ISSN 0021-3640, JETP Letters, 2024, Vol. 120, No. 1, pp. 20–27. © The Author(s), 2024. This article is an open access publication.
Russian Text © The Author(s), 2024, published in Pis'ma v Zhurnal Eksperimental'noi i Teoreticheskoi Fiziki, 2024, Vol. 120, No. 1, pp. 17–25.

OPTICS
AND LASER PHYSICS

Hong–Ou–Mandel Interference in Quantum Optics, Monogamy of Entanglement, Nonorthogonality, and Untrusted Nodes

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

[a] *Center of Quantum Technologies, Moscow State University, Moscow, 119991 Russia*
[b] *Institute of Solid State Physics, Russian Academy of Sciences, Chernogolovka, Moscow region, 142432 Russia*
**e-mail: sergei.molotkov@gmail.com*

Received June 5, 2024; revised June 6, 2024; accepted June 6, 2024

Quantum key distribution systems with an untrusted intermediate node described by the so-called measurement device independent (MDI) protocol have been actively studied in the last decade. In early works, it was only argued why such a quantum key distribution system ensures the security of distributed keys mentioning that the security proof of the MDI protocol, which was not presented, is similar to that for the basic Bennett–Brassard 84 (BB84) protocol. *For this reason, despite the existing experimental implementations of the MDI quantum key distribution system, physical reasons for the protocol security are still questionable*. Such quantum key distribution systems provide a common key between two network nodes connected through the intermediate untrusted node, which does not require protection of the equipment on it, and an eavesdropper sees the entire operation of the equipment, including the results of the operation of photodetectors. In this work, the MDI protocol has been analyzed. It has been shown that the physical reasons for the protocol security are based on fundamental properties such as the interference of photons from different sources, monogamy of entanglement, and nonorthogonality of states. *A simple and explicit derivation is given showing the equivalence of the MDI and BB84 protocols and physical reasons for the identity of the corresponding expressions for the length of the final key.*

DOI: 10.1134/S0021364024601994

INTRODUCTION

The idea of measurement device independent (MDI) quantum key distribution was proposed in [1], where it was only argued why such a quantum key distribution system ensures the security of distributed keys mentioning that the security proof of the MDI protocol, which was not presented, is similar to that for the basic Bennett–Brassard 84 (BB84) protocol [2–9].

The remarkable quantum optical effect called Hong–Ou–Mandel interference [10] is related to the *distinguishability/indistinguishability of photons under a transformation on a beam splitter.* Another effect called the *monogamy of quantum entanglement* means that *a pair of particles in the entangled state cannot be entangled, i.e., correlated with the third quantum system [11].* The *nonorthogonality* of quantum states plays a fundamental role in quantum cryptography and guarantees the detection of attacks on a quantum communication channel due to fundamental quantum mechanical laws [12].

New protocols have appeared in the last decade in view of the development of quantum key distribution networks [1]. Networks allow key distribution through trusted nodes [13–17], where the operation of the equipment is inaccessible to an eavesdropper. However, quantum theory allows one to distribute keys through untrusted nodes, where the operation of the equipment is inaccessible to an eavesdropper [1], which is not obvious. Such a protocol was proposed in [1], where the detailed analysis of the reasons for its security was not carried out. Formulas presented to analyze the protocol were those previously used for the BB84 quantum key distribution protocol in the point–point configuration [1–9]. Such systems were later implemented experimentally. Nevertheless, doubts and misperception of reasons for guaranteed protocol security still appear. This occurs apparently because the protocol security has not been analyzed to fundamental origins.

In [18], we analyzed the protocol and obtained an exact result involving fundamental entropy uncertainty relations [19–23]. These relations allowed us to avoid the consideration of various attacks on transmitted states; therefore, the exact solution is implicit. Entropy uncertainty relations relate information loss to the perturbation of quantum states and errors on the receiver side. Information leakage through side communication channels often does not perturb information quantum states; consequently, information leakage through side communication channels cannot be

taken into account with entropy uncertainty relations [23]. For this reason, to take into account side information leakage channels in quantum key distribution systems, it is necessary to design explicit eavesdropper attacks on states in the quantum communication channel [24].

Below, we analyze the protocol, demonstrate the explicit physical reasons for the protocol security that are based on the aforementioned fundamental phenomena—Hong–Ou–Mandel interference, monogamy of entanglement, and nonorthogonality of quantum states, and explicitly reduce the key distribution protocol through untrusted nodes to the classical BB84 key distribution protocol in the point–point configuration.

HONG–OU–MANDEL INTERFERENCE FROM TWO SOURCES

Let Alice and Bob have two existing independent sources of single-photon quantum states (see Fig. 1) that generate Fock states with different polarizations $i = h,v$ and $j = h,v$ described by the creation operators a_i^+ and b_j^+. States are subjected to the following transformations.

The transformation on a nonpolarizing beam splitter.

The transformation of the operators has the form

$$a_i^+ \to \frac{1}{\sqrt{2}}(c_i^+ + d_i^+), \quad b_j^+ \to \frac{1}{\sqrt{2}}(c_j^+ - d_j^+). \tag{1}$$

The states in two channels c and d of the beam splitter are transformed as

$$\begin{aligned}|\psi^{\text{out}}\rangle_{CD} &= U_{BS}|\Psi_{\text{in}}\rangle_{ab} = U_{BS}(a_i^+ b_j^+|\text{vac}\rangle_{ab}) \\ &= \frac{1}{2}(c_i^+ c_j^+ + c_j^+ d_i^+ - c_i^+ d_j^+ - d_i^+ d_j^+)|\text{vac}\rangle_{cd}.\end{aligned} \tag{2}$$

The states at the output of the beam splitter BS (*see* Fig. 1) *depend on the polarizations of photons.*

(1) *Photons have different polarizations* $i \neq j$, e.g., $i = h$ and $j = v$; i.e., photons are distinguishable in polarization. In this case, *the common entangled state* at the outputs c and d of the beam splitter has the form

$$\begin{aligned}|\psi^{\text{out}}\rangle_{CD} &= \frac{1}{2}(c_h^+ c_v^+ + c_v^+ d_h^+ - c_h^+ d_v^+ - d_h^+ d_v^+)|\text{vac}\rangle_{cd} \\ &= \frac{1}{2}\left(|h\rangle_c|v\rangle_c + |v\rangle_c|h\rangle_d - |h\rangle_c|v\rangle_d - |h\rangle_d|v\rangle_d\right).\end{aligned} \tag{3}$$

After the passage of states from the channel D (C) through the polarizing beam splitter PBS (see Fig. 1), the polarization components h and v of the states given by Eqs. (1) and (2) were directed to the outputs D_h and D_v (C_h and C_v), respectively.

Thus, in the case of photons with different polarizations, *coincidences of outcomes simultaneously in two detectors occur with the same probability.* The detectors where outcomes coincide at $i \neq j$ are presented in rows 1 and 2 of Table 1. In particular, if $|v\rangle_A$ and $|h\rangle_B$ are the Alice and Bob states, respectively, then outcomes will be in one of the four pairs of detectors C_vC_h, C_vD_h, C_hD_v, and D_hD_v (see Table 1).

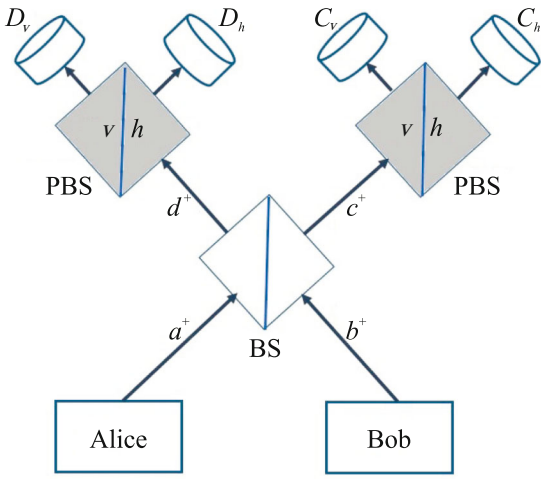

Fig. 1. (Color online) Schematic of the detection of states on the untrusted node: (BS) nonpolarizing symmetric 50/50 beam splitter, (PBS) polarizing beam splitter, and (D_v, D_y, C_v, C_h) detectors.

The same pair outcomes in detectors will occur if the Alice and Bob states are $|h\rangle_A$ and $|v\rangle_B$, respectively. This circumstance is of fundamental importance for the key distribution protocol with the untrusted node. This means that the eavesdropper, knowing outcomes in a pair of detectors, does not know the states sent by Alice and Bob because outcomes from the Alice and Bob states $|h\rangle_A$, $|v\rangle_B$ or $|v\rangle_A$, $|h\rangle_B$ are the same (see below).

(2) *Photons have the same polarizations* $i = j = h$ or $i = j = v$, i.e., indistinguishable photons. The common entangled state at the outputs c and d of the beam splitter will have the form

$$\begin{aligned}|\psi^{\text{out}}\rangle_{CD} &= \frac{1}{2}(c_i^+ c_i^+ + c_i^+ d_i^+ - c_i^+ d_i^+ - d_i^+ d_i^+)|\text{vac}\rangle_{cd} \\ &= \frac{1}{2}\left(|i\rangle_c|i\rangle_c - |i\rangle_d|i\rangle_d\right),\end{aligned} \tag{4}$$

and both photons synchronously enter the channels c and d, which is a manifestation of the indistinguishability of particles characteristic of the Bose–Einstein statistics. This effect is Hong–Ou–Mandel interference [10].

After the passage of states from the channel D through the polarizing beam splitter PBS (see Fig. 1), both identical polarization components h or v of the state given by Eq. (2), i.e., *both photons* with the corresponding polarization h or v were directed to the output D_h or D_v, respectively.

Thus, for photons with identical polarizations, *outcomes from both photons will occur only in one of the*

Table 1. Detectors, where detection depends on the input polarization of Alice and Bob states in the direct and conjugate bases, probabilities of outcomes in different detectors, and the corresponding values of logical bits for different quantum states

N	Alice state	Bob state	Detector outcome	Outcome probability	Alice–Bob bit value
1	$\|v\rangle_A$	$\|h\rangle_B$	$C_vC_h, C_hD_v,\ C_vD_h, D_vD_h$	$\frac{1}{4}4 = 1$	1
2	$\|h\rangle_A$	$\|v\rangle_B$	$C_vC_h, C_hD_v,\ C_vD_h, D_vD_h$	$\frac{1}{4}4 = 1$	0
3	$\|h\rangle_A$	$\|h\rangle_B$	C_hC_h, D_hD_h	$\frac{1}{2}2 = 1$	–
4	$\|v\rangle_A$	$\|v\rangle_B$	C_vC_v, D_vD_v	$\frac{1}{2}2 = 1$	–
5	$\|ad\rangle_A$	$\|ad\rangle_B$	C_hC_v, D_hD_v	$\frac{1}{4}2 = \frac{1}{2}$	0
6	$\|d\rangle_A$	$\|d\rangle_B$	$C_hC_h, C_vC_v, D_hD_h, D_vD_v$	$\frac{1}{4}2 = \frac{1}{2}$	–
7	$\|ad\rangle_A$	$\|d\rangle_B$	C_hD_v, C_vD_h	$\frac{1}{4}2 = \frac{1}{2}$	1
8	$\|d\rangle_A$	$\|ad\rangle_B$	$C_hC_h, C_vC_v, D_hD_h, D_vD_v$	$\frac{1}{4}2 = \frac{1}{2}$	–

detectors; i.e., *no coincidence of outcomes simultaneously in two different detectors will occur* (see rows 3 and 4 in Table 1).

States with the same polarization do not contribute to the key, i.e., are not involved in the quantum key distribution protocol, double counts in one of the detectors are rejected because an outcome in the detector with h and v allows one to reliably determine the states and, correspondingly, logical bits sent by Alice and Bob.

The transformations of states in the direct basis are presented above. In the conjugate basis, the diagonal, d, and antidiagonal, ad, Alice and Bob input states have the form

$$|d\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|h\rangle_{A,B} + |v\rangle_{A,B}\right),$$
$$|ad\rangle_{A,B} = \frac{1}{\sqrt{2}}\left(|h\rangle_{A,B} - |v\rangle_{A,B}\right). \quad (5)$$

The analysis of a transformation of states in the conjugate basis is similar to the analysis in the direct basis. *For subsequent consideration, it is important that outcomes in detectors in the conjugate basis are the same as in the direct one* (see rows 5–8 in Table 1).

TRANSFORMATION OF INFORMATION STATES AND THE MONOGAMY OF PAIR ENTANGLEMENT

Before the consideration of an eavesdropper (Eve) attack on transmitted states, we consider the transformation of states in the absence of Eve. More conventional notation of information states in quantum cryptography is more convenient below. We denote states in the direct + basis as

$$|v\rangle \to |0\rangle, \quad |h\rangle \to |1\rangle, \quad (6)$$

and information states in the conjugate × basis are

$$|d\rangle \to |0^\times\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right),$$
$$|ad\rangle \to |1^\times\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle - |1\rangle\right). \quad (7)$$

We consider outcomes from the transmitted Alice and Bob states in the absence of Eve.

The transmission of states on the untrusted node in the + basis:

states $|0\rangle_A|0\rangle_B$ and $|1\rangle_A|1\rangle_B$ result in pair outcomes only in one detector (4); these outcomes are rejected;

states $|0\rangle_A|1\rangle_B$, $|1\rangle_A|0\rangle_B$ are conveniently represented as $|\Psi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B\right)$, which correspond to coinciding outcomes in the channels (3), i.e., to the *projections on entangled states due to the entanglement of the input states by the beam splitters.*

In the absence of perturbation of states, there are perfect correlations between Alice and Bob bits. Eve's attack on states $|0\rangle_A|1\rangle_B$ or $|1\rangle_A|0\rangle_B$ in the communication channel violates perfect correlations. The most general Eve's attack is reduced to the entanglement of auxiliary Eve state (ancilla) with Alice and Bob states. The monogamy of pair entanglement [11] *guarantees that any entanglement of a pair of states with the third state*

violates the perfect entanglement and, thereby, perfect correlations between Alice and Bob bits, i.e., leads to errors. The pair entanglement at the untrusted node physically guarantees the detection of any attacks on the quantum communication channel. We again emphasize that, even knowing the detectors where outcome occurs, Eve does not receive any information on the transmitted bits without an attack on the communication channel. Indeed, the states $|0\rangle_A|0\rangle_B$ and $|1\rangle_A|1\rangle_B$ give identical outcomes (3). *At the same time, Alice and Bob, knowing outcomes of the detectors and bits they sent, can reliably determine the bit sent by a partner and attach to one of the bits, e.g., Alice bit.*

The state $|0^\times\rangle_A|0^\times\rangle_B = \frac{1}{2}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B + |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{AB} + |\Psi^+\rangle_{AB})$ gives outcomes in the channel $|\Psi^+\rangle_{AB}$.

The state $|1^\times\rangle_A|1^\times\rangle_B = \frac{1}{2}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B - |0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}(|\Phi^+\rangle_{AB} - |\Psi^+\rangle_{AB})$ provides outcomes in the channel $|\Psi^+\rangle_{AB}$.

The transmission of states to the untrusted node in the conjugate × basis.

The states in the × basis can also be represented as superpositions of a pair of entangle states $|\Phi^\pm\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B)$.

The states $|0^\times\rangle_A|1^\times\rangle_B = \frac{1}{2}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B - |0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{AB} - |\Psi^-\rangle_{AB})$ in the channel $|\Phi^+\rangle_{AB}$ give outcomes only in one detector (4); such outcomes are rejected. These states in the channel $|\Psi^+\rangle_{AB}$ provide outcomes by coincidence of two detectors (3).

The states $|1^\times\rangle_A|0^\times\rangle_B = \frac{1}{2}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B + |0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B) = \frac{1}{\sqrt{2}}(|\Phi^-\rangle_{AB} + |\Psi^-\rangle_{AB})$ give outcomes similar to the states $|0^\times\rangle_A|1^\times\rangle_B$. Similar to the + basis, access to outcomes in two detectors in the coincidence scheme (3) in the × basis without an attack on the quantum channel provides to Eve no information on bits transmitted by Alice and Bob because the states $|0^\times\rangle_A|1^\times\rangle_B$ and $|1^\times\rangle_A|0^\times\rangle_B$ give the same outcomes.

COORDINATION OF THE ALICE AND BOB BITS

Let the common bit be attached to the Alice bit.

The + basis.

The states $|0\rangle_A|0\rangle_B$ sent in the + basis give no outcomes in the detectors in the absence of Eve's attack on the quantum channel. An attack on the communication channel results in outcomes in two detectors in the channels $|\Psi^\pm\rangle_{AB}$. In this case, such outcomes are erroneous. If an outcome occurs, Bob inverts his bit $0 \to 1$. As a result, Alice has the 0 bit and Bob has erroneous the 1 bit. The transmission of the states $|1\rangle_A|1\rangle_B$ in the + basis provides a similar result.

In other words, an outcome in the channels $|\Psi^\pm\rangle_{AB}$ *will be erroneous when the states* $|1\rangle_A|1\rangle_B$ or $|0\rangle_A|0\rangle_B$ are transmitted. Known this, the eavesdropper has no reason to introduce errors to messages where Alice and Bob send the states $|1\rangle_A|1\rangle_B$ or $|0\rangle_A|0\rangle_B$. Performing nondemolition measurements (see below), Eve can identify messages where Alice and Bob send identical states. Detecting the states $|1\rangle_A|1\rangle_B$ or $|0\rangle_A|0\rangle_B$ in the channel, Eve resends them to on the untrusted node, states give outcomes only in one of the detectors, which are rejected and are not involved in the formation of the key. Informally speaking, Eve acts "transparently" on states in such messages.

The states $|0\rangle_A|1\rangle_B$ or $|1\rangle_A|0\rangle_B$ sent in the + basis in the absence of the eavesdropper will yield outcomes in two detectors equiprobably in both the channels $|\Psi^-\rangle_{AB}$ and $|\Psi^+\rangle_{AB}$. when outcomes occur in two detectors, Bob inverts his bit $0 \to 1$. As a result, Alice in this session has the 0 bit, and Bob obtains the correct 0 bit, which is similar to the transmission of the states $|1\rangle_A|1\rangle_B$ in the + basis.

Thus, Alice and Bob bits are coordinated to obtain a common bit in the + basis.

The × basis.

The states $|0^\times\rangle_A|0^\times\rangle_B$ sent in the × basis in the absence of the eavesdropper will yield correct outcomes in detectors only in the channel $|\Psi^+\rangle_{AB}$. In this case, both Alice and Bob have the 0 bit. *Bob should not invert his bit in the case of the outcome in the channel* $|\Psi^+\rangle_{AB}$. The situation with the transmission of the states $|1^\times\rangle_A|1^\times\rangle_B$ in the × basis is similar.

The states $|0^\times\rangle_A|1^\times\rangle_B$ sent in the × basis in the absence of the eavesdropper will yield correct outcomes in detectors only in the channel $|\Psi^-\rangle_{AB}$. Alice has the 0 bit, and Bob after inversion has the 1 bit. *Bob inverts his bit at the outcome in the channel* $|\Psi^-\rangle_{AB}$ *and does not invert it at the outcome in the channel* $|\Psi^+\rangle_{AB}$.

The situation with the transmission of the states $|1^\times\rangle_A|0^\times\rangle_B$ in the × basis is similar.

Attacks on the communication channel lead to outcomes in the channel $|\Psi^+\rangle_{AB}$, which are erroneous.

Thus, Alice and Bob bits are coordinated to obtain a common bit in the × basis.

STRATEGY OF AN EAVESDROPPER ATTACK ON TRANSMITTED STATES

Before the final proof of the equivalence of the MDI and BB84 protocols, we discuss the strategy of an attack on quantum states in the communication channel. *We recall that outcomes of the detectors on the untrusted node accessible for Eve give no information to her on transmitted Alice and Bob bits without attacks on the quantum communication channel* (see discussion above).

Since measurements implement only projections on the states $|\Psi^{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B)$ of coinciding outcomes in two detectors, while double outcomes only in one detector, which are described by the projections on the states $|\Phi^{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B \pm |1\rangle_A|1\rangle_B)$, are rejected, Eve *can preliminarily project transmitted states on entangled states, i.e., perform non-demolition measurement of the state of a pair of photons.*

We describe this procedure in more detail.

Let Alice and Bob send the states $|0\rangle_A|0\rangle_B$ or $|1\rangle_A|1\rangle_B$ in the + basis. These states do not give outcomes because the measurements are reduced to the projections on the states $|\Psi^{\pm}\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B \pm |1\rangle_A|0\rangle_B)$ that do not include the states $|0\rangle_A|0\rangle_B$ or $|1\rangle_A|1\rangle_B$.

Outcomes will occur only when Alice and Bob send the states $|0\rangle_A|1\rangle_B$ or $|1\rangle_A|0\rangle_B$ in the + basis.

For this reason, if the eavesdropper performs *preliminary non-demolition measurements*, which are specified by the decomposition of unity $I_{AB} = \mathcal{P}_{\Phi^+} + \mathcal{P}_{\Phi^-} + \mathcal{P}_{\Psi^+} + \mathcal{P}_{\Psi^-}$ and have two outcomes corresponding to the projection on $\mathcal{P}_{\Phi^{\pm}} = |\Phi^{\pm}\rangle_{ABAB}\langle\Phi^{\pm}|$ and $\mathcal{P}_{\Psi^{\pm}} = |\Psi^{\pm}\rangle_{ABAB}\langle\Psi^{\pm}|$.

Such measurements are in essence non-demolition measurements that do not perturb transmitted Alice and Bob states.

If an outcome occurs in the channel $\mathcal{P}_{\Phi^{\pm}}$, the eavesdropper sends one of the states $|\Phi^{\pm}\rangle_{AB}$ that do not yield erroneous outcomes. Such resending of states is *transparent, Alice and Bob states* (00 *or* 11) *are unknown to Eve but they will give an outcome in only one detector and will be rejected.*

If an outcome occurs in the channel $\mathcal{P}_{\Psi^{\pm}}$, Eve also does not know Alice and Bob states (01 or 10), and the measurement itself does not perturb them.

Since non-demolition measurements and outcomes in detectors after these measurements provide Eve with no information on the transmitted states, to obtain information on the transmitted states, Eve should perform measurements that will perturb states, i.e., make an unitary attack (see below).

We now discuss that occurs when states in the × basis are sent to the channel. It is important to note that preliminary Eve measurements with projection on entangled states are non-demolition measurements in terms of outcomes in the detectors in any basis.

If an outcome occurs in the channel $\mathcal{P}_{\Psi^{\pm}}$, Eve sends one of the states $|\Psi^{\pm}\rangle$, knowing that these could be the states

$$|0\rangle_A|1\rangle_B, \text{ or } |1\rangle_A|0\rangle_B, \text{ or } |0^{\times}\rangle_A|1^{\times}\rangle_B, \quad (8)$$

$$\text{or } |1^{\times}\rangle_A|0^{\times}\rangle_B, \text{ or } |0^{\times}\rangle_A|0^{\times}\rangle_B, \text{ or } |1^{\times}\rangle_A|1^{\times}\rangle_B.$$

If the outcome occurs in the channel $\mathcal{P}_{\Phi^{\pm}}$, Eve sends one of the states $|\Phi^{\pm}\rangle$, knowing that these could be the states

$$|0\rangle_A|0\rangle_B, \text{ or } |1\rangle_A|1\rangle_B, \text{ or } |0^{\times}\rangle_A|1^{\times}\rangle_B, \quad (9)$$

$$\text{or } |1^{\times}\rangle_A|0^{\times}\rangle_B, \text{ or } |0^{\times}\rangle_A|0^{\times}\rangle_B, \text{ or } |1^{\times}\rangle_A|1^{\times}\rangle_B.$$

Preliminary Eve measurements are non-demolition measurements and provide no information on transmitted bits but allow Eve to decide whether or not it is necessary to make an attack already with the perturbation of states. If the outcome occurs in the channel $\mathcal{P}_{\Phi^{\pm}}$, Eve only resends the states. If the outcome occurs in the channel $\mathcal{P}_{\Psi^{\pm}}$, Eve makes an attack on states in order to determine the transmitted bit.

EQUIVALENCE OF THE MEASUREMENT DEVICE INDEPENDENT AND BB84 PROTOCOLS

We are now ready to prove the formal equivalence of the MDI and BB84 protocols. In contrast to the previous indirect proof of the equivalence of the protocols [18], which is based on fundamental entropy uncertainty relations [19–23], the proof below involves the direct construction, which will allow one to further include side information leakage channels requiring the knowledge of the explicit Eve attack (see, e.g., [24]).

After projection, the states are as follows.

States in the + basis in the communication channel:

$|\bar{0}\rangle_{AB} = |01\rangle_{AB}$ logic 0 bit,

$|\bar{1}\rangle_{AB} = |10\rangle_{AB}$ logic 1 bit.

The states $|\bar{0}\rangle_{AB}$ and $|\bar{1}\rangle_{AB}$ *inside the basis are orthogonal to each other* and provides the outcome in the channel $|\Psi^{\pm}\rangle_{AB}$.

Table 2. Information states for the BB84 and MDI protocols

BB84 protocol	MDI protocol
+ basis, $\|0\rangle, \|1\rangle$	+ basis, $\bar{\bar{0}}\rangle_{AB}, \bar{\bar{1}}\rangle_{AB}$
× basis, $\|0^{\times}\rangle = \frac{\|0\rangle + \|1\rangle}{\sqrt{2}}, \|1^{\times}\rangle = \frac{\|0\rangle - \|1\rangle}{\sqrt{2}}$	× basis, $\bar{\bar{0^{\times}}}\rangle_{AB} = \frac{\bar{\bar{0}}\rangle_{AB} + \bar{\bar{1}}\rangle_{AB}}{\sqrt{2}}, \bar{\bar{1^{\times}}}\rangle = \frac{\bar{\bar{0}}\rangle_{AB} - \bar{\bar{1}}\rangle_{AB}}{\sqrt{2}}$

Bob inverts his bit at the outcome in both channels $|\Psi^{+}\rangle_{AB}$ and $|\Psi^{-}\rangle_{AB}$. As a result, the common bit is obtained. We recall that attachment is made to the Alice bit.

States in the × basis in the communication channel:

The logic 0 bit appears from the states $|0^{\times}\rangle_A|0^{\times}\rangle_B$, and the states in the channel that are seen by the eavesdropper are

$$|0^{\times}\rangle_A|0^{\times}\rangle_B \to \bar{\bar{0}}\rangle_{AB} = \frac{1}{\sqrt{2}}(\bar{0}\rangle_{AB} + \bar{1}\rangle_{AB}) = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB});$$

the logic 1 bit appears from the states $|1^{\times}\rangle_A|1^{\times}\rangle_B$,, and the states in the channel that are seen by the eavesdropper are

$$|1^{\times}\rangle_A|1^{\times}\rangle_B \to \bar{\bar{0}}\rangle_{AB} = \frac{1}{\sqrt{2}}(\bar{0}\rangle_{AB} + \bar{1}\rangle_{AB}) = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}).$$

This circumstance guarantees the security of keys in the MDI protocol even if Eve sees outcomes in detectors. Alice and Bob obtain their common 0 or 1 bit from the same states, which Eve "sees" in the communication channel. States for the logic 0 and 1 bits in the communication channel are indistinguishable to Eve.

If the outcome occurs in the channel $|\Psi^{+}\rangle_{AB}$, Bob does not invert his bit; as a result, the common bit attached to the Alice bit appears.

The states for the 0 and 1 bits in the communication channel look identically to the eavesdropper; consequently, knowing the outcome on the untrusted node, the eavesdropper does not know the transmitted bit unlike Alice and Bob knowing their sent states.

The logic 0 bit also appears from the states $|0^{\times}\rangle_A|1^{\times}\rangle_B$, and the states in the channel that are seen by the eavesdropper are

$$|0^{\times}\rangle_A|1^{\times}\rangle_B \to \bar{\bar{1}}\rangle_{AB} = \frac{1}{\sqrt{2}}\left(\bar{0}\rangle_{AB} - \bar{1}\rangle_{AB}\right) = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right).$$

The logic 1 bit also appears from the states $|1^{\times}\rangle_A|0^{\times}\rangle_B$, and the states in the channel that are seen by the eavesdropper are

$$|1^{\times}\rangle_A|0^{\times}\rangle_B \to \bar{\bar{1}}\rangle_{AB} = \frac{1}{\sqrt{2}}(\bar{0}\rangle_{AB} - \bar{1}\rangle_{AB}) = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}).$$

The states for the 0 and 1 bits are indistinguishable to Eve; i.e., the situation is similar to the case considered above.

If the outcome occurs in the channel $|\Psi^{-}\rangle_{AB}$, Bob inverts his bit; as a result, the common bit attached to the Alice bit appears.

In fact, the eavesdropper sees that Alice and Bob send equiprobably one of four states: $\bar{0^{+}}\rangle_{AB}$ and $\bar{1^{+}}\rangle_{AB}$ in the + basis and $\bar{\bar{0^{\times}}}\rangle_{AB}$ $\bar{\bar{1^{\times}}}\rangle_{AB}$ is the × basis.

The states $\bar{0^{+}}\rangle_{AB}$ and $\bar{1^{+}}\rangle_{AB}$ are orthogonal inside the + basis, and the states $\bar{\bar{0^{\times}}}\rangle_{AB}$ and $\bar{\bar{1^{\times}}}\rangle_{AB}$ are orthogonal inside *the × basis. The states from different bases are pairwise nonorthogonal in the total analogy with the* BB84 *protocol.*

The states for the MDI and BB84 protocols are summarized in Table 2.

Thus, the MDI and BB84 protocols are formally bijective; consequently, the results for the BB84 protocol can be used to explicitly construct an attack on the MDI protocol.

Any transformation of quantum states in quantum states is described by a superoperator, i.e., a completely positive map [25, 26]. Any superoperator is unitarily representable, i.e., can be implemented as an initial state with an ancilla and an entangling transformation, which *is specified by an unitary operator implementing a unitary attack.*

Since *after preliminary non-demolition measurements* the BB84 and MDI protocols are equivalent with a changed notation for the information states (see Table 2), the explicit attack on the MDI protocol can be constructed using the results for the BB84 protocol [8]. Let Alice and Bob have reference states (marked below by the subscript $A'B'$), which they retain, and their copies (marked below by the subscript AB) are sent through the communication channel to the

untrusted node. For states in the + basis, we obtain (see details in [8, 9])

$$\begin{aligned}&|\bar{0}\rangle_{A'B'}U_{ABE}(|\bar{0}\rangle_{AB}|E\rangle)\\&=|\bar{0}\rangle_{A'B'}\left\{\sqrt{1-Q}|\bar{0}\rangle_{AB}|\Phi_0\rangle+\sqrt{Q}|\bar{1}\rangle_{AB}|\Theta_0\rangle\right\},\end{aligned}\tag{10}$$

$$\begin{aligned}&|\bar{1}\rangle_{A'B'}U_{ABE}\left(|\bar{1}\rangle_{AB}|E\rangle\right)\\&=|\bar{1}\rangle_{A'B'}\left\{\sqrt{1-Q}|\bar{1}\rangle_{AB}|\Phi_1\rangle+\sqrt{Q}|\bar{0}\rangle_{AB}|\Theta_1\rangle\right\},\end{aligned}\tag{11}$$

where Q is the probability error between the Alice and Bob bits.

States in the conjugate × basis are obtained by the linear combination of Eqs. (6) and (7) (see also Table 2).

Here, in order to avoid mistakes, a fundamental comment is necessary. Although the BB84 and MDI protocols are formally equivalent, they have difference. After the Eve attack and the measurements on the receiver side in the BB84 protocol, the states $|0,1\rangle_B$ sent from Alice to Bob are accessible to Bob and are inaccessible to Eve.

We also suggest that the $|\bar{0}\rangle_{AB}$ and $|\bar{1}\rangle_{AB}$ on the right-hand sides of Eqs. (10) and (11) after the measurements on the untrusted node are inaccessible to Eve although Eve knows the outcomes in the detectors. This seems contradictory because measurements in the MDI protocol are conducted on the untrusted node and are known to Eve, in contrast to the BB84 protocol.

However, any contradictory is absent because, as discussed in detail above, the knowledge of the outcome in the channel $|\Psi^{\pm}\rangle$ provides Eve with no information on the transmitted pair (0, 1) or (1,0) of the Alice and Bob bits. Eve can obtain information on the transmitted bits only from her ancilla states $|\Phi_{0,1}\rangle$ and $|\Theta_{0,1}\rangle$. For this reason, as in the BB84 protocol, the states $|\overline{0,1}\rangle_{AB}$ should be treated as inaccessible to Eve. *In fact, this occurs because the logic 0 and 1 bits in each basis are associated with the same quantum state, which is seen to Eve in the communication channel* (see discussion above).

This circumstance can be clarified in terms of information theory. In the known basis, Alice and Bob each sends one 0 or 1 information bit. As a result, two information bits appear in the communication channel and on the untrusted node from Alice and Bob. From measurements on the untrusted node, Eve obtains one information bit; in fact, it is the parity bit of transmitted Alice and Bob bits because the outcomes from the states for the $(0_A,1_B)$ and $(1_A,0_B)$ bits are seen to Eve as the same. The knowledge of the outcome gives one information bit to Eve. One bit remains unknown to Eve; informally speaking, this bit is used to form the common secrete Alice and Bob bit attached to the Alice bit.

The density matrix in the + basis after the measurements on the untrusted node takes the form

$$\begin{aligned}\rho_{A'B'ABE}=&\frac{1}{2}|\bar{0}\rangle_{A'B'A'B'}\langle\bar{0}|\{(1-Q)|\bar{0}\rangle_{ABAB}\langle\bar{0}||\Phi_0\rangle\langle\Phi_0|\\&+Q|\bar{1}\rangle_{ABAB}\langle\bar{1}||\Theta_0\rangle\langle\Theta_0|\}\\&+\frac{1}{2}|\bar{1}\rangle_{A'B'A'B'}\langle\bar{1}|\{(1-Q)|\bar{1}\rangle_{ABAB}\langle\bar{1}||\Phi_1\rangle\langle\Phi_1|\\&+Q|\bar{0}\rangle_{ABAB}\langle\bar{0}||\Theta_1\rangle\langle\Theta_1|\}.\end{aligned}\tag{12}$$

The key length is determined in terms of conditional quantum von Neumann entropies, which are expressed in terms of partial density matrices. For the key length ℓ in the asymptotic limit of long sequences, similar to the BB84 protocol, we obtain (see details in, e.g., [8, 9])

$$\begin{aligned}\ell&=H(\rho_{A'B'E}\,|\,\rho_E)-H(\rho_{A'B'AB}\,|\,\rho_{AB}),\\H(\rho_{A'B'E}\,|\,\rho_E)&=H(\rho_{A'B'E})-H(\rho_E),\\H(\rho_{A'B'AB}\,|\,\rho_{AB})&=H(\rho_{A'B'AB})-H(\rho_{AB}).\end{aligned}\tag{13}$$

Partial density matrices have the form

$$\rho_{A'B'E}=\mathrm{Tr}_{AB}\{\rho_{A'B'ABE}\},\quad \rho_E=\mathrm{Tr}_{A'B}\{\rho_{A'B'E}\},$$

$$\rho_{A'B'AB}=\mathrm{Tr}_{E}\{\rho_{A'B'ABE}\},\quad \rho_{AB}=\mathrm{Tr}_{A'B'E}\{\rho_{A'B'ABE}\}.$$

Further, for brevity, we assume that the detectors on the untrusted node have the same quantum efficiency. The solution can be generalized for the detectors with different quantum efficiencies, e.g., using the method from [24, 27]; the corresponding generalization is lengthy. At the same quantum efficiencies of the detectors, the optimal attack providing the maximum information leakage to Eve at a given error probability Q is reached at [5, 8]

$$\begin{aligned}\langle\Phi_0\,|\,\Phi_1\rangle&=1-2Q,\\\langle\Theta_0\,|\,\Theta_1\rangle&=1-2Q,\quad \langle\Phi_{0,1}\,|\,\Theta_{0,1}\rangle=0;\end{aligned}\tag{14}$$

i.e., the states $|\Phi_{0,1}\rangle$ and $|\Theta_{0,1}\rangle$ lie in orthogonal subspaces.

Formulas (10)–(14) applied to calculate the key length per message leads to the famous formula

$$\begin{aligned}&\ell(1-h(Q))-h(Q),\\&h(Q)=-Q\log_2(Q)-(1-Q)\log_2(1-Q),\end{aligned}\tag{15}$$

for the key length in the BB84 protocol, which was obtained in several works using different methods (see [5–9]). Here, the first and second terms are Eve and Bob missing information on the Alice key bit, respectively.

CONCLUSIONS

To summarize, despite the significantly different structures of the MDI and BB84 protocols, we have explicitly demonstrated the formal equivalence of the MDI and BB84 protocols, and have discussed in detail

physical reasons for the identity of the corresponding expressions for the length of the final key.

To conclude, we note that one of the main inspirations for the MDI protocol is that the protection of the detectors from external attacks on the communication channel, which can change their normal operation, is not necessary in the case of an untrusted node and untrusted detectors and outcomes of detectors accessible to the eavesdropper. Besides the MDI protocol [1], there is a simpler method to implement untrusted detectors open for the eavesdropper [28] without complex experimental methods to ensure interference from different sources.

Finally, the MDI protocol involves only linear optical elements at the untrusted node. It is known that linear optics allows projections only on a pair of Bell states; such incomplete Bell measurements are also used in quantum teleportation [29]. Complete Bell measurements require nonlinear optical elements, which was implemented for the first time in teleportation experiments in [30].

ACKNOWLEDGMENTS

We are grateful to I.M. Arbekov, V.L. Eliseev, and A.V. Urivskii for interest in this work, discussions, and remarks, and to colleagues from the Academy of Cryptography of the Russian Federation and staff of the InfoTex and SFB Laboratories, who in fact initiated this work to support experimental studies.

FUNDING

This work was supported by ongoing institutional funding. No additional grants to carry out or direct this particular research were obtained.

CONFLICT OF INTEREST

The authors of this work declare that they have no conflicts of interest.

OPEN ACCESS

REFERENCES

1. H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
2. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (1984), p. 175.
3. D. Mayers, J. ACM **48**, 351 (2001).
4. H.-K. Lo and H. F. Chau, Science (Washington, DC, U. S.) **283**, 2050 (1999).
5. P. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
6. R. Renner, arXiv/quant-ph: 0512258 (2005).
7. M. Tomamichel, Ch. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 1 (2012).
8. S. N. Molotkov and A. V. Timofeev, JETP Lett. **85**, 524 (2007).
9. S. N. Molotkov, Laser Phys. Lett. **16**, 075203 (2019).
10. C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987).
11. M. Koashi and A. Winter, Phys. Rev. A **69**, 022309 (2004).
12. C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
13. D. D. Sukachev, Phys. Usp. **64**, 1021 (2021).
14. I. M. Arbekov and S. N. Molotkov, Mat. Vopr. Kripogr. **14** (3), 9 (2023).
15. S. N. Molotkov, JETP Lett. **117**, 476 (2023).
16. Q. Zhang, F. Xu, Y.-A. Chen, C.-Zh. Peng, and J. Pan, Opt. Express **26**, 24260 (2018).
17. https://www.youtube.com/watch?v=0WAuDcYhKbo
18. S. P. Kulik and S. N. Molotkov, JETP Lett. **118**, 74 (2023).
19. D. Deutsch, Phys. Rev. Lett. **50**, 631 (1983).
20. H. Maassen and J. B. M. Uffink, Phys. Rev. Lett. **60**, 1103 (1988).
21. M. Tomamichel and R. Renner, Phys. Rev. Lett. **106**, 110506 (2011).
22. M. Tomamichel, PhD Thesis (ETH, Zürich, 2012); arXiv/quant-ph: 1203.2142.
23. P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, Rev. Mod. Phys. **89**, 015002 (20017).
24. S. N. Molotkov, J. Exp. Theor. Phys. **133**, 272 (2021).
25. K. Kraus, *States, Effects and Operations: Fundamental Notions of Quantum Theory* (Springer, Berlin, 1983).
26. A. S. Holevo, *Quantum Systems, Channels, Information* (MTsNMO, Moscow, 2010; De Gryuter, Berlin, 2013).
27. S. N. Molotkov, Laser Phys. Lett. **18**, 045202 (2021).
28. K. A. Balygin, S. P. Kulik, and S. N. Molotkov, JETP Lett. **116**, 128 (2022).
29. D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, Nature (London, U.K.) **390**, 575 (1997).
30. Y.-H. Kim, S. P. Kulik, and Y. Shih, Phys. Rev. Lett. **86**, 1370 (2001).