electronics

MDPI

Article

Development of Quantum Protocol Modification CSLOE–2022, Increasing the Cryptographic Strength of Classical Quantum Protocol BB84

Larissa V. Cherckesova [1], Olga A. Safaryan [1,*], Alexey N. Beskopylny [2,*] and Elena Revyakina [1]

[1] Department of Cyber Security of Information Systems, Don State Technical University, 344003 Rostov-on-on, Russia
[2] Department of Transport Systems, Faculty of Roads and Transport Systems, Don State Technical University, 344003 Rostov-on-Don, Russia
* Correspondence: safari_2006@mail.ru (O.A.S.); besk-an@yandex.ru (A.N.B.); Tel.: +7-(863)-238-15-18 (O.A.S.); +7-(863)-273-84-54 (A.N.B.)

Abstract: Quantum cryptography protocols make it possible not only to ensure the protection of data transmitted in a communication channel from unauthorized access by intruders, but also to detect the existence of any attempted interception. This scientific direction is currently relevant, since it is related to the problem of security and data protection in current information and communication networks. The article is devoted to quantum cryptography; it describes the development of quantum protocols as quantum key distribution systems. Grounded on the laws of quantum mechanics, the elaboration of modifications of secure data transfer protocols is shown. The authors considered the best-known protocol to be BB84 of quantum key distribution; a more modern modification of this protocol is BB84 Info-Z. Comparative analysis of these has also been carried out. It has been established that the BB84-Info-Z quantum protocol works more efficiently than BB84 since its lower error threshold allows the interceptor to obtain much less information about the secret key. The authors put forward a new idea to improve the BB84 protocol (which has been quite outdated for almost 40 years), due to the increase in modern requirements for quantum cryptography protocols. The modification is called CSLOE-2022. It enables significant intensification of cryptographic strength and the entanglement degree of the interceptor (cryptanalyst), which greatly complicates the very possibility of intercepting information. The ultimate goal of the CSLOE-2022 modification is to complicate the eavesdropping process so much that it can be considered completely useless for an attacker in terms of wasting time and resources. The modification allows exceeding the known speed limit of key generation without repeaters since it uses two sources, the phases of which, in addition to the hundreds of kilometers of fiber between them, are very difficult to stabilize. Comparison of the protocols by working distance showed that for BB84, this distance does not exceed 70 km; for BB84-Info-Z it is similar, at no more than 70 km, and the modification of CSLOE-2022 proposed by the authors theoretically allows increasing the working distance of the quantum protocol to 511 km (7.3 times).

Keywords: quantum protocol; quantum cryptography; quantum key distribution; error threshold; modification of the quantum protocol BB84

Citation: Cherckesova, L.V.; Safaryan, O.A.; Beskopylny, A.N.; Revyakina, E. Development of Quantum Protocol Modification CSLOE–2022, Increasing the Cryptographic Strength of Classical Quantum Protocol BB84. *Electronics* **2022**, *11*, 3954. https://doi.org/10.3390/electronics11233954

Academic Editor: Lucas Lamata

Received: 22 October 2022
Accepted: 25 November 2022
Published: 29 November 2022

1. Introduction

The article is devoted to quantum cryptography. It particularly concerns quantum cryptographic protocols, which scientists have been investigating for almost forty years. Quantum cryptography is considered technology capable of adding to the new, unique look of telecommunication networks of the future.

However, no one can predict with full confidence what the formed quantum infrastructure will look like, and to what outcome it may lead. Today, quantum cryptography allows

us not only to provide increased protection against unauthorized access to transmitted information, but also to reveal the very existence of such attempt with higher probability. In modern information-based society, this aspect is extremely important, since humanity is striving to achieve, in fact, complete digitalization.

In parallel with this process, the global modernization of technological equipment, computer software and hardware is rapidly taking place; load on telecommunications networks is increasing. Volumes of secret data, confidential information, and personal data of users are increasing. At the same time, the number of computer security incidents is inevitably increasing. Attackers are modernizing the types of threats and ways to implement them, causing serious problems with information security and data protection.

Maintaining the reliability and operability of technical equipment in communication networks is becoming an increasingly difficult task. Recent cyberattacks in various countries of the world have partially paralyzed the public activity of citizens and caused serious problems in government apparatus. Many countries face similar incidents of computer security every day, and in some cases, users become practically helpless. National governments are extremely concerned about this situation, which threatens their critical infrastructure.

The moment is not far off when the process of modernization of the available means of information protection will come to a standstill, and then the transition to safer quantum technologies will become the ubiquitous inevitability.

Therefore, many countries of the world are optimistic for quantum cryptography technologies. In this regard, the process of transition to quantum technologies seems inevitable, and the attitude to scientific research in this area has become much more serious.

The article proposed by the authors is aimed at analyzing the foundations of quantum cryptography protocols, comparing their cryptographic strength, and the possibilities for their modification. Two well–known quantum protocols are taken as examples: the outdated, but still competitive BB84, and its modification BB84 Info-Z, which has its own distinctive features. Understanding the grounds and principles of quantum protocol functioning is becoming a necessity for many information security specialists. The priority directions of the development of quantum key distribution systems are demonstrated, and the construction of safe and secure data transmission protocols grounded on quantum mechanics laws is shown.

This article puts forward new assumptions about the possibility of universal improvement of quantum protocols on the example of modification of the quantum protocol BB84. The application of the idea put forward by the authors is based on the theory of man-made reconstruction of photons and their further use, which allows significantly reducing the danger of potential threats, and in some cases, to avoid situations related to vulnerabilities of quantum protocols. This method is combined; together with the application of false photon states and the creation of many traps, in order to increase the computing resources spent on cyberattacks by hackers, in the end, it nullifies this attack, making it useless. An attacker, or "eavesdropper", will find a much smaller opportunity to guess the desired data transfer qubit, as well as the photon polarization state. The simulated copies, in addition to their main task, will become good bait for hackers, capable of driving him into the trap, thereby confirming his presence in the communication channel. In this case, the process of disconnecting the communication channel will not be mandatory.

2. Protocol BB84

This quantum protocol is named after the first letters of the surnames of its creators and the year of its publication [1]. The BB84 protocol is designed to transmit secret information encoded in binary. Figure 1 shows how, in the BB84 protocol, one bit can be encoded in the polarization state of photon. Binary 0 is defined as the polarization of 0° in the rectilinear coordinate basis, or 45° on a diagonal basis. Binary 1 can also be equal to 90° on a rectilinear coordinate basis, or 135° on a diagonal basis. Thereby, one bit can be represented by the polarization of a photon in one of two coordinate bases.

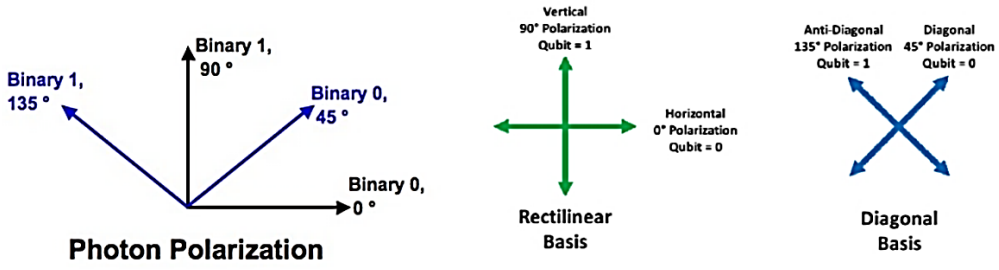

Figure 1. Encoding of the bit in protocol BB84.

Currently, the participants in the transmission of the data process, Alice and Bob, agree to approve some big number n, the threshold of error pa and the linear correction code of error C, with the parity check matrix PC of the order r × n.

The linear key generation function (to enhance confidentiality), represented by P_K matrix of order $m \times n$, is also agreed upon. Both matrices can be known in advance or can be determined during the execution of the protocol, and then can be sent via the classical channel. In turn, the matrix $(r + m) \times n$, the rows of which are the rows P_C and P_K, if taken together, must have the rank $r + m$. Alice randomly selects the sequences of bits: strings i from $2n$ – bit, $b \in {F_2}^{2n}$, where F_2 defines the field of 2 elements {0; 1}, that is, field of integer numbers modulo 2. Then, the state $\left|i^b\right\rangle = \left|i_1^{b_1}\right\rangle \ldots \left|i_{2n}^{b_{2n}}\right\rangle$ is encoded. For each bit, the coordinate basis is randomly selected, rectilinear or diagonal, with which the bit will be encoded. When transmitting the photon from Alice, Bob will inform her about the photon receiving, but will not measure it.

For each photon that Bob receives, he will measure the polarization of the photon on the randomly selected coordinate basis, applying it to his own state. If Bob chose the same coordinate basis of his state for particular photon as Alice did, when he performed the transformation $H^b = H^{b_1} \otimes \ldots \otimes H^{b_{2n}}$, he switches to the state $|i\rangle = |i_1 \ldots i_{2n}\rangle$. Bob should measure the same polarization in the line i^B, and thus output the bit that Alice sent correctly, in the case of absence of noise and signs of eavesdropping on the communication line from the side of an attacker.

To detect eavesdropping, Alice will randomly select n bits that will be used to detect the presence of attackers. By selecting a $2n$–bit string containing n units exactly, Alice must ensure that equality $|s| = n$ was fulfilled. Alice sends to Bob s bits publicly, such, that $s_j = 0$, which are applicated for testing, and the rest of the bits are employed for generating of the final key. Let us denote the corresponding substrings, appropriate for testing process values i and b, while the substrings appropriate for the generation of a key will be defined as i_s and $b_{s.}$ For every $j \in [1 \ldots 2n]$, such, that the value $s_j = 0$, the participants of the data transfer process Alice and Bob publish the value of the bit with jth number.

If Bob chose the incorrect basis of coordinates, then his outcome and, consequently, the bit that he received will be random. It is worth noting that if the mismatch of the bits determined in the published values of the jth bit by comparison exceeds the np_a, then they interrupt the protocol execution. The preliminarily fixed parameter p_a of the protocol, in fact, is the relationship of permitted bit flips, intended for the testing process.

Alice and Bob save the values of the residue n bits in the strict confidence. The string of Alice is designated as $x = i_s$ and is called the *information string*. The appropriate string of bits on the side Bob is determined as x^B.

At the second stage, Bob must inform Alice, via any unprotected channel of communication, what coordinate basis he has used to measure every photon. Then, Alice informs Bob if he chose the proper coordinate basis for each photon. At this stage, Alice and Bob throw out the bits appropriating the photons that Bob has measured with another coordinate basis. On the condition that no errors occurred, or no one managed the photons, Alice and Bob now should possess the same string of bits, which is named the *sifted key*.

The example demonstrated below (Figure 2) illustrates the bits that Alice selected; the coordinate bases in which she encoded her bits; and the coordinate bases that Bob

applicated for his dimension. In addition, Figure 2 shows the resulting *sifted key*, after the stage when Bob and Alice rejected their bits, as indicated above. However, Alice and Bob, before they finish, have to approve a subset of random bits for the comparison of the provision of the consistency of their actions. For verification, Alice sends Bob an r–bit string of error correction. Bob will use ξ, to compare or rectify his string x^B as necessary. String $\xi = xP_C^T$ is named the *syndrome* of *string* x (relative to P_C). If bits correspond, then they are rejected, and other bits create the common secret m–bit key.

Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 2. Sifted key.

If there is no noise and there are no other dimension errors, a mismatch in any of the compared bits would specify the availability of an *interceptor* presenting in the quantum channel. The reason for this is that if attacker Eve was trying to define the key value, then she would not have any other choice but to measure the photons dispatched by Alice before transmitting these photons to Bob.

Therefore, Eve should attach the separate quantum probe (at quantum sensing [2–6]), which, as she assumed, is in a pure state, and apply the unitary transformation U_j to the composite system. This is true because the theorem on prohibition of cloning (anti–cloning theorem) [7] guarantees that it is impracticable to reproduce a particle of an unknown state.

In view of the fact that Eve will not know which coordinate bases Alice have applicated to encode the bit while she discussed her measurements with Bob, she will be forced to guess. If she measures the states of photons in the wrong coordinate bases, then, as the uncertainty principle of Heisenberg guarantees, the information that was encoded in another coordinate basis will be lost.

Therefore, when a photon reaches Bob, his dimension will be random, and he will receive incorrect information in 50% of cases. Taking into account that the interceptor Eve will choose the basis of measurement incorrectly in 50% cases, on average, then 25% the bits measured by Bob will discern from the bits of Alice. If interceptor Eve captures all possible bits, then, after comparisons of n–bit by Alice and Bob, they would decrease the possibility that attacker Eve can remain unnoticed by a value of $\frac{3}{4}n$.

Therefore, the probability that the interceptor–attacker Eve has investigated the secret is insignificant if relatively long bit sequences are compared and identified.

3. Protocol BB84–Info–Z

Modification of BB84 and the considered quantum protocol BB84–Info–Z, is analogous to BB84 [8], except that it applies the following differences:

- Generalized numbers of bits n, n_z and n_x (n–the numbers of informational bits, where Z and X are the test bits, accordingly);
- Section $P = (s, z, b)$ to divide n–bit string i into three non–overlapping sets (I, T_Z и T_X);
- Two special thresholds, which are separate ($p_{A,z}$ and $p_{A,x}$) in place of one threshold (p_A).

Before starting the quantum protocol functioning, Alice and Bob must select some general parameters or public parameters:

- numbers denoted as n, n_z and n_X (specified as the relationship $N = n + n_z + n_x$);
- thresholds of errors denoted as $P_{A,Z}$ and $P_{A,X}$, $r \times n$ (which correspond to the linear code of error correction C);
- matrices of privacy enhancement $m \times n$ (representing the linear key of generation function).

It is important that all rows $R + M$ of the previously considered P_C and P_K matrices are assembled as linearly independent.

Alice randomly selects the section $\mathcal{P} = (s, z, b)$ of the N–bit strings, randomly choosing N–bit strings denoted as, $z,\ b\ \in F_2^N$, which satisfy the conditions:

$$\mid s \mid = n;\ \mid z \mid = n_z;\ \mid B \mid = n_x; \text{ and } \mid s + z + b \mid = N.$$

Thereby, the section $\mathcal{P}$ splits the set of indexes denoted as $\{1, 2, \ldots, N\}$ into three non-overlapping and disjointed sets:

- I (information bits, where $s_j = 1$) size n;
- T_Z (test bits Z, where $z_j = 1$) with size n_z;
- T_X (test bits X, where $b_j = 1$) with size n_x.

Alice selects N–bit strings randomly, where $i \in F_2^N$, and performs the dispatch of N qubits $\left|i_2^{b_1}\right\rangle$, $\left|i_2^{b_2}\right\rangle$, $\ldots$, $\left|i_N^{b_N}\right\rangle$, one by one, through the quantum information channel. At the same time, Alice uses coordinate basis Z to send the information of test Z–bits, as well as X coordinate basis to send X–bits. Initially, Bob stores every qubit he has received in the quantum memory, without measuring this qubits.

Next, Alice dispatches the string of bits $b = b_1 \ldots b_N$ via the classical channel to Bob. Bob gauges and measures every qubit that he has received and saved. When measuring ith qubit, Bob measures it in the Z–coordinate basis if $b_i = 0$, and measures it in the X–coordinate basis if $b_i = 1$. This string of bits that Bob measured is designated as i^B. If noise and eavesdropping are absent, then the bit string is equal to $i^B = i$.

After that, Alice sends Bob the string of bits, designated as s. The information bits (which will be applied for the final key generating) are n bits $s_j = 1$, while test Z and X bits (which will be applied for testing) are $n_Z + n_X$ with $s_j = 0$. Substrings are denoted by i and b, and correspond to information bits i_S and b_S, accordingly.

Next, Alice and Bob publish together the values of bits, which they obtain for all test bits Z and X, and then the bit values are compared. If, for Alice and Bob, more than $n_Z \cdot p_{a,Z}$ test Z–bits are, or more than $n_X \cdot p_{a,X}$ test X–bits between them are different, then they interrupt this protocol, where $p_{a,Z}$ and $p_{a,X}$ are preliminarily coordinated thresholds of errors. Alice and Bob keep values of residual n bits (information bits where $s_j = 1$) a strict secret. The bit chain of Alice is designated as $x = i_s$, and the bit string of Bob is denoted as x^B.

Then, the syndrome x should be dispatched from Alice to Bob (regarding code C correction of errors and its check on parity of the P_C matrix), which includes r bits and is determined as $\xi = xP_C^T$. Using the value ξ, Bob rectifies the errors in his string of bits x^B (it is similarly x). The final key is m–bit sequence and is determined as $k = xP_K^T$. Alice and Bob, together, calculate it. It is obvious that the protocols are very similar.

Let us consider their security against collective attacks [9,10], which are one of the most powerful theoretical cyberattacks.

4. Description of Cyberattack of Eve and the Properties of It

To every j qubit $\left|i_j^{b_j}\right\rangle_{T_j}$ shipped by Alice $(1 \leq j \leq N)$, Eve attaches the separate quantum probe (at quantum sensing), which, as it assumed, is in pure state, and applies the unitary transformation U_j to the composite system. Then, she stores her quantum probes in the quantum memory for the subsequent measurements, and dispatches to Bob his part of the system [11].

Therefore, for every qubit there is a certain trial Hilbert space and a certain unitary transformation U_j; they are determined by Eve in advance and, thus, are corrected and fixed for all feasible variants and options of i, b and s.

4.1. Cyberattack of Eve on the Separate Qubit

Because the cyberattack is bitwise, it is possible to focus the analysis on some selected fixed qubit, temporarily discarding subindex j and expressing the general impact of the actions of Eve on the concrete qubit relative to the coordinate basis $\left|0^b\right\rangle$, $\left|1^b\right\rangle$

$$U\left|0^E\right\rangle\left|0^b\right\rangle = \left|E_{00}^b\right\rangle\left|0^b\right\rangle + \left|E_{01}^b\right\rangle\left|1^b\right\rangle = \left|\phi_0^b\right\rangle. \tag{1}$$

$$U\left|0^E\right\rangle\left|1^b\right\rangle = \left|E_{10}^b\right\rangle\left|0^b\right\rangle + \left|E_{11}^b\right\rangle\left|1^b\right\rangle = \left|\phi_1^b\right\rangle. \tag{2}$$

where $\left|E_{00}^b\right\rangle$,$\left|E_{01}^b\right\rangle$,$\left|E_{10}^b\right\rangle$ and $\left|E_{11}^b\right\rangle$ represent the vectors, or non–normalized states, in the trial Hilbert space of Eve, respective to this concrete qubit. Because the transformation U is unitary, then $\left|\phi_0^b\right\rangle$ and $\left|\phi_1^b\right\rangle$ have norm 1 and are orthogonal. This means that

$$\left\langle E_{00}^b\middle|E_{00}^b\right\rangle + \left\langle E_{01}^b\middle|E_{01}^b\right\rangle = 1. \tag{3}$$

$$\left\langle E_{10}^b\middle|E_{10}^b\right\rangle + \left\langle E_{11}^b\middle|E_{11}^b\right\rangle = 1. \tag{4}$$

$$\left\langle E_{00}^b\middle|E_{10}^b\right\rangle + \left\langle E_{01}^b\middle|E_{11}^b\right\rangle = 0 \quad \left\langle E_{10}^b\middle|E_{00}^b\right\rangle + \left\langle E_{11}^b\middle|E_{01}^b\right\rangle = 0. \tag{5}$$

4.2. Spreading the Cyberattack to the Several Qubits–Collective Cyberattack

For every qubit $\in [1 \ldots 2n]$ Eve uses the transformation Uj in the space $\mathcal{H}_j^E \otimes \mathcal{H}_2$, where $\mathcal{H}_j^E$ is Eve's trial space, $\mathcal{H}_2$– is the space of qubits. The coordinate basis bj, expressed relative to Eve's point of view, is obtained by tracking Bob from the $\left|\phi_0^{b_j}\right\rangle_j$ and $\left|\phi_1^{b_j}\right\rangle_j$, resulting in the following density matrices:

$$\left(\rho_0^{b_j}\right)_j = \left|E_{00}^{b_j}\right\rangle_j\left\langle E_{00}^{b_j}\right| + \left|E_{01}^{b_j}\right\rangle_j\left\langle E_{01}^{b_j}\right| \tag{6}$$

$$\left(\rho_1^{b_j}\right)_j = \left|E_{10}^{b_j}\right\rangle_j\left\langle E_{10}^{b_j}\right| + \left|E_{11}^{b_j}\right\rangle_j\left\langle E_{11}^{b_j}\right|. \tag{7}$$

If Alice dispatches the string i applying the coordinate basis b, then the global state of Eve is the tensor product of these states $\left(\rho_{i_j}^{b_j}\right)_j$. After revealing the test bits [12], Eve requires only those values $\left(\rho_{i_j}^{b_j}\right)_j$, or which $s_j = 1$. The set $\{j \,|s_j = 1\}$ has n elements and is global. The global corresponding values s, b, x can now be saved as:

$$\rho_x^{b_s} = \left(\rho_{i_{j_1}}^{b_{j_1}}\right)_{j_1} \otimes \ldots \otimes \left(\rho_{i_{j_n}}^{b_{j_n}}\right)_{j_n} = \otimes_{l=1}^{n}\left(\rho_{i_{jl}}^{b_l}\right)_{j_l} \tag{8}$$

4.3. Probability of Errors

Supposing that the qubit is under cyberattack by transformation U, as determined in (1) and (2), then an error emerges if Alice dispatches 0 and Bob measures 1, or if Alice dispatches 1 and Bob measures 0. Let k be the value Bob has measured, i the value dispatched by Alice for the concrete qubit, and b the coordinate basis applied by Alice for encoding i.

Then, the possibility of Bob measuring the error is expressed as:

$$p_{\epsilon}^{b} \triangleq \frac{1}{2}\Big[\Big\langle E_{01}^{b}|E_{01}^{b}\Big\rangle + \Big\langle E_{10}^{b}|E_{10}^{b}\Big\rangle\Big]. \tag{9}$$

4.4. Probability of Errors Occurrence in the Conjugate Basis

Now we study the expression $p_{e}^{\bar{b}}$, where $\bar{b} = 1 - b$ (when $\bar{0} = 1, \bar{1} = 0$), which responds to the basis, conjugating to the basis that was given and specified as b.

Cyberattack U is described usually by formulas (1) and (2), in the coordinate basis b.

To compute the probability of error when Alice encodes i_j as $\left|i_j^{\bar{b}}\right\rangle$ instead $\left|i_j^{b}\right\rangle$, it is necessary to represent U in the coordinate basis $\bar{b}$. From the Equation (10), it is known that in this circumstance, the probability of errors is determined by the expression:

$$p_{\epsilon}^{\bar{b}} = \frac{1}{2}\Big[\Big\langle E_{01}^{\bar{b}}\Big|E_{01}^{\bar{b}}\Big\rangle + \Big\langle E_{10}^{\bar{b}}\Big|E_{10}^{\bar{b}}\Big\rangle\Big] \tag{10}$$

Using the fact that

$$|0\rangle^{\bar{b}} = \frac{1}{\sqrt{2}}\Big[\Big|0^{b}\Big\rangle + \Big|1^{b}\Big\rangle\Big], \;\; |1\rangle^{\bar{b}} = \frac{1}{\sqrt{2}}\Big[\Big|0^{b}\Big\rangle - \Big|1^{b}\Big\rangle\Big]$$

and using linearity U, expressions are derived from (1) and (2):

$$U\Big|0^{E}\Big\rangle\Big|0^{\bar{b}}\Big\rangle = \frac{1}{\sqrt{2}}\Big(\Big|E_{00}^{b}\Big\rangle + \Big|E_{10}^{b}\Big\rangle\Big)\Big|0^{b}\Big\rangle + \frac{1}{\sqrt{2}}\Big(\Big|E_{01}^{b}\Big\rangle + \Big|E_{11}^{b}\Big\rangle\Big)\Big|1^{b}\Big\rangle \tag{11}$$

$$U\Big|0^{E}\Big\rangle\Big|1^{\bar{b}}\Big\rangle = \frac{1}{\sqrt{2}}\Big(\Big|E_{00}^{b}\Big\rangle - \Big|E_{10}^{b}\Big\rangle\Big)\Big|0^{b}\Big\rangle + \frac{1}{\sqrt{2}}\Big(\Big|E_{01}^{b}\Big\rangle - \Big|E_{11}^{b}\Big\rangle\Big)\Big|1^{b}\Big\rangle \tag{12}$$

Replacing $\left|0^{b}\right\rangle$ and $\left|1^{b}\right\rangle$ in the right parts of expressions on their magnitudes from the positions $\left|0^{\bar{b}}\right\rangle$ and $\left|1^{\bar{b}}\right\rangle$ I, i.e., $\left|0^{b}\right\rangle = \frac{1}{\sqrt{2}}\Big[\left|0^{\bar{b}}\right\rangle + \left|1^{\bar{b}}\right\rangle]$ and $\left|1^{b}\right\rangle = \frac{1}{\sqrt{2}}\Big[\left|0^{\bar{b}}\right\rangle + \left|1^{\bar{b}}\right\rangle]$ I, we receive

$$\begin{aligned} U\Big|0^{E}\Big\rangle\Big|0^{\bar{b}}\Big\rangle &= \frac{1}{2}\Big[\Big|E_{00}^{b}\Big\rangle + \Big|E_{10}^{b}\Big\rangle + \Big|E_{01}^{b}\Big\rangle + \Big|E_{11}^{b}\Big\rangle\Big]\Big|0^{\bar{b}}\Big\rangle \\ &+ \frac{1}{2}\Big[\Big(\Big|E_{00}^{b}\Big\rangle - \Big|E_{11}^{b}\Big\rangle\Big) + \Big(\Big|E_{10}^{b}\Big\rangle - \Big|E_{01}^{b}\Big\rangle\Big)\Big]\Big|1^{\bar{b}}\Big\rangle \end{aligned} \tag{13}$$

$$\begin{aligned} U\Big|0^{E}\Big\rangle\Big|1^{\bar{b}}\Big\rangle &= \frac{1}{2}\Big[\Big|E_{00}^{b}\Big\rangle - \Big|E_{11}^{b}\Big\rangle - \Big|E_{10}^{b}\Big\rangle - \Big|E_{01}^{b}\Big\rangle\Big]\Big|0^{\bar{b}}\Big\rangle \\ &+ \frac{1}{2}\Big[\Big(\Big|E_{00}^{b}\Big\rangle - \Big|E_{11}^{b}\Big\rangle\Big) + \Big(\Big|E_{10}^{b}\Big\rangle - \Big|E_{01}^{b}\Big\rangle\Big)\Big]\Big|1^{\bar{b}}\Big\rangle \end{aligned} \tag{14}$$

where components for $\left|E_{01}^{\bar{b}}\right\rangle$ and $\left|E_{10}^{\bar{b}}\right\rangle$ are enclosed in parentheses, we can easily see that:

$$p_{\epsilon}^{\bar{b}} = \frac{1}{2}\Big[\Big\langle E_{01}^{\bar{b}} \mid E_{01}^{\bar{b}}\Big\rangle + \Big\langle E_{10}^{\bar{b}} \mid E_{10}^{\bar{b}}\Big\rangle\Big] = \frac{1}{4}\Big[(\langle E_{00}^{b}| - \langle E_{11}^{b}|)\Big(\Big|E_{00}^{b}\Big\rangle - \Big|E_{11}^{b}\Big\rangle\Big) + \Big(\Big\langle E_{10}^{b}\Big| - \Big\langle E_{01}^{b}\Big|\Big)\Big(\Big|E_{10}^{b}\Big\rangle - \Big|E_{01}^{b}\Big\rangle\Big)\Big|$$

Let us distribute this result applying Equalities $\langle\phi|\psi\rangle = \Big\langle\overline{\psi|\phi}\Big\rangle$ and $\mathcal{Z} + \overline{\mathcal{Z}} = 2Re(\mathcal{Z})$ for $\mathcal{Z} \in C$ (where the complex conjugation is denoted above the line [13]). Using the Equalities (3) and (4), we obtain the following expressions:

$$\begin{aligned} p_{e}^{\bar{b}} &= \frac{1}{4}\Big[2 - \Big\langle E_{00}^{b} \mid E_{11}^{b}\Big\rangle - \Big\langle E_{11}^{b} \mid E_{00}^{b}\Big\rangle - \Big\langle E_{01}^{b} \mid E_{10}^{b}\Big\rangle - \Big\langle E_{10}^{b} \mid E_{01}^{b}\Big\rangle\Big] \\ p_{e}^{\bar{b}} &= \frac{1}{2}\Big[1 - \mathrm{Re}\Big(\Big\langle E_{00}^{b} \mid E_{11}^{b}\Big\rangle + \Big\langle E_{01}^{b} \mid E_{10}^{b}\Big\rangle\Big)\Big] \end{aligned} \tag{15}$$

This expression will be applied to relate the perturbation caused by Eve while Alice is encoding i_j bits in the coordinate basis $\overline{b}_j$, so $s_j = 1$, with the information which Eve obtains, while Alice will encode it in this coordinate basis.

According to the principle of «Information against perturbation» [14], the more information Eve receives while the encoding is carried out in the coordinate basis b, the more interference it causes while the bits are encoding and checking in conjugate coordinate basis. Therefore, it is possible to limit Eve's knowledge about the key by limiting the allowable rate (frequency) of errors in this quantum protocol.

5. Security Confirmation of Classical Protocol BB84 against the Collective Cyberattacks

Proof of Security

Let us choose such code $\frac{d_{r,m}}{2n} > p_a + \epsilon$, or some small value ϵ; then the expression $2m\sqrt{P\left[\left(\frac{|C_I|}{n} \geq \frac{d_{r,m}}{2n}\right) \wedge \left(\frac{|C_T|}{n} \leq p_a\right)\right]}$ will be less than value $P\left[\left(\frac{|C_I|}{n} > p_a + \epsilon\right) \wedge \left(\frac{|C_T|}{n} \leq p_a\right)\right]$, which by itself is exponentially small in n.

We can apply Heffding's selection from [8] (the theorem) for every specific row $c_1 \ldots c_{2n}$, appropriate to all qubit measurements in some valid coordinate basis b. Let $\overline{X} = \frac{|C_I|}{n}$ be the average value of selection respective to incorrect bits of information;

$\mu = \frac{|C_I|+|C_T|}{2n}$–is the mathematical expectation $\overline{X}$, which is equal to the expression $2\mu - \overline{X} \leq p_a$, or is identical to inequality $\overline{X} - \mu \geq \mu - p_a$.

To the rows $\left(\frac{|C_I|}{n} > p_a + \epsilon\right)$ and $\left(\frac{|C_T|}{n} \leq p_a\right)$ we will rewrite the conditions as:

$$\left(\overline{X} - \mu > \epsilon + p_a - \mu\right) \wedge \left(\overline{X} - \mu \geq \mu - p_a\right) \tag{16}$$

whence it follows that using Heffding's theorem [15], the relation is obtained:

$$P\left[\left(\frac{|C_I|}{n} > p_a + \epsilon\right) \wedge \left(\frac{|C_T|}{n} \leq p_a\right)\right] \leq P\left[\overline{X} - \mu > \frac{\epsilon}{2}\right] \leq e^{-\frac{1}{2}n\epsilon^2} \tag{17}$$

It is necessary to make sure that the rate of errors in the bits of information is less than the maximum speed at which the error correction code can process.

This condition is necessary for the key to be reliable.

6. Security Proof for the Protocol BB84–Info–Z against the Collective Cyberattacks

6.1. General Collective Cyberattack of Eve

Let us assume that, before executing the quantum key distribution (QKD) protocol, Eve chooses to carry out a collective cyberattack [8]. Let the *j*th qubit be given, sent by Alice to Bob. Eve attaches the quantum probe state (at quantum sensing) and applies some unitary operator U_j to the composite system. Then, Eve holds in her quantum memory subsystem E_j, which is the state of her quantum probe; next, she dispatches to Bob the subsystem T_j. This subsystem is the qubit dispatched from Alice to Bob (it may be modified by Eve's cyberattack U_j).

The biggest common collective cyberattack U_j of Eve is directed on the *j*th qubit, presented by orthonormal coordinate basis. The cyberattack described as:

$$U_j\left|0^E\right\rangle E_j\left|0^{b_j}\right\rangle T_j = \left|E_{00}^{b_j}\right\rangle E_j\left|0^{b_j}\right\rangle T_j + \left|E_{01}^{b_j}\right\rangle E_j\left|1^{b_j}\right\rangle T_j \tag{18}$$

$$U_j\left|0^E\right\rangle E_j\left|0^{b_j}\right\rangle T_j = \left|E_{10}^{b_j}\right\rangle E_j\left|0^{b_j}\right\rangle T_j + \left|E_{11}^{b_j}\right\rangle E_j\left|1^{b_j}\right\rangle T_j \tag{19}$$

where $\left|E_{00}^{b_j}\right\rangle E_j$, $\left|E_{01}^{b_j}\right\rangle E_j$, $\left|E_{10}^{b_j}\right\rangle E_j$, and $\left|E_{11}^{b_j}\right\rangle E_j$ are non–normalized states in Eve's quantum probe of system E_j, that was fastened and fixed to *j*th qubit.

So, it can be noticed that the quantum probe state can change the initial state of the composite system product, $\left|0^E\right\rangle E_j \left|i_j^{b_j}\right\rangle T_j$, to an entangled state. This implies that Eve's cyberattack can cause the entangling of her quantum probe with Bob's probe (at quantum sensing).

Firstly, this can clarify the situation, and bring some kind of information about the state of Bob; secondly, it is the reason for the disturbance, and can be discovered by him. The information received the day before and the disturbance that Eve caused, by their nature, are interrelated with their relationship—this is the main reason why the QKD protocols are secure and safe.

6.2. Proof of Security

As was mentioned earlier [8], the random variable $\widetilde{C}_i$ matches the errors in the string of bits in information bits if they were encoded in the coordinate basis X. Bits of TEST–X are also encoded in basis X. The C_{TX} random variable matches the string of bits of the errors, on these bits. Hence, it is possible to consider the choice of n–bits indexes of information (Info) and n_x–bits TEST–X as a random selection (after n, n_z and n_x numbers; and bit indexes TEST–Z, which was selected already) and to apply the theorem of Heffding [9].

Hence, for every string of bits $c_1 \ldots c_{n+nx}$, which consists of errors in the bits $n + n_x$ Info and TEST–X, if Info bits were coded in the coordinate basis X, then we can use Heffding's theorem: let us take the sample with size n without changing from combination $c_1, \ldots, c_{n+nx}$. In the above discussion [8], the following theorem is actually proven:

Theorem. *Let the values $\delta > 0$ and $R > 0$; for infinite number of values n, the vectors family is given, which is linearly independent $\left\{v_1^n, \ldots, v_{r_n+m_n}^n\right\}$, such, that $\delta < \frac{d_{r_n,m_n}}{n}$, $\frac{m_n}{n} \leq R$. Hence, for anyone $p_{a,Z}, p_{a,X} > 0$, such, that $p_{a,x} + \epsilon_{sec} \leq \frac{\delta}{2}$, and for any n, n_z, $n_x > 0$ and two final keys k, k' that are the m_n–bit keys, the distance between the states of Eve, appropriate to k and k', meets the following requirements and boundaries:*

$$\left\langle \Delta_{Eve}^{(p_{a,z},p_{a,x})}\left(k,k'\right)\right\rangle \leq 2Rne^{-(\frac{n_x}{n+n_x})^2 n\epsilon_{sec}^2}. \tag{20}$$

6.3. Reliability

By itself, the security is insufficient; it is also necessary that the key be reliable. More specifically, it must be identical for Alice and Bob [16]. It assumes it a need to ensure that quantity of errors in the Info bits was less than the maximum error number, which can be rectified by the error correction code. To do this, it is necessary that the code for error correction can really correct the errors. Consequently, the final key reliability, having exponentially low failure probability, is provided by the inequality below:

$$P\left[\left(\frac{|C_l|}{n} > p_{a,z} + \epsilon_{rel}\right) \wedge \left(\frac{|C_{T_z}|}{n_z} \leq p_{a,z}\right)\right] \leq e^{-2(\frac{n_z}{n+n_z})^2 n\epsilon_{rel}^2} \tag{21}$$

The choice of the Info bits indexes, and the bits of TEST–Z, is random separation of $n + n_Z$ bits into two subsets, with sizes n and n_Z (provided that the bits indexes of TEST–X was already selected). Thus, it matches Heffding's sample.

7. Protocol CSLOE–2022 (BB84–CSLOE–2022)

It is recommended to become acquainted with the new modification proposed by the authors and named CSLOE–2022, for the old but still effective quantum protocol using the quantum distribution of the key–BB84. For the protocol BB84, it is possible to modify significantly the cryptographic strength and degree of entanglement of the listener, which in their perspective will complicate the possibility of intercepting information from such an interceptor (or cryptanalyst) targeting confidential messages.

It is known that after coordination of the coordinate bases in the classic protocol BB84, an interceptor can receive accurate information about the transmitted state.

The final purpose of modification is to complicate eavesdropping process to the point of uselessness, in terms of spending time and resources, as well as to confirm the guesses about the real possibility of using such a method. The idea consists in the following: it is known that the process of replicating the quantum state, recorded as $\psi \rightarrow \psi \otimes \psi$, (cloning) can be performed perfectly, with probability of 1, then and only then if the coordinate basis to which ψ refers is understood and known [17]. Otherwise, the ideal cloning is not possible, since the copies are not perfect. These are contents and consequences of the theorem prohibiting quantum information cloning. This circumstance will be useful.

If it is impossible to reproduce an exact clone of a photon, in order to obtain information from it, it is necessary to measure the characteristics of the original. The only way to measure the characteristics of the photon is to use a detector of single photons. However, as soon the photon reaches the detector, it transmits energy and disappears. That is, the measurement destroys the photon itself [9]. It is worth considering that each photon is unique [18]. However, it is possible to create some kind of photon (kind of similarity). It is known, thanks to quantum teleportation, that it is possible to obtain an exact copy of a photon [17], which, in turn, can be used also to construct such a similarity. For simplicity, we call it a «pseudo-photon». The interceptor will perceive such a pseudo-photon either as a real photon with its own specific set of characteristics, or as some distortion in the channel.

To detect and recognize such a clone in the communication channel, it is necessary to make considerable efforts. In the theory, at the first stage, as in the classic protocol BB84, Alice will communicate with Bob via the quantum communication channel. In turn, Alice will transmit to Bob the modified sequence consisting of cloned pseudo–photons and forming a dictionary (glossary) for each bit with corresponding polarization.

As mentioned earlier, the pseudo-photon will be a kind of photon created artificially [4]. In each concrete case, it is possible to form new sequences that generate the dynamic dictionary, thereby reducing the repetition during encryption.

Knowing that each photon is unique [18], one pseudo-photon cannot be used for each bit, but the whole group with a certain range of values that will be corrected, rectified, adjusted, shifted or expanded can [19].

Each bit, or their sequence, even if they are repeated, will have random pseudo-photons from a certain range of values that are attributed to the concrete bit or bit sequence. When sending the dictionary for decoding, it is possible to send it in parts, to maintain secrecy, and to avoid declassification.

If listening is detected at this first step, the dictionary can be expanded and the intercepted part discarded, as was described earlier [20], or data transmitting can be stopped and a new dictionary created. After successful transmission of the dictionary, it is possible to start sending encoded messages via the communication channel in which real photons, as well as their created copies, will alternate and have absolutely random positions in the sequence. It is worth noting that the protocol can be further complicated. For example, four quantum states can be used to encode bits in two coordinate bases, which corresponds to the quantum protocol BB84 (4 + 2) [21]. Further, such a protocol works according to the classical scenario, but using the dictionary–glossary.

Every time Bob receives a qubit, he reports it to Alice, but does not measure it. Subsequently, for each photon and pseudo-photon which Bob obtains, he will measure the value of polarization on the randomly selected coordinate basis, applying it to his state. If Bob has chosen the same coordinate basis of state for the particular photon, then when he performs transformation H^b, as Alice does, then he goes into the same state. Then, Bob must measure the same polarization in the string i^B. Hence, he can output properly the bit that Alice was going to dispatch in that case, if there is no noise orsigns of eavesdropping in the communication channel.

On the second step, Bob must tell Alice, using any unsecured communication channel, which coordinate basis he applied to quantify and to measure every photon. Then, Alice informs Bob which photons were real by sending the encrypted ranges, and informs him whether he has chosen the right coordinate basis for every original photon.

On this step, Alice and Bob reject the bits corresponding to pseudo-photons and the bits that Bob have quantified and measured in other coordinate bases. If there were no errors and nobody manipulated the photons, Bob and Alice must acquire the same bits string that is named as the sifted key (Table 1). The example below (Figure 3) demonstrates the bits which Alice selected [22]; the coordinate bases in which she encoded it; and bases that Bob used to measure them. In addition, the sifted key, obtained in the result, is demonstrated after Bob and Alice rejected their bits.

Table 1. Sifted key.

Bit of Alice	0	1	1	0	1	0	0	1
Basis of Alice	×	+	+	×	+	×	+	×
Polarization of Alice	↗	↑	→	↖	→	↖	↑	↗
Basis of Bob	×	×	×	+	+	×	+	+
Measurement of Bob	↗	↖	↗	→	→	↖	↑	→
Public discussion	×	+	+	*	+	×	+	*
Shared secret key	0				1	0	0	

↑, →, ↖, ↗—is the state of polarization of photon 1, 0 at angles 0°, 45°, 90°, 135°.

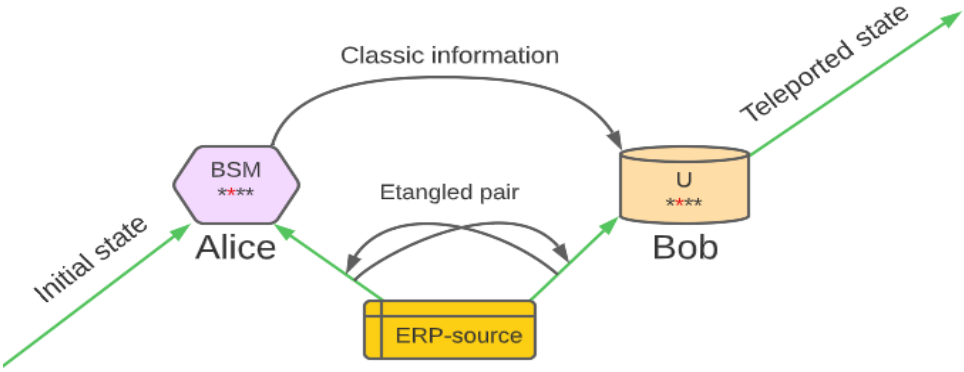

Figure 3. Results of the protocol CSLOE–2022 work.

The principle of imperfect replication is not new, and it is used often in telecommunications practice. In fact, information transmitted in optical fibers is encoded in the light state; thus, this process is quantum coding [23]. The information is strengthened several times on the way from source to receiver; hence, its quality must deteriorate. However, the telecommunication signal includes a large amount of photons being prepared in an identical quantum state. Strengthening in telecommunications boils down to creating several new copies of ψ from $\psi \otimes N$.

That is, the theorem of prohibition of cloning is applied to the amplification of the telecommunication signals, due to the fact that spontaneous radiation is usually available in the amplifiers. Nevertheless, the copy is practically ideal, as the stimulated radiation is the dominant effect. In addition, the sensitivity of modern equipment is quite high, and at this stage is such that quantum limitation must be achieved in the nearest future. Thus, information encoding following the theorem of the prohibition of cloning can also be useful for quantum key distribution protocols [24].

The impossibility of exact and accurate copying of quantum information cannot negate the whole conception of the quantum information. On the contrary, it serves as a demonstration and illustration of power. It is impossible to copy the state of a certain quantum system for intelligent information coding completely using a set of states which are non–orthogonal.

Therefore, if a similar system reaches the receiver undisturbed, that proves that no opponent has copied it. This means that, due to the theorem of the prohibition of cloning,

quantum information supports the tools to complete such tasks, which are impossible to solve applying only familiar information. For example, the detection of any eavesdropping device on the communication channel is possible only with the application of the ideas of quantum cryptography.

7.1. Cloning Methods

Let us consider the possible methods of non–ideal cloning of discrete quantum systems, which are performed in the protocol BB84.

There are several variants of such machines:

(1) Optimal symmetric universal quantum copying machine (UQCM) proposed by Vladimir Bužek (Buzhek, in various sources is spelled differently)–Mark Hillery (BH) in 1996;
(2) Symmetric universal quantum copying machine (UQCM) proposed by Nickolas Gisin–Serge Massar and their scientific group in 1997;
(3) Asymmetric universal quantum copying machine (copier)–UQCM.

The symmetric UQCM qubits cloning for $1 \to 2$, developed by Buzhek and Hillery (BH) accepts the cloning qubit as input, and uses the separate qubit as an auxiliary qubit [25]. The action of such a universal quantum–copying machine in the computational base of initial original qubit is described by the expression:

$$\begin{aligned} |0\rangle|\mathrm{R}\rangle|\mathrm{M}\rangle &\to \sqrt{\frac{2}{3}}|0\rangle|0\rangle|1\rangle - \sqrt{\frac{1}{3}}|\psi^{+}\rangle|0\rangle \\ (-|1\rangle)|E\rangle|M\rangle &\to \sqrt{\frac{2}{3}}|1\rangle|1\rangle|0\rangle - \sqrt{\frac{1}{6}}|\psi^{+}\rangle|1\rangle \end{aligned} \tag{22}$$

where $\psi^{+}\rangle = \frac{1}{\sqrt{2}}[|1\rangle|0\rangle + |0\rangle|1\rangle]$. By its linearity, these ratios cause the next action on the most common and general input state: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$:

$$|\psi\rangle|R\rangle|M\rangle \to \sqrt{\frac{2}{3}}|\psi\rangle|\psi\rangle\left|\psi^{\perp}\right\rangle - \sqrt{\frac{1}{6}}\left[|\psi\rangle\left|\psi^{\perp}\right\rangle + \left|\psi^{\perp}\right\rangle|\psi\rangle\right]|\psi\rangle \tag{23}$$

where $\left|\psi^{\perp}\right\rangle = \alpha * |1\rangle - \beta * |0\rangle$.

As can be seen from the Equation (23), α and β can swap their places. In addition, for all input states, this transformation has the similar shape $|\psi\rangle$.

Therefore, the quantum copying machine (QCM) is universal and symmetric. For the original and the copy, its partial states are expressed as:

$$\rho_A = \rho_B = \frac{5}{6}|\psi\rangle\langle\psi| + \frac{1}{6}\left|\psi^{\perp}\right\rangle\left\langle\psi^{\perp}\right| = \frac{1}{2}\left(1 + \frac{2}{3}\hat{m} + \vec{\sigma}\right) \tag{24}$$

The symmetric universal quantum copying machine for NM qubits was developed by Nickolas Gisin and Serge Massar in 1997. It generalizes the Buzhek–Hillery UQCM, and its correctness is determined by the following expression:

$$F_{N\to M} = \frac{MN + M + N}{M(N+2)}\ (d = 2) \tag{25}$$

which reproduces $F_{1\to 2} = \frac{5}{6}$ for $N = 1$ and $M = 2$.

Gisin and Massar provided numerical proofs of the optimality of their universal quantum copying machine. Later, Dagmar Bruss, Artur Eckert and Chiara Machiavelli gave analytical proof for this optimality in 1998. They suggested that the output state appertains to the M qubits symmetric subspace. Further, Reinhard Werner generalized this outcome for the quantum systems of whatever dimension [26].

The universal and asymmetric cloning relate to such a state of affairs where the resulting clones may have varying accuracy in reproduction.

We should concentrate on universal cloning $1 \rightarrow 1 + 1$. Several researchers studied cases that are more general in 2005. Let us look at some of these ideas with their experimental implementation. In the detailed research of cloning $1 \rightarrow 1 + 1$, Chi–Sheng Niu and Robert Griffiths, in 1998, obtained, in particular, the optimal asymmetric universal quantum copying machine $1 \rightarrow 1 + 1$. Nickolas Cerf in 1998 and 2000 independently obtained the same result. He used the algebraic method, along with Vladimir Bužek and Mark Hillery in 1998 [27], who developed the method of quantum schemes, which was improved compared to the previous construction used for symmetric cloning.

Optimality is illustrated by confirming and proving the accuracy of reproduction of two clones, F_A and F_B, that confirms the inequality of non–cloning:

$$\sqrt{(1 - F_A)(1 - F_B)} \geq \frac{1}{2} - (1 - F_A) - (1 - F_B) \tag{26}$$

The authors managed to extend the development of their schemes far beyond the individual case of qubits. Based on the above, to improve the cryptographic strength of protocol BB84, the universal quantum copying machine (UQCM) of Bužek–Hillery is best suited, as it is the simplest quantum copier to implement all the concepts discussed above.

7.2. Comparison of Protocols

Since the protocols BB84, BB84–Info–Z and the CSLOE–2022 modification proposed by the authors have a lot in common, several parameters can be distinguished for their comparison. Let us start by comparing the threshold of errors.

This parameter is necessary to determine whether there was eavesdropping. In the practical implementation of the protocol of quantum keys distribution (QKD), the disadvantages of individual separate components will always show and manifest themselves, and some qubits will be unsuitable for the forming of a secret key.

In addition, listening to the quantum channel makes changes to the transmitted qubits, which also prevents them from being used when forming the secret key.

In the case of the classic protocol BB84, the threshold value of the error rate is 11% [28]. For an ideal model, the number of bits received as the result, the final secret key (R) for the bit of the sifted key, is expressed by the relationship:

$$R = 1 - 2\, H(QBER), \tag{27}$$

where the value H is the binary entropy of Shannon and QBER is number of errors measured by Bob. The dependence of R on QBER is demonstrated in the Figure 4:

This may not always be the case. The quality of execution of the equipment implementing the protocol may allow reducing the threshold.

In the protocol BB84–Info–Z, in addition to the information qubits responsible for key generation, the test qubits X and Z are used [7].

They are necessary for the eavesdropping check. The error threshold for this modification is slightly smaller, at 7.56% [9] (Figure 5).

For the modification proposed by the authors of CSLOE–2022, the threshold of errors is theoretically similar to the original one, since during key formation, imperfect copies of photons used to achieve the entanglement of a listener (eavesdropping interceptor) are discarded, and then the originals are checked, as in the classical protocol. On the other hand, when trying to listen, it is unlikely that the photons will be distorted, since their quantity is significantly lower than the number of copies.

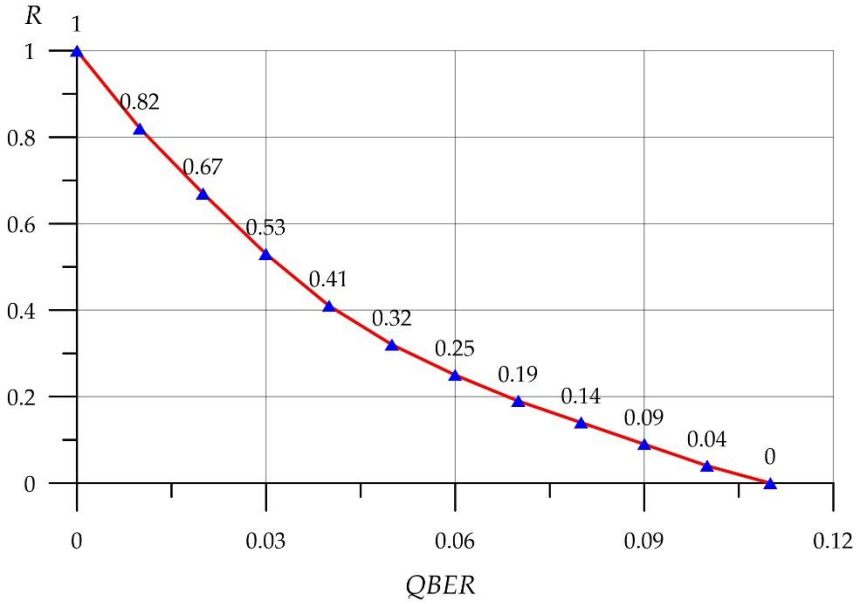

Figure 4. Error threshold for protocol BB84.

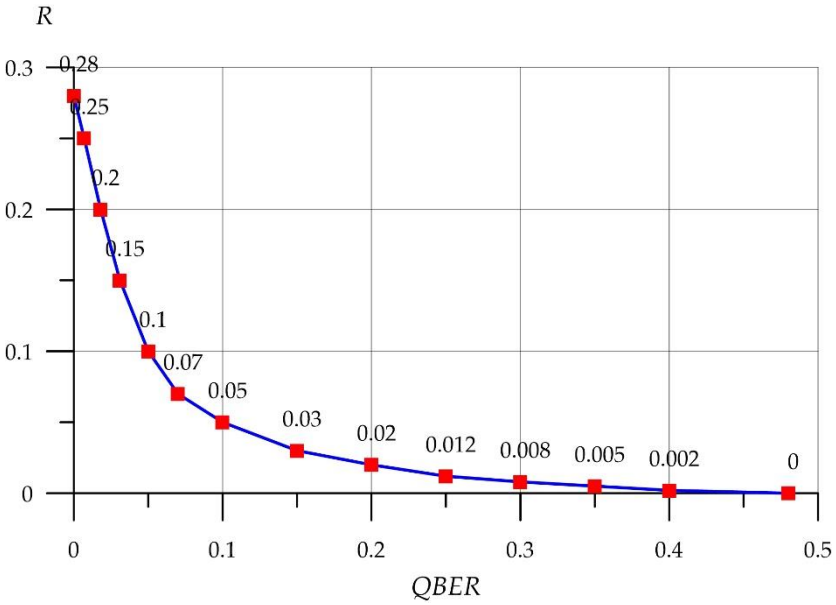

Figure 5. Safe zone of asymptotic rates of errors for BB84–Info–Z protocol.

From publication [17] it is known that the code of Steane (CSS), otherwise known as Calderbank–Shor–Steane, is the tool of quantum error correction, introduced by Andrew Steane in 1996. Steane's code uses the classical binary Hamming's code to correct the errors of the qubit flip (X–errors) and the double Hamming code to correct the errors of the phase flip (Z–errors), in practice allowing:

$$1 - 2 * H(\delta)]n \tag{28}$$

qubits, where δ–number of measured errors, and n–length of qubits sequence.

If expression (28) would be written as: $f(x) = 1 - 2 * H(x)$, then the chart (graph) will intersect the axis X at the point 0.11, which gave us the threshold of errors of 11% in the classical quantum protocol BB84 [29].

For the protocol CSLOE–2022, the dependence of the number of bits of the final resulting secret key R from the quantity of recorded and fixed errors QBER is preserved,

as is shown in Figure 6, since all photons, both the original and their copies in the form of pseudo-photons, will be distorted during transmission. Thus, the comparison of protocols by the threshold of errors can be observed in Table 2:

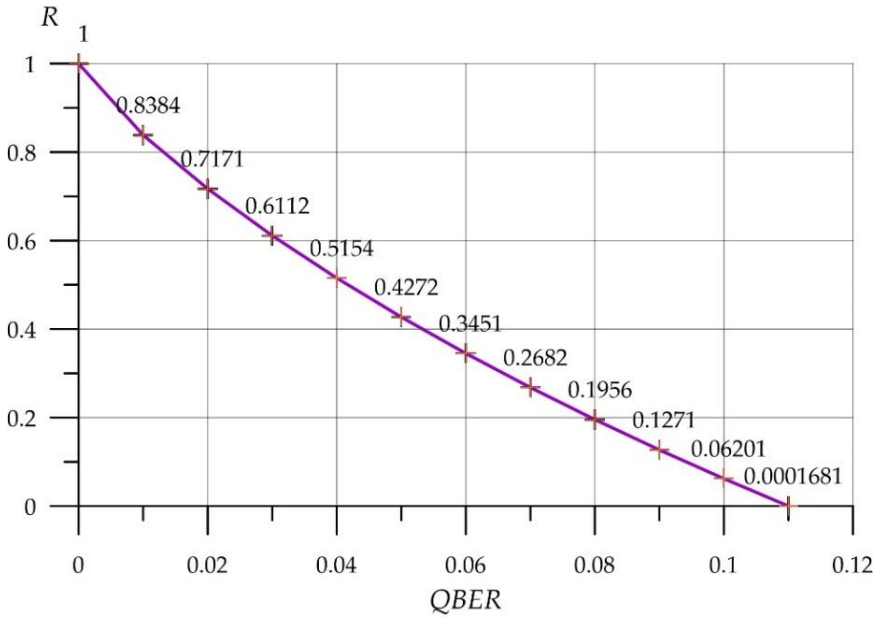

Figure 6. The threshold of errors for the modification CSLOE–2022 proposed by the authors.

Table 2. Comparative characteristics of protocols by threshold of errors.

Protocol	Error Threshold
BB84	11%
BB84–Info–Z	7.56%
CSLOE–2022	11%

The protocol BB84–Info–Z differs for the better from all the others, since a much smaller threshold of errors will allow the eavesdropping intruder to receive significantly less information about the secret key.

Another important parameter is the working distance. The protocols of quantum keys distribution (QKD) operate with single photons, which can be distorted during transmission. Therefore, the working distance is relatively small. For example, for protocol BB84, it is about 70 km [30]. When implementing the protocols DPS and COW, it became possible to reach distances of 250 and 307 km, respectively, but their safety has not yet been proven.

Based on the findings of the research, it was suggested that in the case of using pseudo-photons, it is impossible to declare the numbers of photon losses correctly. If the losses occur from the number of pseudo-photons, and they are used as the trap and entanglement, they may have completely different behavior and completely different interactions, which can lead to both a decrease in losses, or an increase. To declare this confidently without conducting a series of experiments is incorrect and unpredictable. In the case of the protocols BB84 and BB84–Info-Z, the loss of photons is particularly significant. However, the feature of the CSLOE–2022 protocol is its modularity and application of pseudo-photons, which fundamentally distinguishes it from its predecessors.

Therefore, it is possible to make another hypothesis to rely on it, and refer to the fact that the method is based on the cloning of pseudo-photons. At large distances, the transmission of information with photons is carried out with large losses of ($\eta \simeq 0$), and this limitation can be exceeded only by using quantum repeaters. In turn, they will have to

be used without limitation for the transmission of recreated pseudo-photons. In addition, it is necessary to be able to combine them with ordinary photons which can be transmitted without repeaters at all.

It is known that quantum communications guarantee the reliable transmission of quantum information and efficient distribution of entanglement, together with the generation of completely secure keys. However, it should be borne in mind that, at long distances, photon transmissions incur significant losses. Quantum repeaters can surpass this limitation. The article [31] discusses the theoretical aspects of the possible limit for ensuring the transmission of information without repeaters.

Relying on this article is possible if the objective is to increase the distance between repeaters. However, the studies themselves given in [31] are difficult to use for the clear practical application without conducting of series of experiments, and especially in combination of multi-qubit states, which is what some scientists are trying to practice now.

However, in the case considered by the authors, pseudo-photons are used (that is, recreated from real photons with clear differences), which, in turn, may display completely different, unpredictable behavior. This can lead to both a decrease in the losses or an increase in them. In the case of real photons, for the channel with losses, the article [31] proves that $Q_2 = K = -\log_2(1-\eta)$, where η is the coefficient of transmission. In particular, the transmission capacity of the secret key of the channel with losses is the maximum speed achievable with any optical implementation of the quantum key distribution (QKD). At large distances, that is, with large losses, $\eta \simeq 0$, finding the optimal scaling of losses and the speed of $K \simeq 1.44\,\eta$ secret bits per channel use, the fundamental limitation is obtained, which, at this point in time, can be overcome, practically, only with repeaters.

A team of Chinese physicists succeeded in transmitting a secret quantum key at a distance of 511 km in real-world conditions [20]. They were thus able to implement the quantum line of data transmission outside laboratory conditions.

Physicists continue to search for different ways to increase the distance to hundreds and thousands of kilometers, developing repeaters for existing protocols, as well as new ones. For example, the protocol of the twin fields TF (Twin Field). Unlike the standard protocol, for example, BB84, in which Alice directly sends photons to Bob, the protocol TF [32] includes an additional Charlie node, which is located between Alice and Bob. In that case, Alice and Bob carry out the transfer and transmit their information on the weak coherent pulse to Charlie, who compares them and announces whether the received bits coincide or not.

However, Charlie has no information about the bits he has received; he can only compare them and declare whether they have coincided at the moment or not, so Charlie is considered to be an untrusted node.

This approach allows exceeding the known limit of the key generation rate without repeaters. It uses two photon sources, the phases of which, in addition to hundreds of kilometers of optical fiber between them, are not easy to stabilize.

Thus, we can summarize the comparison of protocols BB84, BB84–Info–Z and CSLOE–2022 by working distance and record the results in Table 3:

Table 3. Working distance of protocols.

Protocol	Working Distance
BB84	70 km
BB84–Info–Z	70 km
CSLOE–2022	511 km

8. Conclusions

The article shows that the quantum protocol BB84–Info–Z is protected completely from collective attacks—one of the most powerful cyberattacks.

It is found that the results of the quantum protocol BB84 have much in common with the BB84–Info–Z quantum protocol, with two significant exceptions:

1. The rate of errors should be checked separately so that it remains below the threshold values $p_{a,\,z}$ and $p_{a,\,x}$ for bits TEST–Z and TEST–X; accordingly, when in the quantum protocol BB84, the threshold value of error rate p_a is applied to all bits of TEST jointly [7].
2. The indexes and information indicators of the interceptor Eve (in security terms) and probability of the error-correcting code failure (in reliability terms) differ from the indexes and indicators in the case of classical quantum protocol BB84 [8].

It can be concluded that if the quantum protocol BB84 is modified so that the bits Info would be only at the coordinate basis *Z*, this will not weaken its reliability and security (against the collective cyberattacks, at least). It will not even change the threshold of the asymptotic rate of errors [8].

Protocol BB84–Info-Z can be applied safely to distribute the secret key; its security has ideal implementation, and it is protected against collective cyberattacks.

It is shown that modification of classical quantum protocol BB84 (CSLOE–2022) proposed by the authors could be used for quantum key distribution, since the applied principle of imperfect copying does not violate the laws of physics, but allows increasing the cryptographic strength of the protocol. So far, this modification is just an idea, and it needs to be proven by a series of practical experiments using specific equipment.

However, it is known that the principle of imperfect copying has already been applied experimentally in communication channels, as is mentioned in [33–47], which makes it possible to transmit information over much longer distances.

Nevertheless, for quantum key distribution, there are other requirements for the quality of performance of individual components.

Therefore, these new ideas are being put forward, and engineers are given specific tasks in order to prove the correctness of the new hypotheses.

Further, the authors plan to research the optical quantum memory of photons and pseudo-photons for the possibility of recording information into them. Based on the data obtained, it is necessary to identify theoretical limitations as well as to find the ways to level and neutralize them, both for photons and for pseudo-photons recreated on their basis.

Author Contributions: Conceptualization, L.V.C., O.A.S., A.N.B. and E.R.; methodology, L.V.C. and O.A.S.; software, O.A.S. and E.R.; validation, L.V.C., O.A.S. and E.R.; formal analysis, L.V.C., O.A.S. and E.R.; investigation, L.V.C. and O.A.S.; resources, A.N.B.; data curation, L.V.C. and O.A.S.; writing—original draft preparation, O.A.S. and A.N.B.; writing—review and editing, O.A.S. and A.N.B.; visualization, O.A.S.; supervision, L.V.C. and A.N.B.; project administration, L.V.C. and E.R.; funding acquisition, A.N.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: The study did not report any data.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key Distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984.
2. Aiello, C.D.; Hirose, M.; Cappellaro, P. Composite-pulse magnetometry with a solid-state quantum sensor. *Nat. Commun.* **2013**, *4*, 1419. [CrossRef] [PubMed]
3. Kröll, S.; Gallo, K.; Hennrich, M. *Research in Quantum Sensing*; Wallenberg Centre for Quantum Technology, Science Advances; Chalmers University of Technology: Gothenburg, Sweden, 2022. [CrossRef]

4. Riexinger, F.; Kutas, M.; Haase, B.; Bortz, M. *General Simulation Method for Quantum-Sensing Systems*; Institute for Industrial Mathematics ITWM, Department of Physics and Research Center OPTIMAS: Kaiserslautern, Germany, 2022. Available online: https://arxiv.org/pdf/2112.07243v1.pdf (accessed on 28 November 2022).
5. Schowengerdt, R. *Remote Sensing. Models and Methods for Image Processing*; Elsevier: Amsterdam, The Netherlands, 2007.
6. Molotkov, S.N. On the Resistance of Quantum Cryptography Systems with Phase-Time Coding to Active Probing Attacks. *J. Exp. Theor. Phys.* **2008**, *158*, 1011–1031.
7. Park, J.L. The concept of transition in quantum mechanics. *Found. Phys.* **1970**, *1*, 23–33. [CrossRef]
8. Boyer, M.; Liss, R.; Mor, T. Composable Security against Collective Attacks of Modified BB84 QKD Protocol with Information Only in One Basis. *Theor. Comput. Sci.* **2020**, *801*, 96–109. [CrossRef]
9. Biham, E.; Mor, T. Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.* **1997**, *78*, 2256–2259. [CrossRef]
10. Boyer, M.; Gelles, R.; Mor, T. Security of the Bennett–Brassard Quantum Key Distribution Protocol against Collective Attacks. *Algorithms* **2009**, *2*, 790–807. [CrossRef]
11. Vercruysse, D.; Sapra, N.; Yang, K.; Vukovi, J. Inverse–Designed Photonic Crystal Devices for Optical Beam Steering. *arXiv* **2021**, arXiv:2102.00681. [CrossRef]
12. Buckley, S.; Radulaski, M.; Zhang, J.; Petykiewicz, J.; Biermann, K.; Vučković, J. Nonlinear Frequency Conversion Using High Quality Modes in GaAs Nanobeam Cavities. *Opt. Lett.* **2014**, *39*, 5673–5676. [CrossRef]
13. Cerf, N.; Ipe, A.; Rottenberg, X. Cloning of Continuous Quantum Variables. Ecole Polytechnique, CP 165. *Phys. Rev. Lett.* **2000**, *85*, 1754–1757. [CrossRef]
14. Fuchs, C.; Peres, A. Quantum–State Disturbance versus Information Gain: Uncertainty Relations for Quantum Information. *Phys. Rev.* **1996**, *53*, 2038–2045. [CrossRef]
15. Skori'c, B.; Wolfs, Z. Diagrammatic Security Proof for 8–State Encoding. *arXiv* **2021**, arXiv:2103.01936v1.
16. Morimae, T. *Quantum Randomized Encoding, Verification of Quantum Computing, No–Cloning, and Blind Quantum Computing*; Yukawa Institute for Theoretical Physics, Kyoto University: Kyoto, Japan, 2020.
17. Schimpf, C.; Reindl, M.; Huber, D.; Lehner, B.; Silva, S.; Manna, S.; Vyvlecka, M.; Walther, P. Quantum Cryptography with Highly Entangled Photons from Semiconductor Quantum Dots. *arXiv* **2020**, arXiv:2007.12726v1. [CrossRef] [PubMed]
18. Tan, X. *Introduction to Quantum Cryptography*; IntechOpen: London, UK, 2013. [CrossRef]
19. Shor, P.; Preskill, J. *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol*; AT&T Labs Research: Florham Park, NJ, USA, 2000.
20. Huttner, B.; Imoto, N.; Gisin, N.; Mor, T. Quantum cryptography with coherent states. *Phys. Rev. A* **1995**, *51*, 1863–1869. [CrossRef] [PubMed]
21. Djordjevic, I. *Quantum Information Processing, Quantum Computing, and Quantum Error Correction*, 2nd ed.; Academic Press: Cambridge, MA, USA, 2021. [CrossRef]
22. Bouwmeester, D.; Pan, J.-W.; Mattle, K.; Eibl, M.; Weinfurter, H.; Zeilinger, A. Experimental quantum teleportation. *Nature* **1997**, *390*, 575–579. [CrossRef]
23. Houça, R.; Belouad, A.; El Choubabi, B.; Kamal, A.; El Bouziani, M. Quantum teleportation via a two-qubit Heisenberg XXX chain with x-component of Dzyaloshinskii–Moriya interaction. *J. Magn. Magn. Mater.* **2022**, *563*, 169816. [CrossRef]
24. Yang, L.; Liu, Y.C.; Li, Y.S. Quantum Teleportation of Particles in an Environment. *Chin. Phys. B* **2020**, *29*, 060301. [CrossRef]
25. Chen, J.; Zhang, C.; Liu, Y.; Li, Y.; Liu, H.; Jiang, H.; Chen, T.; Zhang, Q.; Pan, J. Twin–Field Quantum Key Distribution over 511 km Optical Fiber Linking two Distant Metropolitans areas. *Nat. Photon.* **2021**, *15*, 570–575. [CrossRef]
26. Nang Paing, S.; Setiawan, J.W.; Tariq, S.; Talha Rahim, M.; Lee, K.; Shin, H. Counterfactual Anonymous Quantum Teleportation in the Presence of Adversarial Attacks and Channel Noise. *Sensors* **2022**, *22*, 7587. [CrossRef] [PubMed]
27. Gisin, N. *Quantum Randomness. Non–Locality, Teleportation and Other Quantum Wonders*; Alpina non–fiction: Moscow, Russia, 2018; 208p.
28. Safaryan, O.A.; Lemeshko, K.S.; Beskopylny, A.N.; Cherckesova, L.V.; Korochentsev, D.A. Mathematical Analysis of Parametric Characteristics of the Consensus Algorithms Operation with the Choice of the Most Priority One for Implementation in the Financial Sphere. *Electronics* **2021**, *10*, 2659. [CrossRef]
29. Wang, Y.; Hu, M.-L. Quantum Teleportation and Dense Coding in Multiple Bosonic Reservoirs. *Entropy* **2022**, *24*, 1114. [CrossRef] [PubMed]
30. Wen, X.; Chen, Y.; Zhang, W.; Jiang, Z.L.; Fang, J. Blockchain Consensus Mechanism Based on Quantum Teleportation. *Mathematics* **2022**, *10*, 2385. [CrossRef]
31. Pirandola, S.; Laurenza, R.; Ottaviani, C.; Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **2017**, *8*, 15043. [CrossRef] [PubMed]
32. Lucamarini, M.; Yuan, Z.; Dynes, J.; Shields, A. Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef] [PubMed]
33. Yan, F.; Wang, D. Probabilistic and controlled teleportation of unknown quantum states. *Phys. Lett. A* **2003**, *316*, 297–303. [CrossRef]
34. Khawasik, M.; El-Sayed, W.G.; Rashad, M.Z.; Younes, A. A Secured Half-Duplex Bidirectional Quantum Key Distribution Protocol against Collective Attacks. *Symmetry* **2022**, *14*, 2481. [CrossRef]

35. Cardoso-Isidoro, C.; Delgado, F. Shared Quantum Key Distribution Based on Asymmetric Double Quantum Teleportation. *Symmetry* **2022**, *14*, 713. [CrossRef]
36. Blunt, N.S.; Camps, J.; Crawford, O.; Izs'ak, R.; Leontica, S.; Mirani, A.; Moylett, A.E.; Scivier, S.A.; S¨underhauf, C.; Schopf, P.; et al. A Perspective on the Current State–of–the–art of Quantum Computing for Drug. *arXiv* **2022**, arXiv:2206.00551.
37. Chamberland, C.; Noh, K.; Arrangoiz–Arriola, P.; Campbell, E.T.; Hann, C.T.; Iverson, J.; Putterman, H.; Bohdanowicz, T.C.; Flammia, S.T.; Keller, A.; et al. Building a Fault–Tolerant Quantum Computer Using Concatenated Cat Codes, PRX Quantum 3. *arXiv* **2022**, arXiv:2012.04108.
38. Chamberland, C.; Campbell, E.T. Universal Quantum Computing with Twist–Free and Temporally Encoded Lattice Surgery. *PRX Quantum* **2022**, *3*, 010331. [CrossRef]
39. Kivlichan, I.D.; Gidney, C.; Berry, D.W.; Wiebe, N.; McClean, J.; Sun, W.; Jiang, Z.; Rubin, N.; Fowler, A.; Aspuru–Guzik, A.; et al. Improved Fault-Tolerant Quantum Simulation of Condensed–Phase Correlated Electrons via Trotterization, Quantum 4. *arXiv* **2020**, arXiv:1902.10673. [CrossRef]
40. Lu, D.; Li, Z.; Yu, J.; Han, Z. A Verifiable Arbitrated Quantum Signature Scheme Based on Controlled Quantum Teleportation. *Entropy* **2022**, *24*, 111. [CrossRef] [PubMed]
41. Hermans, S.L.; Pompili, M.; Beukers, H.K.C.; Baier, S.; Borregaard, J.; Hanson, R. Qubit Teleportation between Non–nbeighbouring Nodes in a Quantum Network. *Nature* **2022**, *605*, 663–668. [CrossRef]
42. Sun, Q.-C.; Mao, Y.-L.; Chen, S.-J.; Zhang, W.; Jiang, Y.-F.; Zhang, Y.-B.; Miki, S.; Yamashita, T.; Terai, H.; Jiang, X.; et al. Quantum teleportation with independent sources and prior entanglement distribution over a network. *Nat. Photon.* **2016**, *10*, 671–675. [CrossRef]
43. Xu, J.; Chen, X.; Xiao, H.; Wang, P.; Ma, M. A Performance–Consumption Balanced Scheme of Multi-Hop Quantum Networks for Teleportation. *Appl. Sci.* **2021**, *11*, 10869. [CrossRef]
44. Wu, H.; Liu, X.; Zhang, H.; Ruan, X.; Guo, Y. Performance Analysis of Continuous Variable Quantum Teleportation with Noiseless Linear Amplifier in Seawater Channel. *Symmetry* **2022**, *14*, 997. [CrossRef]
45. Benatti, F.; Floreanini, R.; Marzolino, U. Entanglement and Non-Locality in Quantum Protocols with Identical Particles. *Entropy* **2021**, *23*, 479. [CrossRef]
46. Raj, R.; Banerjee, S.; Panigrahi, P.K. Remote State Design for Efficient Quantum Metrology with Separable and Non-Teleporting States. *Quantum Rep.* **2021**, *3*, 228–241. [CrossRef]
47. Liss, R.; Mor, T. Quantum Communication—Celebrating the Silver Jubilee of Teleportation. *Entropy* **2020**, *22*, 628. [CrossRef] [PubMed]