) [Translated into English (New York: John Wiley, 1980)]
40. Landau L D, Peierls R *Z. Phys.* **69** 56 (1931) [Translated into Russian, in Landau L D *Sobranie Trudov* (Collected Works) Vol. 1 (Moscow: Nauka, 1969) p. 56]; *Z. Phys.* **62** 188 (1930) [Translated into Russian, in Landau L D *Sobranie Trudov* (Collected Works) Vol. 1 (Moscow: Nauka, 1969) p. 33]
41. Bohr N, Rosenfeld L *Kgl. Danske Vidensk. Selskab. Math.-Fys. Medd.* **12** (8) 3 (1933) [Translated into English, in *Quantum Theory and Measurement* (Eds J A Wheeler, W H Zurek) (Princeton, NJ: Princeton Univ. Press, 1983) p. 470; translated into Russian, in Bohr N *Sobranie Nauchnykh Trudov* (Collected Scientific Works) Vol. 1 (Moscow: Nauka, 1969) p. 39]
42. Jaffee A M *Phys. Rev.* **158** 1454 (1967)
43. Hegerfeldt G C *Phys. Rev. D* **10** 3320 (1974); Hegerfeldt G C, Ruijsenaars S N M *Phys. Rev. D* **22** 377 (1980)
44. Kirzhnits D A *Usp. Fiz. Nauk* **90** 129 (1966) [*Sov. Phys. Usp.* **9** 692 (1967)]
45. Paley R E A C, Wiener N *Fourier Transforms in the Complex Domain* (New York: American Mathematical Society, 1934) [Translated into Russian (Moscow: Nauka, 1964)]
46. Bialynicki-Birula I *Phys. Rev. Lett.* **80** 5247 (1998)
47. Newton T D, Wigner E P *Rev. Mod. Phys.* **21** 400 (1949)
48. Fleischhauer M, Lukin M D *Phys. Rev. Lett.* **84** 5094 (2000)
49. Kotel'nikov V A, in *Vsesoyuznyi Energeticheskii Komitet. Materialy k I Vsesoyuznomy S'ezdu po Voprosam Tekhnicheskoi Rekonstruktsii Dela Svyazi i Razvitiya Slabotochnoi Promyshlennosti* (All-Union Energy Committee. Materials prepared for the I All-Union Congress on the Technical Reconstruction of Communication Facilities and the Progress in Low-Currents Industry) (Moscow: Upravlenie Svyazi RKKA, 1933) pp. 1 – 19; reprint: "O propusknoi sposobnosti 'efira' i provoloki v elektrosvyazi" ("On the transmission capacity of 'ether' and wire in electric communications") (Moscow: Institut Radiotekhniki i Elektroniki MEI (TU), 2003)
50. Slepian D, Pollak H O *Bell Syst. Tech. J.* **40** 43 (1961); Slepian D "Some asymptotic expansions for prolate spheroidal wave functions" *J. Math. Phys.* **44** 99 (1965)
51. Landau L D, Lifshitz E M *Statisticheskaya Fizika* (Statistical Physics) Pt. 1 (Moscow: Fizmatlit, 1995) [Translated into English (Oxford: Pergamon Press, 1980)]
52. Kholevo A S *Problemy Peredachi Informatsii* **8** (1) 63 (1972); **15** (4) 3 (1979) [*Probl. Inf. Transm.* **15** 247 (1980)]; Holevo A S *Usp. Mat. Nauk* **53** (6) 193 (1998) [*Russ. Math. Surv.* **53** 1295 (1998)]; Kholevo A S *Vvedenie v Kvantovuyu Teoriyu Informatsii* (Introduction to Quantum Information Theory) [Ser. Sovremennaya Matematicheskaya Fizika. Problemy i Metody (Modern Mathematical Physics. Problems and Methods) Issue 5] (Moscow: Izd. MTsNMO, 2002)
53. Molotkov S N *Pis'ma Zh. Eksp. Teor. Fiz.* **78** 1087 (2003) [*JETP Lett.* **78** 597 (2003)]