NANOSYSTEMS:
PHYSICS, CHEMISTRY, MATHEMATICS

Goncharov R., et al. *Nanosystems: Phys. Chem. Math.*, 2022, **13** (3), 290–298.
http://nanojournal.ifmo.ru
DOI 10.17586/2220-8054-2022-13-3-290-298

Original article

Overview of device-independent continuous-variable quantum key distribution

Roman Goncharov[a], Egor Bolychev, Irina Vorontsova, Eduard Samsonov, Vladimir Egorov

ITMO University, St. Petersburg, 197101, Russia

[a]rkgoncharov@itmo.ru

Corresponding author: R. Goncharov, rkgoncharov@itmo.ru

PACS 03.67.-a, 42.50.-p

ABSTRACT The objects of study of this paper are quantum key distribution (QKD) protocols and systems, in particular, continuous variable (CV) ones with untrusted devices (measurement devices or light sources). The present work is devoted to the consideration of such systems, namely, device-indepentent CV-QKD, and to the discussion of their performance.

KEYWORDS device-independent, quantum key distribution, continuous variables.

ACKNOWLEDGEMENTS The work was done by Leading Research Center “National Center for Quantum Internet” of ITMO University by order of JSCo Russian Railways.

FOR CITATION Goncharov R., Bolychev E., Vorontsova I., Samsonov E., Egorov V. Overview of device-independent continuous-variable quantum key distribution. *Nanosystems: Phys. Chem. Math.*, 2022, **13** (3), 290–298.

1. Introduction

Nowadays, the secure exchange of information plays an increasingly important role. Modern developments in the field of quantum communications help to solve a large number of relevant problems. One of them, quantum key distribution (QKD) [1], is a key transfer method that uses quantum phenomena to guarantee secure stable communication. This technology allows two parties connected via an open classical authenticated and imitated communication channel to create a common random key known only to them and use it to encrypt and decrypt messages transmitted over the classical channel.

Currently, there are a huge number of works (see, for example, [2–4]) devoted to QKD protocols, each of them has its own advantages, disadvantages, and a certain area of application. In a typical QKD protocol, two users, Alice (sender) and Bob (receiver), share a quantum channel to transmit information, and it is always assumed that this channel is being attacked by a third party, in other words, the eavesdropper (Eve) is trying to access the encoded quantum information. But her intervention creates various kinds of disturbances in the system, which leads to additional noise. Legitimate parties, in turn, can quantify the noise (parameter estimation) introduced by Eve, carry out error correction and security amplification procedures to minimize information potentially available to the intruder. They can then use the resulting key in symmetric encryption protocols, such as the one-time pad. The fundamental mechanism of QKD operation is clearly preserved in more complex communication configurations.

The most modern QKD systems are based on the point-to-point principle and the assumption of trust between sender and receiver nodes. The latter circumstance opens up the possibility for an intruder to carry out certain attacks on equipment [5] and, as a result, to extract information not only through a quantum channel. There are a number of countermeasures against such attacks, but the most effective way to get rid of them is to develop and implement new schemes based on the presence of untrusted equipment in the system. The present work is devoted to the consideration of such systems.

Several approaches can be distinguished against attacks on legitimate users’ equipment. The first approach to solving the problem involves using a measurement-device-independent (MDI) protocol [6] and lies in the fact that the measuring node is available to Eve. In addition, she has information about which detectors clicked and at what time frame, but does not know which quantum state was used in the sender and receiver blocks. The latter is implemented due to the interference of weak coherent pulses on the beam splitter inside the untrusted registration node. At the post-selection stage, legitimate users identify the result of single-photon interference that led to the trigger and the corresponding states that were used. This approach is very difficult to implement in practice and is almost never used in conditions close to real.

Twin-Field (TF) protocol [7] can be considered a development of the MDI approach using phase encoded states with the announcement by the measuring node (available to Eve) of the result of the interference of coherent states on the beam splitter, leading to the operation of single photon detectors. In the TF protocol, in contrast to MDI, to minimize the phase correlation of the pulse train from each of the sources, the result of the interference of coherent states is used

with the definition of sectors on the phase plane and the rejection of phase states corresponding to different sectors in the post-processing, while the MDI protocol implies their randomization, that is, changing the phase in a random way.

The concept of the MDI protocol can be implemented on the base of CV-QKD. This version of the MDI protocol allows the parties to recover each other's variables based on the knowledge of the parameter relating the coherent states of the sender and receiver via detectable quadratures, which is open, so that they can locally rebuild the sender-receiver covariance matrix without disclosing any information.

Among the independent approaches, one can also single out the source-device-independent (SDI) one, where it is assumed that there is not a detector, but a light source on an untrusted node, which distributes the signal over several quantum channels to legitimate parties.

The paper is organized as follows. In the Section 2, we briefly describe CV-QKD protocols. In Section 3, we review the concept of MDI CV-QKD and discuss the results of numerical investigations. In section 4, we review an alternative approach to implementing a DI CV-QKD scheme with an untrusted source in a relay. In section 5 we present conclusions and discuss the prospects of the described technologies.

2. CV-QKD

For the first time QKD was presented with single photons as information carriers, sometimes called discrete variable QKD (DV-QKD). In such protocols, the quantum state is encoded by the polarization, phase, or time interval in finite degrees of freedom of the transmitted qubits, and Bob receives the secret key after detecting individual photons via single-photon detector.

The first of the QKD protocols, BB84, was proposed by Bennett and Brassard in 1984 [8]. This protocol was based on the use of two mutually unbiased photon polarization states.

Fifteen years after the first DV-QKD protocol, CV-QKD was considered as a promising alternative the hallmark of which is the ease of implementation and better compatibility with modern telecommunication systems, as the usage of compact balanced receivers instead of large single-photon ones.

First proposed with discrete [9] and Gaussian [10] encoding of squeezed states, this concept was soon developed further by CV-QKD with coherent states [11]. CV-QKD with Gaussian modulation (GG02) of coherent states is currently considered to be the most successfully implemented in practice [3, 11, 12].

The advantage of the coherent-state protocols over the squeezed-state ones lies mainly in the absence of the need to generate squeezed light (which is quite technically difficult). A comprehensive theoretical overviews of the CV-QKD are presented in [1, 13, 14]. To date, a lot of papers have been written on the experimental applications of CV-QKD, and they emphasize the possibility of practical implementation of exactly with coherent states.

Of course, the experimental results should be considered in the context of various assumptions. In the end, the CV-QKD setup is primarily evaluated by secure key rate that can be achieved at a given channel losses. The security, however, largely depends on the capabilities of a potential eavesdropper, the effectiveness of reconciliation, accounting for finite key effects, the classification of the so-called trusted noise, the security of a given modulation alphabet, etc. Moreover, different experimental demonstrations show different vulnerabilities to side-channel attacks.

For example, several papers have successfully demonstrated the CV-QKD at large distances with a non-zero key rate for a channel length of 80–100 km [15] and 200 km [16]. The presence of security assumptions is disclosed by the authors in part.

It should be noted that unconditional security of the discrete modulation protocols of CV-QKD against general (coherent) attacks is considered only in the case of infinite or close to infinite keys [17, 18]. However, the papers devoted to the CV-QKD GG02 offer a proof that gives non-zero secret key rates even for practical block sizes [19–23].

3. MDI CV-QKD

Despite theoretically provable security of QKD protocols, it is still a problem [24] to achieve it in real devices. In fact, before any security proof can be applied to practical scenarios, the various disadvantages of the devices used must be carefully examined. For example, a mismatch in the efficiency of a detector which can be used by Eve to implement an eponymous attack [25] or attacks with a time shift [26].

More recently, other flaws such as detector post-gate pulses and dead time have also been exploited in quantum hacking strategies. Although certain countermeasures have been proposed in each case, in order to completely eliminate such attacks, it is necessary to deal with the problem at the root. Referring to recent advances in the field of MDI QKD, alternative practical schemes have been proposed that are resistant to loopholes in detection, thus protecting against all the above-mentioned attacks in QKD systems [4, 27].

Security gaps in QKD systems essentially stem from existing problems in Bell's inequalities. There are three main loopholes corresponding to the three assumptions:

- a locality loophole that involves the assumption that two communicating parties are separated in a space,
- an efficiency loophole, which is related to the assumption of sample fairness,
- a loophole of randomness, which is related to the assumption that the bases of the dimension are chosen randomly.

In the context of the QKD, some of these loopholes have been more damaging than others. For example, it is reasonable to assume that the information in the two sides of the QKD, Alice and Bob, is protected from Eve. Thus, the locality loophole does not necessarily lead to hacking strategies. Given the recent developments in quantum random number generators, the randomness loophole may not pose a problem either. However, the efficiency loophole opens up many opportunities for quantum attacks. In fact, all of the aforementioned attacks fall into this category.

One of the approaches to overcome the drawbacks of the devices used is the applying of DI QKD schemes. Unfortunately, such schemes impose serious restrictions on the physical devices used. For example, the allowable quantum bit error rate (QBER) is 7.1%, and the minimum required transmittance is 92.4%, which makes the experimental demonstration an extremely difficult task. In order to reduce the above limitations, several QKD schemes with softer restrictions have been proposed, i.e. MDI QKD schemes.

3.1. Common MDI QKD protocol

This section discusses the MDI QKD scheme with phase coding [28]. The key component of the scheme is a partial Bell state measurement (BSM) module, implemented using 50/50 beam splitters and single-photon detectors, which we will hereafter refer to as a "relay" (Charlie). It is assumed that Alice and Bob are using improved single photon sources. Fig. 1 illustrates how the scheme works. The MDI QKD coding scheme works as follows. Both Alice and Bob prepare the single photon state and pass them through 50:50 beam splitters. The two resulting modes are called the reference and signal modes, denoted respectively by $\mathrm{a_r}$ and $\mathrm{a_s}$ on Alice's side and $\mathrm{b_r}$ and $\mathrm{b_s}$ on Bob's side.

To generate the four states of the BB84 protocol, the phase modulators respectively introduce relative phase shifts θ_a and θ_b between the reference and signal modes of Alice and Bob. To comply with the BB84 protocol, Alice and Bob randomly select θ_a and θ_b from two basis sets $\{0,\, \pi\}$ and $\{\pi/2,\, 3\pi/2\}$. The phase values 0 and $\pi/2$ represent bit "1" and the other two represent bit "0". When single-photon sources are used, the common phase does not affect the final result and will not be taken into account.

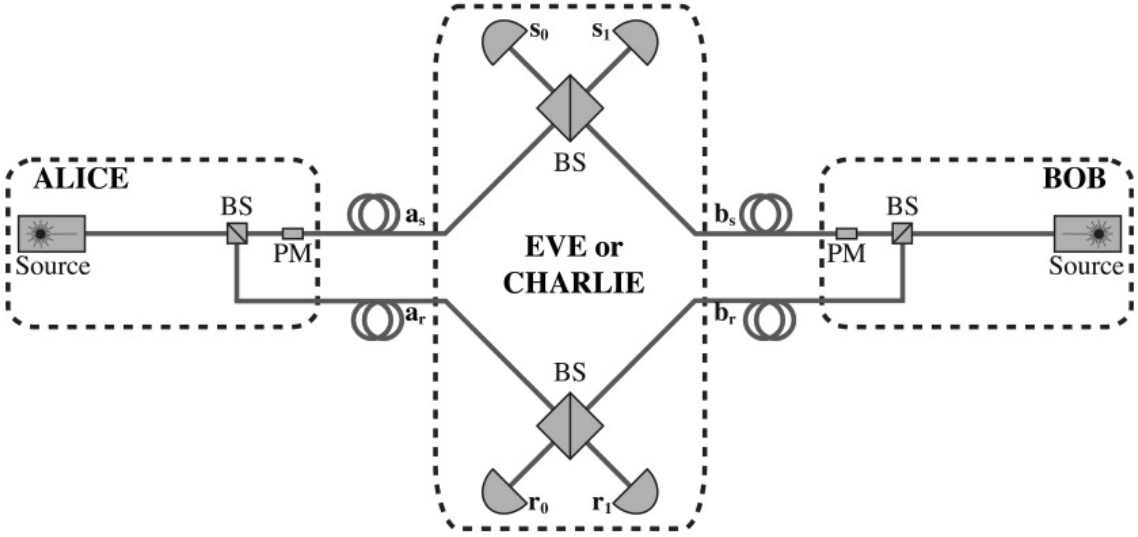

FIG. 1. Common MDI QKD scheme. BS is a beam splitter and PM is a phase modulator

In this implementation of MDI QKD, channel losses and dark counting effects are not taken into account. It is also assumed that the relative phase between the reference and signal modes is maintained. A successful partial BSM occurs when one and only one of $\mathrm{r_0}$ and $\mathrm{r_1}$ and one and only one of $\mathrm{s_0}$ and $\mathrm{s_1}$ are clicked. All other events, such as the case when $\mathrm{r_0}$ and $\mathrm{r_1}$ are clicked at the same time, are discarded.

If $\theta_\mathrm{a} - \theta_\mathrm{b} = \pm\pi$, then detectors $\mathrm{r_0}$ and $\mathrm{s_0}$, and only these detectors, click or $\mathrm{r_1}$ and $\mathrm{s_1}$ click. Otherwise, if $\theta_\mathrm{a} - \theta_\mathrm{b} = 0$, then detectors $\mathrm{r_0}$ and $\mathrm{s_1}$, or $\mathrm{r_1}$ and $\mathrm{s_0}$ click. In all other cases, when $\theta_\mathrm{a} - \theta_\mathrm{b} = \pm\pi/2$, two random detectors out of four will work, and then Alice's and Bob's qubits will not correlated. Such events will be eliminated using a standard screening procedure. Clicks only on the reference (signal) detectors will also be excluded. Eventually, Alice's and Bob's bits, determined by the relative phases θ_a and θ_b, will be correlated or anticorrelated depending on the detection results at the central relay.

Then, in the case of a single-photon MDI scheme, the secure key fraction can be calculated as follows [28]

$$r > Y_{11}[1 - fh(e_{11}) - h(e_{11})], \tag{1}$$

where $h(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, Y_{11} is a detector efficiency, e_{11} is a QBER, and f is an error correction efficiency.

3.2. MDI CV-QKD

Recently, several strategies for attacking real detectors have also been proposed in the CV-QKD systems. For example, the short pulse attack [29] and the LO calibration [30] attack manipulate measurement results, which provokes Alice and Bob to overestimate the security of the key. A saturation attack [31] can cause Alice and Bob to underestimate the excess noise by saturating the homodyne detector, which can hide the intercept-resend attack.

The most logical option to eliminate these attacks in the CV-QKD system was to characterize each specific loophole and find countermeasures. However, it is quite difficult to fully characterize real detectors and account for all loopholes. That is why it is so important to figure out how to defend against all the attacks on detectors in practical MDI CV-QKD systems.

Taking into account all the problems in the field of detection, the corresponding CV-QKD protocol was proposed, which can also prevent leakage through side channels [4, 32]. The basic idea, as in standard MDI QKD, is that both Alice and Bob are senders, and an untrusted third party (Charlie) is introduced to perform the measurement. The measurements on Charlie's relay will be used by Alice and Bob in post-processing to generate secure keys.

3.3. MDI CV-QKD protocol description

It is easier to describe the security analysis against arbitrary collective attacks by introducing the entanglement-based (EB) scheme of this protocol. It is based on the fact that the MDI CV-QKD scheme (Fig. 2) is equivalent to the prepare-and-measure (PM) scheme of CV-QKD with coherent states and heterodyne detection (Fig. 3). Moreover, the effectiveness of such a protocol against collective attacks is presented using numerical simulation methods.

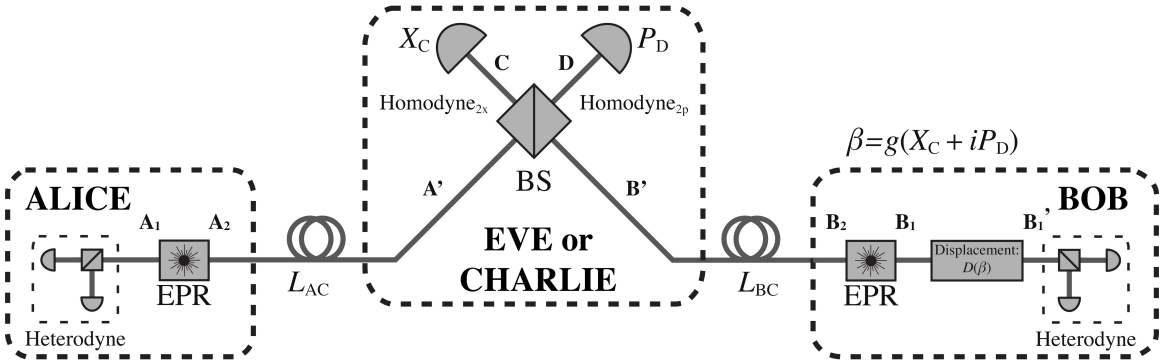

FIG. 2. EB MDI CV-QKD scheme

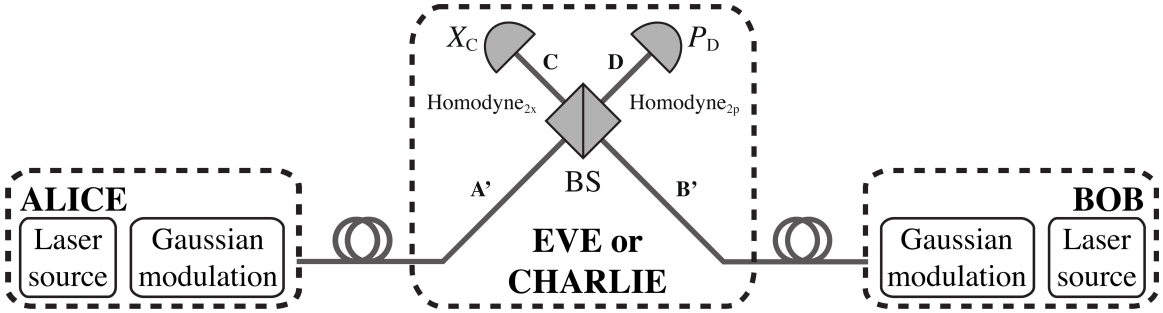

FIG. 3. PM MDI CV-QKD scheme

The MDI CV-QKD in the EB scenario (see Fig. 2) is executed according to the following steps:

(1) Both Alice and Bob generate a two-mode squeezed vacuum state, keeping one mode each (A_1, B_1), and the other sent over a quantum channel to a third untrusted party Charlie (A_2, B_2);

(2) Alice's and Bob's modes (A', B') obtained by Charlie interfere in a beam splitter with two output modes C and D. The x-quadrature of the C mode and the p-quadrature of the D mode are measured via homodyning. Charlie then publicly announces the result $\{X_\mathrm{C},\ P_\mathrm{D}\}$;

(3) Bob displace his state B_1 using the displacement operator $\widehat{D}(\beta)$ (with $\beta = g(X_\mathrm{C}+iP_\mathrm{D})$, where g is a bias factor). After all the operations, Alice and Bob measure their states B_1' and A_1 via heterodyning. After the displacement, the final states of Alice and Bob become entangled, that is, their final received information is correlated;

(4) Alice and Bob use the authenticated public channel to complete the parameter estimation, information reconciliation, and privacy amplification.

It should be borne in mind that Charlie is an untrusted party and can be completely under the control of Eve. It is also necessary to consider a scheme more convenient for practical implementation (see Fig. 3), in this embodiment, where Alice and Bob prepare coherent states modulated in accordance with a two-dimensional Gaussian distribution (GG02), which are easier to generate than a two-mode squeezed vacuum state:

(1) Alice and Bob generate a coherent state $|x_{\mathrm{A}} + ip_{\mathrm{A}}\rangle$ and $|x_{\mathrm{B}} + ip_{\mathrm{B}}\rangle$, where the quadratures x and p have variance $V_{\mathrm{A}} - 1$ ($V_{\mathrm{B}} - 1$) in shot noise units (SNU). Both Alice and Bob send their states to Charlie's untrusted relay via quantum channels;
(2) Alice's and Bob's modes interfere at the beam splitter. The quadratures of Charlie's C and D modes are measured on a homodyne detectors. After that, Charlie announces publicly the resulting state $\{X_{\mathrm{C}},\ P_{\mathrm{D}}\}$;
(3) At the end, as in the case of the EB scheme, only Bob changes his state in the following way: $X_{\mathrm{B}} = x_{\mathrm{B}} + kX_C, P_{\mathrm{B}} = p_{\mathrm{B}} - kP_{\mathrm{D}}$ (k is the gain associated with channel losses), while Alice preserves her state unchanged;
(4) legitimate parties perform standard procedures for parameter estimation, information reconciliation, and privacy amplification;

As described above, the EB and PM scenarios are equivalent in proving the security of the CV-QKD protocols against collective attacks [3, 33] and are reduced to one another by transforming the covariance matrix.

3.4. Security proof for MDI CV-QKD protocol

From the point of view of the theoretical security proof, Eve can have access to almost the entire QKD system, including relays, quantum channels, and even Bob's state displacement operation in the EB scheme. In this case, one can consider the MDI CV-QKD protocol as a special case of a typical one-way CV-QKD protocol [12].

Then the secure key fraction can be estimated in accordance with the Devetak-Winter bound [34, 35]

$$r = \beta I(X_{\mathrm{A}},\ P_{\mathrm{A}} : X_{\mathrm{B}},\ P_{\mathrm{B}}) - \chi(X_{\mathrm{B}},\ P_{\mathrm{B}} : E), \tag{2}$$

where β is reconciliation efficiency, I is a mutual information Alice-Bob, $\chi(X_{\mathrm{B}}, P_{\mathrm{B}} : E) = S(\widehat{\rho}_E) - S(\widehat{\rho}_E|X_{\mathrm{B}}, P_{\mathrm{B}})$ is a Holevo bound, and $S(\widehat{\rho}_E)$ is a von Neumann entropy of quantum state $\widehat{\rho}_E$.

Based on the assumption that Eve can attack through a full purge, which means $\chi(X_{\mathrm{B}},\ P_{\mathrm{B}} : E) = \chi(X_{\mathrm{B}},\ P_{\mathrm{B}} : A_1, B_1')$, one can obtain the final expression for the secret fraction

$$r = \beta I(X_{\mathrm{A}},\ P_{\mathrm{A}} : X_{\mathrm{B}}, P_{\mathrm{B}}) - S(\widehat{\rho}_{\mathrm{A_1B_1'}}) - S(\widehat{\rho}_{\mathrm{A_1B_1'}}|X_{\mathrm{B}}, P_{\mathrm{B}}). \tag{3}$$

Moreover, the upper bound $\chi(X_{\mathrm{B}},\ P_{\mathrm{B}} : \mathrm{A}_1, \mathrm{B}_1')$ is determined only using the covariance matrix $\gamma_{\mathrm{A_1B_1'}}$.

3.5. Estimation of covariance matrix

The whole system is supposed to be under two independent entangling cloner attacks [11]. Then the covariance matrix has the form

$$\Xi = \begin{pmatrix} V_{\mathrm{A}} I_2 & \sqrt{(T(V_{\mathrm{A}}^2 - 1)\sigma_z)} \\ \sqrt{(T(V_{\mathrm{A}}^2 - 1)\sigma_z)} & [(V_{\mathrm{A}} - 1) + 1 + T\xi']I_2 \end{pmatrix}, \tag{4}$$

$$T = \frac{\eta_{\mathrm{A}}}{2} g^2, \tag{5}$$

$$\xi' = 1 + \frac{1}{\eta_{\mathrm{A}}}[\eta_{\mathrm{B}}(\Xi_{\mathrm{B}} - 1) + \eta_{\mathrm{A}}\Xi_{\mathrm{A}}] + \frac{1}{\eta_{\mathrm{A}}}(\frac{\sqrt{2}}{g}\sqrt{V_{\mathrm{B}} - 1} - \sqrt{\eta_{\mathrm{B}}}\sqrt{V_{\mathrm{B}} + 1})^2, \tag{6}$$

$$\Xi_{\mathrm{A}} = \frac{1 - \eta_{\mathrm{A}}}{\eta_{\mathrm{A}}} + \xi_{\mathrm{A}},\ \Xi_{\mathrm{B}} = \frac{1 - \eta_{\mathrm{B}}}{\eta_{\mathrm{B}}} + \xi_{\mathrm{B}}, \tag{7}$$

$$\eta_{\mathrm{A}} = 10^{-\alpha L_{\mathrm{AC}}/10},\ \eta_{\mathrm{B}} = 10^{-\alpha L_{\mathrm{BC}}/10}, \tag{8}$$

where η_{A} (η_{B}) is a channel (Alice-Charlie or Bob-Charlie) transmittance, $\xi_{\mathrm{A}}(\xi_{\mathrm{B}})$ is an excess noise, g is an offset factor, I_2 is an identity matrix, and σ is a Pauli z-matrix.

To minimize excess noise, the offset factor is set as

$$g = \sqrt{\frac{2}{\eta_{\mathrm{B}}}}\sqrt{\frac{V_{\mathrm{B}} - 1}{V_{\mathrm{B}} + 1}}. \tag{9}$$

Then the excess noise is expressed as

$$\xi' = \xi_{\mathrm{A}} + \frac{1}{\eta_{\mathrm{A}}}[\eta_{\mathrm{B}}(\xi_{\mathrm{B}} - 2) + 2]. \tag{10}$$

3.6. MDI CV-QKD system performance

The symmetrical implementation in MDI CV-QKD schemes seems to be the most logical when the distance between Alice and the relay is equal to the distance between the relay and Bob. The system parameters in this implementation are [4]: $\beta = 1,\ L_{\mathrm{AC}} = L_{\mathrm{BC}}$. Security is evaluated in the presence of collective attacks for keys of finite length. The dotted line in Figure 4 denotes the ideal case of high modulation dispersion ($V_{\mathrm{A}} = V_{\mathrm{B}} = 10^5$) with almost no excess noise . The black solid line indicates the case when $V_{\mathrm{A}} = V_{\mathrm{B}} = 40,\ \xi_{\mathrm{A}} = \xi_{\mathrm{B}} = 0.002$.

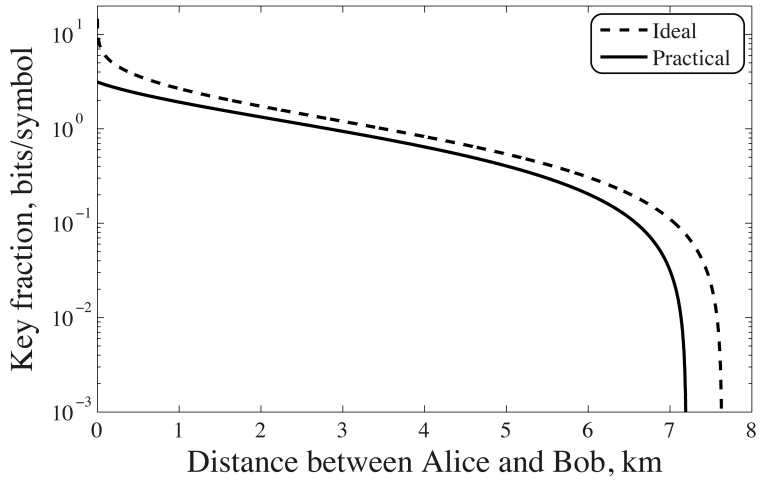

FIG. 4. Secure key fraction versus the distance between Alice and Bob in the symmetrical MDI CV-QKD implementation.

As can be seen, the maximum achievable transmission distance for the symmetrical case is only 7 km. Key transmission over long distances in this configuration is not possible. However, the symmetrical case can be used for MDI communication over short distances.

However, there is a way to increase the key transmission distance. Considering that only Bob changes his state, it becomes clear that ξ' is not symmetrical. In this case, consider the situation where $L_{\mathrm{AC}} \neq L_{\mathrm{BC}}$. The results of such an implementation are shown in Figure 5. Again, the dotted line represents the ideal case ($V_{\mathrm{A}} = V_{\mathrm{B}} = 10^5,\ \xi_{\mathrm{A}} = \xi_{\mathrm{B}} = 0$),

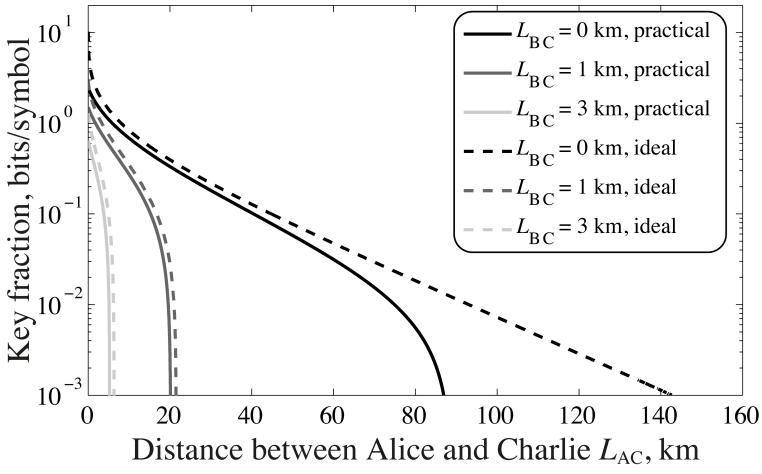

FIG. 5. Secure key fraction versus the distance between Alice and Bob in the symmetrical MDI CV-QKD implementation

and the parameters for the solid line, in turn, are as follows: $V_{\mathrm{A}} = V_{\mathrm{B}} = 40,\ \xi_{\mathrm{A}} = \xi_{\mathrm{B}} = 0.002$.

Obviously, in the asymmetric case, the results obtained are much superior to the symmetric one. The maximum achievable transmission distance is 80 km when the relay is as close to Bob as possible.

Thus, in accordance with the MDI CV-QKD protocols, it is possible to distribute the secure key with a generation rate comparable to one-way QKD protocols. Moreover, such systems are resistant to all collective attacks on the detectors, fluctuation attacks on the LO, and calibration attacks.

An ideal reconciliation ($\beta = 1$) was also assumed in all cases. In real systems, this is a difficult task, but some scientific groups demonstrate efficiency up to $\beta = 0.99$ [16]. But if we take a more typical value of efficiency for CV-QKD systems $\beta = 0.95$ [4], the maximum distance at which a key distribution session is possible will be halved.

3.7. Finite key aspects

Another obvious problem of CV-QKD getting in the way of integration into the telecommunications infrastructure is taking into account the finite size of the distributed key. Indeed, in real systems, parties cannot exchange an infinite number of bits to generate a key. And it is logical to assume that by creating keys of a finite size, it is impossible to achieve the same security results as in the asymptotic case of infinite keys.

To fill this gap, it is necessary to evaluate the effects of finite size effects on the security parameter of MDI CV-QKD protocol that has been done in [36].

The parameters of Gaussian quantum channel (transmittance and excess noise) are determined within the confidence intervals. Confidence intervals are used to select the worst case scenario by selecting the lowest channel bandwidth and highest excess noise. The secure key fraction is then numerically calculated using the estimated transmittance and noise values

$$r = \frac{n}{\widetilde{N}}(r^{\infty}(\xi,\, V_{\mathrm{A}},\, \tau_{\mathrm{A}}^{\mathrm{low}},\, \tau_{\mathrm{B}}^{\mathrm{low}},\, V_{\mathrm{q},\,\xi}^{\mathrm{up}},\, V_{\mathrm{p},\,\xi}^{\mathrm{up}}) - \Delta(n)), \tag{11}$$

where $n = \widetilde{N} - m$ is a number of signals used for key generation, $\widetilde{N}$ is a total number of signals exchanged, $\tau_{\mathrm{A}}^{\mathrm{low}}$, $\tau_{\mathrm{B}}^{\mathrm{low}}$ are the smallest possible values of Alice's and Bob's channel transmittance coefficients, $V_{\mathrm{q},\,\xi}^{\mathrm{up}}$, $V_{\mathrm{p},\,\xi}^{\mathrm{up}}$ are the most pessimistic values for excess noise variance, $\Delta(n) \sim \sqrt{\frac{1}{n}\log_2(2\varepsilon_{\mathrm{pa}}^{-1})}$, and $\varepsilon_{\mathrm{pa}}$ is a privacy amplification security parameter.

As expected, by increasing the key block size, one can achieve performance comparable to the ideal conditions of the asymptotic case. The final results show that with a block size in the range of $10^6 \div 10^9$ signals, it is possible to provide a positive secure key generation rate of about 10^{-2} bits/symbol in the presence of high excess noise $\xi = 0.01$ and attenuation caused by using standard optical fiber over long distances

4. SDI CV-QKD

Alternative DI CV-QKD systems of KKNKP are also worth mentioning. One example of such schemes is SDI QKD [27]. The main idea, just as in the case of MDI, is the ability to protect against attacks associated with non-ideal equipment used in QKD systems.

As in MDI, three independent modules are involved in communication: Alice, Bob and Charlie relay. The main difference is how the relay is used as a source in this system (see Fig. 6). After all, it is Charlie who prepares the two-mode squeezed vacuum state and sends it to Alice and Bob. Since the modes are entangled, Alice and Bob receive correlated information. However, it is still assumed that Charlie is a completely untrusted party that can be completely under the control of Eve in the same way as both quantum channels.

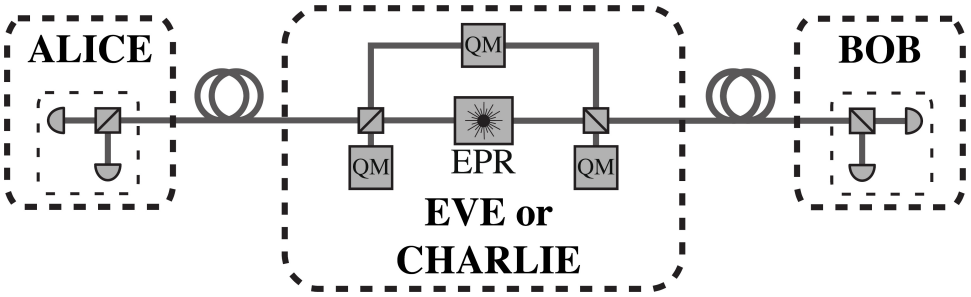

FIG. 6. SDI CV-QKD Scheme. QM is a quantum memory needed to carry out an attack

For SDI CV-QKD system, security to both collective attacks and coherent attacks was proved due to an additional energy test. But the maximum key distribution distance, even in a situation of collective attacks, does not exceed 20 km. While in the presence of coherent it is below 5 km.

5. Conclusion

In this review, we have considered DI CV-QKD protocols. Numerical simulations in the presence of entangling cloner attacks on MDI CV-QKD show that the transmission distance between Alice and Bob is severely limited in the symmetrical case ($L_{\mathrm{AC}} = L_{\mathrm{BC}}$). In addition, this QKD protocol requires only minor modifications to existing QKD systems and thus can be easily implemented in practice. SDI CV-QKD protocol is also of interest for further study, but does not show the proper level of performance at the moment.

References

[1] Pirandola S., Andersen U.L., Banchi L., Berta M., Bunandar D., Colbeck R., Englund D., Gehring T., Lupo C., Ottaviani C., Pereira J.L., Razavi M., Shamsul Shaari J., Tomamichel M., Usenko V.C., Vallone G., Villoresi P., and Wallden P. Advances in quantum cryptography, *Advances in Optics and Photonics*, 2020, **12**, P. 1012.

[2] Shor P.W. and Preskill J. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, *Physical Review Letters*, 2000, **85**, P. 441–444.

[3] Laudenbach F., Pacher C., Fung C.-H. F., Poppe A., Peev M., Schrenk B., Hentschel M., Walther P., and Hübel H., Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations. *Advanced Quantum Technologies*, 2018 **1**(8), P. 1800011.

[4] Li Z., Zhang Y.-C., Xu F., Peng X., and Guo H. Continuous-variable measurement-device-independent quantum key distribution. *Physical Review A*, 2014, **89**(5), P. 052301.

[5] Xu F., Ma X., Zhang Q., Lo H.-K., and Pan J.-W. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 2020, **92**(5), P. 025002.

[6] Lo H.-K., Curty M., and Qi B. Measurement-Device-Independent Quantum Key Distribution. *Physical Review Letters*, 2012, **108**(3), P. 130503.

[7] Lucamarini M., Yuan Z.L., Dynes J.F., and Shields A.J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 2018, **557**(5), P. 400–403.

[8] Bennett C.H. and Brassard G. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 2014, **560**(12), P. 7–11.

[9] Hillery M. Quantum cryptography with squeezed states. *Physical Review A*, 2000, **61**(1), P. 22309.

[10] Cerf N.J., Lévy M., and Assche G.V. Quantum distribution of Gaussian keys using squeezed states. *Physical Review A*, 2001, 63(4), P. 052311.

[11] Grosshans F., Van Assche G., Wenger J., Brouri R., Cerf N.J., and Grangier P. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 2003, **421**(1), P. 238–241.

[12] Weedbrook C., Lance A.M., Bowen W.P., Symul T., Ralph T.C., and Lam P.K. Quantum Cryptography Without Switching. *Physical Review Letters*, 2004, **93**(10), P. 170504.

[13] Goncharov R., Kiselev A.D., Samsonov E., and Egorov V. Security proof for continuous-variable quantum key distribution with trusted hardware noise against general attacks. *arXiv preprint arXiv:2205.05299*, 5 2022.

[14] Diamanti E. and Leverrier A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy*, 2015, **17**(8), P. 6072–6092.

[15] Huang D., Huang P., Lin D., and Zeng G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, 2016, **6**(5), P. 19201.

[16] Zhang Y., Chen Z., Pirandola S., Wang X., Zhou C., Chu B., Zhao Y., Xu B., Yu S., and Guo H. Long-Distance Continuous-Variable Quantum Key Distribution over 202.81 km of Fiber. *Physical Review Letters*, 2020, **125**(6), P. 010502.

[17] Ghorai S., Grangier P., Diamanti E., and Leverrier A. Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation. *Physical Review X*, 2019, **9**(6), P. 021059.

[18] Lin J., Upadhyaya T., and Lütkenhaus N. Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution. *Phys. Rev. X*, 2019, **9**(12).

[19] Leverrier A. Composable Security Proof for Continuous-Variable Quantum Key Distribution with Coherent States. *Physical Review Letters*, 2015, **114**(2), P. 070501.

[20] Leverrier A. Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction. *Physical Review Letters*, 2017, **118**(5), P. 200501.

[21] Hosseinidehaj N., Walk N., and Ralph T.C. Optimal realistic attacks in continuous-variable quantum key distribution. *Physical Review A*, 2019, **99**(5), P. 1–11.

[22] Pirandola S. Limits and security of free-space quantum communications. *Physical Review Research*, 2021, **3**(3), P. 013279.

[23] Pirandola S. Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks. *Physical Review Research*, 2021, **3**(10), P. 043014.

[24] Koashi M. and Preskill J. Secure Quantum Key Distribution with an Uncharacterized Source. *Physical Review Letters*, 2003, **90**(2), P. 057902.

[25] Makarov V., Anisimov A., and Skaar J. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Physical Review A*, 2006, **74**(2), P. 22313.

[26] Zhao Y., Fung C.H.F., Qi B., Chen C., and Lo H.K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A*, 2008, **78**(4), P. 42333.

[27] Zhang Y., Chen Z., Weedbrook C., Yu S., and Guo H. Continuous-variable source-device-independent quantum key distribution against general attacks. *Scientific Reports*, 2020, **10**(12), P. 6673.

[28] Ma X. and Razavi M. Alternative schemes for measurement-device-independent quantum key distribution. *Physical Review A*, 2012, **86**(6), P. 62319.

[29] Qin H., Huang A., and Makarov V. Short pulse attack on continuous-variable quantum key distribution system. in *QCrypt 2017*, 2017.

[30] Jouguet P., Kunz-Jacques S., and Diamanti E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Physical Review A - Atomic, Molecular, and Optical Physics*, 2013, **87**(6), P. 1–6.

[31] Qin H., Kumar R., and Alléaume R. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Physical Review A*, 2016, **94**(7), P. 012325.

[32] Pirandola S., Ottaviani C., Spedalieri G., Weedbrook C., Braunstein S.L., Lloyd S., Gehring T., Jacobsen C.S., and Andersen U.L. High-rate measurement-device-independent quantum cryptography. *Nature Photonics*, 2015, **9**(6), P. 397–402.

[33] Grosshans F., Cerf N.J., Wenger J., Tualle-Brouri R., and Grangier P., Virtual Entanglement and Reconciliation Protocols for Quantum Cryptography with Continuous Variables. *Quantum Information and Computation*, 2003, **3**(7), P. 535–552.

[34] Devetak I. and Winter A. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 2005, **461**(1), P. 207–235.

[35] Pirandola S., Mancini S., Lloyd S., and Braunstein S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics*, 2008, **4**(9), P. 726–730.

[36] Papanastasiou P., Ottaviani C., and Pirandola S. Finite-size analysis of measurement-device-independent quantum cryptography with continuous variables. *Physical Review A*, 2017, **96**(10), P. 042332.

Submitted 30 May 2022; revised 7 June 2022; accepted 8 June 2022

Information about the authors:

Roman Goncharov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; rkgoncharov@itmo.ru

Egor Bolychev – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; 285799@niuitmo.ru

Irina Vorontsova – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; viovorontsova@niuitmo.ru

Eduard Samsonov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; Edi.samsonov@gmail.com

Vladimir Egorov – ITMO University, Kronverkskiy, 49, St. Petersburg, 197101, Russia; egorovvl@gmail.com

Conflict of interest: the authors declare no conflict of interest.