ISSN 0021-3640, JETP Letters, 2022, Vol. 116, No. 2, pp. 128–132. © Pleiades Publishing, Inc., 2022.
Russian Text © The Author(s), 2022, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2022, Vol. 116, No. 2, pp. 128–132.

QUANTUM INFORMATICS

# Quantum Key Distribution with Untrusted Detectors Accessible to an Eavesdropper

**K. A. Balygin[a], *, S. P. Kulik[a], and S. N. Molotkov[b]**

[a] *Center of Quantum Technologies, Moscow State University, Moscow, 119899 Russia*

[b] *Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, 142432 Russia*

**e-mail: kirill.balygin@gmail.com*

Received June 7, 2022; revised June 7, 2022; accepted June 9, 2022

A simple fundamental modification of quantum key distribution protocols has been proposed: it is not required to protect the results of avalanche detectors from an eavesdropper, but all cryptographic properties of a protocol hold.

**DOI:** 10.1134/S0021364022601142

## 1. INTRODUCTION

To guarantee the security of quantum key distribution, it is fundamentally important to prevent the access of an eavesdropper to the transmitting and receiving devices. Bits of the key on the receiver side are obtained from photocounts of single-photon avalanche detectors, which should be inaccessible to the eavesdropper, which requires certain measures to protect detectors from information leakage at the detection of quantum states.

The eavesdropper (Eve) can know in which of the detectors a count occurs even without direct access to the detectors. Detecting back-flash emission from detectors to the communication channel, the eavesdropper can get information of the bits of the key, remaining undetected.

This particularly concerns quantum key distribution systems involving superconducting detectors. Because of the use of large "dry" cryostats, detectors are located beyond the main receiver device and are connected to it through a fiber and electric cables. For this reason, it is quite difficult to ensure their complete guaranteed isolation from the environment.

*In this regard, there is a fundamental question: Can a quantum key distribution system where detectors are generally accessible and are even located beyond the main instrument and results are accessible to the eavesdropper guarantee the cryptography security of keys?*[1]

The positive answer to this question is given in this work.

We consider below the BB84 protocol [1] in the standard point–point configuration involving phase encoding in optical fiber systems. Two bases, direct + and conjugate ×, and two states corresponding to 0 and 1 in each basis are used in the protocol.

Alice on the transmitter side randomly chooses a basis and a state in it by choosing the relative phase in two pulses of the states. Four phases are generally used. In the + basis, the logical bits $0^+$ and $1^+$ correspond to the phases $\varphi_A = 0$ and $\pi$, respectively. In the × basis, the bits $0^\times$ and $1^\times$ correspond to the phases $\varphi_A = \pi/2$ and $3\pi/2$, respectively.

In the standard version of the protocol, Bob on the receiver side chooses only two phases $\varphi_B = 0$ and $\pi/2$ corresponding to the + and × bases, respectively.

Alice and Bob hold only messages where their bases coincide. On the receiver side, states from the communication channel after passage through a Mach–Zehnder interferometer [2] reach the detectors. The probabilities of a count in detectors $U$ and $D$ are proportional to $\cos^2\left(\frac{\varphi_A - \varphi_B}{2}\right)$ and $\sin^2\left(\frac{\varphi_A - \varphi_B}{2}\right)$, respectively (Fig. 1). When the bases coincide, if Alice sends $0^+$, a count occurs only in the detector $U$ because interference is constructive on the detector $U$ and is destructive on the detector $D$. If Alice sends $1^+$, a count occurs in the detector $D$, whereas a count is absent in the detector $U$.

Similarly, in the × basis, the states $0^\times$ and $1^\times$ initiate a count in the detectors $D$ and $U$, respectively.

*Since bases (not states in a basis) are opened after the transfer of states, if the eavesdropper had access to detectors and knew which of the detectors recorded a count, the*

[1] To avoid misunderstanding, we note that the consideration below concerns the standard point–point configuration rather than twin-field quantum cryptography systems (see below).

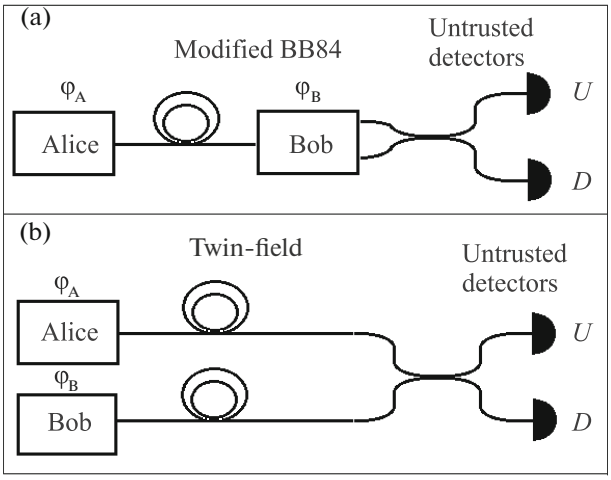


**Fig. 1.** Schemes of the quantum key distribution for (a) a modified protocol with untrusted detectors and (b) a twin-field protocol. The probabilities of a count in detectors $U$ and $D$ are proportional to $\cos^2\left(\frac{\varphi_A - \varphi_B}{2}\right)$ and $\sin^2\left(\frac{\varphi_A - \varphi_B}{2}\right)$, respectively.

*eavesdropper would know the entire transferred key. For this reason, detectors in the standard quantum key distribution systems should be protected; i.e., both the direct and indirect access of the eavesdropper should be excluded*.

## 2. INFORMAL REASONS FOR THE SECURITY OF A MODIFIED PROTOCOL

Below, we describe a modified protocol with untrusted detectors and discuss informal reasons for the security of the new protocol.

The idea is a random choice of four rather than two phase values, two in each basis, on the receiver side. The phases and the corresponding detectors where a count occurs have the form

$$\text{basis} + \begin{cases} \text{bit } 0 \quad \varphi_A = 0 \begin{cases} \varphi_B = 0 \to U \\ \varphi_B = \pi \to D \end{cases} \\ \text{bit } 1 \quad \varphi_A = \pi \begin{cases} \varphi_B = 0 \to D \\ \varphi_B = \pi \to U \end{cases} \end{cases}, \quad (1)$$

$$\text{basis} \times \begin{cases} \text{bit } 0 \quad \varphi_A = \frac{\pi}{2} \begin{cases} \varphi_B = \frac{\pi}{2} \to U \\ \varphi_B = \frac{3\pi}{2} \to D \end{cases} \\ \text{bit } 1 \quad \varphi_A = \frac{3\pi}{2} \begin{cases} \varphi_B = \frac{3\pi}{2} \to U \\ \varphi_B = \frac{\pi}{2} \to D \end{cases} \end{cases}. \quad (2)$$

In each basis, e.g., in the + basis, if Alice sends 0 ($\varphi_A = 0$), depending on the random choice of phases by Bob ($\varphi_B = 0$ or $\pi$), which is unknown to Eve even after the opening of bases, Eve, who does not know Bob's phase, will "see" a random count in one of the detectors $U$ or $D$ for each bit 0 or 1 (see Eqs. (1) and (2)). The procedures for other states are similar.

*Thus, additional randomness introduced by Bob in each basis, which is unknown to Eve, makes it possible to open counts in detectors for Eve, but she will not know the transmitted key bit.*

The possibility of access to detectors for Eve can be illustrated in terms of information theory.

In the standard protocol, Alice chooses a basis and a bit in this basis that are unknown to Eve. Bob chooses only a basis that is also unknown to Eve. Consequently, before the opening of the bases, Eve does not know three bits of information. When the bases are opened, Alice and Bob each open one bit of information. As a result, one of three bits remains unknown to Eve. This bit is a common secret of Alice and Bob. Knowing the basis, Bob obtains this bit through a count in a detector.

In the modified protocol, Alice has two bits of information unknown to Eve before opening of the bases. Bob also has two bits of information before opening of the bases. When the bases are opened, Alice and Bob each open one bit of information. Two bits remain unknown to Eve. If access to counts in detectors is allowed to Eve, she receives one bit of information after a count in a detector. As a result, one bit of information remains unknown to Eve and is present in a key. Bob also knows a detector where a count occurs, but Bob also knows his choice of the phase and, thus, can identify a bit sent by Alice. Eve does not know the phase chosen by Bob and knows only a count in a detector in a given basis. Observing only the count in the detector and knowing the basis, Eve cannot know the bit transmitted by Alice because she does not know the phase by Bob.

It is interesting to compare our protocol with the actively developed twin-field protocol [3, 4],[2] where the detectors are also untrusted and accessible (open) to Eve.

In the twin-field protocol (see Fig. 1), Alice and Bob independently and equiprobably choose two phases in each of the two bases, e.g., in the + basis, $0 \to \varphi_A = 0$ and $1 \to \varphi_A = \pi$ for Alice and $0 \to \varphi_B = 0$ and $1 \to \varphi_B = \pi$ for Bob. Since the interference signals on the detectors $U$ and $D$ are proportional to $\cos^2\left(\frac{\varphi_A - \varphi_B}{2}\right)$ and $\sin^2\left(\frac{\varphi_A - \varphi_B}{2}\right)$, respectively, the count occurs in the detectors $U$ and $D$ at the identical

[2] The idea of interference of states from different sources in quantum key distribution was proposed as early as in 1997 in [5]; this system was called quantum key distribution based on a quantum computer.

and different phases, respectively. The detectors are accessible to the eavesdropper.

Alice generates two bits of information unknown to the eavesdropper: one bit for the choice of the basis and the second bit for a logical 0 or 1 in the basis. Bob also generates two bits of information unknown to Eve. When the bases are opened, Alice and Bob each open one bit of information. Two of four bits remain unknown to Eve. After the count in the detector $U$ or $D$, Eve gets one bit of information. One bit of information remains unknown to Eve and is a common secret of Alice and Bob.

Unlike Eve, knowing the count of the detector and which bit they send, Alice and Bob obtain a common bit. For example, if both Alice and Bob send 0, the count occurs in detector $U$. Such an event takes place if Alice and Bob send identical bits (each of them knows the sent bits). Consequently, preliminarily making an agreement, Alice and Bob will have the common bit 0. If both Alice and Bob send 1, the count also occurs in detector $U$, and Alice and Bob will have the common bit 1. Eve observes only the count in the detector $U$ and does not know the common bit because the count in the detector $U$ can occur from both bits 0 and 1 sent by Alice and Bob.

This is an informal information-theory reason for obtaining the common secret bit by Alice and Bob.

## 3. FORMAL PROOF OF SECURITY

The main idea in the formalization of untrusted detectors accessible to Eve is to reduce the new protocol to an equivalent protocol involving the standard BB84 protocol with the delivery of additional quantum states carrying information on the count in one of the two detectors to Eve.

We consider the standard BB84 protocol. Obtaining a count, 0 or 1 correct or incorrect, in detectors in each basis, which are inaccessible to Eve, Bob reports this result to Eve, randomly and equiprobably interchanging the detectors $U$ and $D$. In particular, if the count occurs in the detector $U$, Bob randomly and equiprobably chooses the detector $U$ or $D$ and reports his choice to Eve.

This procedure is equivalent to the modified protocol where Bob randomly chooses one of two phases in each basis leading to the random permutation (for Eve) of counts in the detectors $U$ and $D$.

Further, we consider a single-photon case with the identical quantum efficiencies of the detectors to avoid excess technical details. The nonequal quantum efficiencies of detectors can be taken into account by the method presented in [6, 7].

Thus, it is sufficient to consider the BB84 protocol supplemented by information for Eve concerning the random permutation of the detector where the count occurs. Because the situation is symmetric in the bases, it is sufficient to consider the situation in one basis, e.g., in the + basis. The results in the × basis are obtained by the unitary transformation of information states.

We use the EPR version of the protocol (see details in, e.g., [6]). Alice prepares the EPR state, i.e., her subsystem $X$, and stores it on her side as a reference subsystem and sends the subsystem $Y$ to Bob. The subsystem $Y$ in the quantum communication channel is attacked by Eve. Alice carries out measurements in the basis $X$; in this process, a state corresponding to 0 or 1 appears randomly and equiprobably. After the measurement, Bob's subsystem $Y$ is transformed to a state corresponding to 0 or 1 because of the structure of the EPR state. The EPR state has the standard form

$$|\Phi^+\rangle_{XY} = \frac{1}{\sqrt{2}}\left(|0\rangle_X \otimes |0\rangle_Y + |1\rangle_X \otimes |1\rangle_Y\right). \quad (3)$$

Since the EPR state has the same structure in both + and × bases, the index of the basis is omitted.

Any transformation of the input quantum state to the output state is described by the action of a superoperator, which is a completely positive map [8]. Any superoperator is representable unitarily (see details in [9]). This means that any superoperator is implemented by entangling the input state with an auxiliary state $|E\rangle_{\mathrm{E}}$ by means of the unitary operator $U_{\mathrm{BE}}$, which is determined by Eve.

Eve's attack described by the unitary operator $U_{\mathrm{BE}}$ gives

$$U_{\mathrm{BE}}\left(|\Phi^+\rangle_{XY} \otimes |E\rangle_{\mathrm{E}}\right)$$

$$= \frac{1}{\sqrt{2}}|0\rangle_X \otimes \left\{\sqrt{1-Q}|0\rangle_Y \otimes |\Phi_0\rangle_{\mathrm{E}} + \sqrt{Q}|1\rangle_Y \otimes |\Theta_0\rangle_{\mathrm{E}}\right\} \quad (4)$$

$$+ \frac{1}{\sqrt{2}}|1\rangle_X \otimes \left\{\sqrt{1-Q}|1\rangle_Y \otimes |\Phi_1\rangle_{\mathrm{E}} + \sqrt{Q}|0\rangle_Y \otimes |\Theta_1\rangle_{\mathrm{E}}\right\}.$$

States of Eve are normalized; for this reason, the coefficients are taken in the form $1-Q$ and $Q$ to preserve normalization. As shown below, $Q$ is the error probability on the receiver side.

Alice and Bob perform measurements in the identical bases $\{|0\rangle_X, |1\rangle_X\}$and $\{|0\rangle_Y, |1\rangle_Y\}$, respectively. Taking into account Eqs. (3) and (4), the resulting Alice–Bob–Eve state is described by the density matrix

$$\begin{aligned}\rho_{XY\mathrm{E}} = \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes \{(1-Q)|0\rangle_{YY}\langle 0| \otimes |\Phi_0\rangle_{\mathrm{EE}}\langle\Phi_0| \\ + Q|1\rangle_{YY}\langle 1| \otimes |\Theta_0\rangle_{\mathrm{EE}}\langle\Theta_0|\} \\ + \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes \{(1-Q)|1\rangle_{YY}\langle 1| \otimes |\Phi_1\rangle_{\mathrm{EE}}\langle\Phi_1| \\ + Q|0\rangle_{YY}\langle 0| \otimes |\Theta_1\rangle_{\mathrm{EE}}\langle\Theta_1|\}.\end{aligned} \quad (5)$$

As previously shown (see, e.g., [6]), the states $\{|\Phi_0\rangle_{\mathrm{E}}, |\Phi_1\rangle_{\mathrm{E}}\}$ and $\{|\Theta_0\rangle_{\mathrm{E}}, |\Theta_1\rangle_{\mathrm{E}}\}$ for Eve's optimal attack lie in orthogonal subspaces and ${}_{\mathrm{E}}\langle\Theta_0|\Theta_1\rangle_{\mathrm{E}} = {}_{\mathrm{E}}\langle\Phi_0|\Phi_1\rangle_{\mathrm{E}} = 1-2Q$. Optimality means

that Eve obtains maximum information on the transmitted key at the observed error $Q$ on the receiver side.

Formula (5) has a simple interpretation. Alice sends 0 or 1 with a probability of 1/2. Bob obtains a correct count with a probability of $1 - Q$ and Eve has the state $|\Phi_0\rangle_E$. Bob obtains an erroneous count with a probability of $Q$ and Eve has the state $|\Theta_0\rangle_E$, similar to the case where Alice sends 1.

## 4. MODIFICATION OF THE PROTOCOL

Let Bob obtain 0 (correct or erroneous), i.e., observe the count in the detector $U$. Bob reports randomly and equiprobably one of the orthogonal states $|U\rangle_D$ and $|D\rangle_D$ to Eve; i.e., Eve receive the density matrix

$$\rho_D = \frac{1}{2}\left(|U\rangle_{DD}\langle U| + |D\rangle_{DD}\langle D|\right). \quad (6)$$

Thus, when Bob records count 0 (count in the upper detector), state (6) is delivered to Eve. Measuring state (6), Eve identifies the detector $U$ or $D$ equiprobably according to Eqs. (1) and (2).

Similarly, if Bob observe count 1 in the detector $D$ (correct or erroneous), measuring state (6), Eve observes the state $U$ or $D$ equiprobably.

As a result, the density matrix $\rho_{XYE}$ is replaced by

$$\begin{aligned}\rho_{XYED} &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes \{(1-Q)|0\rangle_{YY}\langle 0| \otimes |\Phi_0\rangle_{EE}\langle\Phi_0| \otimes \rho_D \\ &+ Q|1\rangle_{YY}\langle 1| \otimes |\Theta_0\rangle_{EE}\langle\Theta_0| \otimes \rho_D\} \quad (7)\\ &+ \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes \{(1-Q)|1\rangle_{YY}\langle 1| \otimes |\Phi_1\rangle_{EE}\langle\Phi_1| \otimes \rho_D \\ &+ Q|0\rangle_{YY}\langle 0| \otimes |\Theta_1\rangle_{EE}\langle\Theta_1| \otimes \rho_D\}.\end{aligned}$$

## 5. KEY LENGTH, UNTRUSTED DETECTORS

According to [10], the length of the secret key in the asymptotic limit of a long sequence (this limit is considered to avoid lengthy technical details; a finite length of transmitted sequence can be taken into account in the way proposed in [7]) is given by the expression

$$\ell \geq H(\rho_{XED}|\rho_{ED}) - H(\rho_{XY}|\rho_Y). \quad (8)$$

Here, $H(\rho_{XED}|\rho_{ED})$ is the lack of information in bits on Alice's reference bit string $X$ to Eve under the condition that Eve has quantum systems $ED$, and $H(\rho_{XY}|\rho_Y)$ is the lack of information on Alice's string to Bob under the condition that Bob has the bit string $Y$ with errors. The difference between the deficits of information of Alice's bit string $X$ to Eve and Bob is the common secret of Alice and Bob.

The corresponding partial density matrices in Eq. (8) have the form

$$\begin{aligned}\rho_{XED} &= \mathrm{Tr}_Y\{\rho_{XYED}\}\\ &= \frac{1}{2}|0\rangle_{XX}\langle 0| \otimes \{(1-Q)|\Phi_0\rangle_{EE}\langle\Phi_0| \otimes \rho_D \\ &+ Q|\Theta_0\rangle_{EE}\langle\Theta_0| \otimes \rho_D\} \quad (9)\\ &+ \frac{1}{2}|1\rangle_{XX}\langle 1| \otimes \{(1-Q)|\Phi_1\rangle_{EE}\langle\Phi_1| \otimes \rho_D \\ &+ Q|\Theta_1\rangle_{EE}\langle\Theta_1| \otimes \rho_D\};\end{aligned}$$

$$\begin{aligned}\rho_{ED} &= \mathrm{Tr}_{XY}\{\rho_{XYED}\}\\ &= \frac{1}{2}\{(1-Q)|\Phi_0\rangle_{EE}\langle\Phi_0| \otimes \rho_D + Q|\Theta_0\rangle_{EE}\langle\Theta_0| \otimes \rho_D\} \quad (10)\\ &+ \frac{1}{2}\{(1-Q)|\Phi_1\rangle_{EE}\langle\Phi_1| \otimes \rho_D + Q|\Theta_1\rangle_{EE}\langle\Theta_1| \otimes \rho_D\}.\end{aligned}$$

Further,

$$\begin{aligned}\rho_{XY} &= \mathrm{Tr}_{ED}\{\rho_{XYED}\}\\ &= \frac{1}{2}|0\rangle_{XX}\langle 0|\{(1-Q)|0\rangle_{YY}\langle 0| + Q|1\rangle_{YY}\langle 1|\} \quad (11)\\ &+ \frac{1}{2}|1\rangle_{XX}\langle 1|\{(1-Q)|1\rangle_{YY}\langle 1| + Q|0\rangle_{YY}\langle 0|\};\end{aligned}$$

$$\rho_Y = \mathrm{Tr}_{XED}\{\rho_{XYED}\}\frac{1}{2}\{|0\rangle_{YY}\langle 0| + |1\rangle_{YY}\langle 1|\}. \quad (12)$$

Calculating the eigenvalues of the matrices (9)–(12), we obtain the following relations for the conditional von Neumann entropies:

$$\begin{aligned}H(\rho_{XED}|\rho_{ED}) &= H(\rho_{XED}) - H(\rho_{ED})\\ &= H(\rho_{XE} \otimes \rho_D) - H(\rho_E \otimes \rho_D)H(\rho_{XE}) - H(\rho_E) \quad (13)\\ &= 1 + h(Q) - 2h(Q) = 1 - h(Q),\end{aligned}$$

$$H(\rho_{XY}|\rho_Y) = H(\rho_{XY}) - H(\rho_Y)h(Q). \quad (14)$$

Finally, taking into account Eqs. (13) and (14), we determine the key length

$$\ell = 1 - 2h(Q). \quad (15)$$

Thus, the length of the secret key in the modified protocol is the same as in the standard BB84 protocol [1, 10]. The critical error at which the key length vanishes is determined from the relation $2h(Q_c) = 1$ as $Q_c \approx 11\%$; i.e., the modification of the protocol does not "destroy" the cryptographic properties of the protocol.

## 6. CONCLUSIONS

An effective solution has been proposed for systems where it is technically difficult to ensure the cryptographic protection of detectors. This solution is reduced to the modification of the protocol such that detectors become untrusted and even counts in them are completely accessible to the observation of the

eavesdropper. The proposed modification does not require any significant changes in the protocol and in the quantum key distribution system. Analogy with the twin-field protocol provides a qualitative information-theory explanation reasons for the security of keys in the case of detectors accessible to the eavesdropper.

Furthermore, the accessibility of detectors ensures natural protection from the detector mismatch attack, making it completely inefficient.

To conclude, this modification is achieved without significant changes in the equipment of the quantum key distribution system and does not reduce the key distribution rate.

## FUNDING

S.P. Kulik acknowledges the support of the Interdisciplinary Scientific Educational School "Photon and Quantum Technologies. Digital Medicine," Moscow State University.

## CONFLICT OF INTEREST

The authors declare that they have no conflicts of interest.

## REFERENCES

1. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec. 9–12, 1984,* p. 175.
2. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).
3. M. Lucamarini, L. M. Yuan, J. F. Dynes, and A. J. Shields, Nature (London, U.K.) **557**, 400 (2018).
4. S. N. Molotkov and I. V. Sinilshchikov, Laser Phys. Lett. **16**, 105205 (2019).
5. S. N. Molotkov, JETP Lett. **66**, 773 (1997).
6. S. N. Molotkov, Laser Phys. Lett. **18**, 045202 (2021).
7. S. N. Molotkov, J. Exp. Theor. Phys. **133**, 272 (2021).
8. K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer, Berlin, 1983).
9. W. F. Stinespring, Proc. Am. Math. Soc. **6**, 211 (1955).
10. R. Renner, PhD Thesis (ETH Zürich, Switzerland, 2005); arXiv: 0512258.

*Translated by R. Tyapaev*