07

On the cryptographic strength of the quantum key distribution protocol based on vector optical vortices

© D.D. Reshetnikov, E.R. Zinatullin, E.N. Bashmakova, A.V. Baeva, E.A. Vashukevich

St. Petersburg State University, St. Petersburg, Russia

e-mail: d.reshetnikov@spbu.ru

Received November 12, 2025
Revised November 12, 2025
Accepted December 10, 2025

The study investigates the cryptographic security of a quantum key distribution (QKD) protocol that utilizes vector optical vortices with an axially symmetric spatial polarization profile. A theoretical analysis is presented for the protocol's resistance against two types of attacks: the receive-send attack and the incoherent symmetric attack. Special attention is given to the analysis of potential advantages an eavesdropper (Eve) may have when using quantum systems with higher-dimensional state spaces (ququarts). The analysis showed that for this QKD protocol, the critical error level for both attacks under consideration is 25%. It is demonstrated that Eve's employment of ququart strategies does not reduce this threshold or provide her with an additional benefit over qubit-based attacks.

Keywords: Quantum key distribution, quantum cryptography, vector optical vortices, cryptographic strength.

DOI: 10.61011/EOS.2026.02.63466.8777-25

1. Introduction

Quantum key distribution (QKD) is a cryptographic technology that allows two legitimate users (Alice and Bob) to generate a common secret key, the security of which is guaranteed by the fundamental laws of quantum mechanics. Unlike classical cryptosystems, whose security is based on the computational complexity of certain mathematical problems, the security of QKD is unconditional and does not depend on the hacker's (Eve's) computational power [1].

The very first QKD protocol, BB84 [2] , is based on the use of two conjugate bases to encrypt the classical information using quantum states of single photons. This makes unambiguous discrimination of states by Eve impossible due to the no-cloning theorem. However, the key obstacle to the widespread application of this protocol was the lack of true single-photon sources. Later, protocols adapted for the use of weak coherent states instead of single photons were created. The most famous is the SARG04 protocol [3], which is resistant to the photon number splitting (PNS) attack, as well as protocols based on the decoy-state method [4,5]. Protocols based on continuous variables (CV-QKD), where information is encrypted in the quadratures of coherent states of light and detection is performed using homodyne measurement [6], have become widespread.

The theoretical security proof is a cornerstone of QKD systems and protocols. The approach to security proof can be divided into two main areas. The first area, dating back to the paper by Mayer [7], uses methods of quantum information theory. This approach allows calculating the secret key rate based on the Shannon mutual information between the quantum subsystems of the legitimate users and the hacker [8]. This approach is fundamental, however, it is based on asymptotic approximations of information theory and does not take into account aspects such as finite key length or possible multiple key usage.

The second area, known as the composable security method, was formalized in the papers by R. Renner et al. [9,10]. It is based on the paradigm of universal security, which guarantees the protocol's resistance not only in isolation but also when used together with other cryptographic systems. This method allows taking into account the finite number of transmitted quantum states, which is critically important for practical QKD implementations.

Despite proven theoretical security, practical implementations of QKD protocols are vulnerable to hardware attacks. This class of attacks is called „side-channel attacks„. The most famous examples are attacks blinding single-photon detectors, where a hacker uses bright illumination to switch the detectors into linear mode, allowing them to fully control their actuation [11]. Also, laser source attenuators are exposed to critical vulnerability; they can be switched by a hacker into multiphoton generation mode. This instantly opens up the possibility of a PNS attack, reducing the effectiveness of the decoy-state method [12–14].

Free-space QKD systems play an important role in practical implementation. In addition to solving the above problems, it is necessary to use degrees of freedom of the quantum system to encrypt raw key bits that would be resistant both to the influence of atmospheric turbulence (random refractive index fluctuations) and to spontaneous rotations of the polarization plane. The features of polarization encryption also manifest themselves in the so-called pointing problem. In free space, the relative orientation of the transmitting and receiving modules can change arbitrarily due to mechanical vibrations, temperature drifts, and atmospheric turbulence, which leads to unpredictable

rotations of the photon polarization plane and, consequently, to an increase in the quantum bit error rate (QBER) and complete disruption of the protocol operation [1,15]. To solve this problem, a number of approaches have been proposed in the literature, including the use of active feedback tracking systems based on measuring the Stokes vectors of a reference signal [16], or the use of passive methods, such as optical compensators based on liquid crystals [17].

An alternative and more fundamental solution is the transition to protocols insensitive to global rotation of the polarization plane. The paper [18] proposed a protocol based on quantum states of light with an axially symmetric polarization distribution, which has a number of advantages. Firstly, such an encryption method does not require prior alignment of the polarization planes of the transmitting and receiving equipment (as, for example, in the case of the conventional BB84 protocol based on linear polarization bases). Secondly, a well-developed theoretical and experimental apparatus for wave front reconstruction of such beams allows them to be effectively used under atmospheric optical turbulence (the „last mile“ problem) [19]. An important feature of the proposed protocol is also the possibility of fast generation of quantum states encrypting information. This is a critical aspect of protocols using spatial mode states, since common and widely used methods to generate states using spatial light modulators (SLMs) are very limited for use in real technical implementations of QKD systems due to the relatively low speed of the modulator [20]. We proposed an interference scheme for both generation and detection of quantum code states, which allows them to be generated at the speed of the phase modulator [21]. The paper is dedicated to assessing the cryptographic strength of the protocol against key and most common types of attacks on the protocol: the intercept-resend attack and the incoherent symmetric attack.

2. Quantum key distribution protocol based on axially symmetric vector beams

Before proceeding to the procedure for assessing cryptographic strength, we will describe the QKD protocol based on axially symmetric polarization beams and note its key features [18–22]. The protocol is based on 4 basis states ($|\Phi_{11}\rangle$ — radially polarized (RP) beam, $|\Phi_{12}\rangle$ — axially polarized (AR) beam, $|\Phi_{21}\rangle$ — right-twisted polarization (RTP) beam, $|\Phi_{22}\rangle$ — left-twisted polarization (LTP) beam), used to encrypt the secret key bits:

$$|\Phi_{11}\rangle = |\mathbf{D_R}|LG_{0,1}|\rangle, |\Phi_{12}\rangle = |\mathbf{D_A}|LG_{0,1}|\rangle, \quad (1)$$

$$|\Phi_{21}\rangle = |\mathbf{D_{RR}}|LG_{0,1}|\rangle, |\Phi_{22}\rangle = |\mathbf{D_{LR}}|LG_{0,1}|\rangle, \quad (2)$$

where $\mathbf{D_i}$ — Jones vectors specified in Fig. 1, $|LG_{0,1}|$ — Laguerre-Gaussian function module [23].

The pair of orthogonal states $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$, as well as the pair $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$, form a basis of a 2-dimensional Hilbert space, and the bases are conjugate. Within the framework of the described protocol, the generation of axially symmetric polarization states is carried out by adding optical beams with orbital angular moment (topological charge) ± 1 and circular polarizations in a Mach-Zehnder interferometer scheme (Fig. 2,*a*). The expansion of the basis states is as follows:

$$|\Phi_{11}\rangle = \frac{1}{\sqrt{2}}(|R\rangle \otimes |+1\rangle + |L\rangle \otimes |-1\rangle) = \frac{1}{2}\left(\begin{pmatrix}1\\ i\end{pmatrix}||LG_{0,1}|\rangle e^{i\phi} + \begin{pmatrix}1\\ -i\end{pmatrix}||LG_{0,1}|\rangle e^{-i\phi}\right), \quad (3)$$

$$|\Phi_{12}\rangle = \frac{1}{\sqrt{2}}(|R\rangle \otimes |+1\rangle - |L\rangle \otimes |-1\rangle) = \frac{1}{2}\left(\begin{pmatrix}1\\ i\end{pmatrix}||LG_{0,1}|\rangle e^{i\phi} - \begin{pmatrix}1\\ -i\end{pmatrix}||LG_{0,1}|\rangle e^{-i\phi}\right), \quad (4)$$

$$|\Phi_{21}\rangle = \frac{1}{\sqrt{2}}(|R\rangle \otimes |+1\rangle + i|L\rangle \otimes |-1\rangle) = \frac{1}{2}\left(\begin{pmatrix}1\\ i\end{pmatrix}||LG_{0,1}|\rangle e^{i\phi} + i\begin{pmatrix}1\\ -i\end{pmatrix}||LG_{0,1}|\rangle e^{-i\phi}\right), \quad (5)$$

$$|\Phi_{22}\rangle = \frac{1}{\sqrt{2}}(|R\rangle \otimes |+1\rangle - i|L\rangle \otimes |-1\rangle) = \frac{1}{2}\left(\begin{pmatrix}1\\ i\end{pmatrix}||LG_{0,1}|\rangle e^{i\phi} - i\begin{pmatrix}1\\ -i\end{pmatrix}||LG_{0,1}|\rangle e^{-i\phi}\right). \quad (6)$$

Here the ket-vectors $|R\rangle$ and $|L\rangle$ denote polarization modes with right- and left-circular polarizations, respectively. The ket-vectors $|\pm 1\rangle$ are responsible for the orbital angular moment of the optical vortex, with the plus sign corresponding to clockwise phase rotation and the minus sign — to counterclockwise rotation.

Fig. 2, *a* shows a simplified diagram of the generation of optical vortices with the required polarization states and topological charge in a modified Mach-Zehnder interferometer scheme with corner reflectors.

At the output of the scheme, a state is formed

$$|\Phi_{\text{out}}\rangle = 1/\sqrt{2}(|R, +1\rangle + e^{iP}|L, -1\rangle). \quad (7)$$

The sender (Alice) can encrypt key bit values in the basis $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$ or in the basis $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$. To do this, she selects the required phase value P using a phase modulator PM ($0, \pi$ for the first basis and $\pi/2, -\pi/2$ for the conjugate one) between states $|R, +1\rangle$ and $|L, -1\rangle$ and adds them in the output Mach-Zehnder interferometer.

The optical vortex detection scheme is shown in Fig. 2, *b*. The receiver (Bob) uses a similar Mach-Zehnder interferometer to expand the azimuthally symmetric polarization states, after which, using static optical elements (OAM phase holograms ± 1), he transforms them into states with

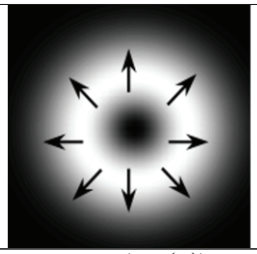
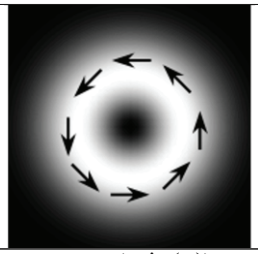
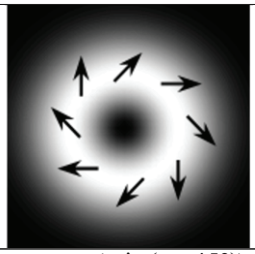
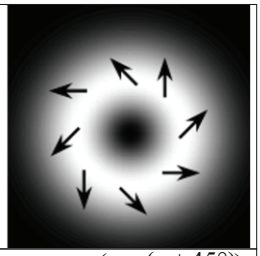
Beam structure				
Jones vector	$\mathbf{D_{RP}}=\begin{pmatrix}\cos(\varphi)\\ \sin(\varphi)\end{pmatrix}$	$\mathbf{D_{AP}}=\begin{pmatrix}-\sin(\varphi)\\ \cos(\varphi)\end{pmatrix}$	$\mathbf{D_{LRP}}=\begin{pmatrix}-\sin(\varphi+45°)\\ \cos(\varphi+45°)\end{pmatrix}$	$\mathbf{D_{RRP}}=\begin{pmatrix}\cos(\varphi+45°)\\ \sin(\varphi+45°)\end{pmatrix}$

Figure 1. Basis modes used in the quantum key distribution protocol and their corresponding Jones vectors.

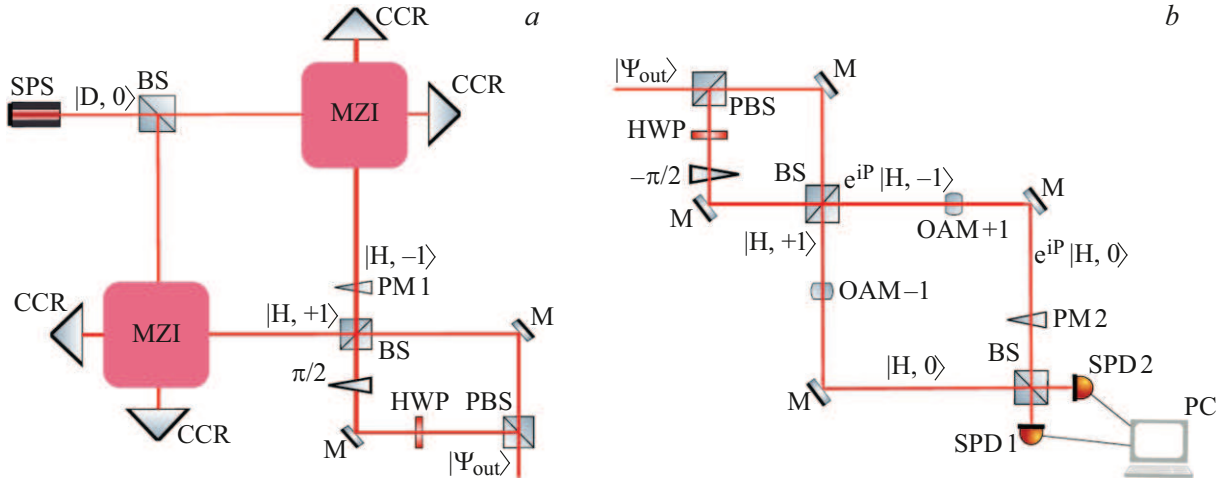


Figure 2. Simplified generation diagram (a) and detection diagram (b) of the basis states of the quantum key distribution protocol. SPS — single-photon source, BS — beam splitting cube, PBS — polarization beam splitting cube, MZI — Mach-Zehnder interferometer, CCR — cube corner reflector, HWP — $\lambda/2$-plate, $\pm\pi/2$ — phase plate, PM — controlled phase modulator, M — mirror, OAM ±1 — phase holograms that change the value of the orbital angular moment of the beam, SPD — single-photon detector.

zero topological charge and linear polarization. Bob's choice of additional phase of PM 2 determines the detection basis: phase 0 corresponds to detection in the basis $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$, phase $\pi/2$ —to detection in basis $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$. Finally, Bob mixes the beams on a conventional beam splitter BS and performs measurements in both output channels using single-photon detectors. When measuring in the basis $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$, the actuation of detector SPD 1 will mean that the phase difference between the beams is 0, and therefore Alice sent the state $|\Phi_{11}\rangle$. In turn, the actuation of detector SPD 2 indicates the presence of a phase difference π and the sending of the state $|\Phi_{12}\rangle$. Moreover, if such states are measured in the conjugate basis, the detectors will actuate with equal probability. The key sifting and privacy amplification procedures are carried out similarly to the BB84 protocol.

After the sifting procedure, Alice and Bob disclose a part of the secret key for comparison to determine attempts to intrude into the quantum key distribution channel. Based on the comparison results, they conclude whether a third party (Eve) listens. When assessing the cryptographic strength of the protocol, we will limit ourselves to the case of symmetric attacks. In this case, the results of Eve's actions will be statistically indistinguishable from physical noise in the quantum channel, and Alice and Bob will conclude whether Eve is present in the communication channel based on comparing the QBER with a certain critical error level. In the next section, we will determine the critical error level for two types of attacks: the intercept-resend attack and the collective symmetric attack.

3. Intercept-resend attack

The simplest listening strategy is the intercept-resend attack. Within the framework of this attack, Eve intercepts each state that Alice sends to Bob. She then measures it and sends Bob a state that is a copy of the measured one. Let us estimate the amount of information that Eve has access to. In general, the Shannon information is defined as follows:

$$I_{\text{Eve}} = \log_2 d + \sum_{i=1}^{d} p_i \log_2 p_i, \tag{8}$$

where p_i are the probabilities of various measurement outcomes, and d is the dimension of the state space used.

Before moving on to estimating the information available to Eve, let us note one important feature of the protocol. The basis states used can be described in a higher-dimensional space, namely, in a ququart space, with a logical basis of the form

$$\begin{aligned}|1\rangle &= |H\rangle \otimes |+1\rangle,\\ |2\rangle &= |H\rangle \otimes |-1\rangle,\\ |3\rangle &= |V\rangle \otimes |+1\rangle,\\ |4\rangle &= |V\rangle \otimes |-1\rangle,\end{aligned} \tag{9}$$

where the ket-vectors $|H\rangle$, $|V\rangle$ describe the states of a photon with horizontal and vertical polarization, respectively, and the ket-vectors $|+1\rangle$, $|-1\rangle$ describe the states of a photon with a topological charge equal to ± 1. In this basis, Alice's code states are written as follows:

$$\begin{aligned}|\Phi_{11}\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle \otimes |+1\rangle + |L\rangle \otimes |-1\rangle\right)\\ &= \frac{1}{2}\left(|1\rangle + |2\rangle + i|3\rangle - i|4\rangle\right),\end{aligned} \tag{10}$$

$$\begin{aligned}|\Phi_{12}\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle \otimes |+1\rangle - |L\rangle \otimes |-1\rangle\right)\\ &= \frac{1}{2}\left(|1\rangle - |2\rangle + i|3\rangle + i|4\rangle\right),\end{aligned} \tag{11}$$

$$\begin{aligned}|\Phi_{21}\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle \otimes |+1\rangle + i|L\rangle \otimes |-1\rangle\right)\\ &= \frac{1}{2}\left(|1\rangle + i|2\rangle + i|3\rangle + |4\rangle\right).\end{aligned} \tag{12}$$

$$\begin{aligned}|\Phi_{22}\rangle &= \frac{1}{\sqrt{2}}\left(|R\rangle \otimes |+1\rangle - i|L\rangle \otimes |-1\rangle\right)\\ &= \frac{1}{2}\left(|1\rangle - i|2\rangle + i|3\rangle - |4\rangle\right).\end{aligned} \tag{13}$$

Such a representation of basis states provides Eve with a potential opportunity to build her attacks from a higher-dimensional space, therefore in the following discussion we will consider 2 types of attacks: Eve using states from a qubit space and states from a ququart space.

3.1. Intercept-resend attack in qubit space

First, let us estimate the amount of Eve's information during an attack in qubit space ($d = 2$):

• Let Eve correctly guesses the basis, i.e., her measurement basis coincides with the one Alice used to encrypt the state. The probability distribution of measuring various states has the form $p_i = \{1; 0\}$, i.e. Eve will always receive the state sent by Alice when measuring. Then the Shannon entropy is

$$H_{\text{success}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -(1\log_2 1 + 0\log_2 0) = 0\,\text{bit}. \tag{14}$$

• Let Eve incorrectly guesses the basis, i.e., her basis does not coincide with the basis Alice used for encryption. The probability distribution of measuring various states has the form $p_i = \{\frac{1}{2}; \frac{1}{2}\}$, i.e., Eve will receive the state sent by Alice when measuring only with a 50% probability. Then the Shannon entropy is

$$\begin{aligned}H_{\text{failure}} &= -\sum_{i=1}^{d} p_i \log_2 p_i\\ &= -\left(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}\right) = 1\,\text{bit}.\end{aligned} \tag{15}$$

• Since in this attack Eve selects one of two bases ($\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$ or $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$) randomly, the Eve's average information is

$$I_{\text{Eve}} = \log_2 d - \frac{1}{2}H_{\text{success}} - \frac{1}{2}H_{\text{failure}} = \frac{1}{2}\,\text{bit}, \tag{16}$$

and Eve has access to the half of the sent information. The total error is equal to the product of the error probabilities of Eve's and Bob's detection and is

$$P_{\text{sum}} = P_{\text{Eve}}P_{\text{Bob}} = \frac{1}{2}\frac{1}{2} = \frac{1}{4}. \tag{17}$$

These results are completely similar to the estimate for the BB84 protocol on linear polarizations [25].

3.2. Intercept-resend attack in ququart space

Now let us estimate the information available to Eve in the case of an attack using a ququart basis for measurements ($d = 4$). Since the probability distribution of measuring various states directly depends on the expansion coefficients of Alice's states in the detection basis states, it is necessary to construct all possible projectors of states to estimate Eve's optimal strategy. In ququart space, there are 5 different mutually unbiased bases (MUB) that Eve can use [24]. At the same time, estimating the „correctness„ of the guessed basis becomes a non-trivial task. Appendix A calculates all projections of the states used for encoding by Alice onto the states that make up the mutually unbiased bases of Eve's measurement ququart space. The most information for Eve will be provided by measurements in those bases that yield the least uncertainty, i.e., the greatest possibility of distinguishing states. Of primary interest from the point of view of maximizing probabilities are measurements in bases IV and V:

$$|\langle\Phi_{11}|\Psi_{\text{IV},1}\rangle|^2 = 1, \quad |\langle\Phi_{11}|\Psi_{\text{V},1}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\mathrm{IV},2}\rangle|^2 = 0, \quad |\langle\Phi_{11}|\Psi_{\mathrm{V},2}\rangle|^2 = \frac{1}{4};$$
$$|\langle\Phi_{11}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0, \quad |\langle\Phi_{11}|\Psi_{\mathrm{V},3}\rangle|^2 = \frac{1}{4};$$
$$|\langle\Phi_{11}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0, \quad |\langle\Phi_{11}|\Psi_{\mathrm{V},4}\rangle|^2 = \frac{1}{4};$$
$$|\langle\Phi_{12}|\Psi_{\mathrm{IV},1}\rangle|^2 = 0, \quad |\langle\Phi_{12}|\Psi_{\mathrm{V},1}\rangle|^2 = \frac{1}{4};$$
$$|\langle\Phi_{12}|\Psi_{\mathrm{IV},2}\rangle|^2 = 1, \quad |\langle\Phi_{12}|\Psi_{\mathrm{V},2}\rangle|^2 = \frac{1}{4};$$
$$|\langle\Phi_{12}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0, \quad |\langle\Phi_{12}|\Psi_{\mathrm{V},3}\rangle|^2 = \frac{1}{4};$$
$$|\langle\Phi_{12}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0, \quad |\langle\Phi_{12}|\Psi_{\mathrm{V},4}\rangle|^2 = \frac{1}{4};$$
$$|\langle\Phi_{21}|\Psi_{\mathrm{IV},1}\rangle|^2 = \frac{1}{2}, \quad |\langle\Phi_{21}|\Psi_{\mathrm{V},1}\rangle|^2 = 0;$$
$$|\langle\Phi_{21}|\Psi_{\mathrm{IV},2}\rangle|^2 = \frac{1}{2}, \quad |\langle\Phi_{21}|\Psi_{\mathrm{V},2}\rangle|^2 = 0;$$
$$|\langle\Phi_{21}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0, \quad |\langle\Phi_{21}|\Psi_{\mathrm{V},3}\rangle|^2 = \frac{1}{2};$$
$$|\langle\Phi_{21}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0, \quad |\langle\Phi_{21}|\Psi_{\mathrm{V},4}\rangle|^2 = \frac{1}{2};$$
$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},1}\rangle|^2 = \frac{1}{2}, \quad |\langle\Phi_{22}|\Psi_{\mathrm{V},1}\rangle|^2 = \frac{1}{2};$$
$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},2}\rangle|^2 = \frac{1}{2}, \quad |\langle\Phi_{22}|\Psi_{\mathrm{V},2}\rangle|^2 = \frac{1}{2};$$
$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0, \quad |\langle\Phi_{22}|\Psi_{\mathrm{V},3}\rangle|^2 = 0;$$
$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0, \quad |\langle\Phi_{22}|\Psi_{\mathrm{V},4}\rangle|^2 = 0. \qquad (18)$$

Here the index of state $|\Psi_{i,j}\rangle$ $i \in \{\mathrm{I}, \mathrm{II}, \mathrm{III}, \mathrm{IV}, \mathrm{V}\}$ means MUB, index $j \in \{1, 2, 3, 4\}$ — serial number of basis vector in this MUB. The full information on the expansion coefficients is available in Appendix A.

To clearly distinguish the states from basis $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$, Eve must measure in IV MUB. And if Eve attempts to measure the states from basis $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$, she will receive the equally probable projects to states $|\Psi_{\mathrm{IV},1}\rangle$ and $|\Psi_{\mathrm{IV},2}\rangle$. To distinguish these states, she will have to measure in basis II or V (they are equal from this point of view). Let us assume that Eve will be using basis V. In this case when states $|\Psi_{\mathrm{V},3}\rangle$ or $|\Psi_{\mathrm{V},4}\rangle$ are detected, she concludes that Alice sent state $|\Phi_{21}\rangle$, and when states $|\Psi_{\mathrm{V},1}\rangle$ or $|\Psi_{\mathrm{V},2}\rangle$ are detected — that Alice sent state $|\Phi_{22}\rangle$ (obviously, if Eve guessed the encryption basis right). Let us assume the scope of information available to Eve in the described approach to the attack:

• Let Eve correctly guesses the basis, i. e., she performs measurements in the most suitable of the available MUBs for the state sent by Alice. Consider the case of Eve using basis IV. In this basis, Eve can unambiguously identify states $|\Phi_{11}\rangle$ and $|\Phi_{12}\rangle$. The probability distribution of measuring various states has the form $p_i = \{1; 0; 0; 0\}$, i. e. Eve will always receive the state sent by Alice when measuring. Then the Shannon entropy is

$$H_{\mathrm{success_{IV}}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -(1\log_2 1 + 0\log_2 0 + 0\log_2 0 + 0\log_2 0) = 0\,\mathrm{bit}. \qquad (19)$$

If Eve uses basis V, Eve does not unambiguously distinguish states $|\Phi_{12}\rangle$ and $|\Phi_{22}\rangle$, but with probability $1/2$ she receives states $|\Psi_{\mathrm{V},1}\rangle$ and $|\Psi_{\mathrm{V},2}\rangle$ or $|\Psi_{\mathrm{V},3}\rangle$ and $|\Psi_{\mathrm{V},4}\rangle$ as a result of the measurement for the Alice's states $|\Phi_{21}\rangle$ and $|\Phi_{22}\rangle$ respectively. The probability distribution of measuring various states has the form $p_i = \{\frac{1}{2}; \frac{1}{2}; 0; 0\}$. Then the Shannon entropy is

$$H_{\mathrm{success_V}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -\Big(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2} + 0\log_2 0 + 0\log_2 0\Big) = 1\,\mathrm{bit}. \qquad (20)$$

• Let Eve incorrectly guesses the basis, i. e., she performs measurements in a MUB unsuitable for Alice's state. Consider the case of Eve using basis IV. When trying to measure states $|\Phi_{21}\rangle$ and $|\Phi_{22}\rangle$ in this basis, Eve will detect states $|\Psi_{\mathrm{V},1}\rangle$ and $|\Psi_{\mathrm{V},2}\rangle$ with equal probabilities. The probability distribution of measuring various states has the form $p_i = \{\frac{1}{2}; \frac{1}{2}; 0; 0\}$. Then the Shannon entropy is

$$H_{\mathrm{failure_{IV}}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -\Big(\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2} + 0\log_2 0 + 0\log_2 0\Big) = 1\,\mathrm{bit}. \qquad (21)$$

If Eve uses basis V to measure states $|\Phi_{11}\rangle$ and $|\Phi_{12}\rangle$, she will detect any of the basis states with equal probability. The probability distribution of measuring various states has the form $p_i = \{\frac{1}{4}; \frac{1}{4}; \frac{1}{4}; \frac{1}{4}\}$. Then the Shannon entropy is

$$H_{\mathrm{failure_V}} = -\sum_{i=1}^{d} p_i \log_2 p_i = -\Big(\frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4} + \frac{1}{4}\log_2\frac{1}{4}\Big) = 2\,\mathrm{bit}. \qquad (22)$$

• Since in this attack Eve selects the basis randomly (IV or V), the averaged information available to Eve is

$$I_{\mathrm{Eve}} = \log_2 d - \frac{1}{2}H_{\mathrm{success}} - \frac{1}{2}H_{\mathrm{failure}} = 2 - \frac{1}{2}\Big(\frac{1}{2}0 + \frac{1}{2}1\Big) - \frac{1}{2}\Big(\frac{1}{2}1 + \frac{1}{2}2\Big) = 1\,\mathrm{bit}, \qquad (23)$$

and Eve resumes access to the half of the sent information. The probability of the total error is equal to the product of the error probabilities of Eve and Bob and is

$$P_{\mathrm{sum}} = P_{\mathrm{Eve}}P_{\mathrm{Bob}} = \frac{1}{2}\frac{1}{2} = \frac{1}{4}. \qquad (24)$$

Thus, Eve's use of a higher-dimensional state space does not give her an advantage when conducting an intercept-resend attack, and the critical error level is 25%. The obtained results are similar to the intercept-resend attack at the classical BB84 protocol, with Eve also has access to half of the sent information [25].

4. Incoherent symmetric attack

Some papers [26,27] proposed an optimal strategy for Eve, when she receives the maximum information value with the minimum introduced disturbance. Eve is acting as follows: she intercepts Alice's states, entangles them with her auxiliary system and sends the initial Alice's state that was intercepted and is now disturbed, to Bob. Then Eve saves the state of the auxiliary system in the quantum memory and waits for the public disclosure of bases, and measures afterwards. The scope of information that Eve is now receiving, depends on the value of impact at the Alice's states, and also on the method of auxiliary system state measurement. The stronger the impact, the more information Eve receives, but at the same time the disturbance she introduces into the quantum communication channel increases as well.

This attack in qubit space was analyzed in detail in paper [27]. Fundamental entropy ratios were used to show that the critical error level from Eve's interference into the communication channel was

$$D_c = \frac{1}{2} - \frac{1}{4}\sqrt{2} \approx 0.146 \tag{25}$$

or 14.6 %. Next, we will consider Eve's strategy when using basis states of a higher-dimensional space ($d = 4$) and compare the obtained result with the critical error in the case of an attack using a 2-dimension Hilbert space.

In the general case the Eve's strategy in the ququart space is the following:

$$\begin{aligned}
U|0\rangle \otimes |E\rangle &= \sqrt{D-1}|0\rangle \otimes |E_{00}\rangle + \sqrt{D/3}|1\rangle \otimes |E_{01}\rangle \\
&+ \sqrt{D/3}|2\rangle \otimes |E_{02}\rangle + \sqrt{D/3}|3\rangle \otimes |E_{03}\rangle, \\
U|1\rangle \otimes |E\rangle &= \sqrt{D/3}|0\rangle \otimes |E_{10}\rangle + \sqrt{D-1}|1\rangle \otimes |E_{11}\rangle \\
&+ \sqrt{D/3}|2\rangle \otimes |E_{12}\rangle + \sqrt{D/3}|3\rangle \otimes |E_{13}\rangle, \\
U|2\rangle \otimes |E\rangle &= \sqrt{D/3}|0\rangle \otimes |E_{20}\rangle + \sqrt{D/3}|1\rangle \otimes |E_{21}\rangle \\
&+ \sqrt{D-1}|2\rangle \otimes |E_{22}\rangle + \sqrt{D/3}|3\rangle \otimes |E_{23}\rangle, \\
U|3\rangle \otimes |E\rangle &= \sqrt{D/3}|0\rangle \otimes |E_{30}\rangle + \sqrt{D/3}|1\rangle \otimes |E_{31}\rangle \\
&+ \sqrt{D/3}|2\rangle \otimes |E_{32}\rangle + \sqrt{D-1}|3\rangle \otimes |E_{33}\rangle,
\end{aligned} \tag{26}$$

where $|i\rangle$, $i \in \{0, 1, 2, 3\}$ — vectors of state of logical basis in ququart space, $|E\rangle$ and $|E_{00}\rangle, |E_{01}\rangle, \ldots$ — normalized vectors of Eve's auxiliary state before and after interaction, accordingly, D — value of disturbance introduced by Eve into the communication channel, U — unitary intertwining transformation. In virtue of operator U unitarity, Eve's states must satisfy the orthogonality property:

$$\langle E| \otimes \langle i|U^\dagger U|j\rangle \otimes |E\rangle = 0, \, i, \, j \in \{0, 1, 2, 3\}. \tag{27}$$

During the attack Eve attempts to maximize the information on the Alice's quantum system available to her, while introducing the least possible disturbance. In fact Eve chooses her auxiliary states so that this optimization task is solved. Eve's interaction with the random Alice's state causes excitation of the state received by Bob $D_{(k)}$, which may be found as

$$D_{(k)} = 1 - \langle k|\rho^{(k)}_{B,\mathrm{Out}}|k\rangle, \tag{28}$$

where $\langle k| \in \{|\Phi_{11}\rangle, |\Phi_{12}\rangle, |\Phi_{21}\rangle, |\Phi_{22}\rangle\}$ — one of the possible Alice's states, and $\rho^{(k)}_{B,\mathrm{Out}}$ — reduced matrix of density of the state sent to Bob after exposure to Eve. It may be calculated as follows:

$$\rho^{(k)}_{B,\mathrm{Out}} = \mathrm{Tr}_E[U|k\rangle \otimes |E\rangle\langle E| \otimes \langle k|U^\dagger]. \tag{29}$$

The value of the introduced disturbance depends on the selection of the Eve's auxiliary states and subsequent procedure of their measurement. Therefore, it is necessary to receive the clear relation between disturbance D and scalar products of auxiliary states. Since we consider the case of the symmetric attack, all disturbances $D_{(k)}$ must be equal to each other:

$$\begin{aligned}
1 - \langle k|\mathrm{Tr}_E[U|k\rangle \otimes |E\rangle\langle E| \otimes \langle k|U^\dagger]|k\rangle = D, \\
k \in \{\Phi_{11}, \Phi_{12}, \Phi_{21}, \Phi_{22}\}.
\end{aligned} \tag{30}$$

The action of the operator U at the Alice's states is calculated using equations (26). Therefore, solving system (30) together with orthogonality conditions (27), we obtain expressions relating the value of the disturbance to the scalar products of Eve's auxiliary states $|E_{ij}\rangle$. Due to the symmetry of the problem, the following scalar products are nonzero:

$$\langle E_{ii}|E_{jj}\rangle = s, \quad \text{where} \quad i \neq j, \tag{31}$$

$$\begin{aligned}
\langle E_{ij}|E_{hk}\rangle = w, \quad \text{where} \quad j \neq i, \\
(h = j \ \text{ and } k = i) \ \text{ or } \ (h \neq k \neq i \neq j),
\end{aligned} \tag{32}$$

and the value of the disturbance is related to them as

$$s = \frac{1 - wD}{1 - D} + \frac{4}{3}\frac{D}{D-1}. \tag{33}$$

It is important to note that the obtained relationship (33) is similar to that obtained in [26] for the case of two encryption bases in ququart space.

Now let us find how the mutual information of the Alice-Eve subsystems is related to the choice of Eve's auxiliary states. To do this, consider possible situations. In the first case, Bob correctly determines Alice's state with probability

$1 - D$, and Eve also correctly determines this state with some probability $p_1(s, w, D)$. The explicit form of the dependence of probability on the problem parameters is quite cumbersome, and we will limit ourselves here to a reference to [26], where a similar theory is presented more fully. In the second case, Bob, when measuring, obtains a state different from the one sent by Alice with probability D. Eve will correctly determine the sent state with probability $p_2(s, w, D)$. Then the mutual information of the Alice-Eve subsystems I_{AE} is

$$I_{AE}(s, w, D) = (1 - D)I_4(p_1) + DI_4(p_2), \qquad (34)$$

where Shannon information $I_4(x)$ in ququart space is

$$I_4(x) = 1 + x\log_4(x) + (1 - x)\log_4\left(\frac{1 - x}{3}\right). \qquad (35)$$

Eve seeks to obtain maximum information about Alice's system, and therefore chooses the auxiliary states in an optimal way. The mutual information of the Alice-Eve subsystems $I_{AE}(s, w, D)$ reaches its maximum value when

$$w = 1 - \frac{4}{3}D. \qquad (36)$$

Conditions (33), (36) determine Eve's choice of auxiliary states, and the probabilities $p_1(s, w, D)$ and $p_2(s, w, D)$ now depend only on the value of the disturbance D and have the following form:

$$p_1(D) = \frac{2D^2 - D - 2\sqrt{3}\sqrt{-(D-1)^3 D} - 1}{4(D-1)}, \qquad (37)$$

$$p_2(D) = \frac{1}{4}\left(2D + 2\sqrt{3}\sqrt{-(D-1)D} + 1\right). \qquad (38)$$

Finally, we can determine the critical error level in the case of an incoherent symmetric attack by Eve. The critical error threshold is the value of the disturbance D_c at which the mutual information of the Alice-Eve subsystems $I_{AE}(D)$ and the Alice-Bob subsystems $I_{AB,4}(D)$ is compared. The latter in ququart space is found as follows:

$$I_{AB,4}(D) = 1 + (1 - D)\log_4(1 - D) + D\log_4\frac{D}{3}. \qquad (39)$$

Solving the equation

$$I_{AE}(D_c) = I_{AB,4}(D_c), \qquad (40)$$

we find that the critical error level for an incoherent symmetric attack is $D_c = 0.25$ (25%). Comparing this result to expression (25), note that Eve's use of ququart space of states did not benefit her in case of an incoherent attack. Therefore, the optical strategy of Eve's actions in case of an incoherent attack will be a symmetric attack from qubit space. In this case with the same value of the available information Eve will introduce less disturbance into the communication channel.

5. Conclusion

We have demonstrated the resistance of the protocol based on axially symmetric polarization vortices to the two most common types of attacks: intercept-resend and incoherent symmetric attack. Besides, a feature of the protocol was taken into account, related to the fact that Alice's code states can be described both in qubit and ququart Hilbert spaces. It has been strictly demonstrated that Eve's use of attacks from a higher-dimensional state space does not provide an advantage in terms of reducing the critical error. At the same time, we did not consider a coherent attack with collective measurements, where Eve interacts simultaneously with all of Alice's quantum systems. This type of attack is optimal because it leads to the lowest critical error (11% for the BB84 protocol). However, a coherent attack is the most difficult to implement in practice. Moreover, in [28,29] it was shown that this type of attack in an arbitrary-dimensional space reduces to fundamental entropy relations, regardless of the code states used by Alice. The critical error also increases with increasing space dimension.

Analyzing the protocol resistance to the attacks at the technical component of the QKD systems, one can note that within the considered protocol and methods of basis state generation and detection, the relevant attacks are the attacks related to probing of radiation and interference into the operation of the phase and amplitude modulators on the Alice's side, as well as similar impact on the phase modulator and detectors of single photons on the Bob's side. However, it has been shown in papers [30,31] that for systems with phase methods of generating basis states, attacks blinding avalanche detectors and the Detectors Mismatch attack are ineffective.

Our further interest in the study of QKD protocols is focused on the area of high-dimensional protocols that use non-binary logic to encrypt information, since the considered vector states with an axially symmetric polarization state have a natural description in a 4-dimensional logical space. However, extending the protocol to the ququart case requires an analysis of methods for generating and detecting such radiation, as well as a detailed study of the cryptographic strength issues of high-dimensional QKD protocols.

Funding

The work was supported with grant of JSC „RZD“ (agreement № 5950981 dated December 17, 2024).

Conflict of interest

The authors declare that they have no conflict of interest.

Logical basis states of MUB in ququart space

Basis number	Basis states
I	$\|0\rangle$ $\|1\rangle$ $\|2\rangle$ $\|3\rangle$
II	$\frac{1}{2}(\|0\rangle + \|1\rangle + \|2\rangle + \|3\rangle)$ $\frac{1}{2}(\|0\rangle - \|1\rangle + \|2\rangle - \|3\rangle)$ $\frac{1}{2}(\|0\rangle + \|1\rangle - \|2\rangle - \|3\rangle)$ $\frac{1}{2}(\|0\rangle - \|1\rangle - \|2\rangle + \|3\rangle)$
III	$\frac{1}{2}(\|0\rangle + i\|1\rangle + i\|2\rangle - \|3\rangle)$ $\frac{1}{2}(\|0\rangle - i\|1\rangle + i\|2\rangle + \|3\rangle)$ $\frac{1}{2}(\|0\rangle + i\|1\rangle - i\|2\rangle + \|3\rangle)$ $\frac{1}{2}(\|0\rangle - i\|1\rangle - i\|2\rangle - \|3\rangle)$
IV	$\frac{1}{2}(\|0\rangle + \|1\rangle + i\|2\rangle - i\|3\rangle)$ $\frac{1}{2}(\|0\rangle - \|1\rangle + i\|2\rangle + i\|3\rangle)$ $\frac{1}{2}(\|0\rangle + \|1\rangle - i\|2\rangle + i\|3\rangle)$ $\frac{1}{2}(\|0\rangle - \|1\rangle - i\|2\rangle - i\|3\rangle)$
V	$\frac{1}{2}(\|0\rangle + i\|1\rangle + \|2\rangle - i\|3\rangle)$ $\frac{1}{2}(\|0\rangle + i\|1\rangle - \|2\rangle + i\|3\rangle)$ $\frac{1}{2}(\|0\rangle - i\|1\rangle + \|2\rangle + i\|3\rangle)$ $\frac{1}{2}(\|0\rangle - i\|1\rangle - \|2\rangle - i\|3\rangle)$

Appendix A. Projects of Alice's code states to MUB states in ququart space

In ququart space with logical basis of $\{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ type there are 5 MUB. If the quantum system is prepared in the intrinsic state of one of MUB, it is predicted that all measurement results relative to any other MUB will happen with equal probability $1/d$. Here d — dimension of Hilbert space, where the quantum system is described. In 4 dimension Hilbert space this set of bases looks like in the table.

Coefficients of expansion of code states $|\Phi_{11}\rangle, |\Phi_{12}\rangle, |\Phi_{21}\rangle, |\Phi_{22}\rangle$ into logical states of MUB are calculated as the projector square module:

$$|\langle\Phi_{11}|0\rangle|^2 = \left|\left(\frac{1}{2}(|1\rangle + |2\rangle + i|3\rangle - i|4\rangle)\right)|0\rangle\right|^2$$

$$= \frac{1}{4}\left|\langle 0|0\rangle + \langle 1|0\rangle + \langle 2|0\rangle + \langle 3|0\rangle\right|^2 = \frac{1}{4}, \qquad \text{(A1)}$$

in virtue of orthogonality of states $\langle i|j\rangle = 0, \ i \neq j$, $i, j \in \{0, 1, 2, 3\}$. Similarly all other expansion coefficients are calculated. State index $|\Psi_{i,j}\rangle \ i \in \{\text{I, II, III, IV, V}\}$ means MUB, index $j \in \{1, 2, 3, 4\}$ — serial number of basis vector in this MUB:

$$|\langle\Phi_{11}|\Psi_{\text{I},1}\rangle|^2 = \frac{1}{4}, |\langle\Phi_{11}|\Psi_{\text{II},1}\rangle|^2 = \frac{1}{4}, |\langle\Phi_{11}|\Psi_{\text{III},1}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{11}|\Psi_{\text{IV},1}\rangle|^2 = 1, \ |\langle\Phi_{11}|\Psi_{\text{V},1}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\text{I},2}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{11}|\Psi_{\text{II},2}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{11}|\Psi_{\text{III},2}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{11}|\Psi_{\text{IV},2}\rangle|^2 = 0, \ |\langle\Phi_{11}|\Psi_{\text{V},2}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\text{I},3}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{11}|\Psi_{\text{II},3}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{11}|\Psi_{\text{III},3}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{11}|\Psi_{\text{IV},3}\rangle|^2 = 0, \ |\langle\Phi_{11}|\Psi_{\text{V},3}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{11}|\Psi_{\text{I},4}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{11}|\Psi_{\text{II},4}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{11}|\Psi_{\text{III},4}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{11}|\Psi_{\text{IV},4}\rangle|^2 = 0, \ |\langle\Phi_{11}|\Psi_{\text{V},4}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\text{I},1}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{12}|\Psi_{\text{II},1}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{12}|\Psi_{\text{III},1}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{12}|\Psi_{\text{IV},1}\rangle|^2 = 0, \ |\langle\Phi_{12}|\Psi_{\text{V},1}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\text{I},2}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{12}|\Psi_{\text{II},2}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{12}|\Psi_{\text{III},2}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{12}|\Psi_{\text{IV},2}\rangle|^2 = 1, \ |\langle\Phi_{12}|\Psi_{\text{V},2}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\text{I},3}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{12}|\Psi_{\text{II},3}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{12}|\Psi_{\text{III},3}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{12}|\Psi_{\text{IV},3}\rangle|^2 = 0, \ |\langle\Phi_{12}|\Psi_{\text{V},3}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{12}|\Psi_{\text{I},4}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{12}|\Psi_{\text{II},4}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{12}|\Psi_{\text{III},4}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{12}|\Psi_{\text{IV},4}\rangle|^2 = 0, \ |\langle\Phi_{12}|\Psi_{\text{V},4}\rangle|^2 = \frac{1}{4};$$

$$|\langle\Phi_{21}|\Psi_{\text{I},1}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{21}|\Psi_{\text{II},1}\rangle|^2 = 0, \ |\langle\Phi_{21}|\Psi_{\text{III},1}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{21}|\Psi_{\text{IV},1}\rangle|^2 = \frac{1}{2}, \ |\langle\Phi_{21}|\Psi_{\text{V},1}\rangle|^2 = 0;$$

$$|\langle\Phi_{21}|\Psi_{\text{I},2}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{21}|\Psi_{\text{II},2}\rangle|^2 = \frac{1}{2}, \ |\langle\Phi_{21}|\Psi_{\text{III},2}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{21}|\Psi_{\text{IV},2}\rangle|^2 = \frac{1}{2}, \ |\langle\Phi_{21}|\Psi_{\text{V},2}\rangle|^2 = 0;$$

$$|\langle\Phi_{21}|\Psi_{\text{I},3}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{21}|\Psi_{\text{II},3}\rangle|^2 = \frac{1}{2}, \ |\langle\Phi_{21}|\Psi_{\text{III},3}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{21}|\Psi_{\text{IV},3}\rangle|^2 = 0, \ |\langle\Phi_{21}|\Psi_{\text{V},3}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{21}|\Psi_{\text{I},4}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{21}|\Psi_{\text{II},4}\rangle|^2 = 0, \ |\langle\Phi_{21}|\Psi_{\text{III},4}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{21}|\Psi_{\text{IV},4}\rangle|^2 = 0, \ |\langle\Phi_{21}|\Psi_{\text{V},4}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\text{I},1}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{22}|\Psi_{\text{II},1}\rangle|^2 = \frac{1}{2}, \ |\langle\Phi_{22}|\Psi_{\text{III},1}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{22}|\Psi_{\text{IV},1}\rangle|^2 = \frac{1}{2}, \ |\langle\Phi_{22}|\Psi_{\text{V},1}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\text{I},2}\rangle|^2 = \frac{1}{4}, \ |\langle\Phi_{22}|\Psi_{\text{II},2}\rangle|^2 = 0, \ |\langle\Phi_{22}|\Psi_{\text{III},2}\rangle|^2 = \frac{1}{4},$$

$$|\langle\Phi_{22}|\Psi_{\text{IV},2}\rangle|^2 = \frac{1}{2}, \ |\langle\Phi_{22}|\Psi_{\text{V},2}\rangle|^2 = \frac{1}{2};$$

$$|\langle\Phi_{22}|\Psi_{\mathrm{I},3}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{22}|\Psi_{\mathrm{II},3}\rangle|^2 = 0,\ |\langle\Phi_{22}|\Psi_{\mathrm{III},3}\rangle|^2 = \frac{1}{4},$$
$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},3}\rangle|^2 = 0,\ |\langle\Phi_{22}|\Psi_{\mathrm{V},3}\rangle|^2 = 0;$$
$$|\langle\Phi_{22}|\Psi_{\mathrm{I},4}\rangle|^2 = \frac{1}{4},\ |\langle\Phi_{22}|\Psi_{\mathrm{II},4}\rangle|^2 = \frac{1}{2},\ |\langle\Phi_{22}|\Psi_{\mathrm{III},4}\rangle|^2 = \frac{1}{4},$$
$$|\langle\Phi_{22}|\Psi_{\mathrm{IV},4}\rangle|^2 = 0,\ |\langle\Phi_{22}|\Psi_{\mathrm{V},4}\rangle|^2 = 0. \qquad \text{(A2)}$$

Measurements in MUB I and III are least informative for Eve, since each of Alice's code states has the same projects to vectors of these MUBs. We also note that there is no basis in which the expansion coefficients of all Alice's states would be equal to 1. This means that none of the 5 MUBs in ququart space allows Eve to unambiguously determine an arbitrary code state of Alice. To distinguish Alice's states from the basis $\{|\Phi_{11}\rangle, |\Phi_{12}\rangle\}$ from the point of view of maximizing information, it is advantageous for Eve to use IV MUB; to distinguish Alice's states from the basis $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$ — II or V MUB. In this case, II and V MUB turn out to be equivalent, since there are nonzero projections of Alice's code states $|\Phi_{21}\rangle$ and $|\Phi_{22}\rangle$ onto two non-overlapping pairs of basis vectors. This means that when detecting any vector from the pair, Eve will know exactly which code state of Alice from the basis $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$ she measured. Therefore, when analyzing the intercept-resend attack in the main part of the paper, we use only one basis — V MUB.

We also note that the projections of Alice's states from the basis $\{|\Phi_{21}\rangle, |\Phi_{22}\rangle\}$ onto the vectors of IV MUB have a similar value $\frac{1}{2}$, however, nonzero projections exist only on those basis vectors as for states $|\Phi_{11}\rangle$, $|\Phi_{12}\rangle$, which complicates Eve's task of maximizing information about Alice's state during measurement.

References

[1] N. Gisin, G. Ribordy, W. Tittel, H. Zbinden. Rev. Mod. Phys., **74** (1), 145 (2002). DOI: 10.1103/RevModPhys.74.145

[2] C.H. Bennett, G. Brassard. Theoretical Computer Science, **560** (1), 7 (2014). DOI: 10.1016/j.tcs.2014.05.025

[3] V. Scarani, A. Ac'ın, G. Ribordy, N. Gisin. Physical Review Letters, **92** (5), 057901 (2004). DOI: 10.1103/PhysRevLett.92.057901

[4] S.P. Kulik, S.N. Molotkov. Laser Phys. Lett., **14**, 125205 (2017). DOI: 10.1088/1612-202X/aa8ecc

[5] K.S. Kravtsov, S.N. Molotkov. Phys. Rev. A, **100**, 042329 (2019). DOI: 10.1103/PhysRevA.100.042329

[6] F. Grosshans, P. Grangier. Physical Review Letters, **88** (5), 057902 (2002). DOI: PhysRevLett.88.057902

[7] D. Mayers. Journal of the ACM (JACM), **48** (3), 351 (2001). DOI: 10.1145/382780.382781

[8] P.W. Shor, J. Preskill. Physical Review Letters, **85** (2), 441 (2000). DOI: 10.1103/PhysRevLett.85.441

[9] R. Renner. *Security of quantum key distribution*. Doctoral dissertation (Swiss Federal Institute Of Technology, Zurich, 2005). URL: https://arxiv.org/pdf/quant-ph/0512258

[10] R. Renner, R. König. In: *Theory of Cryptography. TCC 2005*, ed. by. J. Kilian. Lecture Notes in Computer Science (Springer, Berlin, Heidelberg, 2005), vol. 3378. DOI: 10.1007/978-3-540-30576-7_22

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, V. Makarov. Nature Photonics, **4** (10), 686 (2010). DOI: 10.1038/nphoton.2010.214

[12] G. Brassard, N. Lütkenhaus, T. Mor, B.C. Sanders. Physical Review Letters, **85** (6), 1330 (2000). DOI: 10.1103/PhysRevLett.85.1330

[13] I. Sushchev, K. Bugai, S. Molotkov, D. Bulavkin, A. Sidelnikova, D. Melkonian, V. Vakhrusheva, R. Lokhmatov, D. Dvoretskiy. DOI: 10.48550/arXiv.2507.15446

[14] S.N. Molotkova, K.S. Kravtsov, M.I. Ryzhkin. Zhurnal Eksperimentalnoy i Teoreticheskoy Fiziki (ZhETF), **155** (4), (in Russian) 636 (2018). DOI: 10.1134/S0044451019040060

[15] M. Gellert, D. Sulimov, B. Nasedkin, R. Goncharov, I. Filipov, P. Morozova, F. Goncharov, D. Yashin, V. Chistiakov, E. Samsonov, V. Egorov, B. Pervushin, I. Adam. Journal of Optical Technology, **90** (2), 55 (2023). DOI: 10.1364/JOT.90.000055

[16] S. Lorenz, N. Korolkova, G. Leuchs. Appl. Phys. B, **79**, 273 (2004). DOI: 10.1007/s00340-004-1574-7

[17] A. Jimenez-Girela, D. Merino-Pérez, A. Campos-Jara, Negrín, J. Socas, Parejo, P. Garcia, A. Álvarez-Herrero. Phys. Rev. Applied, **23** (6), 064070 (2025). DOI: 10.1103/8plr-m6n8

[18] D.D. Reshetnikov, A.L. Sokolov, E.A. Vashukevich, V.M. Petrov, T.Yu. Golubeva. Radiophys Quantum El., **67**, 51 (2024). DOI: 10.1007/s11141-025-10352-z

[19] J.S. Sidhu, T. Brougham, D. McArthur, R.G. Pousa, D.K.L. Oi. Commun Phys., **6**, 210 (2023). DOI: 10.1038/s42005-023-01299-6

[20] S. Turtaev, I.T. Leite, K.J. Mitchell, M.J. Padgett, D.B. Phillips, T. Cizmá. Opt. Express, **25**, 29874 (2017). DOI: 10.1364/OE.25.029874

[21] I.-C. Benea-Chelmus, S. Mason, M.L. Meretska, D.L. Elder, D. Kazakov, A. Shams-Ansari, L.R. Dalton, F. Capasso. Nat Commun., **13**, 3170 (2022). DOI: 10.1038/s41467-022-30451-z

[22] D.D. Reshetnikov, A.A. Ryzhaya, M.E. Pavelina, E.A. Vashukevich, A.A. Sevryugin, A.L. Sokolov, V.Yu. Venediktov, V.M. Petrov. Optichesky zhurnal, **92** (3), 58 (2025) (in Russian). DOI: 10.17586/1023-5086-2025-92-03-58-67

[23] L. Allen, M.W. Beijersbergen, R.J.C. Spreeuw, J.P. Woerdman. Phys. Rev. A, **45**, 8185 (1992). DOI: 10.1103/PhysRevA.45.8185

[24] E. Nagali, L. Sansoni, L. Marrucci, E. Santamato, F. Sciarrino. Phys. Rev. A., **81**, 052317 (2010). DOI: 10.1103/PhysRevA.81.052317

[25] S.P. Kulik, A.P. Shurupov. Atoms, Molecules, Optics, **104**, 736 (2007). DOI: 10.1134/S106377610705007X

[26] F. Caruso, H. Bechmann-Pasquinucci, C. Macchiavello. Phys. Rev. A, **72**, 032340 (2005). DOI: 10.1103/PhysRevA.72.032340

[27] C.A. Fuchs, N. Gisin, R.B. Griffiths, C.-S. Niu, A. Peres. Phys. Rev. A, **56**, 1163 (1997). DOI: 10.1103/PhysRevA.56.1163

[28] S. Pirandola. International Journal of Quantum Information, **6**, 765 (2008). DOI: 10.1142/S0219749908004080

[29] L. Sheridan, V. Scarani. Phys. Rev. A, **82**, 030301 (2011). DOI: 10.1103/PhysRevA.82.030301

[30] K.A. Balygin, A.N. Klimov, I.B. Bobrov, K.S. Kravtsov, S.P. Kulik, S.N. Molotkov. Laser Physics Letters, **15** (9), 095203 (2018). DOI: 0.1088/1612-202X/aad1c9

[31] W.-Y. Hwang. Physical Review Letters, **91** (5), 057901 (2003). DOI: 10.1103/PhysRevLett.91.057901

Translated by M.Verenikina