

https://doi.org/10.1070/QEL16469

Demonstration of a quantum key distribution network in urban fibre-optic communication lines

E.O. Kiktenko, N.O. Pozhar, A.V. Duplinskiy, A.A. Kanapin, A.S. Sokolov, S.S. Vorobey, A.V. Miller, V.E. Ustimchik, M.N. Anufriev, A.T. Trushechkin, R.R. Yunusov, V.L. Kurochkin, Yu.V. Kurochkin, A.K. Fedorov

Abstract. **We report the results of the implementation of a quantum key distribution (QKD) network using standard fibre communication lines in Moscow. The developed QKD network is based on the paradigm of trusted repeaters and allows a common secret key to be generated between users via an intermediate trusted node. The main feature of the network is the integration of the setups using two types of encoding, i.e. polarisation encoding and phase encoding. One of the possible applications of the developed QKD network is the continuous key renewal in existing symmetric encryption devices with a key refresh time of up to 14 s.**

Keywords: *quantum distribution of communication keys, fibre communication channels, polarisation and phase encoding.*

1. Introduction

In recent decades, significant progress has been gained in theory, experimental research and quantum key distribution (QKD) technology [1–3]. Nevertheless, there exist a number of problems, such as short distance, low key generation rate, practical security of QKD systems, etc. [1–3]. To implement the QKD between several (more than two) users, it is necessary to develop a QKD network [4]. There are a number of major projects to create such networks, in particular in the US, Europe, China and Japan [5–13]. QKD networks have many promising applications, for example, the development of secure distributed databases [14]. First of all, they guarantee the informational-theoretical security of communications between nodes and can also be used for the continuous key renewal in currently available symmetric encryption devices.

One of the most important problems in the development of networks is the generation of secret keys beyond the laboratory. As a consequence, it is important to use a QKD protocol that guarantees secrecy in urban fibre-optic communication channels exhibiting significant losses. This circumstance is one of the most important distinguishing factors of experiments on the quantum key distribution in urban conditions. It is important to note that post-processing procedures of sifted keys are also an integral part of QKD networks [15, 16].

The purpose of this work is an experimental demonstration of QKD networks for systems with different types of quantum-state encoding in urban conditions. The quantum key distribution is implemented using a 'dark', high-loss optical fibre, which is laid together with the available communication lines. One of possible applications of the developed QKD network is the continuous key renewal in the currently available symmetric encryption devices. Russian encryption standards assume the use of keys with a length of 256 bits, and therefore, taking into account the use of QKD networks, they can be refreshed approximately every 14 s.

2. QKD network

In this work, we employ the SECOQC approach [6], which defines a QKD network as an infrastructure based on a point-to-point topology utilising the QKD. Then any two nodes of the network can generate a common private key at the information-theoretical level of security. The network protocol (in the case under consideration, three nodes and two QKD links) operates as follows (Fig. 1). Nodes 1 and 2 as well as nodes 2 and 3 generate secret keys k_{12} and k_{23}. These keys are stored in the memory of the corresponding nodes. Using a quantum random number generator, node 1 generates the K key and then forwards it in an encrypted form using a one-time pad, $K \oplus k_{12}$, to the intermediate trusted node (node 2). Using the previously established key k_{23}, node 2 transmits $K \oplus k_{23}$ to node 3. As a result, arbitrary nodes (and all nodes together) in the QKD network can establish a common private key. To ensure that the received keys are sent by a particular node, information-theoretic secure authentication can be applied [6].

The developed QKD network allows a common quantum key to be established for users with various optical QKD topologies that implement polarisation and phase encoding. The basis for this experiment is the recently presented modu-

E.O. Kiktenko Russian Quantum Center, ul. Novaya 100, Skolkovo, 143025 Moscow, Russia; Steklov Mathematical Institute, Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russia; Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, 105005 Moscow, Russia;
N.O. Pozhar, M.N. Anufriev Russian Quantum Center, ul. Novaya 100, Skolkovo, 143025 Moscow, Russia; Bauman Moscow State Technical University, 2-ya Baumanskaya ul. 5, 105005 Moscow, Russia;
A.V. Duplinskiy Russian Quantum Center, ul. Novaya 100, Skolkovo, 143025 Moscow, Russia; Moscow Institute of Physics and Technology (State University), Institutskiy per. 9, 141700 Dolgoprudnyi, Moscow region, Russia;
A.A. Kanapin Russian Quantum Center, ul. Novaya 100, Skolkovo, 143025 Moscow, Russia; M.V. Lomonosov Moscow State University, Vorob'evy Gory, 119991 Moscow, Russia;
A.S. Sokolov, S.S. Vorobey, A.V. Miller, V.E. Ustimchik, R.R. Yunusov, V.L. Kurochkin, Yu.V. Kurochkin, A.K. Fedorov Russian Quantum Center, ul. Novaya 100, Skolkovo, 143025 Moscow, Russia; e-mail: y.kurochkin@gmail.com;
A.T. Trushechkin Steklov Mathematical Institute, Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russia

Received 7 June 2017; revision received 10 August 2017
Kvantovaya Elektronika **47** (9) 798–802 (2017)
Translated by M.A. Monastyrskiy

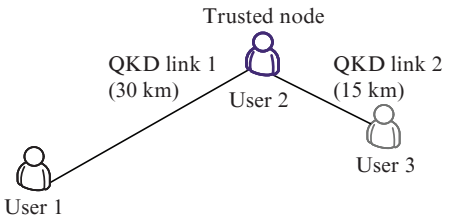

Figure 1. Scheme of a QKD network with the quantum keys distributed among three users via an intermediate trusted node.

lar QKD device [15], which is driven by National Instruments (NI) boards supporting an open source LabView code for control and operation, an open source Python code for post-processing and an open source protocol for external applications [16–18]. The QKD device can operate with any single-photon detectors. The external drivers of single-photon detectors, phase modulators and synchronisation detectors are removable modules. Each device can drive up to four detectors and has six universal ports for connecting lasers, phase or amplitude modulators. The software solution responsible for controlling the system is written using the LabView environment.

The electro-optical modulators are controlled by a PCIe-7811R (NI) board installed in personal computers [15]. An LDI-DFB2.5G semiconductor laser controlled by a Spartan-6 FPGA board generates optical pulses with a repetition rate of 10 MHz at a standard telecommunication wavelength of 1.55 μm. Single-photon ID230 detectors are used [19]. Beam splitters, Faraday mirrors, circulators, variable optical attenuator and phase and intensity modulators are standard optical components.

The first link of the developed QKD network generates quantum keys using a polarisation-encoding scheme based on the BB84 protocol [20]. In this case, use is made of the Pockels effect in low-voltage electro-optical phase modulators based on $LiNbO_3$ (Fig. 2a). Note that this method allows one to empoy a single laser source, whereas most implementations of polarisation encoding face the problem of indistinguishability of the pulses emitted by different sources [21]. In addition, only two single-photon detectors are required, in contrast to standard polarisation-encoding schemes with four detectors. This link ensures the exchange of keys at a distance of up to 30 km (in urban fibre with a loss of 13 dB, the average number of photons in the pulse $\mu_{pol} = 0.02$) at the sifted key generation rate of about 0.1 Kbit s^{-1}.

The second link uses a phase-encoding scheme for the QKD (Fig. 2b) implementing the BB84 protocol. This scheme has already been tested for the QKD in urban fibre-optic lines [22]. This link allows one to generate secret keys at a distance of up to 15 km (in urban fibre-optic lines with a loss of 7 dB, the average number of photons in the pulse $\mu_{ph} = 0.03$), the key generation rate being about 0.2 Kbit s^{-1}.

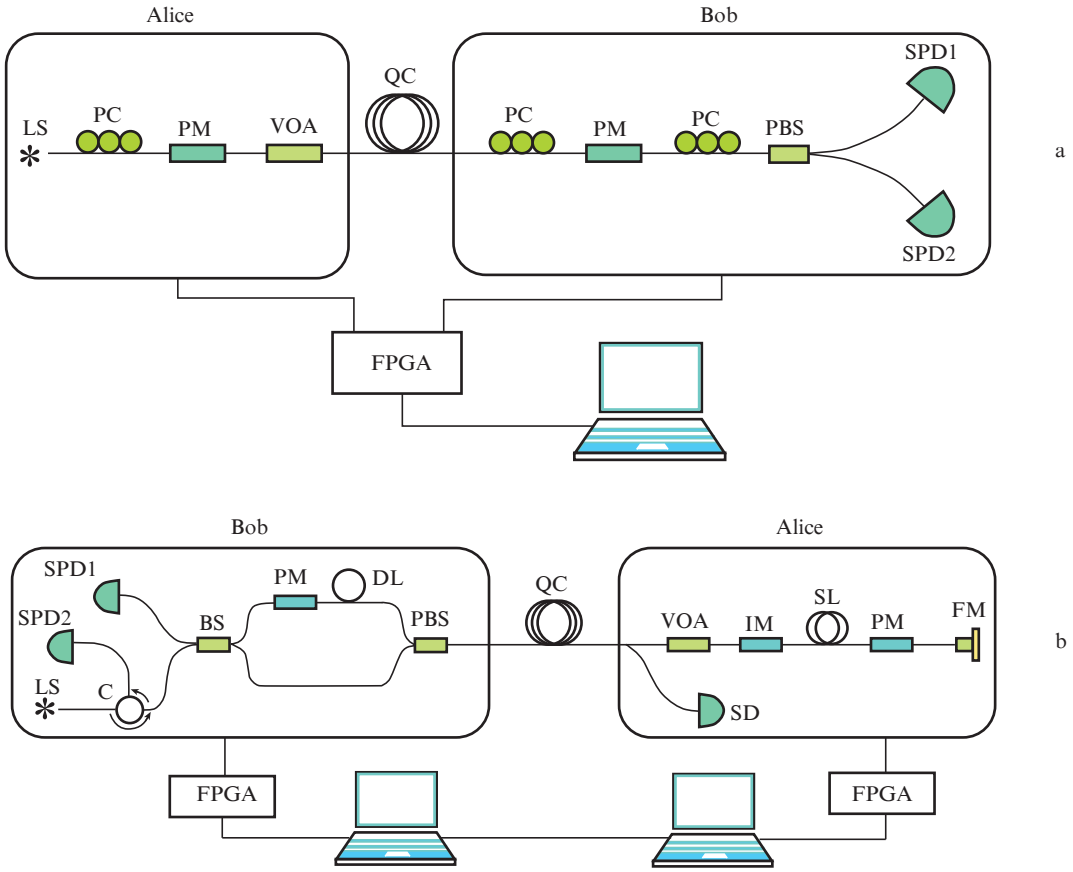

Figure 2. Schemes of (a) the first QKD link for the generation of quantum keys using the polarisation-encoding scheme [(LS) light source; (PC) polarisation controller; (PM) phase modulator; (VOA) variable optical attenuator; (QC) quantum channel (urban fibre-optic line); (PBS) polarisation beam splitter; (SPD) single-photon detector] and (b) the second QKD link that employs the phase-encoding scheme [(C) circulator; (BS) beam splitter; (DL) delay line; (SL) storage line; (SD) synchronisation detector; (IM) intensity modulator; (FM) Faraday mirror].

Figure 3 shows the time dependence of the average value of the quantum bit error rate (QBER) (data during 6 hours). The change in the QBER value is caused by external factors (mechanical and thermal impacts). It can be seen that the real share of errors in the sifted key is a few percent, which is too great for direct applications, for example, to be used as keys for encryption with a one-time pad or for refreshing a key in symmetric ciphers. To eliminate this share of errors and also to reduce the potential information of an eavesdropper to insignificant values, we use the post-processing procedure described below.

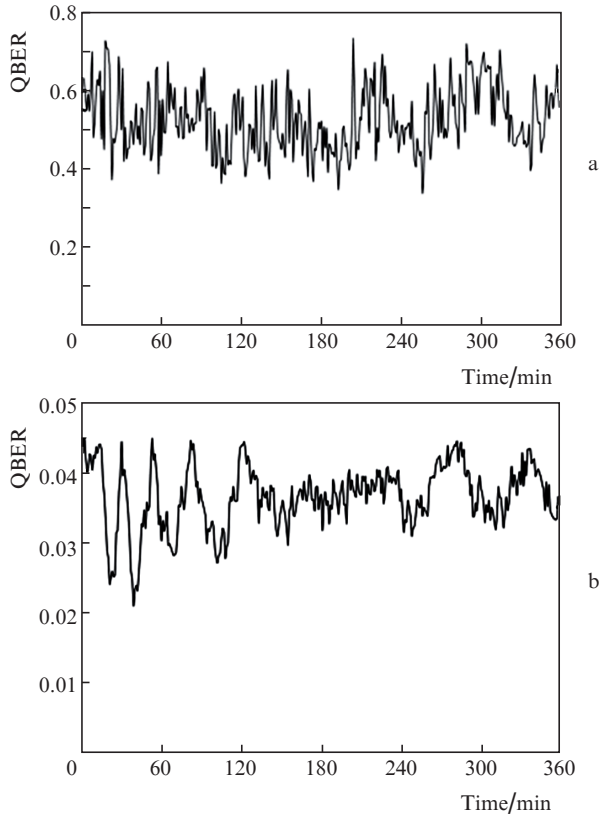

Figure 3. Average QBER value as function of time (6 hours) for (a) the polarisation-encoding scheme and (b) phase-encoding scheme.

3. Secret key generation rate

The sifted keys from both QKD links represent the input data for the post-processing procedure, which includes information reconciliation, parameter estimation, privacy amplification and authentication [16]. The procedure consists of a number of steps.

1. Sifted keys from QKD links pass through the information reconciliation stage based on the method described in [17], which employs the low-density parity-check codes [23–25]. Note that this method allows information reconciliation with a very rough or even missing QBER estimate. In addition, the blind information reconciliation protocol significantly improves the efficiency of the error correction procedure and reduces its interactivity [17].

2. After the information reconciliation stage, there is still a certain probability that not all errors are corrected. To detect possible remaining errors, we implement a subsequent verification protocol using universal hash functions [26]. The probability of the presence of errors after successful verification of a block of ~1 Mbit keys is limited to the value $\varepsilon_{\text{ver}} = 2 \times 10^{-11}$ when using a hash tag of 50 bits in length. A detailed description of the verification protocol is presented in [26]. A general binary sequence obtained at this stage is called a verified key.

3. At the parameter estimation stage, the parties obtain the actual QBER level for their key blocks via direct comparison of the keys before and after the information reconciliation. In fact, this step is performed on Bob's side, where the modification of the sifted key has been performed at the previous stage. If the QBER value is above the critical value needed for effective privacy amplification, users abort the protocol. Otherwise, the verified key blocks pass on to the privacy amplification stage, and the estimated QBER value is used in the next rounds of the information reconciliation [16].

4. The privacy amplification stage is used to reduce potential information of an eavesdropper about the verified blocks to an insignificant value [16]. This is achieved by contracting the input key. The secret key length is given by the expression:

$$L_{\text{sec}} = L_{\text{ver}}\,\hat{Y}_1[1 - h(\hat{q}_1)] - \text{leak}_{\text{ec}} - 5\log_2(1/\epsilon_{\text{pa}}), \tag{1}$$

where L_{ver} is the length of the verified key; $\hat{Y}_1$ is the estimate of the fraction of the sifted key bits generated from the single-photon pulses; $\hat{q}_1$ is the QBER estimate for the single-photon pulses;

$$h(q) = -q\log_2 q - (1-q)\log_2(1-q)$$

is the binary entropy function; leak_{ec} is the total number of bits disclosed at the information reconciliation and verification stages; and ε_{pa} is the probability of failure at the privacy amplification stage, resulting from the finiteness of the length of an input verified key. In our procedure, we accepted $\epsilon_{\text{pa}} = 10^{-12}$.

The estimate for $\hat{Y}_1$ appears as:

$$\hat{Y}_1 = \frac{\eta\mu - p_2}{\eta\mu}, \tag{2}$$

where η is the quantum channel transmittance; μ is the intensity of laser pulses; and $p_2 = e^{-\mu}\mu^2/2$ is the two-photon radiation probability in the generation of coherent pulses [27]. This estimate is obtained on the assumption that Eve can perform an attack with a separation of the number of photons, as well as other operations with quantum states being transmitted, but it cannot influence Alice's and Bob's setups (for instance, it cannot modify the intensity of the signals sent by Alice or the efficiency of Bob's detector). In Eqn (2), we also have neglected the probability of emission of a signal with the number of photons $n > 2$. This assumption is reasonable, since very low-intensity pulses are used in our QKD setups ($\mu_{\text{pol}} = 0.02$ and 0.03). The estimated QBER in single-photon pulses, under the assumption that all errors appear only in those pulses, is given by the expression

$$\hat{q}_1 = \frac{q}{\hat{Y}_1}, \tag{3}$$

where q is the QBER value obtained at the parameter estimation stage.

After calculating the length of the final key (for each verified block), according to the method presented in [16], privacy amplification can be performed: the block of the secret key is calculated as a result of applying a universal hash function of the second order to the verified key. In our post-processing procedure, the Toeplitz hashing is used [28, 29]. The resulting key is called a secret key.

5. Finally, the parties check the authenticity of their classic channel by exchanging hash values of the entire incoming traffic. In our system, we use the Toeplitz hashing in combination with a one-time pad. The hash value length l_{auth} is set equal to 40 bits, which limits the probability of a successful man-in-the-middle attack at the level

$$\epsilon_{\text{auth}} = 2 \times 2^{-l_{\text{auth}}} < 2 \times 10^{-12}. \quad (4)$$

If authentication is completed, the parties reserve $2l_{\text{auth}}$ bits of their secret keys for the next post-processing stage. Then we obtain the expression:

$$L_{\text{fin}} = L_{\text{sec}} - 2\,l_{\text{auth}}, \quad (5)$$

where L_{fin} is the number of bits of the final key that can be used for cryptographic purposes. This is the final product of the QKD.

The secrecy level of the final key has the form

$$\epsilon_{\text{QKD}} = \epsilon_{\text{ver}} + \epsilon_{\text{pa}} + \epsilon_{\text{auth}} < 2.3 \times 10^{-11}. \quad (6)$$

Note that the secrecy level of the key distributed over the QKD network with N nodes is determined by the expression:

$$\epsilon_{\text{QKD Net}} = (N-1)(\epsilon_{\text{QKD}} + \epsilon_{\text{auth}}). \quad (7)$$

Here, the additional term ϵ_{auth} is stipulated by the need for additional authentication. For our QKD network with $N = 3$, we have $\epsilon_{\text{QKD Net}} < 5 \times 10^{-11}$.

The generation rate of the final secret key of length L_{fin} can be defined as:

$$R_{\text{fin}} = \frac{L_{\text{fin}}}{\tau}, \quad (8)$$

where τ is the time required for generation. By applying our post-processing procedure to the experimentally generated keys, we find that the first QKD link provides a key exchange over 30 km with a final key generation rate of about 0.02 Kbit s^{-1}. The second QKD link allows secret keys to be generated at a distance of more than 15 km, the generation rate of the final key being approximately 0.1 Kbit s^{-1}. We should note that the key generation rate in the trusted repeater's paradigm is limited by the minimum generation rate in all links used. Thus, for our QKD network, the key generation rate between User 1 and User 3 constitutes about 0.02 Kbit s^{-1}.

The main application of quantum-distributed keys is the continuous key renewal in the currently available symmetric encryption devices. Russian encryption standards assume the use of keys with a length of 256 bits, and therefore, taking into account the use of QKD networks, these keys can be refreshed approximately every 14 s. This refresh period is limited by the rate of key generation.

4. Conclusions

We have described in detail the implemented QKD networks based on the trusted repeater's paradigm. The developed QKD network has been tested using standard fibre-optic communication lines in Moscow. It is important to note that the network connects users with two different optical schemes of phase and polarisation encoding.

In designing the network, we have used a 'dark' fibre, laid jointly with the communication lines in use, which produce parasitic illumination at the telecommunication wavelength. One of the network links represents a device based on a single-pass scheme of key distribution. This scheme, in contrast to an auto-compensating one, allows one to send continuous sequences of pulses; however, it requires stabilisation relative to the fluctuation of the polarisation state in the quantum channel, caused by external factors (mechanical and thermal effects). Unlike the laboratory conditions, tests in a real urban communication line require regular adjustment of parameters and calibration. The tests confirmed the capability of the system to compensate for external impacts in conditions of real urban communication lines [21], which allows, in the future, these devices to be integrated into the existing infrastructure.

The main application of such quantum keys is the continuous key renewal in currently available symmetric encryption devices.

Acknowledgements. The work was supported by the Russian Science Foundation (Grant No. 17-71-20146).

References

1. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys*., **74**, 145 (2002).
2. Lo H.-K., Curty M., Tamaki K. *Nat. Photonics*, **8**, 595 (2014).
3. Diamanti E., Lo H.-K., Yuan Z. *npj Quantum Information*, **2**, 16025 (2016), doi: 10.1038/npjqi.2016.25.
4. Salvail L., Peev M., Diamanti E., Alleaume R., Lütkenhaus N., Laenger T. *J. Comput. Sec.*, **18**, 61 (2010).
5. Elliott C., Colvin A., Pearson D., Pikalo O., Schlafer J., Yeh H. *Proc. SPIE*, **5815**, 138 (2005).
6. Peev M. et al. *New J. Phys*., **11**, 075001 (2009).
7. Stucki D., Legre M., Buntschu F., Clausen B., Felber N., Gisin N., Henzen L., Junod P., Litzistorf G., Monbaron P., Monat L., Page J.-B., Perroud D., Ribordy G., Rochas A., Robyr S., Tavares J., Thew R., Trinkler P., Ventura S., Voirol R., Walenta N., Zbinden H. *New J. Phys*., **13**, 123001 (2011).
8. Chen T.-Y., Liang H., Liu Y., Cai W.-Q., Ju L., Liu W.-Y., Wang J., Yin H., Chen K., Chen Z.-B., et al. *Opt. Express*, **17**, 6540 (2009).
9. Chen T.-Y., Wang J., Liang H., Liu W.-Y., Liu Y., Jiang X., Wang Y., Wan X., Cai W.-Q., Ju L., Chen L.-K., Wang L.-J., Gao Y., Chen K., Peng C.-Z., Chen Z.-B., Pan J.-W. *Opt. Express*, **18**, 27217 (2010).
10. Wang S., Chen W., Yin Z.-Q., Zhang Y., Zhang T., Li H.W., Xu F.-X., Zhou Z., Yang Y., Huang D.-J., Zhang L.-J., Li F.-Y., Liu D., Wang Y.-G., Guo G.-C., Han Z.-F. *Opt. Lett*., **35**, 2454 (2010).
11. Sasaki M. et. al. *Opt. Express*, **19**, 10387 (2011).
12. Frohlich D., Dynes J.F., Lucamarini M., Sharpe A.W., Yuan Z., Shields A.J. *Nature*, **501**, 69 (2013).
13. Zhang Q. http://spectrum.ieee.org/telecom/security/chinas-2000km-quantum-link-is-almost-complete.
14. Kiktenko E.O., Pozhar N.O., Anufriev M.N., Trushechkin A.S., Yunusov R.R., Kurochkin Y.V., Lvovsky A.I., Fedorov A.K. ArXiv:1705.09258.
15. Sokolov A.S., Miller A.V., Kanapin A.A., Rodimin V.E., Losev A.V., Trushechkin A.S., Kiktenko E.O., Pozhar N.O., Fedorov A.K., Kurochkin V.L., Kurochkin Y.V. ArXiv:1612.04168.

16. Kiktenko E.O., Trushechkin A.S., Kurochkin Y.V., Fedorov A.K. *J. Phys. Conf. Ser.*, **741**, 012081 (2016).
17. Kiktenko E.O., Trushechkin A.S., Lim C.C.W., Kurochkin Y.V., Fedorov A.K. ArXiv:1612.03673.
18. Kiktenko E.O., Trushechkin A.S., Anufriev M.N., Pozhar N.O., Fedorov A.K. https://dx.doi.org/10.5281/zenodo.200365 (2016).
19. ID Quantique, www.idquantique.com.
20. Bennet C.H., Brassard G. *Proc. IEEE Intern. Conf. Computers, Systems and Signal Processing* (Bangalore, India) (New York: IEEE, 1984) p. 175.
21. Duplinskiy A., Ustimchik V., Kanapin A., Kurochkin Y. *Proc. SPIE*, **10224**, 102242W (2016).
22. Kurochkin V.L., Kurochkin Y.V., Miller A.V., Sokolov A.S., Kanapin A.A. *Proc. SPIE*, **10224**, 102242U (2016).
23. Gallager R. *IRE Trans. Inf. Theory*, **8**, 21 (1962).
24. MacKay D.J.C. *IEEE Trans. Inf. Theory*, **45**, 399 (1999).
25. Krovetz T., Rogaway P. *Lect. Notes Comp. Sci.*, **2015**, 73 (2001).
26. Kiktenko E.O., Trushechkin A.S., Fedorov A.K. ArXiv:1705.06664 [quant-ph].
27. Lutkenhaus N. *Phys. Rev. A*, **61**, 052304 (2000).
28. Krawczyk H. *Lect. Notes Comp. Sci.*, **839**, 129 (1994).
29. Krawczyk H. *Lect. Notes Comp. Sci.*, **921**, 301 (1995).