Quantum control attack: Towards joint estimation of protocol and hardware loopholes

Anton Kozubov,[1,2,3,*] Andrei Gaidash,[1,2,3] and George Miroshnichenko[4,5]

[1]*Department of Mathematical Methods for Quantum Technologies, Steklov Mathematical Institute of Russian Academy of Sciences, Moscow 119991, Russia*

[2]*Laboratory of Quantum Processes and Measurements, ITMO University, 199034, Kadetskaya Line 3b, Saint Petersburg, Russia*

[3]*Leading Research Center "National Center for Quantum Internet", ITMO University, 197101, 49 Kronverksky Pr., Saint Petersburg, Russia*

[4]*Waveguide Photonics Research Center, ITMO University, 197101, 49 Kronverksky Pr., Saint Petersburg, Russia*

[5]*Institute "High School of Engineering", ITMO University, 197101, 49 Kronverksky Pr., Saint Petersburg, Russia*

(Received 29 March 2021; accepted 26 July 2021; published 9 August 2021)

In this paper we present the approach for description of quantum control attack based on combined protocol and hardware loopholes. It consolidates intercept-resend attack and detection node control (detector blinding attack). In the basic version of B92 protocol detection control is not that crucial; however, when one scales the number of states the state imposing plays a significant role. Protocols that operate with arbitrary even symmetric linearly independent nonorthogonal (e.g., coherent) states are of interest. The cornerstone of the considered approach is that we combine both state discrimination by eavesdropper and different methods of state imposing. In principle, detection control allows one to exclude any bit correlations between legitimate users, which are unknown to Eve, and can be considered as the necessary part of most intercept-resend attacks, including a faked-state attack impossible without a hardware loophole. Moreover, the issue related to unified quantum description of the intercept-resend attack was solved by combining the concepts of von Neumann's measurement scheme and ambiguity of square root extraction for operators. We also present a generalized countermeasure based on additional parameter estimation analysis. As an example, with some numerical estimations we investigate the attack on quantum key distribution systems based on utilization of symmetric coherent states and consider appropriate countermeasures.

DOI: 10.1103/PhysRevA.104.022603

I. INTRODUCTION

Quantum key distribution (QKD) systems [1–3] in the past decades extend beyond the laboratory research and go straight ahead to the market. Nevertheless a lot of vulnerabilities for real QKD systems are not covered in the various research in both theoretical and experimental areas. It is commonly assumed that equipment is nonideal. Due to this fact some attacks can be performed on real QKD systems, although the most theoretical security proofs are based on the common assumption that the eavesdropper has no direct access to receiving and transmitting equipment. However, in real life implementations Eve can influence the hardware of a legitimate user in some way and one needs to take this into consideration. For instance, first steps towards an approach for security evaluation and certification of a complete quantum communication system have already been done; e.g., see Ref. [4].

Moreover, estimation of some protocol attacks also requires the consideration of hardware and its loopholes. In particular, the class of intercept-resend attacks is of interest. The majority focus their attention only on the problem of the state discrimination [5–9] and often neglect or crucially simplify the problem of further state imposing, though this problem should also be considered since incorrect imposing may cause violation of conditional detection probability at the Bob's side. The papers cited above estimate the security of the considered systems according to the preservation of Bob's estimated detection rate.

To do so it is assumed that after discrimination Eve just increases the intensity of the pulse and sends it to Bob. This method seems reasonable for the case of B92 protocol; thus it provides the almost perfect ($\approx$1) detection probability. However, when the number of states is increased, this way of state imposing has some loopholes and can in principle be revealed on the parameter estimation step using a technique from [10]. One of the possible solutions of this problem in the case is detection control. A crucial advantage is that it allows one to exclude any bit correlations between legitimate users, which are unknown to Eve, and in principle preserve the detection statistics. Thus it should be considered as the necessary part of most intercept-resend attacks.

Possibility of detection control was considered in the context of a faked-state attack [11–18]. Recently, a lot of experimental demonstrations of the attack were proposed for different QKD systems. Many researchers are trying to find the appropriate hardware solution to prevent it. Most of them are based on some modifications of single-photon detectors (SPD). However, a universal experimental countermeasure that allows one to overcome this attack is still missing. One of the reliable ways to deal with Eve's

*avkozubov@itmo.ru

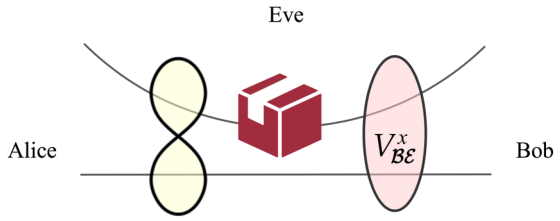

FIG. 1. Visual interpretation of considered quantum control attack. The attack is based on the fact that Eve can use unitary decomposition of her POVM operators, which allows her to perform the feedforward operation and change the states in the channel after her measurement. Here $V^x_{\mathcal{BE}}$ denotes the unitary operation that modifies the states.

strategy yet is measurement-device-independent (MDI) [19–24] or twin-field (TF) [25–30] QKD systems. However, the most of commercial systems are utilizing a point-to-point scheme; thus the possibility of detection control should be included in security analysis.

In this paper we propose quantum control attack (Fig. 1), which can be considered as the generalization of intercept-resend attacks combined with control of Bob's detection node. The current work is dedicated to symmetric nonorthogonal linearly independent states, so it is more convenient to compare the proposed ideas with the latter cited paper. First of all we generalize the approach towards increase of the number of states and their variety compared to only two coherent states that were considered in [8]. Also there was an issue related to the unified quantum description of the channel considered in the latter cited paper. Hence we further demonstrate the explicit way of how the considered attack can be described in terms of quantum operators.

The paper is organized as follows. Section II presents the generalized optical scheme of the considered type of QKD systems. In Sec. III we present the mathematical description of the proposed attack. Section IV describes the conditions for successful eavesdropping. Section V gives an explicit description of two possible realizations of the attack based on different initial conditions and provides their comparison for B92 protocol. In Sec. VI we consider the security issues related to the attack and possible countermeasures. Section VII concludes the article.

II. OPTICAL SCHEME

We suppose that all further discussion will be made taking into account the optical scheme as follows. We would like to consider prepare-and-measure protocol that operates with nonorthogonal linearly independent states. In particular we aim for phase-coded weak coherent states and other states with similar structure.

We assume that stated further is natural for a generic QKD protocol. All the states have equal *a priori* probabilities p and are equally distributed on the phase plane, e.g., states are encoded with a set of phases $\phi_n = \frac{\pi}{N}n$. Consequently, there is even number $(2N)$ of states that can be combined in N pairs (bases) and states in each pair can be discriminated by legitimate users. It should be noted that a proposed symmetric set of states is necessary only for estimation purposes; description of the attack further still holds for an arbitrary set of nonorthogonal linearly independent states.

Alice prepares a state with a device (it can be the well-known unbalanced Mach-Zehnder interferometer as in [31–33], or any other interferometric schemes, for instance [34–37], or even more complicated interferometric schemes) that produce the state of the following form:

$$|\psi\rangle = |\psi_1\rangle_R \otimes |\psi_2(\phi_A)\rangle_S, \tag{1}$$

where R denotes reference mode, S denotes signal mode (it could be any separate modes, for instance, time-bin, polarization, frequency modes, etc.), and ϕ_A denotes phase that is relative to the reference and encodes bit. It should be emphasized that we do not assume any kind of general phase randomization of the state. We believe this kind of assumption is rather strong and its experimental implementation is quite challenging.

Then the state travels through the quantum channel into Bob's module where he operates an analogous device as Alice. The output states are functions of phase difference $\phi_A - \phi_B$, where the latter is Bob's induced phase. The detection scheme might contain either one or two detectors; it depends on the particular kind of Bob's device. For instance, in the case of an unbalanced Mach-Zehnder interferometer there are two detectors (phase differences $\phi_A - \phi_B = 0$ and $\phi_A - \phi_B = \pi$ produce detection events in different detectors), while in the case of electro-optical phase modulators [34] there is only one (phase difference $\phi_A - \phi_B = 0$ produces detection events in the detector). Probability of detection events in either scheme is proportional to

$$c|\alpha|^2[1 \pm \cos(\phi_A - \phi_B)]\eta, \tag{2}$$

where c is a proportionality coefficient dependent on a particular optical scheme (for instance, it may be 2 for the phase-modulator case or $\frac{1}{2}$ for the Mach-Zehnder interferometer case), where $|\alpha|^2$ is the mean photon number (power) of an optical signal and η is the overall losses in the system. Despite the different technological approach the main approach of the considered optical schemes is basically the same.

III. DESCRIPTION OF THE ATTACK

The protocol of the attack can be described as follows.

Step 1. Let $\mathcal{A}, \mathcal{B}, \mathcal{E}$ be Hilbert spaces of Alice, Bob, and Eve, respectively. Eve exchanges the channel with a lossless channel and makes her initial states (ancillas) $|\psi\rangle_{\mathcal{E}}$ interact with the states prepared by Alice $\{|u_1\rangle_{\mathcal{A}}, \ldots, |u_{2N}\rangle_{\mathcal{A}}\}$ using nonlocal unitary operator $U_{\mathcal{AE}}$ as follows:

$$|u_n\rangle_{\mathcal{A}} \otimes |\psi\rangle_{\mathcal{E}} \xrightarrow{U_{\mathcal{AE}}} |\tilde{u}_n\rangle_{\mathcal{B}} \otimes |\psi_n\rangle_{\mathcal{E}}, \tag{3}$$

where $\{|\tilde{u}_n\rangle_{\mathcal{B}}\}_n$ and $\{|\psi_n\rangle_{\mathcal{E}}\}_n$ are the spaces of altered states in the quantum channel and Eve's ancillas accordingly after Eve implies the unitary nonlocal operation $U_{\mathcal{AE}}$ and $n = 1, 2, \ldots, 2N$. This step is closely related with the first step in von Neumann measurement. In the general case the unitary operation should entangle states with each other. However, there always exists the moment when the states become untangled as considered in Eq. (3). We investigate the case here;

hence it seems to be optimal from Eve's point of view when any set of linearly independent states is used.

Step 2. Eve needs to construct the positive-operator valued measure (POVM) with the family of positive semidefinite operators $\{M^x_{\mathcal{EB}}\}_{x\in\mathcal{X}}$ (inconclusive result for $x=0$ is also included in the notation):

$$\mathbb{I} = \sum_x M^x_{\mathcal{EB}}, \quad M^x_{\mathcal{EB}} = \mathbb{I}_{\mathcal{B}} \otimes A^x_{\mathcal{E}}, \tag{4}$$

where $M^x_{\mathcal{EB}}$ act on both Eve's ancillas and states in the channel. Using the polar decomposition technique (also called the unitary decomposition or quantum control) [38–41] of POVM operators

$$K^x_{\mathcal{BE}} = V^x_{\mathcal{BE}}\sqrt{M^x_{\mathcal{EB}}}, \tag{5}$$

where $K^x_{\mathcal{BE}}$ is the Kraus operator, $V^x_{\mathcal{BE}}$ is the nonlocal unitary operator, which allows one to alter the states after measurement depending on its result, and index $x = 0, 1, \ldots, 2N$ denotes the set of possible outcomes of implemented POVM. Due to this uncertainty in choosing the nonlocal unitary operator one is able to choose the required one. Thus Eve can provide any possible configuration of the states after the measurement or, in other words, renormalize the input conditions in the quantum channel using the active feedback.

The measurement result depends on Eve's states after the first nonlocal unitary operation $|\psi_n\rangle_{\mathcal{E}}$ and local measurement operator $\sqrt{A^x_{\mathcal{E}}}$ as follows:

$$|\psi_{nx}\rangle_{\mathcal{E}} = \frac{\sqrt{A^x_{\mathcal{E}}}|\psi_n\rangle_{\mathcal{E}}}{\sqrt{\mathcal{P}(x|n)}}, \tag{6}$$

where $\mathcal{P}(x|n)$ denotes the conditional probability matrix described as

$$\mathcal{P}(x|n) = \mathrm{Tr}_{\mathcal{E}}\left(A^x_{\mathcal{E}}|\psi_n\rangle_{\mathcal{E}}\langle\psi_n|\right). \tag{7}$$

Step 3. According to the measurement result Eve alters the states in the channel using an appropriate unitary operator from polar decomposition of the POVM operator as follows:

$$|\tilde{u}_n\rangle_{\mathcal{B}} \otimes |\psi_{nx}\rangle_{\mathcal{E}} \xrightarrow{V^x_{\mathcal{BE}}} |\tilde{u}_{nx}\rangle_{\mathcal{B}} \otimes |\tilde{\psi}_{nx}\rangle_{\mathcal{E}}. \tag{8}$$

According to the overlapping preservation for unitary operation and conditions in Eq. (8) we assume that

$$_{\mathcal{B}}\langle\tilde{u}_k|\tilde{u}_n\rangle_{\mathcal{BE}}\langle\psi_{kx'}|\psi_{nx}\rangle_{\mathcal{E}} = {}_{\mathcal{B}}\langle\tilde{u}_{kx'}|\tilde{u}_{nx}\rangle_{\mathcal{BE}}\langle\tilde{\psi}_{kx'}|\tilde{\psi}_{nx}\rangle_{\mathcal{E}}. \tag{9}$$

All distinguished by Eve states should be altered in a special manner using appropriate unitary transformation and resent directly to Bob. To stay unrevealed Eve should not only maintain both detection and error rates regarding the presence of errors and inconclusive results at the Bob side (they always appear due to nonorthogonality of the states, losses in the channel, and nonideal equipment), but also preserve the conditional detection probability. This step can be considered as the detection control.

IV. CONDITIONS FOR SUCCESSFUL EAVESDROPPING

We would like to recall that the successful eavesdropping strategy should be based on the following conditions.

(1) Eve should obtain at least the same information as Bob does; otherwise, Eve's knowledge can be removed from the key on privacy amplification.

(2) Eve should not be noticed by legitimate users.

Further we demonstrate that it is so (or at least can be so) for the considered attack.

A. Information supremacy

The crucial moment in the QKD scenario is that we are transmitting the classical information using quantum states. Thus in the case of intercept-resend attacks consideration of classical variables (key bits) looks reasonable. If a smart intercept-resend attack (with proper discrimination of states and their further imposing assuming detection control, for instance) takes place, then Bob only receives bits that are known to Eve. Moreover, there are no clicks at Bob's side in case of an inconclusive result at the eavesdropper. Therefore, mutual information between classical variables of Alice and Eve are always not less than between Alice and Bob. For the simplicity let us consider the tripartite probability distribution between random variables A, E, B, which relates to Alice, Eve, Bob values of bits after measurement, respectively. According to the concept of wire-tap channel [42–44] random variables A, E, B are said to form a Markov chain in that order $A \to E \to B$.

Thus according to the fact that the considered quantum channel can be presented as the Markov chain of classical variables we can use the well-known data-processing inequality and claim that

$$I(A;E) \geqslant I(A;B). \tag{10}$$

There $I(X;Y) = H(X) - H(X|Y)$ is mutual information. Thus the first condition is naturally satisfied.

B. Statistics preservation

The second important condition for successful attack is that Eve must not be disclosed by legitimate users. It is well known that in the case of linearly dependent states Eve can be easily revealed by simply monitoring the error rate. The main reason for that is the fundamental impossibility to provide discrimination of linearly dependent states without errors. However, for the case of linearly independent states Eve, for instance, can provide unambiguous state discrimination (USD) measurement [45–48] and identify states without errors, but with only inconclusive results.

In general in order to satisfy the second condition Eve should adjust her attack so that Bob's detection rate should remain almost the same, i.e., losses in the original channel should be balanced with the probability of inconclusive results and error rates should not be higher than before interception (as generalization of [8]):

$$\sum_{b\neq 0} \mathcal{P}(b|a) \leqslant \sum_{b\neq 0} \tilde{\mathcal{P}}^{\mathcal{E}}(b|a), \tag{11}$$

$$\sum_{b\neq a,0} \mathcal{P}(b|a) \geqslant \sum_{b\neq a,0} \tilde{\mathcal{P}}^{\mathcal{E}}(b|a), \tag{12}$$

$$\tilde{\mathcal{P}}^{\mathcal{E}}(b|a) = \sum_e \mathcal{P}^{\mathcal{E}}(b|e)\mathcal{P}^{\mathcal{E}}(e|a), \tag{13}$$

where $\mathcal{P}(b|a)$ is Bob's expected (without Eve's interception) conditional detection probability (thus b is only conclusive results), $\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)$ is Bob's actual (in case of attack) conditional detection probability, where $\mathcal{P}^{\mathcal{E}}(e|a)$ is Eve's conditional discrimination probability, and $\mathcal{P}^{\mathcal{E}}(b|e)$ is Bob's conditional detection probability in case of discriminated states imposing. As a consequence of Eqs. (11) and (12) one may derive an additional inequality as follows:

$$\mathcal{P}(a|a) \leqslant \tilde{\mathcal{P}}^{\mathcal{E}}(a|a). \tag{14}$$

V. EXAMPLE

Further we consider USD-like and faked-state attacks for the following reasons. As stated earlier Bob's overall conditional detection probability in the case of the attack $\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)$ consists of the following two terms: $\mathcal{P}^{\mathcal{E}}(e|a)$ that is determined by chosen discrimination POVM and $\mathcal{P}^{\mathcal{E}}(b|e)$ that is defined by the method of a discriminated state imposing to Bob. In the case of a USD-like attack construction of appropriate discrimination POVM (the former term) is the most crucial part, while the exact method of imposing and its precision have secondary priority. Otherwise, in faked-state attack POVM is trivial (simple guess) and the most peculiar task is to adjust detection probabilities (the latter term) as precisely as possible. We would like to emphasize that we highlight each term separately in following subsections in order to consider their individual peculiarities in more details, despite the fact that Eve should pay maximal attention to both terms simultaneously in order to perform an ideal attack.

A. USD-like attack

In [8] a simple case was considered when Eve performs USD POVM. It was shown that Eve can be revealed if we satisfy the condition [that is opposite of Eq. (14)]

$$\mathcal{P}(b|a) \geqslant \mathcal{P}_U \delta_{ab}, \tag{15}$$

where $\mathcal{P}^{\mathcal{E}}(e|a) \equiv \mathcal{P}_U \delta_{ea}$, $\mathcal{P}_U$ is probability of USD, δ_{ij} is Kronecker symbol, and $\mathcal{P}^{\mathcal{E}}(b|e) \equiv \delta_{be}$ in the worst case scenario that can be achieved by detector control (for more details, see Sec. V B) or increase of mean photon number in the pulse. Although for USD attack

$$\sum_{b\neq a,0} \sum_{e} \mathcal{P}^{\mathcal{E}}(b|e)\mathcal{P}^{\mathcal{E}}(e|a) \equiv \sum_{b\neq a,0} \mathcal{P}_U \delta_{ab} = 0 \tag{16}$$

and Bob's initial error rate is always nonzero; hence one should take into account small perturbation of USD POVM in order to maintain error rate. It also should provide higher discrimination rate. Thus Eve has more freedom of choice in satisfaction of a condition in Eq. (11) and it should be taken into account in security estimation.

1. Eve's POVM construction

Let us consider $2N$ states $|\psi_n\rangle_{\mathcal{E}}$ that Eve should discriminate; further we neglect the index due to simplicity and the fact that we will consider only related to Eve Hilbert space. Also we would like to recall that the case of symmetrical states, i.e., with equal *a priori* probabilities $p_n = p = \frac{1}{2N}$, equal phase-coding distribution $\phi_n = \frac{\pi}{N}n$, and, as a consequence, equal discrimination probabilities $\mathcal{P}_n = \mathcal{P}$, is considered. Let us introduce the POVM $\hat{A}_n$:

$$\hat{A}_n = \mathcal{P}|\varphi_n\rangle\langle\varphi_n|, \tag{17}$$

where

$$|\varphi_n\rangle = \frac{(1-w)|\psi_n^{\perp}\rangle + w|\psi_n\rangle}{\sqrt{C}}, \tag{18}$$

$$C = (1-w)^2\nu + w(2-w), \tag{19}$$

$|\psi_n^{\perp}\rangle$ (non-normalized state; hence $\langle\psi_n^{\perp}|\psi_n^{\perp}\rangle = \nu$, taking into account the symmetrical case) is the state chosen to form a biorthogonal basis with signal states $|\psi_n\rangle$, i.e., $\langle\psi_n^{\perp}|\psi_m\rangle = \delta_{nm}$, and w is a parameter that adjusts the error rate of POVM (for $w = 0$ it is USD POVM with no errors). Each operator $\hat{A}_m$ for $m \geqslant 1$ is related to identification of the signal state $|\psi_m\rangle$ when state $|\psi_n\rangle$ was sent; the appropriate conditional probabilities may be expressed as follows (also recalling that imposing probability is the Kronecker delta):

$$\begin{aligned}\tilde{\mathcal{P}}^{\mathcal{E}}(m|n) &= \mathcal{P}^{\mathcal{E}}(m|n) = \langle\psi_n|\hat{A}_m|\psi_n\rangle \\ &= \mathcal{P}\left(\frac{(1-w^2)\delta_{nm}}{C} + \frac{w^2|\langle\psi_n|\psi_m\rangle|^2}{C}\right),\end{aligned} \tag{20}$$

where δ_{nm} is the Kronecker symbol. Operator $\hat{A}_0$ related to the inconclusive result is denoted by the identity decomposition property:

$$\hat{A}_0 = \hat{I} - \sum_{n=1}^{2N} \hat{A}_n. \tag{21}$$

Eve's POVM should be constructed in a way that probability of an inconclusive result will be as low as possible. The optimization problem is to maximize $\mathcal{P}$ taking into account that $\hat{A}_0$ should remain positive semidefinite. Hence $\mathcal{P}$ is limited by condition

$$\det\left(\hat{I} - \mathcal{P}\sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|\right) = 0, \tag{22}$$

as it was introduced in [48] for USD POVM. The problem may be satisfied if $\mathcal{P}$ is equal to the reciprocal maximal eigenvalue of

$$\sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|. \tag{23}$$

One may solve the spectral problem for any Gram operator as follows:

$$\sum_{n=1}^{2N} |\varphi_n\rangle\langle\varphi_n|\theta_k\rangle = \lambda_k|\theta_k\rangle, \tag{24}$$

$$\lambda_k = \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\varphi_{2N}|\varphi_n\rangle, \tag{25}$$

$$|\theta_k\rangle = \frac{1}{\sqrt{2N\lambda_k}} \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}|\varphi_n\rangle, \tag{26}$$

λ_k is the eigenvalue, and $|\theta_k\rangle$ is the eigenvector. Hence

$$\frac{1}{\mathcal{P}} = \max_k \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\varphi_{2N}|\varphi_n\rangle = \frac{(1-w)^2}{C}\max_k \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\psi_{2N}^{\perp}|\psi_n^{\perp}\rangle + \frac{w^2}{C}\max_k \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\psi_{2N}|\psi_n\rangle + \frac{2w(1-w)}{C}. \quad (27)$$

One may utilize property that is shown in Appendix A in order to make the following replacement:

$$\max_k \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\psi_{2N}^{\perp}|\psi_n^{\perp}\rangle = \left(\min_k \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\psi_{2N}|\psi_n\rangle\right)^{-1}. \quad (28)$$

Thus the conditional probability may be expressed as follows:

$$\tilde{\mathcal{P}}^{\mathcal{E}}(m|n) = \frac{(1-w^2)\delta_{nm} + w^2|\langle\psi_n|\psi_m\rangle|^2}{\frac{(1-w)^2}{\min_k(\mu_k)} + w^2\max_k(\mu_k) + 2w(1-w)}, \quad (29)$$

where

$$\mu_k = \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n}\langle\psi_{2N}|\psi_n\rangle. \quad (30)$$

2. *Detection rate estimation for coherent states*

The latter is a general expression; however, for numerical estimations it is convenient to consider the states as coherent [here we do not consider a reference state as in Eq. (1) because it does not contain any phase-coded information]:

$$|\psi_n\rangle \equiv |\alpha\, e^{i\phi_n}\rangle, \quad (31)$$

where α is the absolute value of the coherent state amplitude and the exponential term adds phase shift $\phi_n = \frac{\pi}{N}n$. Then considering the numerical estimation shown in Appendix B [for the overlap of the states in Eq. (B2), for $\max_k(\mu_k)$ in Eq. (B8), and for $\min_k(\mu_k)$ in Eq. (B9)] one may derive an expression for conditional probabilities as follows:

$$\tilde{\mathcal{P}}^{\mathcal{E}}(m|n) = \frac{(1-w^2)\delta_{nm} + w^2 e^{-2|\alpha|^2[1-\cos(\phi_n-\phi_m)]}}{\frac{(1-w)^2(2N-1)!}{2N(|\alpha|^2)^{2N-1}} + w^2 2N\left(1-|\alpha|^2+\frac{|\alpha|^4}{2}\right) + 2w(1-w)}. \quad (32)$$

One may consider separate terms such as correct discrimination probability $\tilde{\mathcal{P}}^{\mathcal{E}}(n|n)$ and error probability $\sum_{m\neq n,0}\tilde{\mathcal{P}}^{\mathcal{E}}(m|n)$. Then quantum bit error rate (QBER) is as follows (keeping in mind the symmetrical case):

$$\mathcal{Q}^{\mathcal{E}} = \mathcal{Q}^{\mathcal{E}}(m) = \frac{\sum_{m\neq n,0}\tilde{\mathcal{P}}^{\mathcal{E}}(m|n)}{\sum_{m\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(m|n)}. \quad (33)$$

In order to fulfill Eq. (12) value of parameter $w = w_0$ should be found with the following requirement:

$$\mathcal{Q}^{\mathcal{E}} = \mathcal{Q}, \quad (34)$$

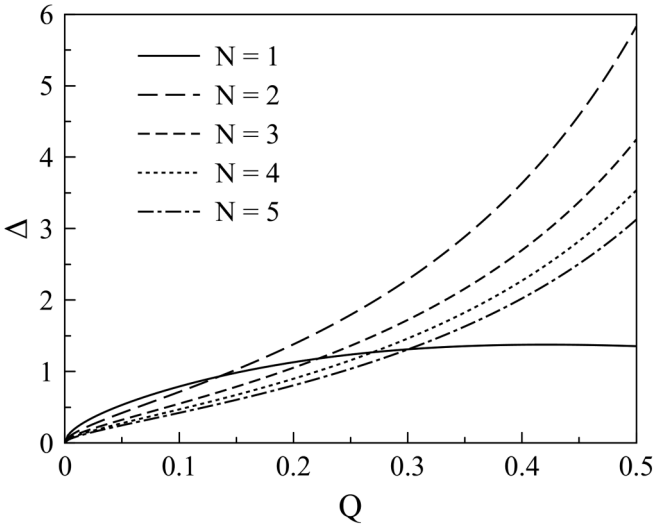

FIG. 2. Relative difference Δ of detection rate with introduced error $\sum_{m\neq 0}\mathcal{P}^{\mathcal{E}}(m|n)$ compared to unambiguous state discrimination probability $\mathcal{P}_U$ (no errors) dependent on expected quantum bit error rate $\mathcal{Q}$ for different number of signal states defined by $2N$. Simulations were performed for symmetric coherent states with phase-coding, mean-photon number $|\alpha|^2 = 0.1$.

where $\mathcal{Q}$ is Bob's initial QBER (without interception). We utilize QBER since legitimate users estimate errors by the QBER value. Results of numerical simulation show that, surprisingly, the relative difference of $\sum_{m\neq 0}\mathcal{P}^{\mathcal{E}}(m|n)$ compared to $\mathcal{P}_U$,

$$\Delta = \frac{\sum_{m\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(m|n)|_{w=w_0} - \mathcal{P}_U}{\mathcal{P}_U}, \quad (35)$$

does not increase a lot (no more than one order), as it is shown in Fig. 2. Such small increase of detection rate indicates that countermeasures against USD attack (e.g., including [8]) are in general as valid as countermeasures against the presented quantum control attack (considering appropriate adjustment of parameters).

At the end of the day in the case of a described modified USD attack Eq. (11) can be expressed as follows [considering substitution of Eq. (12) with Eq. (34)]:

$$c|\alpha|^2\eta_L\eta_B\eta_D \leqslant \sum_{m\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(m|n)|_{w=w_0}, \quad (36)$$

where η_L is attenuation coefficient due to losses in the channel, η_B is attenuation coefficient due to losses at Bob's side, and η_D is detection efficiency. Consideration of the latter inequality as equation can be used in order to find maximal allowed η_L. Since there is ambiguity related to c we show in Fig. 3 difference $\Delta\eta_{L\max}$ between maximal allowed η_L in the case of simple USD and proposed modified USD that takes into account errors; this value is independent of c. It can be seen in the region with relevant $\mathcal{Q} \leqslant 10\%$ that the typical difference is less than 2 dB; that is not much but still should be taken into account, especially for QKD systems that work in channels with close to maximal allowed losses.

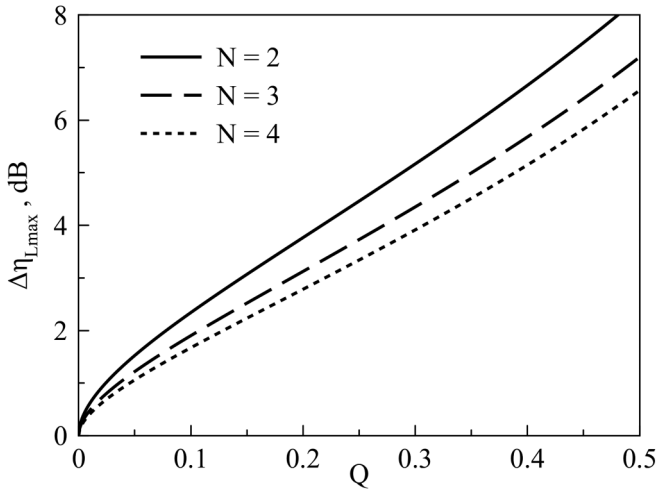

FIG. 3. Difference $\Delta\eta_{L\max}$ between maximal allowed η_L in the case of simple USD and proposed modified USD that takes into account errors dependent on expected quantum bit error rate $\mathcal{Q}$ for different number of signal states defined by $2N$. Simulations were performed for symmetric coherent states with phase-coding, mean-photon number $|\alpha|^2 = 0.1$ and $\eta_B\eta_D = 0.05$.

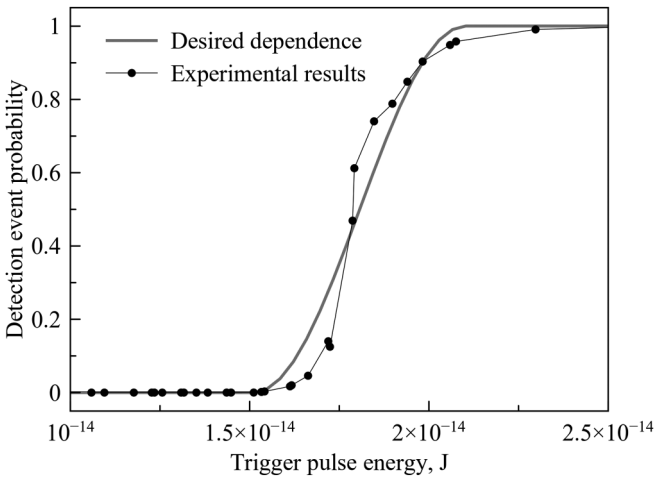

FIG. 4. Dependence of detection event probability on trigger pulse energy. Dotted line represents actual experimental data from [18] for 35 nW blinding power as an example that demonstrates typical shape of the curve. Solid gray line is the desired shape of detector response that can mimic detection probability dependent on phase difference in the interferometric scheme.

B. Faked-state attack

Another possible attack, which can be described with the formalism of quantum control, is the well-known faked-state attack. This attack utilizes the hardware loophole caused by the possibility of detection control. The protocol of the attack is as follows.

(1) Eve changes the quantum channel by a lossless one.

(2) Eve blocks and then guesses the state arrived from Alice.

(3) Eve prepares states with guessed phase and chosen $|\alpha|^2$ in order to blind Bob's detector. Phase difference equal to zero always produces a detection event, phase difference equal to π never produces a detection event, and it depends for other phase differences [18].

Eve guesses states then $\mathcal{P}^{\mathcal{E}}(e|a) = \frac{1}{2N}$. Let us consider several possible outcomes for $\mathcal{P}^{\mathcal{E}}(b|e)$ depending on particular parameters of the detector blinding, i.e., dependence of the detection event on incident optical power. In some cases considered dependence is step-function-like with rapid growth of detection event probability from 0 to almost 1 at some point (for example, see Fig. 3 in [18]). The location of the step point determines $\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)$ to be between $\frac{1}{2N}$ and $\frac{2N-1}{2N}$; we should emphasize that conditional probability in this case does not depend on phase difference. However, in the case of smooth behavior of dependence of the detection event on incident optical power there might be dependence of $\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)$ on phase difference. In the case of four state it is always possible to justify blinding parameters in order to preserve all conditional probabilities. For a higher amount of utilized states it depends on how close behavior of dependence of the detection event on incident optical power is to harmoniclike (phase-difference dependence); for demonstration see Fig. 4. In the particular case the dependence is rather close to the desired one, and Eve can attempt to stay unrevealed since the conditional probability is similar to ideal. At this point it mostly depends on how big Bob's statistical data sample is (see further Sec. VI A for more details on statistical analysis). However, there might be a case when detection parameters are unable to achieve distribution close to a desired one. Nevertheless, we would like to emphasize that it is required to perform experimental measurements in the case of any particular detector in order to estimate precise dependence of detection events on incident optical power.

C. Implementation to B92 protocol

Let us consider a rather simple example of B92 protocol for explicit demonstration of proposed methods. We should start from Eqs. (11) and (12) and define $\mathcal{P}(b|a)$ on one of the detectors (for the second detector in the expression one should change sign) as follows (or something similar depending on particular implementation; however, the following expression represents the most common features):

$$\mathcal{P}(b|a) = c|\alpha|^2[1 - \cos(\pi\delta_{ba})]\eta_L\eta_B\eta_D. \tag{37}$$

Here we neglect dark counts (and similar source of errors) in order to simplify the example. For the left-hand side of Eq. (11) we have several cases as follows.

1. Unambiguous state discrimination

We assume that Eve can make $\mathcal{P}^{\mathcal{E}}(b|e) = \delta_{be}$ either by detection control or by amplification of resent pulses (and further we will notice that if Eve controls detector intercept-resend kind of attack is not optimal). Also $\mathcal{P}^{\mathcal{E}}(e|a) = \mathcal{P}_U\delta_{ea} = 2|\alpha|^2\delta_{ea}$ as it is stated at the end of Appendix B. If

$$\sum_{b\neq 0} c|\alpha|^2[1 - \cos(\pi\delta_{ba})]\eta_L\eta_B\eta_D \geqslant \sum_{b\neq 0} 2|\alpha|^2\delta_{ba} \tag{38}$$

is satisfied then legitimate users can in principle detect USD attack. Even without losses ($\eta_L = 1$) the latter expression barely can be satisfied ($\eta_B\eta_D \geqslant \frac{1}{c}$) for the realistic system's

parameters. Thus sufficient reduction of P_U should be introduced, e.g., by increasing the number of states.

2. *Faked-state attack*

As it is stated earlier Eve guesses states and $\mathcal{P}^{\mathcal{E}}(e|a) = \frac{1}{2}$. The most crucial task for Eve is to adjust imposing of states. First of all, she blinds the detector, e.g., by some background light at different parts of the spectrum, in order to avoid interference with resent signals. If we assume that the detector has the same characteristics as in [18], then the necessary power level could be 35 nW and further discussion can be paired with Fig. 4. She needs to prepare states in such a way that in case of phase mismatch with Bob his detector never produces a detection event, e.g., it has energy equivalent to $1.5 \times 10^{-14} J$. Then she has two extreme options. In the first case she prepares the state that has resulted energy for phase match with Bob slightly higher than $1.5 \times 10^{-14} J$, where detection event probability is numerically equal to $\mathcal{P}(b|a)$ in Eq. (37). In the second case she prepares the state that has resulted energy around $2.2 \times 10^{-14} J$ with guaranteed detection event. And then she triggers background light power from where there is no detection event for chosen energy values at all to appropriate 35 nW with probability that in total restores $\mathcal{P}(b|a)$. Also she always can adjust her imposing as something in between these two extreme cases.

VI. SECURITY ESTIMATION AND ALTERNATIVE COUNTERMEASURES

A. Security issues

In this section we would like to consider the approach of how one may estimate influence of the attack on security criterion. Then the expanded condition of form (6) in [8] should be examined, i.e., upper bound of the amount of detection events in case of interception should be lower than lower bound of the amount of initial detection events, in order to reveal the attack. The latter conditions in general are as follows:

$$n_0 \sum_{b\neq 0} \tilde{\mathcal{P}}^{\mathcal{E}}(b|a) + z\sqrt{\sigma^{\mathcal{E}}} < n_0 \sum_{b\neq 0} \mathcal{P}(b|a) - z\sqrt{\sigma}, \tag{39}$$

$$\sigma^{\mathcal{E}} = n_0 \sum_{b\neq 0} \tilde{\mathcal{P}}^{\mathcal{E}}(b|a)\left(1 - \sum_{b\neq 0} \tilde{\mathcal{P}}^{\mathcal{E}}(b|a)\right), \tag{40}$$

$$\sigma = n_0 \sum_{b\neq 0} \mathcal{P}(b|a)\left(1 - \sum_{b\neq 0} \mathcal{P}(b|a)\right), \tag{41}$$

where n_0 is the number of sent states and z is the arbitrary number of standard deviations σ and $\sigma^{\mathcal{E}}$ within the confidence interval according to the so-called "three-sigma rule." It should be noted that one may count not all detection events; similar inequalities may be constructed for particular phase choices in order to consider detection statistics in more details. Also one may apply any other statistical estimations like Chebyshev's inequality or Chernov bound. It allows us to take into consideration statistical properties of the finite set of observables. Legitimate users should adjust their system that the latter inequality is satisfied with very high probability. However, there is always a small chance of successful attack and its probability $\varepsilon_{\mathrm{QC}}$ can be determined by

$$\varepsilon_{\mathrm{QC}} = 1 - \mathrm{erf}\left(\frac{z_0}{\sqrt{2}}\right) \tag{42}$$

for z_0 that satisfies

$$z_0 = \frac{n_0 \sum_{b\neq 0}[\mathcal{P}(b|a) - \tilde{\mathcal{P}}^{\mathcal{E}}(b|a)]}{\sqrt{\sigma^{\mathcal{E}}} + \sqrt{\sigma}}. \tag{43}$$

It should be mentioned that Eve may intercept not all pulses but only part p_{int} of them. In this case one should estimate at which point p_{int} is significant and allows one to obtain more information compared to other strategies (collective attack, for instance). Taking into account the latter, Eq. (43) can then be expressed as follows:

$$z_0 = \frac{n_0 p_{\mathrm{int}} \sum_{b\neq 0}[\mathcal{P}(b|a) - \tilde{\mathcal{P}}^{\mathcal{E}}(b|a)]}{\sqrt{\sigma^{\mathcal{E}}} + \sqrt{\sigma}}, \tag{44}$$

with

$$\sigma^{\mathcal{E}} = n_0\left((1-p_{\mathrm{int}})\sum_{b\neq 0}\mathcal{P}(b|a) + p_{\mathrm{int}}\sum_{b\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)\right) \times\left[1 - \left((1-p_{\mathrm{int}})\sum_{b\neq 0}\mathcal{P}(b|a) + p_{\mathrm{int}}\sum_{b\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)\right)\right]. \tag{45}$$

Decent addition to the decrease of $\sum_{b\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)$ can be utilization of the monitoring diode as in [18]. Estimation of failure probability of monitoring diode $\varepsilon_{\mathrm{DF}}$ can be combined with probability $\varepsilon_{\mathrm{QC}}$ in unified probability of the proposed attack success as follows:

$$\varepsilon_{\mathrm{attack}} = \varepsilon_{\mathrm{QC}}\varepsilon_{\mathrm{DF}}. \tag{46}$$

B. Alternative countermeasures

Here we would like to briefly discuss alternative approaches that can be implemented by legitimate users. They are either based on decreasing $\sum_{b\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)$ [mostly by decrease of discrimination probability considering $\mathcal{P}^{\mathcal{E}}(e|a)$; for instance, by increase of the number of states] or obtaining more information about imposed by Eve states.

The former type of countermeasures can be done by utilization of uninformative states which provides better performance of QKD phase-coding protocols in the presence of quantum control attack; these additional states do not contain any information about key and are implemented only to reveal Eve's interception as it is shown in [7,8]. This method does not decrease detection rates (compare to $\frac{1}{N}$ for considered method); however, it requires preparation of rather complicated quantum states as in [8]. Also it should be noted that combination of uninformative states utilization and increase of the number of informative states may not in general provide overall decrease of $\sum_{b\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)$ as it shown in [49].

Another type of countermeasure is obtaining more information about states rather than the detection rate and its direct estimation related to them. One of the possible solutions is presented in [10,50,51], where coincidence detection events are monitored. This countermeasure is natural for the

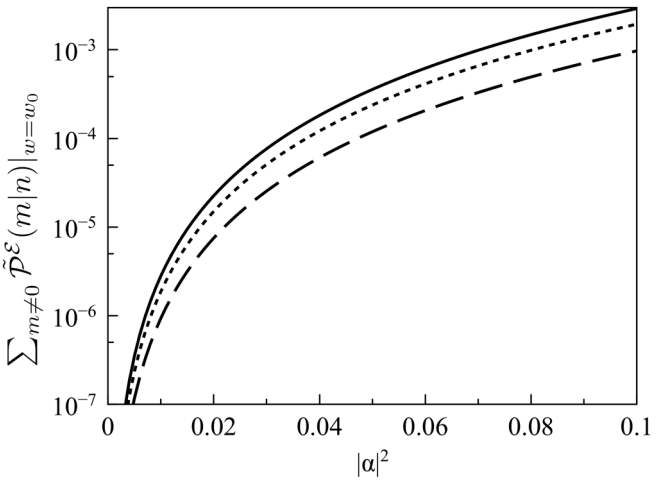

FIG. 5. Dependencies of detection rate with introduced error $\sum_{m\neq 0}\mathcal{P}^{\mathcal{E}}(m|n)$ from mean photon number for different types of state imposing. Solid line corresponds to the case that $\mathcal{P}^{\mathcal{E}}(b|e)=\frac{2N-1}{2N}$. Dotted line corresponds to the case that $\mathcal{P}^{\mathcal{E}}(b|e)$ has harmoniclike (phase-difference dependence) behavior. Dashed line corresponds to the case that $\mathcal{P}^{\mathcal{E}}(b|e)=\frac{1}{2N}$.

schemes containing two detectors at Bob's side (such as generic QKD protocol for a set of coherent states). Also another way of detector control prevention is based on utilization of a variable optical attenuator [52–54]. One more approach to reveal Eve is based on additional detection information from photon-number-resolving (PNR) detectors which allow one to monitor the statistics of states with increased power (e.g., a similar approach can be seen in [55]). Alternative detection schemes are compatible with methods of decreasing $\sum_{b\neq 0}\tilde{\mathcal{P}}^{\mathcal{E}}(b|a)$, although they may change relations (15) or (36), and (39) to more tight ones (based on additional detection information). However, a huge variety of different types of peculiar detection schemes requires individual analysis.

VII. RESULTS AND DISCUSSION

In this paper we present the approach for description of a quantum control attack based on combined protocol and hardware loopholes; it consolidates intercept-resend attack and detection node control. Protocols that operate with arbitrary even symmetric linearly independent nonorthogonal (e.g., coherent) states are of interest. Most intercept-resend attacks are well studied and focus their attention only on the problem of the state discrimination and mostly neglect the problem of further state imposing, though this problem should also be considered since incorrect imposing may cause violation of conditional detection probability at Bob's side. One of the possible solutions in the case is detection control. A crucial advantage is that it allows one to exclude any bit correlations between legitimate users, which are unknown to Eve. Thus it should be considered as the necessary part of most intercept-resend attacks, including the faked-state attack impossible without a hardware loophole. Figure 5 clearly illustrates the dependencies of the detection rate with introduced error $\sum_{m\neq 0}\mathcal{P}^{\mathcal{E}}(m|n)$ from different types of detection control.

Thus the impact of the attack depends on both state discrimination and correct state imposing. Moreover, the issue related to unified quantum description (i.e., in terms of Kraus operators) of the intercept-resend attack was solved by combination of von Neumann's measurement scheme and ambiguity of square root extraction for operators. The cornerstone of the approach is the space extension provided by introduction of Eve's ancillas; then it allows one to satisfy unitarity conditions.

As an example, we consider two different realizations of quantum control attack on the QKD system that operate with symmetric coherent states. In the case of USD-like attack construction of appropriate discrimination POVM is the most crucial part, while the method of imposing and its precision have secondary priority. Otherwise, in faked-state attack POVM is trivial (simple guess) and the most peculiar task is to adjust detection probabilities as precisely as possible. Specialized POVM construction chosen by Eve and detection node control are considered. We provide the expressions of conditional discrimination probability dependent on the number of utilized states and their mean photon number, detection, and error rate are expressed in terms of conditional probabilities.

Therefore, we consider the opposite conditions when Eve cannot preserve detection statistics and introduce appropriate countermeasures based on the analysis of conditional detection probability. From the practical point of view the optimal solution is the increase of the number of signal states (although alternative countermeasures are discussed). Numerical simulations show that in general approach for countermeasures shown in [8] is valid (i.e., decrease Eve's discrimination probability). Besides, security issues are considered and probability of successful attack (even in the case of appropriate countermeasures) is estimated.

ACKNOWLEDGMENTS

The work of A.K. and A.G. was supported by the Russian Science Foundation under Grant No. 20-71-100726 and performed in Steklov Mathematical Institute of Russian Academy of Sciences. The authors are very grateful to V. Chistyakov for provided experimental data from [18].

Sections II, III, V, and VI of the article were written by A.K. and A.G. and Sec. IV by G.M.

APPENDIX A: NOTE ON EIGENVALUES OF GRAM OPERATOR

The problem considered in Sec. V A 1 is closely related to the following useful property of Gram operator. It is known that eigenvalues of Gram operator are the same as eigenvalues of Gram matrix (or overlap matrix) $\Psi_{nm}=\langle\psi_n|\psi_m\rangle$. Further in this Appendix we would like to share our observation about the relation between Ψ_{nm} and $\Psi^{\perp}_{nm}=\langle\psi^{\perp}_n|\psi^{\perp}_m\rangle$ (where $|\psi^{\perp}_n\rangle$ is the state chosen to form a biorthogonal basis with signal states $|\psi_n\rangle$, i.e., $\langle\psi^{\perp}_n|\psi_m\rangle=\delta_{nm}$) that was first shown in [49] without proof and later proven independently in [56]. Further we would like to provide easier and more explicit proof compared to the latter citation.

Let us introduce orthonormal basis $|u_n\rangle$, i.e., $\langle u_n|u_m\rangle=\delta_{nm}$, constructed from nonorthogonal states by, for instance,

the Gram-Schmidt process:

$$|u_n\rangle = \sum_m c_{mn}|\psi_m\rangle, \quad \langle u_n| = \sum_m \langle\psi_m|c^*_{mn}, \tag{A1}$$

where $(\cdot)^*$ denotes complex conjugation and c_{mn} is the corresponding element of matrix C described, for instance, by the Gram-Schmidt process. Now redefine signal states in the orthonormal basis as follows:

$$|\psi_n\rangle = \sum_m d_{mn}|u_m\rangle, \quad \langle\psi_n| = \sum_m \langle u_m|d^*_{mn}, \tag{A2}$$

where d_{mn} is the element of matrix $D = C^{-1}$. Also let us express $|\psi_n^\perp\rangle$ in the same way:

$$|\psi_n^\perp\rangle = \sum_m b_{mn}|u_m\rangle, \quad \langle\psi_n^\perp| = \sum_m \langle u_m|b^*_{mn}, \tag{A3}$$

where b_{mn} is the element of unknown matrix B. One may find B from the condition of biorthogonality $\langle\psi_n^\perp|\psi_m\rangle = \delta_{nm}$:

$$\sum_k \langle u_k|b^*_{kn} \sum_l d_{lm}|u_l\rangle = \sum_k b^*_{kn} d_{km} = \delta_{nm}, \tag{A4}$$

$$B^\dagger D = B^\dagger C^{-1} = I, \quad B = C^\dagger, \tag{A5}$$

where $(\cdot)^\dagger$ denotes Hermitian conjugation. Thus Gram matrices are

$$\Psi_{nm} = \sum_k \langle u_k|d^*_{kn} \sum_l d_{lm}|u_l\rangle = (CC^\dagger)^{-1}_{nm} \tag{A6}$$

and

$$\Psi^\perp_{nm} = \sum_k \langle u_k|c_{nk} \sum_l c^*_{ml}|u_l\rangle = (CC^\dagger)_{nm}. \tag{A7}$$

Therefore, $\Psi^\perp_{nm} = \Psi^{-1}_{nm}$ and their eigenvalues are reciprocal to each other.

APPENDIX B: NUMERICAL ESTIMATIONS OF GRAM OPERATOR EIGENVALUES

Within this Appendix we may consider signal states as phase-coded coherent states using the following notation:

$$|\psi_n\rangle \equiv |\alpha\, e^{i\phi_n}\rangle, \tag{B1}$$

where $|\alpha\rangle$ is the initial coherent state with amplitude α and exponential term adds phase shift $\phi_n = \frac{\pi}{N}n$. The expression for overlap of signal coherent states is as follows:

$$\langle\psi_n|\psi_m\rangle = e^{-|\alpha|^2(1-e^{-i(\phi_n-\phi_m)})}. \tag{B2}$$

Hence

$$\mu_k = \sum_{n=1}^{2N} e^{i\frac{\pi k}{N}n} e^{-|\alpha|^2\left(1-e^{i\frac{\pi}{N}n}\right)}. \tag{B3}$$

From the point of view of numerical calculations eigenvalues can be easily calculated according to the latter expression. However, from the analytical point of view this expression is rather ambiguous since it has nontrivial dependence on $|\alpha|^2$ and N. Thus the idea is to express the latter equation using Jacobi-Anger expansion and then leave only the highest terms of the sum implying small mean photon number $|\alpha|^2$ in the signal:

$$\mu_k = \sum_{j=1}^{2N} e^{i\frac{\pi k}{N}j} e^{-|\alpha|^2\left(1-e^{i\frac{\pi}{N}j}\right)}$$

$$= e^{-|\alpha|^2} \sum_{n,m=-\infty}^{\infty} I_n(|\alpha|^2) J_m(|\alpha|^2) \sum_{j=1}^{2N} e^{i\pi\left(\frac{k+n+m}{N}\right)j}, \tag{B4}$$

where $J_m(|\alpha|^2)$ is a Bessel function of the first kind and $I_n(|\alpha|^2)$ is a modified Bessel function of the first kind. Therefore, finite sum of exponential functions has the following solution:

$$\sum_{j=1}^{2N} e^{i\pi\left(\frac{k+n+m}{N}\right)j} = e^{i\pi\left(\frac{k+n+m}{N}\right)} \frac{1-e^{i2\pi N\left(\frac{k+n+m}{N}\right)}}{1-e^{i\pi\left(\frac{k+n+m}{N}\right)}}. \tag{B5}$$

Argument of exponential function in the numerator of the right-hand side is proportional to $i2\pi$ with any value of k, n, and m; hence the numerator always equals zero. However, for certain values of k, n, m, and N argument of the exponential function in the denominator is also proportional to $i2\pi$, more precisely when $k+n+m = 2Nz$ for arbitrary integer z. Thus there is uncertainty with the well-known solution:

$$\lim_{k+n+m\to 2Nz} \frac{1-e^{i2\pi(k+n+m)}}{1-e^{i\pi\left(\frac{k+n+m}{N}\right)}} \to 2N. \tag{B6}$$

Finally, we obtain the following expression for eigenvalues:

$$\mu_k = e^{-|\alpha|^2} \sum_{n,m=-\infty}^{\infty} I_n(|\alpha|^2) J_m(|\alpha|^2)(2N\delta_{(m+n+k,2Nz)}). \tag{B7}$$

One may use the following property of Bessel functions: $J_n(x) \gg J_{n+1}(x)$ and $I_n(x) \gg I_{n+1}(x)$ for $x < 1$. Then maximal eigenvalue is denoted by $z = m = n = k = 0$ and it is as follows assuming $|\alpha|^2$ small:

$$\max_k(\mu_k) \approx 2N\, e^{-|\alpha|^2} I_0(|\alpha|^2) J_0(|\alpha|^2)$$

$$\approx 2N\left(1 - |\alpha|^2 + \frac{|\alpha|^4}{2}\right). \tag{B8}$$

The main contribution to the minimal eigenvalue is for $z = 1$; hence the minimal value of μ_k is for $k = 1$ and $m + n = 2N - 1$. Then we leave only the largest terms of minimal eigenvalue μ_k as the following approximation:

$$\min_k(\mu_k) \approx \sum_{q=0}^{2N-1} \frac{2N}{q!(2N-1-q)!} \left(\frac{|\alpha|^2}{2}\right)^{2N-1}$$

$$\approx \frac{2N}{(2N-1)!}(|\alpha|^2)^{2N-1}. \tag{B9}$$

Also it should be noted that, in the case of USD, $P_U = \min_k(\mu_k)$.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Inf. **2**, 16025 (2016).

[3] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Adv. Opt. Photon. **12**, 1012 (2020).

[4] S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, A. Kozubov, A. Gaidash, V. Chistiakov, A. Vasiliev, A. Gleim, and V. Makarov, Sci. Rep. **11**, 5110 (2021).

[5] M. Dusek, M. Jahma, and N. Lutkenhaus, Phys. Rev. A **62**, 022306 (2000).

[6] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[7] M. Lucamarini, G. Di Giuseppe, and K. Tamaki, Phys. Rev. A **80**, 032327 (2009).

[8] A. Gaidash, A. Kozubov, and G. Miroshnichenko, Phys. Scr. **94**, 125102 (2019).

[9] D. Kronberg, Lobachevskii J. Math. **41**, 2332 (2020).

[10] H. Ko, B.-S. Choi, J.-S. Choe, and C. J. Youn, Quantum Inf. Process. **17**, 17 (2018).

[11] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).

[12] V. Makarov, New J. Phys. **11**, 065003 (2009).

[13] V. Makarov and D. R. Hjelme, J. Mod. Opt. **52**, 691 (2005).

[14] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).

[15] L. Lydersen, M. K. Akhlaghi, A. H. Majedi, J. Skaar, and V. Makarov, New J. Phys. **13**, 113042 (2011).

[16] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nat. Commun. **2**, 349 (2011).

[17] S. Zhang, J. Wang, and C.-j. Tang, Int. J. Theor. Phys. **51**, 2719 (2012).

[18] V. Chistiakov, A. Huang, V. Egorov, and V. Makarov, Opt. Express **27**, 32253 (2019).

[19] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).

[20] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).

[21] X. Ma and M. Razavi, Phys. Rev. A **86**, 062319 (2012).

[22] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).

[23] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li *et al.*, Phys. Rev. Lett. **111**, 130502 (2013).

[24] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).

[25] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature (London) **557**, 400 (2018).

[26] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Nat. Photon. **13**, 334 (2019).

[27] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Phys. Rev. X **9**, 021046 (2019).

[28] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Phys. Rev. Lett. **123**, 100506 (2019).

[29] X. Ma, P. Zeng, and H. Zhou, Phys. Rev. X **8**, 031043 (2018).

[30] V. Chistiakov, A. Kozubov, A. Gaidash, A. Gleim, and G. Miroshnichenko, Opt. Express **27**, 36551 (2019).

[31] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[32] H.-K. Lo and J. Preskill, Quantum Inf. Comput. **7**, 431 (2007).

[33] C. Gobby, Z. Yuan, and A. Shields, Appl. Phys. Lett. **84**, 3762 (2004).

[34] G. Miroshnichenko, A. Kozubov, A. Gaidash, A. Gleim, and D. Horoshko, Opt. Express **26**, 11292 (2018).

[35] J. Bogdanski, J. Ahrens, and M. Bourennane, *Quantum Communications Realized II* (International Society for Optics and Photonics, Bellingham, WA, 2009), Vol. 7236, p. 72360M.

[36] X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, and G.-C. Guo, Opt. Lett. **30**, 2632 (2005).

[37] T. Brougham, S. M. Barnett, K. T. McCusker, P. G. Kwiat, and D. J. Gauthier, J. Phys. B: At., Mol., Opt. Phys. **46**, 104010 (2013).

[38] J. Shapiro, G. Saplakoglu, S.-T. Ho, P. Kumar, B. Saleh, and M. Teich, JOSA B **4**, 1604 (1987).

[39] J. H. Shapiro, M. C. Teich, B. E. A. Saleh, P. Kumar, and G. Saplakoglu, Phys. Rev. Lett. **56**, 1136 (1986).

[40] G. Feng, F. H. Cho, H. Katiyar, J. Li, D. Lu, J. Baugh, and R. Laflamme, Phys. Rev. A **98**, 052341 (2018).

[41] R. V. Mendes, Phys. Lett. A **373**, 2529 (2009).

[42] I. Csiszár and J. Korner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[43] A. D. Wyner, Bell Syst. Tech. J. **54**, 1355 (1975).

[44] T. M. Cover, *Wiley Series in Telecommunications* (Wiley, New York, 1991).

[45] A. Chefles, Phys. Lett. A **239**, 339 (1998).

[46] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).

[47] I. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[48] A. Peres and D. R. Terno, J. Phys. A: Math. Gen. **31**, 7105 (1998).

[49] A. Gaidash, A. Kozubov, and G. Miroshnichenko, JOSA B **36**, B16 (2019).

[50] G. Gras, D. Rusca, H. Zbinden, and F. Bussières, Phys. Rev. Applied **15**, 034052 (2021).

[51] C. C. W. Lim, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, IEEE J. Sel. Top. Quantum Electron. **21**, 192 (2015).

[52] A. Koehler-Sidki, M. Lucamarini, J. F. Dynes, G. L. Roberts, A. W. Sharpe, Z. Yuan, and A. J. Shields, Phys. Rev. A **98**, 022327 (2018).

[53] M. Alhussein and K. Inoue, Jpn. J. Appl. Phys. **58**, 102001 (2019).

[54] Y.-J. Qian, D.-Y. He, S. Wang, W. Chen, Z.-Q. Yin, G.-C. Guo, and Z.-F. Han, Optica **6**, 1178 (2019).

[55] A. Gaidash, V. Egorov, and A. Gleim, JOSA B **33**, 1451 (2016).

[56] D. Horoshko, M. Eskandari, and S. Y. Kilin, Phys. Lett. A **383**, 1728 (2019).