Quantum key distribution (QKD) provides theoretical information security in communication based on the laws of quantum physics. In this work, we report an implementation of quantum-secured data transmission in the infrastructure of Sberbank of Russia in standard communication lines in Moscow. The experiment is realized on the basis of already deployed urban fiber-optics communication channels with significant losses. We realize the decoy-state BB84 QKD protocol using the one-way scheme with polarization encoding for generating keys. Quantum-generated keys are then used for continuous key renewal in the hardware devices for establishing a quantum-secured VPN Tunnel between two offices of Sberbank. The hybrid approach used offers possibilities for long-term protection of the transmitted data; it is promising for integrating in the already existing information security infrastructure.

Keywords: quantum key distribution, urban fiber-optics channels, polarization encoding.

1. Introduction

Recent progress in creating quantum algorithms faces a serious threat on the central element of currently used tools for ensuring information security – the key distribution infrastructure. The majority of methods for key distribution is based on the assumption of the computational complexity of several mathematical tasks, such as large number factorization [1]. However, Shor’s algorithm for a quantum
computer allows solving these problems in a polynomial time [2]. Moreover, the absence of an efficient classical (nonquantum) algorithm breaking such public-key cryptosystems still remains unproved.

Quantum computers have less of an effect on symmetric cryptographic primitives, such as GOST block cipher, if it is assumed that the master key has been distributed secretly, since Shor’s algorithm does not apply, and then exponential speedups are not expected [2]. Nevertheless, Grover’s search algorithm [3] would allow quantum computers a quadratic speedup in brute force search, which means that the key management in terms of the key size and the key refresh time for such primitives needs to be reconsidered.

An ultimate and practical solution for the key distribution problem is the QKD technology. The QKD method employs the possibility to encode information in states of single photons, transmit them through optical channels, and measure on the receiver side [4–6]. By virtue of a number quantum-mechanical phenomena, this allows one to exclude possibilities for undetectable eavesdropping [4]. It is important to note that the method for preparation and measurements of quantum states, the so-called QKD protocol, should guarantee the absence of undetectable eavesdropping. Presently, decoy-state BB84 QKD is a standard technique, which provides security and significant key rates for a large distance between parties [7–14].

In this work, we report the experimental demonstration of quantum-secured data transmission in standard communication lines in Moscow. Due to significant losses in the urban fiber-optics communication lines, we use recently suggested one-way scheme of key distribution with fast polarization encoding [15]. The setup is based on LiNbO$_3$ phase modulators, single-laser source for states generation, and two single-photon detectors (see Fig. 1). An important improvement in comparison with recent experiments on realizing three-node QKD network in Moscow [16] is the inclusion of an intensity modulator in the optical scheme, as well as updating control units and post-processing software for the implementation of the decoy-state QKD protocol. Quantum-generated keys are then used for continuous key renewal in the hardware devices for establishing quantum-secured VPN Tunnel by Amicon [17]. The used fiber-optics communication lines are deployed between the Sberbank office on Bol’shaya Andron’yevskaya Street (Alice) and the Sberbank office on Vavilov Street (Bob); one is used for QKD and other, for information transmitting.

**Fig. 1.** Setup for quantum key generation using the polarization-encoding scheme with the light source L1, intensity modulator IM, half-wave plate $\lambda/2$, phase modulators PM1 and PM2, variable optical attenuator VOA, synchronization laser L2, analyzing detector AD, wavelength-division multiplexing filter WDM, polarization controller PC, synchronization detector SD, quantum channel (urban fiber-optics channel) QC, polarization beam splitter PBS, and single-photon detectors SPD1 and SPD2. The polarization maintaining fiber is used for connections between L1 and PM1 for Alice, and between PM2 and PBS for Bob.
2. Experiment

The optical scheme (Fig. 1) realizing decoy-state BB84 QKD works as follows [15].

The laser source (L1) emits polarized optical pulses at 1,550 nm. Then polarization controller transforms the polarization state so that the amplitudes along the crystal axes of Alice’s phase modulators (PM1 and PM2) are equal to each other. This allows Alice to encode bits of the secret key in polarization states with the help of the modulator. To weaken the pulse, a variable optical attenuator (VOA) is used. After the quantum channel (QC), the piezo-driven polarization controller (PC) compensates the state of polarization (SOP), drifts, and rotates it so that the polarization components along the lithium niobate crystal axes switch places, compensating the birefringence of LiNbO₃. Bob’s modulator PM2 is used for basis selection. Finally, a half-wave plate (λ/2) converts SOP for polarization beam splitter (PBS) to distinguish states with the help of single-photon detectors (SPD1 and SPD2).

The decoy-state QKD protocol is realized employing intensity modulators. Polarization recalibration is applied once quantum bit error rate (QBER) in decoy pulses rises above the 8% value. Then the gradient descent algorithm is applied for polarization controller to minimize the QBER. As soon as QBER over all types of pulses is under 5.5%, the calibration is over, and key generation is restarted.

![Diagram of QKD technology stack](image)

**Fig. 2.** QKD technology stack, where control units realize the decoy-state QKD protocol. As a result of their work, raw quantum keys go to the basis reconciliation and to the post-processing procedures realized on conjugation units. After these stages, final secret keys can be requested by Amicon devices for establishing VPN tunnels.
The parameters of the QKD setup implementation are as follows: number of pulses in train $9.82 \cdot 10^4$, repetition rate of pulses in train $312.5$ MHz, detector efficiencies $10\%$ and $6.4\%$ (for SPD1 and SPD2, respectively; see Fig. 1), detector’s dead time $5 \mu s$, dark count probability $3 \cdot 10^{-7}$, fiber channel losses $14.05$ dB in the channel of $25$ km length (which corresponds to $\approx 70$ km of standard fiber-optics communication line with $0.2$ dB/km losses), and additional losses on Bob’s side $6$ dB. The communication line between two server rooms consists of eight segments (six segments outside the buildings and two inside the buildings). Few connections give us $\approx 4\%$ of reflection. To prevent detector blinding, we separate clock synchronization signal and quantum signal not only in wavelength but also on time. The resulting raw key generation rate in our experiments is $\approx 2$ kbit/s. After performing the QKD session, we realize the standard sifting procedure, which is needed for dropping the positions with inconsistent bases from the raw quantum keys, using the authenticated communication channel (see below). The resulting keys are called sifted keys. The decoy state statistics [14] is announced at this stage as well.

3. Post-Processing Procedure and Application Level

The sifted keys are the input for a post-processing procedure [18]. The post-processing procedure includes a number of stages: information reconciliation, parameter estimation, privacy amplification and, finally, authentication check. First, sifted keys from the hardware devices go through the information reconciliation stage. We use the recently suggested symmetric blind information reconciliation method [19]. It uses low-density parity-check (LDPC) codes with frame length $l_{\text{frame}} = 4,000$. For a coarse tuning of the code rate, we employ a pool of LDPC codes consisting of nine codes with rates $R = \{0.9, 0.85, \ldots, 0.55, 0.5\}$. For fine tuning the code rate, we employ the shortening and puncturing techniques [20,21]. We note that the total number of shortening and puncturing bits was kept at constant level as follows:

\[
l_{\text{sp}} = 0.05 l_{\text{frame}} = 200 \text{ bits.}
\]  

(1)

The sub-block length of sifted key processed in a single launch of the symmetric blind reconciliation is

\[
l_{\text{sift}} = l_{\text{frame}} - l_{\text{sp}} = 3,800 \text{ bits.}
\]  

(2)

where $N_{\text{sift}} = 100$ sub-blocks of sifted keys were processed in parallel launches of the symmetric blind reconciliation method. The resulting length of the sifted key processed in one round of the post-processing procedure was $L_{\text{sift}} = 380,000$ bits.

After performing the information reconciliation stage, there is still a certain probability that uncorrected errors remain. In order to detect possible remaining errors, we use the subsequent verification protocol employing $\epsilon$-universal hash functions [22]. The probability of the presence of errors after successful verification of the block of $N_{\text{sift}}$ bits is bounded by the value of $\epsilon_{\text{ver}} = 1.4 \cdot 10^{-11}$ with the use of a hash-tag of 50 bit length. Due to the low level of frame error rate of the employed LDPC codes, we obtain the length of verified keys $L_{\text{ver}}$ to be almost always equal to the length of the processed sifted keys, $L_{\text{ver}} \approx L_{\text{sift}}$.

The next stage in the post processing is the parameter estimation stage. At this stage, the parties obtain the actual level of the QBER $q$ for their key blocks via direct comparison of the keys before and after information reconciliation. If the QBER value appears to be higher than the critical value needed for efficient privacy amplification ($11\%$ for the decoy-state BB84 protocol), the parties receive a warning message about possible eavesdropping. Otherwise, the verified key blocks go to the privacy amplification
Fig. 3. QBER (upper curve) and the length of final keys (lower curve) as functions of the generated block indices. Each block of the final key is obtained from a block of the sifted keys of $L_{sift} = 380,000$ bit’s length.

stage, and the estimated QBER is used in the next rounds of the information reconciliation stage. In our experiments, QBER was at the level of 4.8%–6%, so we were able to successfully implement the privacy amplification procedure.

The aim of the privacy amplification stage is to reduce potential information of an adversary about the verified blocks to a negligible quantity [4]. Such a reduction can be achieved by a contraction of the input verified key into a shorter key. The length of the secret key is computed as follows:

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

where $L_{ver}$ is length of the verified key, $\hat{Y}_1$ is an estimation of the portion of the sifted key bits generated from single photons pulses, $h(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$ is binary entropy function, $\hat{q}_1$ is an estimation of the QBER for single-photon pulses, leak_{ec} is total number of bits disclosed in information reconciliation and verification stages, and $\epsilon_{pa}$ is the failure probability of privacy amplification stages ($\epsilon_{pa} = 10^{-12}$ in our setup).

We obtained the estimates of $\hat{Y}_1$ and $\hat{q}_1$ using the decoy-states method. We employed three types of pulses with different intensities $\mu \approx 0.175$ (signal), $\nu \approx 0.067$ (decoy), and $\lambda \approx 0.008$ (vacuum). The corresponding probabilities of generating each type of pulses are $p_\mu = 0.5$ and $p_\nu = p_\lambda = 0.25$. We note that the sifted key was generated using signal pulses only [14]. The length of the secret key can then be calculated as a function of the following form:

$$L_{sec} = L_{sec}(L_{ver}, \mu, \nu, \lambda, N_\mu, n_\mu, N_\nu, n_\nu, N_\lambda, n_\lambda, q),$$

where $N_x$ and $n_x$ are the numbers of sent and detected states of intensity $x \in \{\mu, \nu, \lambda\}$. A detailed description of the function $L_{sec}$ can be found in [14].
After calculating the length of the secret key, the privacy amplification can be realized. In this step, the block of the secret key is computed as a result of application of the two-universal hash function to the verified key [18]. In our setup, we used the Toeplitz hashing. At the final state, the parties need to check the authenticity of their communications over the classical channel by an exchange of hash values of the whole incoming traffic. For this purpose, we employ the information-theoretically secure Toeplitz hashing together with one time-pad encryption [18]. The length of the hash value is \( l_{\text{auth}} = 40 \) bit, which bounds the probability of successful man in the middle attack at the level of

\[
\epsilon_{\text{auth}} = 2 \cdot 2^{-l_{\text{auth}}} < 2 \cdot 10^{-12}.
\]

If the authenticity is verified, the parties reserve \( 2l_{\text{auth}} \) bits of their secret quantum keys for the next post-processing round and obtain \( L_{\text{fin}} = L_{\text{sec}} - 2l_{\text{auth}} \) bits of the final key that can be used in cryptographic purposes. Then we obtain the length of the secret key \( L_{\text{fin}} \) to be \( 0.03 \ldots 0.13 \) of \( L_{\text{ver}} \) depending on QBER (see Fig. 3). The final security level of the obtained key is

\[
\epsilon_{\text{QKD}} = \epsilon_{\text{ver}} + \epsilon_{\text{pa}} + \epsilon_{\text{auth}} < 2 \cdot 10^{-11}.
\]

As a result, after the post-processing procedure, from 2 kbit/s of sifted keys we obtain \( \sim 0.1 \) kbit/s of secret keys. This value can be improved significantly by fine tuning the parameters of the decoy-state QKD protocol, stabilization of the hardware, and improving characteristics of the fiber-optics communication line.

After post processing, quantum-generated keys are used for continuous key renegotiation in the hardware devices for establishing quantum-secured VPN Tunnel. The VPN Tunnel performs L3-level encryption using the Russian symmetric block cipher algorithm (GOST 28147-89) with a 256 bit key size. In our experimental tests, hardware device establishing the VPN Tunnel was connected to the QKD setup via the Ethernet channel. Using the special API protocol, the VPN Tunnel device requests a new quantum key every 400 s, which adds to the master keys of the device. In the case of successful obtaining symmetric quantum-generated keys on both sides, the encryption of transmitted data is performed using both session and quantum keys, i.e., a hybrid scheme. Data transfer rate in the hybrid encryption scheme is \( \sim 1 \) Gbit/s. To our knowledge, this is a first in Russia experimental demonstration of quantum-secured data transmission in urban fiber-optics communication lines, while previously announced results were about implementations of QKD protocols only [23,24].

4. Conclusions

QKD technology provides the ultimate in quantum-safe security, guaranteeing provably secure key exchange for encryption and other security devices on point-to-point backbone, networks, and distributed ledgers, such as blockchains [25]. We emphasize that the realized hybrid approach, where quantum-generated keys are used for continuous key renewal in already existing information security solutions, offers the method for long-term data protection in the post-quantum era. Furthermore, we expect that using a high-quality fiber-optics communication line (e.g., with 0.2 dB/km loss coefficient) and improving all stabilization issues in hardware and software result in an increase in the key generation rate up to 100 kbit/s, which is enough for transmitting audio information in the one-time pad regime.
Acknowledgments

We express our gratitude to Mr. S. V. Lebed’, the head of Cybersecurity Division of the Sberbank and Mr. S. K. Kuznetsov, the Deputy Chairman of the Sberbank Board, as well as the colleagues from Amicon for their help in realizing this experimental work. The work was supported by the Russian Science Foundation under Grant No. 17-71-20146.

References

1. B. Schneier, *Applied Cryptography*, John Wiley, New York (1996).
2. P. W. Shor, *SIAM J. Comput.*, **26**, 1484 (1997).
3. L. K. Grover, in: *Proceedings of the 28th Annual ACM Symposium on the Theory of Computing* (New York, USA, 1996), p. 212.
4. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.*, **74**, 145 (2002).
5. H.-K. Lo, M. Curty, and K. Tamaki, *Nat. Photon.*, **8**, 595 (2014).
6. E. Diamanti, H.-K. Lo, and Z. Yuan, *Quantum Inforn.*, **2**, 16025 (2016).
7. W.-Y. Hwang, *Phys. Rev. Lett.*, **91**, 057901 (2003).
8. H.-K. Lo, X. Ma, and K. Chen, *Phys. Rev. Lett.*, **94**, 230504 (2005).
9. X.-B. Wang, *Phys. Rev. Lett.*, **94**, 230503 (2005).
10. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, *Phys. Rev. A*, **72**, 012326 (2005).
11. M. Curty, F. Xu, W. Cui, et al., *Nat. Commun.*, **5**, 3732 (2014).
12. C. C. W. Lim, M. Curty, N. Walenta, et al., *Phys. Rev. A*, **89**, 022307 (2014).
13. Z. Zhang, Q. Zhao, M. Razavi, and X. Ma, *Phys. Rev. A*, **95**, 012333 (2017).
14. A. S. Trushechkin, E. O. Kiktenko, and A. K. Fedorov, *Phys. Rev. A*, **96**, 022316 (2017).
15. A. Duplinskiy, V. Ustimchik, A. Kanapin, et al., *Opt. Express*, **25**, 28886 (2017).
16. E. O. Kiktenko, N. O. Pozhar, A. V. Duplinskiy, et al., *Quantum Electron.*, **47**, 798 (2017).
17. Amicon FSPU-IP, [https://www.amicon.ru/page.php?link=fpsu-ip].
18. E. O. Kiktenko, A. S. Trushechkin, Y. V. Kurochkin, and A. K. Fedorov, *J. Phys. Conf. Ser.*, **741**, 012081 (2016).
19. E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, et al., *Phys. Rev. Appl.*, **8**, 044017 (2017).
20. D. Elkouss, J. Martínez-Mateo, and V. Martin, “Secure rate-adaptive reconciliation,” in: *Proceedings of the IEEE International Symposium on Information Theory and its Applications (ISITA)*, IEEE, Taichung, Taiwan (2010), p. 179.
21. D. Elkouss, J. Martínez-Mateo, and V. Martin, *Quantum Inform. Comput.*, **11**, 226 (2011).
22. A. S. Trushechkin, E. O. Kiktenko, and A. K. Fedorov, Los Alamos arXiv:1705.06664 (2017).
23. K. A. Balygin, V. I. Zaitsev, A. N. Klimov, et al., *JETP Lett.*, **105**, 606 (2017).
24. A. V. Gleim, V. V. Chistyakov, O. I. Bannik, et al., *J. Opt. Tech.*, **84**, 362 (2017).
25. E. O. Kiktenko, N. O. Pozhar, M. N. Anufriev, et al., Los Alamos arXiv:1705.09258 (2017).