ЖЭТФ, 2010, том 137, вып. 4, стр. 656–663 

# PERFORMANCE OF A QUANTUM KEY DISTRIBUTION PROTOCOL WITH DUAL-RAIL DISPLACED PHOTON STATES

***S. A. Podoshvedov*** *

*School of Computational Sciences, Korea Institute for Advanced Study*
*Seoul,130-722, Korea*

*Department of Physics and Astronomy, Seoul National University*
*Seoul 151-742, Korea*

Received May 13, 2009

We propose a scheme for a quantum key distribution (QKD) protocol with dual-rail displaced photon states. Displaced single-photon states with different amplitudes carry bit values of code that may be extracted, while coherent states carry nothing and only provide an inconclusive outcome. A real resource of single photons is used, involving imperfections associated with experimental technique that result in a photon state with an admixture of the vacuum state. The protocol is robust against the loss of a single photon and the inefficiency of the detectors. Pulses with large amplitudes, unlike the conventional QKD relying on faint laser pulses, are used that may approximate it to standard telecommunication and may show resistance to eavesdropping even in settings with high attenuation. Information leakage to the eavesdropper is determined from comparison of the output distributions of the outcomes with ideal ones that are defined by two additional parameters accessible to only those send the pulses. Robustness to some possible eavesdropping attacks is shown.

## 1. INTRODUCTION

The quantum key distribution (QKD) protocol allows two remote parties (traditionally known as Alice and Bob) sharing a secure random key by communicating over an open channel [1–5]. The two users have two kinds of communication channels at their disposal. One is a classical public channel that may be eavesdropped by any unauthorized person but cannot be modified, and the second is a quantum channel. The quantum channel is used to transmit the secret key, while the classical public channel is used to check possible eavesdropping and to send the encoded message. Quantum mechanics ensures that any activities of potential eavesdroppers can be detected. If Alice and Bob are sure of the security of their key, they finally process the obtained key (the raw key) to produce a much safer key (the final key) using classical methods of error correction and privacy amplification [6, 7].

At present, there is a large collection of variations of QKD protocols [8]. We mention a few, chosen somewhat arbitrarily. The most famous QKD protocol is the four-state scheme, usually referred to as the Bennet–Brassard 1984 (BB84) protocol. In this protocol, the transmission of a single photon randomly polarized along four directions is used [2]. The key idea of the BB84 protocol is that simultaneous measurements of noncommuting observables for a single photon in two conjugate bases are forbidden by quantum mechanics. In other words, the measurement of one observable made on an eigenstate of another observable inevitably introduces disturbance to the state. Eve has no knowledge about the state sent by Alice and therefore she is forced half the time on average to introduce a disturbance into the state, which can be detected as a bit error. One of possible variations of BB84 consists in using quantum systems of dimension greater than 2 [9]. Most of the existing schemes use an imperfect single-photon source because a single-photon resource is difficult to realize experimentally (weak pulses were typically used in practice) [10]. Such an implementation, in the general case, may be vulnerable to the photon number-splitting attack [11]. To deal with an imperfect source of single photons, many interesting methods were proposed [12] involving the decoy state method [13].

Another possible way to implement secret shar-

*E-mail: sap@kias.re.kr

ing coding is based on the use of pairs of Einstein–Podolsky–Rosen (EPR) correlated photons [3]. A communication protocol based on entangled pairs of qubits is presented in [14]. A system, which is conceptually the simplest, involves the use of nonorthogonal quantum states [5]. Two nonorthogonal states cannot be distinguished unambiguously without perturbation only at the cost of some losses [15]. Initially, the implementation of a two-state protocol [5] was proposed using interference of two classical pulses, which is fragile under the influence of decoherence.

Instead of using single photons or weak coherent pulses, an interesting idea that nonclassical field states are useful for quantum information processing and communication was demonstrated with the example of a QKD with squeezed light [16]. Here, we propose to use nonclassical properties of the displaced single-photon states to share secret coding between two sides. The displacement operator imposes an additional varied degree of freedom on a photon state. According to the studied QKD model, the inputs are not single-photon states $|1\rangle$, as in [2], but the dual-rail displaced states. In other words, carriers in the model are the optical pulses with different large amplitudes, as in usual classical communication. The developed QKD protocol is free of problems related with interference. We also mention that a displaced single-photon state was experimentally generated in [17]. A possibility to conditionally generate displaced entangled states via a nonlinear interaction of a powerful pump beam with a crystal with the $\chi^{(2)}$ nonlinearity was proposed in [18]. Another interesting application of the displaced states is the dense coding protocol [19].

## 2. IMPLEMENTATION OF QKD WITH DUAL-RAIL DISPLACED STATES

We describe the protocol. Alice prepares two ensembles of displaced states with different displacement amplitudes

$$\rho = \frac{1}{2}\,\rho_1 + \frac{1}{2}\,\rho_2, \tag{1a}$$

where

$$\rho_1 = P_1|\varphi_1\rangle\langle\varphi_1| + P_1'|\varphi_1'\rangle\langle\varphi_1'|, \tag{1b}$$

$$\rho_2 = P_2|\varphi_2\rangle\langle\varphi_2| + P_2'|\varphi_2'\rangle\langle\varphi_2'|, \tag{1c}$$

($P_1 + P_1' = 1$ and $P_2 + P_2' = 1$) with the dual-rail displaced states defined as

$$|\varphi_1\rangle_{12} = |1,\alpha\rangle_1|0,i\alpha\rangle_2, \tag{2a}$$

$$|\varphi_1'\rangle_{12} = |0,\alpha\rangle_1|0,i\alpha\rangle_2, \tag{2b}$$

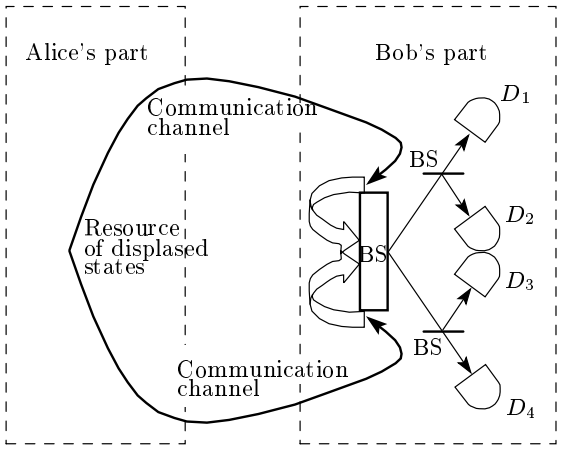


**Fig. 1.** Schematic representation of a QKD protocol based on dual-rail displaced states. Alice prepares her dual-rail displaced state and sends it to Bob, who has a chance to extract a bit value if it was the bit state. Otherwise, Bob obtains an inconclusive outcome and discards it. Bob announces the number at which he successfully obtained a bit value. Alice's input states are separate and can be injected to the optical fiber one after another with some delay. Bob has to introduce the same time delay to receive dual-rail states and try to extract information from them

$$|\varphi_2\rangle_{12} = |1,i\alpha_1\rangle_1|0,i\alpha_1\rangle_2, \tag{2c}$$

$$|\varphi_2'\rangle_{12} = |0,i\alpha_1\rangle_1|0,i\alpha_1\rangle_2, \tag{2d}$$

where $\alpha \neq \alpha_1$ in general. The states $|0,\alpha\rangle = \hat{D}(\alpha)|0\rangle$ and $|1,\alpha\rangle = \hat{D}(\alpha)|1\rangle$ are the displaced vacuum and one-photon states [17–19] and $\hat{D}(\alpha)$ is the displacement operator. Alice's parameters $\alpha$, $\alpha_1$ and $P_1$, $P_1'$, $P_2$, and $P_2'$ are hidden from both Bob and Eve. Because the states $|\varphi_1\rangle_{12}$ and $|\varphi_2\rangle_{12}$ (displaced single-photon states with different amplitudes) may carry bit values (0 or 1 respectively), we call them bit states, and because the states $|\varphi_1'\rangle_{12}$ and $|\varphi_2'\rangle_{12}$ do not carry any information to Bob, we call them disguised states.

This QKD protocol works as follows. Alice injects light in one of the four states (4a)–(4d) into a communication channel in random sequence. Bob prepares the measurement system as it is shown in Fig. 1. The measurement system involves a balanced beam splitter $B_1$ with the matrix

$$B_1 = \frac{1}{\sqrt{2}} \begin{Bmatrix} 1 & i \\ i & 1 \end{Bmatrix}. \tag{3}$$

The outcomes of beam splitter (3) are given by

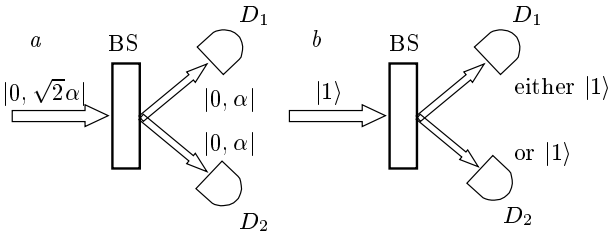


**Fig. 2.** An example of how to distinguish between a coherent state $|0,\sqrt{2}\,\alpha\rangle$ ($a$) and a single photon $|1\rangle$ ($b$). The coherent state mainly give two clicks except for small failure probability to register only one click. A single photon always gives one click. The greater the amplitude of the displaced state we use, the lower the failure probability

$$\hat{B}_1|\varphi_1\rangle_{12} = \frac{1}{\sqrt{2}} \times \times \left(|1\rangle_1 \left|0, i\sqrt{2}\,\alpha\right\rangle_2 + i|0\rangle_1 \left|1, i\sqrt{2}\,\alpha\right\rangle_2\right), \quad (4a)$$

$$\hat{B}_1|\varphi_1'\rangle_{12} = |0\rangle_1 \left|0, i\sqrt{2}\,\alpha\right\rangle_2, \quad (4b)$$

$$\hat{B}_1|\varphi_2\rangle_{12} = \frac{1}{\sqrt{2}} \times \times \left(\left|1, i\sqrt{2}\,\alpha\right\rangle_1 |0\rangle_2 + i\left|0, i\sqrt{2}\,\alpha\right\rangle_1 |1\rangle_2\right), \quad (4c)$$

$$\hat{B}_1|\varphi_1'\rangle_{12} = \left|0, i\sqrt{2}\,\alpha\right\rangle_1 |0\rangle_2, \quad (4d)$$

where we set $\alpha = \alpha_1$ to simplify the calculations below. To unambiguously discriminate outcomes (4a)–(4d) with off-the-shelf photon counters being on/off observables per se (presence or absence of photons), Bob uses the method shown in Fig. 2 for the particular case. The beam splitter in Fig. 2 converts $\left|0, i\sqrt{2}\,\alpha\right\rangle_1 |0\rangle_2 \to \left|0, i\sqrt{2}\,\alpha\right\rangle_1 |0, i\alpha\rangle_2$ and $|10\rangle_{12} \to \left(1/\sqrt{2}\right)(|10\rangle_{12} + |01\rangle_{12})$. If both detectors $D_1$ and $D_2$ register any photons, Bob knows that he detected a state $\left|0, i\sqrt{2}\,\alpha\right\rangle$. On the contrary, if neither $D_1$ nor $D_2$ click, then we cannot unambiguously discriminate such an outcome. It follows from Eqs. (4a)–(4d) that three simultaneous clicks by detectors $D_1$–$D_4$ in Fig. 1 are unambiguously identified as bit values of coding (0 and 1, respectively). All other events with three clicks less or more are identified as inconclusive outcomes and are discarded.

Thus, in the proposed detection system (Fig. 1) triggered on some photon statistics, the presence of three simultaneous clicks in Bob's statistics unambiguously heralds the extraction of bit information from the sent state. The proposed detection scheme is a test by means of a generalized measurement (known as POVM [20]) applied to displaced photon states. Bob cannot determine the displaced photon number state with certainty and he sometimes fails to extract the correct outcome unless his POVM system unambiguously gives an evident answer.

We mention some details of the protocol. All carries sent by Alice are numbered. A one-to-one correspondence between the sent and received pulses is established. At the point where Bob may unambiguously extract a bit value (three simultaneous clicks), they obtain perfectly correlated results. Bob has only to declare the number of the corresponding pulse (but not its result). All other outcomes are discarded by Bob. This allows Alice and Bob to share the mutual information

$$I(A,B) = \log_2(P_1p_1 + P_2p_2) - - \frac{P_1p_1\log_2(P_1p_1) + P_2p_2\log_2(P_2p_2)}{P_1p_1 + P_2p_2}, \quad (5)$$

where $p_1 = p_2 = 0.5\,(1 - P_0(\alpha))$ are the conditional probabilities for Bob to obtain a bit result if Alice respectively sent $|\varphi_1\rangle_{12}$ and $|\varphi_2\rangle_{12}$, and

$$P_0(\alpha) = \exp\left(-2|\alpha|^2\right) + 2\exp\left(-2|\alpha|^2\right)\left(1 - \exp\left(-|\alpha|^2\right)\right)$$

[19]. This protocol admits the possibility $\alpha \neq \alpha_1$ and, moreover, Alice may vary the amplitude of each sent carrier if the phase relations of dual states remain constant to protect the protocol from Eve's more skilful eavesdropping attacks, but these possibilities are beyond our consideration. It is natural to assume that Alice delivers states $|\varphi_1\rangle_{12}$ and $|\varphi_2\rangle_{12}$ with equal probabilities $P_1 = P_2 = P$, which allows Alice and Bob to share 1 bit of mutual information (Eq. (5)).

It is well known that quantum cryptography cannot prevent eavesdropping, but any eavesdropping attempt can be detected by the legitimate users of a communication channel. This is because eavesdropping affects the quantum state of the information carriers and results in an abnormal error rate. Therefore, before Bob publicly declares the number (but not the result of his measurement) at which he successfully extracted a bit value, Alice and Bob have to test their communication channel by sacrificing a part of their data sufficient to estimate the output distributions. Actually, there are three parameters to judge about a possible eavesdropping in the channel. The main such parameter is the output distribution of bit and inconclusive outcomes, which in the absence of eavesdropping is given by

$$P_0^{(Out)} = \frac{P_1}{4}\,(1 - P_0(\alpha)) = \frac{P}{4}\,(1 - P_0(\alpha)), \quad (6a)$$

$$P_1^{(Out)} = \frac{P_2}{4}\left(1 - P_0(\alpha_1)\right) = \frac{P}{4}\left(1 - P_0(\alpha)\right), \quad (6b)$$

$$P_?^{(Out)} = 1 - P_0^{(Out)} - P_1^{(Out)}, \quad (6c)$$

where $P_0^{(Out)}$, $P_1^{(Out)}$ is the probability to extract 0 and 1 bit values, respectively and $P_?^{(Out)}$ is a probability of inconclusive outcomes. We note that neither Bob nor malicious Eve know the output distribution of the bit and inconclusive outcomes because the parameters $P_1 = P_2 = P$ and $\alpha$ are chosen by Alice according to her own strategy and they are hidden from other participants. Eve can only listen to the talk between Alice and Bob through a public channel but she cannot correct the output distribution of the outcomes shared by Alice and Bob. Another important parameter whose change testifies the presence of Eve in the communication channel is what we call the disguised probability $P_d$, the frequency of the appearance of a bit outcome when Alice has sent one of the disguised states. The disguised states can give not a bit outcome but only an inconclusive outcome. The disguised probability $P_d$ must be exactly equal to zero in the ideal case of the absence of eavesdropping. Finally, Alice and Bob may also compare bit values of a chosen subset. For example, it is evident that a single photon is not detected in mode 2 if Alice sends a state $|\varphi_1\rangle_{12}$, and vice versa. Therefore, these parameters may serve as indicators of the presence or absence of eavesdropping in the communication channel. If the parameters do not coincide with the ideal ones, then eavesdropping is detected and transmission is aborted. We note that it is possible to directly check a communication channel without sacrificing any subset of data. Indeed, Bob can call the corresponding number of his bit outcomes for Alice to estimate output distributions and compare it with the ideal ones. After that, they can decide to take the code or to discard it.

We compare the protocol with the well-known B92 one. An infinite set of displaced number states with definite amplitudes $|n,\alpha\rangle = \hat{D}(\alpha)|n\rangle$, $n = 0,1,2,\ldots$, composes a complete set of basis states, $I = \sum_{n=0}^{\infty} |n,\alpha\rangle\langle n,\alpha|$, where $I$ is the identity operator. This means that any displaced photon state with some amplitude can be represented in terms of displaced states but with a different amplitude. We then have the decomposition

$$|1,\gamma\rangle = \exp\left(-\frac{|\beta|^2 + \alpha\beta^* - \beta\alpha^*}{2}\right) \times \times \sum_{k=0}^{\infty} \frac{\beta^k}{\sqrt{k!}} \left(\frac{k}{\beta} - \beta^*\right) |k,\alpha\rangle, \quad (7)$$

where $\alpha + \beta = \gamma$. Applying it to carries (2a) and (2c), we have $\beta = \alpha(i-1)$. In other words, we deal with the special case where the state is known to be one of the two possible pure states, either $|1,\alpha\rangle$ or superposition (7). We imagine that we have some "optical scissors" to snip off only two terms of superposition (7). Then we have two functions $|\psi_1\rangle = |1,\alpha\rangle$ and $|\psi_2\rangle = A_0|0,\alpha\rangle + A_1|1,\alpha\rangle$ ($|A_0|^2 + |A_1|^2 = 1$) in the two-level system that corresponds to a communication channel known as the binary erasure channel with possible outcomes 0, 1, and ? (? means an inconclusive result) or the B92 protocol [5]. Our case is therefore a generalization of the B92 protocol to an infinite set of basis vectors realized on displaced photon states. The coherent states provide inconclusive outcomes and the scheme in Fig. 1 is the POVM for the input displaced states $\rho_1$ and $\rho_2$ (Eqs. (1b) and (1c)).

It is interesting to note that the input states $\rho_1$ and $\rho_2$ (Eqs. (1b) and (1c)) were generated experimentally [17] using a biphoton generated via parametric down conversion. It was discussed in [17] that imperfections associated with the experimental technique result in the photon being prepared with a substantial admixture of the vacuum state $\rho_A = \eta|1\rangle\langle 1| + (1-\eta)|0\rangle\langle 0|$, where $\eta$ is the preparation efficiency. The preparation efficiency may account for the spontaneous parametric converter dark-count events. In such an event, the quantum state in the output mode is not conditioned on that in the converter channel. Alice only needs to estimate the preparation efficiency of her experimental setting for the conditional preparation of a single photon. After that she uses a beam splitter

$$B' = \begin{bmatrix} T & R \\ -R^* & T^* \end{bmatrix}$$

with arbitrary parameters $T$ and $R$ known only to her ($T$ and $R$ are transmittance and reflectance) to overlap her state $\rho_A$ with a coherent field $|0,\alpha_2\rangle$ at an auxiliary mode. The final state to be sent is obtained by taking the trace over states in the auxiliary mode. The beam splitter acts on the incident single-photon state simply as a lossy reflector, reducing its efficiency by the factor $|R|^2$. Also, the beam splitter causes the displacement of the state $\rho_A$, which gives a final statistical mixture of displaced Fock states as

$$\rho_A' = \eta|R|^2 \left(|1,\alpha_1 T\rangle_{11}\langle 1,\alpha_1 T|\right)\left(|0,\alpha_1'\rangle_{22}\langle 1,\alpha_1'|\right) + \\ + \left(\eta|T|^2 + 1 - \eta\right)\left(|0,\alpha_1 T\rangle_{11}\langle 0,\alpha_1 T|\right)\left(|0,\alpha_1'\rangle_{22}\langle 1,\alpha_1'|\right).$$

The state $\rho_A'$ is the state $\rho_1$ in Eq. (1b) if $P_1 = \eta|R|^2$, $P_2 = \eta|T|^2 + 1 - \eta$, $\alpha = \alpha_1 T$, and $i\alpha = \alpha_1'$. The same

applies to the generation of the $\rho_2$ state (Eq. (1c)). We therefore do not need an ideal resource of single photons, which is presently impossible due to technical imperfections of modern detectors. The resource of single photons experimentally realized in [17] is suitable for our protocol. We note that any unauthorized observer may estimate the preparation efficiency $\eta$ but it is hardly possible for him to guess the reduction factor $|R|^2$ and, all the more, the amplitudes of the states that are initially known only to Alice (additional secret parameters).

## 3. ROBUSTNESS TO EAVESDROPPING

We now analyze some eavesdropping strategies. We note that direct measurement of the incoming pulse does not answer which of the four states was sent. If Eve prefers to measure the dependence of the falling field on the relative phase, she may use a scheme that involves homodyning the signal field with a reference signal, known as the local oscillator, before the photodetection. Homodyning with a reference signal of a fixed phase gives the phase sensitivity necessary to yield the quadrature variances. Calculations show that the statistical characteristics $\langle 0,\alpha|\hat{a}|0,\alpha\rangle = \langle 1,\alpha|\hat{a}|1,\alpha\rangle = \alpha$ are equal and, consequently, $\langle 0,\alpha|\hat{X}|0,\alpha\rangle = \langle 1,\alpha|\hat{X}|1,\alpha\rangle$. Then, Eve may not be aware of the type of state (bit or disguised) she has if she measured a definite value of the quadrature component.

The most practical eavesdropping strategy may be an intercept-resend attack. Eve intercepts the quantum carrier on its way from Alice to Bob and performs the same measurement as Bob does, namely, using the beam splitter $B_1$ (Eq. (3)). After the measurement, Eve sends another quantum carrier to Bob in one of the four states (2a)–(2d), dependening on her outcome and following some chosen strategy. Eve's strategy may be as follows. If Eve obtains a bit value, then she again sends the corresponding bit state, either $|\varphi_1\rangle_{12}$ or $|\varphi_2\rangle_{12}$. If Eve detects an inconclusive outcome, then she tries to guess Alice's possible signal and to masquerade as Alice. We consider this in detail in example of the state $\rho_1$. We assume that Eve resends a state $|\varphi_1\rangle_{12}$ with a probability $P_1''$ and $|\varphi_1'\rangle_{12}$ with a probability $P_2''$ ($P_1''+P_2''=1$) in the case of her inconclusive output. Then Eve affects the output of the Alice–Bob probability distribution as

$$P_{0E}^{(Out)} = \frac{P_1(1+P_1'')}{8} + \frac{P_1'P_1''}{4},$$

where we neglect $P_0(\alpha')$ and $\alpha'$ is the amplitude of the displaced states that Eve creates. In general, Eve may choose $P_1''$ such that $P_{0E}^{(Out)}$ is almost similar to $P_0^{(Out)}$ (Eq. (6a)) due to the contribution $P_1'P_1''/4$ (she may sometimes guess the correct distribution $P_0^{(Out)}$). But this happens at the expense of a nonzero disguised probability $P_d = P_1'P_1''/4 \neq 0$, thus betraying Eve's presence. The greater $P_1''$ Eve chooses, the greater disguised probability $P_d$ is observed.

Eve may choose more tricky strategy of eavesdropping. We assume that Eve resends a corresponding disguised state, either $|\varphi_1'\rangle_{12}$ or $|\varphi_2'\rangle_{12}$, if she has obtained a corresponding inconclusive output, but she resends the respective states

$$|\Psi_1\rangle_{12} = \frac{1}{\sqrt{2}} \times \times \left(|1,\alpha'\rangle_1|0,i\alpha'\rangle_2 - i|0,\alpha'\rangle_1|1,i\alpha'\rangle_2\right), \quad (8a)$$

$$|\Psi_2\rangle_{12} = \frac{1}{\sqrt{2}} \times \times \left(-i|1,\alpha_1'\rangle_1|0,\alpha_1'\rangle_2 + |0,i\alpha_1'\rangle_1|1,\alpha_1'\rangle_2\right), \quad (8b)$$

instead of $|\varphi_1\rangle_{12}$ or $|\varphi_2\rangle_{12}$ if she obtains a bit outcome. This strategy gives the correct output distribution between Alice and Bob, Eqs. (6a)–(6c), because

$$\hat{B}_1|\Psi_1\rangle_{12} = |1\rangle_1 \left|0,i\sqrt{2}\,\alpha'\right\rangle_2,$$

$$\hat{B}_1|\Psi_2\rangle_{12} = \left|0,i\sqrt{2}\,\alpha'\right\rangle_1 |1\rangle,$$

except for the difference between $P_0(\alpha)$, $P_0(\alpha_1)$, $P_0(\alpha')$, and $P_0(\alpha_1')$. Then Eve may share bit of information with Alice and Bob. Nevertheless, this method of eavesdropping has a weak point. The states $|\Psi_1\rangle_{12}$ and $|\Psi_2\rangle_{12}$ are sensitive to the influence of decoherence. It is impossible to keep the phase relation in the states $|\Psi_1\rangle_{12}$ and $|\Psi_2\rangle_{12}$ stable when Eve and Bob are separated by a long distance because quantum coherence is fragile under the unavoidable interaction with the environment. The decoherence effects for the density operator can be induced by solving the master equation when it is possible to exactly calculate the coherence parameter and the amplitude damping. Calculations of the parameters for states (8a) and (8b) are beyond our consideration. Nevertheless, we hypothesize that Bob obtains a mixture of states with the density matrix

$$\rho_1' = 0.5\left(\left(|1,\alpha'\rangle_{11}\langle 1,\alpha'|\right)\otimes\left(|0,i\alpha'\rangle_{22}\langle 0,i\alpha'|\right) + + \left(|0,\alpha'\rangle_{11}\langle 0,\alpha'|\right)\otimes\left(|1,i\alpha'\rangle_{22}\langle 1,i\alpha'|\right)\right)$$

by analogy with coherent states with different amplitudes. Such a density matrix introduces error in the output distribution,

$$P_{0E}^{(Out)} = \frac{P\,(1-P_0(\alpha'))}{8}, \quad P_{1E}^{(Out)} = \frac{P\,(1-P_0(\alpha_1'))}{8},$$
$$P_{?E}^{(Out)} = 1 - P_{0E}^{(Out)} - P_{1E}^{(Out)},$$

compared with Eqs. (6a)–(6c), which can be observed. It is possible to show that when Eve eavesdrops a fraction $\eta \le 1$ of the transmissions, the final Alice–Bob distribution

$$P_{0E}^{(Out)} = P_{1E}^{(Out)} = P\left(1-\frac{\eta}{2}\right)\frac{1-P_0(\alpha)}{4}$$

and

$$P_{?E}^{(Out)} = 1 - P_{0E}^{(Out)} - P_{1E}^{(Out)},$$

if $P_0(\alpha) = P_0(\alpha') = P_0(\alpha_1')$ is performed, may approach the ideal distribution given by Eqs. (6a)–(6c) at the expense of 1 bit less of mutual information ($I(A,E) = I(E,B) = \eta$).

We next consider another realistic strategy, a beam splitting attack, where Eve tries to eavesdrop the transmitted signals without observing. We assume that Eve splits both states using her two beam splitters, both described by the matrix

$$B_E = \begin{bmatrix} T & R \\ -R^* & T^* \end{bmatrix},$$

where $T$ and $R$ satisfy the condition $|T|^2 + |R|^2 = 1$. Then the output states are

$$\begin{aligned}\hat{U}\,(|1,\alpha\rangle_1|0,i\alpha\rangle_2) &= \\ &= \hat{B}_{1E_1}\,(|1,\alpha\rangle_1|0\rangle_{E_1})\,\hat{B}_{1E_2}\,(|0,i\alpha\rangle_1|0\rangle_{E_2}) = \\ &= T|1,\alpha T\rangle_1|0,i\alpha T\rangle_2|0,\alpha R\rangle_{E_1}|0,i\alpha R\rangle_{E_2} + \\ &\quad + R|0,\alpha T\rangle_1|0,i\alpha T\rangle_2|1,\alpha R\rangle_{E_1}|0,i\alpha R\rangle_{E_2}, \qquad (9a)\end{aligned}$$

$$\begin{aligned}\hat{U}\,(|0,\alpha\rangle_1|0,i\alpha\rangle_2) &= \\ &= \hat{B}_{1E_1}\,(|0,\alpha\rangle_1|0\rangle_{E_1})\,\hat{B}_{1E_2}\,(|0,i\alpha\rangle_1|0\rangle_{E_2}) = \\ &= |0,\alpha T\rangle_1|0,i\alpha T\rangle_2|0,\alpha R\rangle_{E_1}|0,i\alpha R\rangle_{E_2}, \qquad (9b)\end{aligned}$$

where $E_1$ and $E_2$ are Eve's modes. The same is applicable to the components of $\rho_2$. The best that Eve can do in this case is to choose the parameters of her beam splitters such that the condition $|T| \gg |R|$ be satisfied. For $|R| \ll 1$, Eve may neglect the contribution of the second term in Eq. (9a) for her estimations. Then the output Alice–Bob statistics

$$P_{0E}^{(Out)} = P|T|^2\frac{1-P_0(\alpha T)}{4},$$

$$P_{1E}^{(Out)} = P|T|^2\frac{1-P_0(\alpha T)}{4},$$

$$P_{?}^{(Out)} = 1 - P_{0E}^{(Out)} - P_{1E}^{(Out)}$$

approaches to the ideal in (6a)–(6c) sufficiently close, because $|T|^2 \approx 1$. Alice and Bob compare their statistics and take it as correct, after which Bob announces the corresponding number at which he received the bit value. Eve also listens to their talk, and she needs only to distinguish two states $|0,\alpha R\rangle_{E_1}|0,i\alpha R\rangle_{E_2}$ and $|0,i\alpha_1 R\rangle_{E_1}|0,\alpha_1 R\rangle_{E_2}$ from each other to have an access to the coding. This can be done as Bob does with the help of balanced beam splitter (3),

$$\hat{B}_1\,(|0,\alpha R\rangle_{E_1}|0,i\alpha R\rangle_{E_2}) = |0\rangle_1\left|0,i\sqrt{2}\,\alpha R\right\rangle_2$$

and

$$\hat{B}_1\,(|0,i\alpha_1 R\rangle_{E_1}|0,\alpha_1 R\rangle_{E_2}) = \left|0,i\sqrt{2}\,\alpha_1 R\right\rangle_1|0\rangle_2.$$

Nevertheless, this strategy does not give Eve a sufficient access to coding because the probability

$$P_{vac} = \exp\left(-2|\alpha|^2\left(1-|T|^2\right)\right) \approx 1$$

not to register any photons and distinguish between $|0,\alpha R\rangle_{E_1}|0,i\alpha R\rangle_{E_2}$ and $|0,i\alpha_1 R\rangle_{E_1}|0,\alpha_1 R\rangle_{E_2}$ is high. Eve registers nothing and she loses any information about coding shared by Alice and Bob. Therefore, she can only have access to $\eta = 1 - P_{vac} \approx 0$ bits of mutual information. Moreover, Eve does not know the values of $\alpha$ exactly, to try to define optimal parameters for her beam-splitting attack. This consideration gives an estimate of Alice's amplitude $\alpha$ to satisfy the condition $|\alpha|^2(1-|T|^2) \approx 0$ for $|T|^2 \approx 1$.

We now consider the case where Eve attempts to gain some information on each signal sent by Alice, while minimizing the damage to the state. This strategy can be realized by making the information carrier interact unitarily with a probe, and then letting the signal proceed to Bob, in a slightly modified state. Eve may store her probe and decide which type of measurement to perform on her probe only after Alice and Bob share their coding. For this, Eve supplies her probe in a known initial state $|g\rangle$, and then the combined system may evolve as

$$\begin{aligned}\hat{U}\,(|\varphi_1\rangle|g\rangle) &= |\varphi_{1E}\rangle|e_1\rangle, \\ \hat{U}\,(|\varphi_1'\rangle|g\rangle) &= |\varphi_{1E}'\rangle|e_2\rangle,\end{aligned} \qquad (10a)$$

$$\begin{aligned}\hat{U}\,(|\varphi_2\rangle|g\rangle) &= |\varphi_{2E}\rangle|e_3\rangle, \\ \hat{U}\,(|\varphi_2\rangle|g\rangle) &= |\varphi_{2E}'\rangle|e_2\rangle,\end{aligned} \qquad (10b)$$

where

$$|\varphi_{1E}\rangle_{12} = |1,\alpha_E\rangle_1|0,i\alpha_E\rangle_2,$$

$$|\varphi'_{1E}\rangle_{12} = |0,\alpha_E\rangle_1|0,i\alpha_E\rangle_2,$$
$$|\varphi_{2E}\rangle_{12} = |1,i\alpha_{1E}\rangle_1|0,\alpha_{1E}\rangle_2,$$
$$|\varphi'_{2E}\rangle_{12} = |0,i\alpha_{1E}\rangle_1|0,\alpha_{1E}\rangle_2.$$

The evolution is unitary (Eve can construct some Hamiltonian that generates it) and the scalar product is conserved. This then imposes the condition

$$\langle e_1|e_3\rangle = \exp\left(-\left(|\alpha|^2-|\alpha_E|^2\right)-\left(|\alpha|^2-|\alpha_{1E}|^2\right)\right)\times \times\frac{1-(i\alpha-\alpha)^2}{1-(i\alpha_{1E}-\alpha_E)^2}, \quad (11a)$$

$$\langle e_1|e_4\rangle = \exp\left(-\left(|\alpha|^2-|\alpha_E|^2\right)-\left(|\alpha|^2-|\alpha_{1E}|^2\right)\right)\times \times\frac{i\alpha-\alpha}{i\alpha_{1E}-\alpha_E}, \quad (11b)$$

$$\langle e_3|e_2\rangle = \exp\left(-\left(|\alpha|^2-|\alpha_E|^2\right)-\left(|\alpha|^2-|\alpha_{1E}|^2\right)\right)\times \times\frac{\alpha-i\alpha}{\alpha_E-i\alpha_{1E}}, \quad (11c)$$

$$\langle e_4|e_2\rangle = \exp\left(-\left(|\alpha|^2-|\alpha_E|^2\right)- -\left(|\alpha|^2-|\alpha_{1E}|^2\right)\right). \quad (11d)$$

The composite system is a direct product of the corresponding states if overlaps $|\langle e_i|e_j\rangle|^2 \le 1$ $(i,j=1,\ldots,4)$. After sending the modified carrier to Bob, Eve remains with her probe. The probes are not orthogonal to each other. The idea of Eve is to cause minimal damage to the information carrier and to obtain as much information as possible. To hide her presence, Eve may try to guess Alice's parameters $\alpha \approx \alpha_E$ and $\alpha \approx \alpha_{1E}$ to provide performance of the condition $P_0(\alpha) \approx P_0(\alpha_E) \approx P_0(\alpha_{1E})$. But the overlap $\langle e_1|e_3\rangle$ in Eq. (11a) becomes almost equal to unity $(\langle e_1|e_3\rangle \approx 1)$ in the case where $\alpha \approx \alpha_E$ and $\alpha \approx \alpha_{1E}$. Because the states $|e_1\rangle$ and $|e_3\rangle$ are not orthogonal and, moreover, their overlap is sufficiently large, Eve cannot distinguish them exactly and, as consequence, she can share only 1 bit less of mutual information.

## 4. DISCUSSION AND CONCLUSION

Optical quantum cryptography is based on the use of single-photon states. Unfortunately, these states are difficult to realize experimentally. At present, practical implementations rely on faint laser pulses in which the photon number distribution obeys the Poisson statistics, or on entangled photon pairs. Both possibilities suffer from a small probability of generating more than one photon. For large losses in the quantum channel, small fractions of these multiphotons can have important consequences for the security of the key. We propose a QKD protocol that can use the actually existing resources of single photons. The way to create pseudo-single-photon states is to generate photon pairs and use one photon as a trigger for the conditional generation of the other. Imperfections associated with the experimental technique lead to only a mixture of the single-photon and the vacuum states [17]. Nevertheless, if we modulate such a statistical mixture by a coherent state on a beam splitter, we produce a mixture of the displaced photon states with coherent states that are applicable for the proposed QKD protocol. We emphasize that the modulation of the mixture is the main feature for the protocol to work. As is well known, the phase of a Fock number state is random. If we modulate a photon number state $|n\rangle$ (or, equivalently, apply a displacement operator), we impose a phase on the state $|n,\alpha\rangle$ that is definitely determined. This allows having different outcomes (Eqs. (4a) and (4c)) for the input displaced single-photon states, with only their phase varying. We emphasize that the protocol in not applicable for a single photon or a pair of photons without displacement because the phase of photon number states is not definitive. This feature mainly distinguishes this protocol from others. Also, such a modulation allows Alice to use two additional parameters accessible to nobody, namely, the initial distributions of her input states and the amplitudes of her fields that she may change. Our QKD deals with optical pulses as carriers, unlike the quantum QKD with a single photon that approximates it to standard telecommunication. With the availability of the sources of quantum states for the communication, the success of quantum cryptography also essentially depends on the ability to detect single photons. In principle, this can be achieved using a variety of techniques, for instance, photomultipliers, avalanche photodiodes, multichannel plates, and superconducting Josephson junctions. In our case, commercial detectors (the usual on-off observables) are used.

We consider an optical fiber version of a Mach–Zehnder interferometer made out of two symmetric beam splitters connected to each other, with one phase modulator in each arm. This interferometer combined with a single-photon source and photon-counting detectors can be used for quantum cryptography if the phase shift is kept constant. Although such a scheme may be perfect on an optical table, it is impossible to keep the path difference between two modes stable for a longer distance. To avoid this, Alice can introduce some delay

between the pulses in the input modes and send them one after another through the same optical fiber, where they may experience the same phase shift in the environmentally sensitive part of the system. This can be done because the input states are separate. This allows preserving phase relations of the incoming pulses at the output on Bob's side if he also makes the same delay for the first pulse before combining two pulses (dual-rail output) in the beam splitter. A detailed analysis of the influence of decoherence on the displaced single photon state is the subject of future investigation. Remarkably, this protocol is robust against the loss of a single photon and the inefficiency of the detectors. Those factors would cause the corresponding detectors to be silent, and such cases can simply be discarded. Therefore, this only affects the output distributions and has to be taken into account in realistic cases. We only express idea that use of pulses with large amplitudes, in contrast to conventional schemes of quantum cryptography, may show resistance to eavesdropping even in settings with high attenuation.

The proposed QKD protocol is a generalization of the B92 protocol [5] applied to the displaced photon number states. Our protocol works as a binary erasure channel as the B92 protocol does [5]. We note that the optical scheme of a two-state protocol [5] can be implemented using the interference between a macroscopic bright pulse and a dim pulse with less than one photon on average [5]. The proposed optical scheme is not that of a Mach–Zehnder interferometer and, as consequence, it is free of the interference effect and of attendant problems. Our analysis involves the study of only a restricted number of possible eavesdropping attacks and shows that the protocol is secure. The consideration of other aspect of our protocol deserves separate investigations.

This work was partially supported by the IT R&D program of MKE/IITA (2008-F-035-01).

## REFERENCES


1. S. Wiesner, SIGAST Newa **15**, 78 (1983).
2. C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing*, Bangalore, India, 175 (1984).
3. A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
4. C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
5. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
6. C. H. Bennett, G. Brassard, C. Crepeau, and M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
7. C. H. Bennett, F. Bessette, G. Brassard, I. Salvail, and J. Smolin, J. Cryptology **5**, 2 (1992).
8. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
9. H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000); H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000); M. Bourennane, A. Karlsson, and G. Bjorn, Phys. Rev. A **64**, 012306 (2001).
10. P. D. Townsend, J. G. Rarity, and P. R. Tapster, Electron. Lett. **29**, 1291 (1993); A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993).
11. B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H. P. Yuen, Quant. Semiclass. Opt. **8**, 939 (1996); G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
12. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004); M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004); D. A. R. Dalvit, R. L. de Matos Filho, and F. Toscano, New J. Phys. **8**, 276 (2006).
13. X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, Phys. Rep. **448**, 1 (2007); W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
14. K. Bostrom and T. Felbinger, Phys. Rev. Lett. **89**, 187902 (2002).
15. I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
16. M. Hillery, Phys. Rev. A **61**, 022309 (2000).
17. A. I. Lvovsky and S. A. Babischev, Phys. Rev. A **66**, 11801 (2002).
18. S. A. Podoshvedov and J. Kim, Phys. Rev. A **74**, 033810 (2006).
19. S. A. Podoshvedov, Phys. Rev. A **79**, 012319 (2009).
20. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press, Cambridge (2000).