IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 6 December 2025, accepted 22 December 2025, date of publication 26 December 2025, date of current version 2 January 2026.

Digital Object Identifier 10.1109/ACCESS.2025.3648803

RESEARCH ARTICLE

Adaptation of Error Correction Procedures to the Time-Bin Quantum Key Distribution Protocol Implementation

VLADIMIR I. MOROZOV[1], MIKHAIL S. ELEZOV[1], OLEG O. EVSUTIN[1], AND ROMAN V. OZHEGOV[1,2,3]

[1]HSE University, 101000 Moscow, Russia
[2]NTI Quantum Communication Center, University of Science and Technology MISIS, 119049 Moscow, Russia
[3]JSC Superconducting Nanotechnology, 119021 Moscow, Russia

Corresponding author: Oleg O. Evsutin (oevsyutin@hse.ru)

This work was supported by the Basic Research Program at the National Research University Higher School of Economics (HSE University).

ABSTRACT Error correction is a crucial stage in quantum key distribution (QKD) protocols — a promising field of modern cryptography where the secrecy of the shared key information is guaranteed by the laws of quantum mechanics. Currently, there are many effective approaches to error correction in QKD. However, most of them, due to their generic nature, fail to leverage the specific features of particular protocol implementations. This work demonstrates that accounting for the hardware specifics of a QKD system implementing the time-bin protocol enables a significant increase in error correction performance. For the considered QKD system, we have experimentally obtained estimates of the Quantum Bit Error Rate (QBER) observed for each combination of bit and detector. The differences in the obtained estimates reveal that the quantum channel can be modeled as a non-uniform binary channel. Furthermore, based on computational experiments with a model of the quantum channel, it was established that adapting the error correction procedure to its properties can achieve up to a 2.7-fold reduction in the LDPC code decoding failure rate at low error levels.

INDEX TERMS Information security, quantum key distribution, error-correcting codes, time-bin protocol, non-uniform binary channel, quantum channel.

I. INTRODUCTION

The development of modern technologies opens new opportunities for cybersecurity. However, alongside cybersecurity tools, hacking methods are also advancing. The dramatic increase in computational power and the advancement of quantum computing pose a serious threat to cybersecurity. Given that most digital information today is protected cryptographically, the relevance of developing new, more robust protocols in this area is beyond doubt.

One of the most dangerous attacks against cryptographic protocols is the ''man-in-the-middle'' (MitM) attack. An eavesdropper connects to the communication channel and intercepts transmitted information without either legitimate participant detecting the intrusion. A variant of this attack occurs when the eavesdropper actively participates in the transmission, impersonating one of the legitimate parties. One promising method for countering such attacks is quantum key distribution (QKD). In QKD, the fundamental information carriers are quantum particles (typically photons), replacing traditional electrical signals. Information is encoded in the quantum states of these particles, such as phase, time of arrival, or polarization. Quantum particles obey the laws of quantum mechanics, including the no-cloning theorem [1]. This theorem states that it is impossible to create an identical copy of an arbitrary unknown quantum state. For QKD, this means an eavesdropper cannot measure the quantum state of a photon received from Alice and then

The associate editor coordinating the review of this manuscript and approving it for publication was Peng-Yong Kong.

prepare a new photon in the same state for transmission to Bob. Any such interception attempt would be easily detected with high probability.

Numerous protocols have been developed for the implementation of QKD systems, including BB84 [2], B92 [3], E91 [4], COW [5], MDI [6], among others.

The most prevalent and extensively studied protocol is BB84. A security proof of the protocol has been established [7]. Different physical parameters of quantum particles can be used to encode information: polarization [2], phase [8], [9], and arrival time of photon [10].

The main advantage of the BB84 protocol with polarization encoding is the relative simplicity of assembly and configuration, as well as the high stability of the optical schemes of the transmitter and receiver. However, its significant drawback is polarization distortions that occur when photons propagate in single-mode optical fiber. The polarization state of photons is randomly distorted due to polarization mode dispersion (PMD), temperature instability, mechanical vibrations, bends, and pressure on the fiber. These distortions are unstable and can change rapidly over time. Compensating for them requires an active polarization stabilization system, which leads to significant complication, increased cost, and reduced overall reliability of the QKD system [11].

Despite this, the BB84 protocol with polarization encoding has found its niche in quantum satellite communication. In the atmosphere and vacuum, polarization states are practically undistorted: atmospheric turbulence does not cause as chaotic and strong a change in polarization as in optical fiber. This is precisely why all successful experiments with satellite QKD systems (e.g., MICIUS [12]) were conducted using polarization encoding—due to its stability in space conditions and simplicity of implementation onboard a satellite [13], [14].

For the practical implementation of the BB84 protocol with phase encoding [8], interferometers are used in the transmitter and receiver. The transmitter randomly modulates the phase in one arm of the interferometer, and the receiver randomly chooses in which arm of its interferometer to introduce a phase shift to measure in one basis or the other. This protocol is widely used in commercial systems because maintaining phase stability in optical fiber networks is much easier than maintaining polarization stability. This eliminates the need for a complex and expensive active polarization stabilization system, sharply increasing reliability and simplifying system operation. Unlike polarization, the phase of a photon is less sensitive to external disturbances in optical fiber.

However, phase encoding also has its challenges: due to slow temperature drifts in interferometers, phase instability arises. To eliminate it, the interferometers must be thermally stabilized [15]. Furthermore, the receiver's interferometer must be perfectly matched to the transmitter's interferometer, and the path length difference in the receiver's interferometer must remain stable within a fraction of the photon's wavelength.

One variation of the BB84 protocol with phase encoding is the protocol with phase-time encoding [16] (time-bin protocol). Its main advantages are the insensitivity of the transmitted qubits to depolarization and polarization mode dispersion (PMD) in the quantum communication channel, as well as high resistance to environmental effects on optical fibers. Another important advantage of the time-bin protocol is its insensitivity to temperature fluctuations in the optical fiber interferometers for the Z-basis. Thus, the time-bin encoding is one of the most suitable options for use in commercial quantum key distribution systems over ultra-long distances via optical fiber with acceptable speed. In this work, we employ the BB84 protocol with phase-time encoding.

However, due to physical imperfections in both the transceiver hardware and the quantum channel, secure key generation faces significant limitations. Consider a quantum channel implemented using single-mode optical fiber. For quantum key distribution implementations, it is essential to account for the following intrinsic fiber characteristics: optical loss at the carrier wavelength, Rayleigh scattering, geometric imperfections (e.g., micro- and macrobends), various dispersion types, polarization distortions, and related phenomena. Furthermore, external factors such as temperature, atmospheric pressure, and mechanical stress impact fiber performance. This leads to an exponential increase in both bit-erasure errors and bit-flipping errors (quantified by the Quantum Bit Error Rate, QBER) within the distributed keys as the channel length increases [17], [18]. To suppress bit-erasure errors during key generation, highly accurate clocks synchronized between the communicating parties are utilized. Conversely, Error-Correcting Codes (ECC) are employed to mitigate bit-flip errors.

The results presented here are as follows. Firstly, we obtain, for the first time, statistical estimates of the QBER levels specific to each individual bit and detector combination within the time-bin protocol [16]. Secondly, we demonstrate enhanced efficiency in correcting bit-flipping errors within the key information. This improvement is achieved by refining the channel model using the obtained QBER estimates (i.e., considering the quantum channel as a non-uniform binary channel — NUBC). Thirdly, we propose a novel methodology for assessing error correction efficiency in non-uniform communication channels.

The paper is structured as follows. Section II provides a brief overview of existing quantum key distribution protocols and their employed error correction methods. Section III details the experimental setup implementing the time-bin protocol with decoy states [16]. Section IV describes the approach for channel model refinement and presents a series of experiments demonstrating the resulting enhancement in error-correcting code efficiency. This enhancement is quantified by a reduction in decoding failures at a given channel bit error rate. This section also discusses the experimental results. Finally, Section V summarizes the findings of this study.

II. RELATED WORKS

One of the main goals in developing quantum key distribution systems is to increase the key generation rate. Two principal approaches are employed to achieve this goal:

1) Enhancing the quality of quantum information transmission at the physical level. This can be accomplished, for example, by improving the hardware components or utilizing various characteristics of quantum carriers for information encoding and employing other related techniques.
2) Optimizing the post-processing of information received from the quantum channel. A key strategy within this approach is to increase the efficiency of the error-correcting code used to correct errors in the sifted key.

In the field of sifted key post-processing, two main research directions can be identified: works dedicated to continuous-variable quantum key distribution (CV-QKD) and discrete-variable (DV) QKD. The protocol considered in this paper implements DV-QKD; therefore, the following survey focuses on research in this area.

In the early stages of quantum cryptography development, researchers paid little attention to error correction in the sifted key. Error correction was not addressed in the seminal work of Bennett and Brassard [2]. Subsequent works [19], [20] employed the simplest algorithms based on parity checks of bit sequences. However, the efficiency of these algorithms is far from optimal, as they result in a significant portion of the key being discarded.

Modern approaches utilize more efficient error-correcting codes. Among these, Low-Density Parity-Check (LDPC) [21] and polar [22] codes have gained significant popularity. LDPC has high error-correcting capability, speed, and low requirements for network resources. A defining feature of LDPC codes is the low density of non-zero elements in their parity-check matrix, which enables relatively simple implementation of the encoding and decoding procedures. The remainder of this section is devoted to a more detailed examination of approaches to implementing modern error-correcting codes in quantum key distribution protocols.

A number of works [23], [24], [25], [26] focus on so-called blind information reconciliation. In this approach, the quantum bit error rate is not estimated prior to the error correction stage. Instead, an iterative procedure adjusts the code rate to achieve a high probability of correcting all errors. This adjustment employs puncturing [27] and shortening [28] techniques, widely used in error-correcting coding. These techniques require appending additional bits to the key information during error correction. Moreover, the authors of [23] note that this method necessitates a trade-off between throughput and error-correcting capability.

As an evolution of blind reconciliation, researchers in [29], [30] propose performing a rough preliminary QBER estimation—e.g., via syndrome analysis [30] or results from prior protocol iterations [29]. They then suggest selecting the initial code rate as a function of the estimated error rate. Furthermore, [30] introduces a scheme for additional key identity verification between transmitting and receiving parties. While these highly interactive approaches demonstrate significantly higher key generation rates compared to classical methods, such results are only shown for messages of tens of thousands of bits, which is not always feasible in QKD systems with link lengths exceeding 100 km.

Alongside reconciliation schemes requiring intensive communication (e.g., the CASCADE method [31] and its optimizations [32]), single-pass protocols have gained traction. Their distinguishing feature is that all necessary information is transmitted from Alice to Bob in a single message, eliminating further interaction. Building on foundational non-interactive key distribution approaches [33], [34], [35], the authors of [36] propose their own single-pass QKD scheme. Their method incorporates Wire Link Permutation (WLP), Cyclic Redundancy Codes (CRC), and Hamming codes to modify baseline algorithms. Among its advantages, the resulting protocol shows higher error-correction efficiency at high QBER levels compared to interactive schemes.

Other works [37], [38] explore modifications to the encoding procedure. Reference [37] partitions the sifted key into fixed-length short blocks and selects an optimal parity-check matrix for each block. Meanwhile, [38] employs a two-stage error correction: first using polar codes, followed by LDPC codes.

Some works significantly shift the balance between decoding speed and error-correction efficiency. For example, [39] prioritizes decoding speed but notes its negative impact on error-correcting capability. Conversely, [24] introduces intensive preprocessing of key information before decoding, enhancing correction efficiency at the cost of reduced speed.

Finally, at the intersection of physical and algorithmic innovations, studies [40], [41] address non-binary quantum key distribution protocols. These protocols replace qubits (carrying 1 bit) with qudits—systems with d states encoding $\log_2(d)$ bits. Non-binary LDPC codes are used to correct errors in such systems. In [40], authors achieve significant improvements in final key length (compared to binary approaches) using LDPC encoding and the CASCADE protocol, while [41] demonstrates even greater gains for large messages (3×10^4) by optimizing the weight distribution of the LDPC parity-check matrix.

A common trend across these works is the broad applicability of proposed error-correction methods. They are suitable for diverse QKD protocol implementations—an undeniable advantage, enabling reuse of existing algorithms in new schemes. However, such generalization prevents leveraging hardware-specific features of QKD systems when designing error-correcting codes. This work demonstrates how adapting codes to specific QKD implementations enhances error-correcting code performance—defined here

as the decoding failure rate (frame error rate — FER — the fraction of data blocks with uncorrected errors at a given channel bit error rate).

The information reconciliation protocol based on LDPC coding was selected for consideration in this article for the following reasons. Firstly, this approach is recommended in one of the seminal articles on the considered quantum key distribution protocol [16]. Secondly, recent reviews (e.g., [42]) note the LDPC-based approach to information reconciliation as "the most competitive among forward error correction protocols" for DV-QKD. Thirdly, as LDPC codes were introduced into widespread use some time ago, numerous works are dedicated to their adaptation to various characteristics of the information transmission medium, including non-uniform channels (e.g., [43], [44]). This enables further improvement of the approach proposed in this work. Moreover, LDPC codes are widely used in recent articles on information reconciliation for quantum key distribution (e.g., [30], [45]) and demonstrate good performance.

III. EXPERIMENTAL SETUP

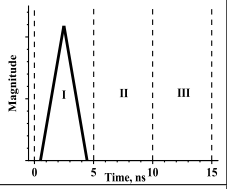
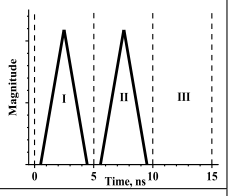
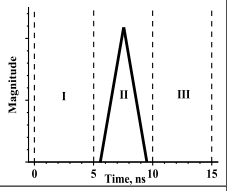
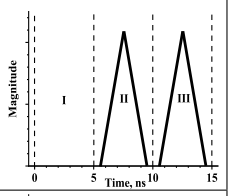
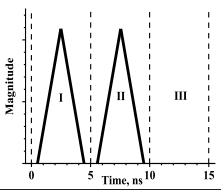
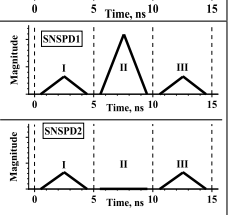
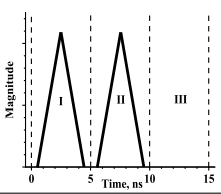
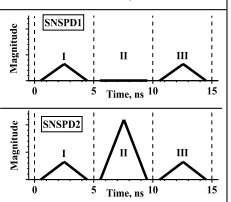
A. EXPERIMENTAL SETUP AND EXPERIMENT

We employ a quantum key distribution system operating over distances exceeding 200 km (see Fig. 1). The quantum channel consisted of a single-mode fiber SMF-28e with an average optical loss of 0.174 dB/km. The experiment was conducted under laboratory conditions. Optical pulse generation is performed by a Gooch & Housego AA1406 laser (wavelength 1550 nm, full width at half maximum (FWHM) spectral linewidth 1 MHz) operating in continuous wave mode, and an intensity modulator (bandwidth 10 GHz) with a repetition rate of 5 MHz. The pulse FWHM duration is 2 ns. After passing through two beam splitters and a delay line DL1, the pulse is split into two with a temporal interval of 5 ns. Using a variable fiber optic attenuator, we set the optical pulse power to 0.25 photons per pulse.

Since strongly attenuated radiation is used instead of a single-photon source to generate quantum states, the photon distribution per pulse follows the Poisson distribution $P(\mu, n) = \frac{\mu^n}{n!}e^{-\mu}$, where μ is mean photon number and $n = 0, 1, 2, \ldots$ At $\mu = 0.25$, the fraction of single-photon pulses relative to the total number of non-empty pulses is approximately $\frac{P(0.25,1)}{1-P(0.25,0)} \approx 88\%$. The proportion of multi-photon pulses is $\frac{1-P(0.25,0)-P(0.25,1)}{1-P(0.25,0)} \approx 12\%$. This is sufficient to counter a potentially possible photon number splitting attack [46] and satisfies requirements for the optimal average number of photons in a protocol with decoy states [47].

The receiver of the QKD system employs a passive fiber-optic scheme incorporating a delay line DL3 (5 ns), a 50:50 beam splitter, a circulator, two Faraday mirrors, and two Superconducting Nanowire Single-Photon Detectors (SNSPDs or SSPDs) with a quantum efficiency of 65% and dark count rates of 0.5 Counts Per Second (cps). Passive basis choice for qubit state measurement is implemented using a fiber beam splitter with a fixed 50:50 splitting ratio. To simplify the experiment, this ratio is fixed for all measurements and not optimized for the specific quantum channel length. Photon detection events were registered using a time-correlated single-photon counting (TCSPC) system. Synchronization between the transmitter and receiver was ensured electrically.

TABLE 1. Encoding of quantum states.

Basis, bit	Quantum state	Transmitted temporal mode	Received temporal mode
Z,0	$\|\psi_0\rangle$		
Z,1	$\|\psi_1\rangle$		
X,0	$\|\psi_+\rangle$		
X,1	$\|\psi_-\rangle$		

In the Z-basis, Alice encodes bits "0" and "1" as states $|\psi_0\rangle$ and $|\psi_1\rangle$, respectively. In the X-basis, she encodes them as: $|\psi_+\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle + |\psi_1\rangle)$ and $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|\psi_0\rangle - |\psi_1\rangle)$. The X-basis can be used for additional quantum state transfer ($|\psi_+\rangle, |\psi_-\rangle$) or for eavesdropper information estimation ($|\psi_+\rangle$) [15]. Each quantum state corresponds to specific temporal modes (see Table 1). There are QKD implementations that use three or four BB84 states. In the general case, four quantum states are used.

Photon-qubit state encoding is implemented using the BB84 protocol with time-bin encoding [16]. This protocol offers undeniable advantages: the transmitted qubits are insensitive to depolarization and polarization mode dispersion (PMD) in the quantum communication channel, making it ideal for ultra-long-distance QKD systems.

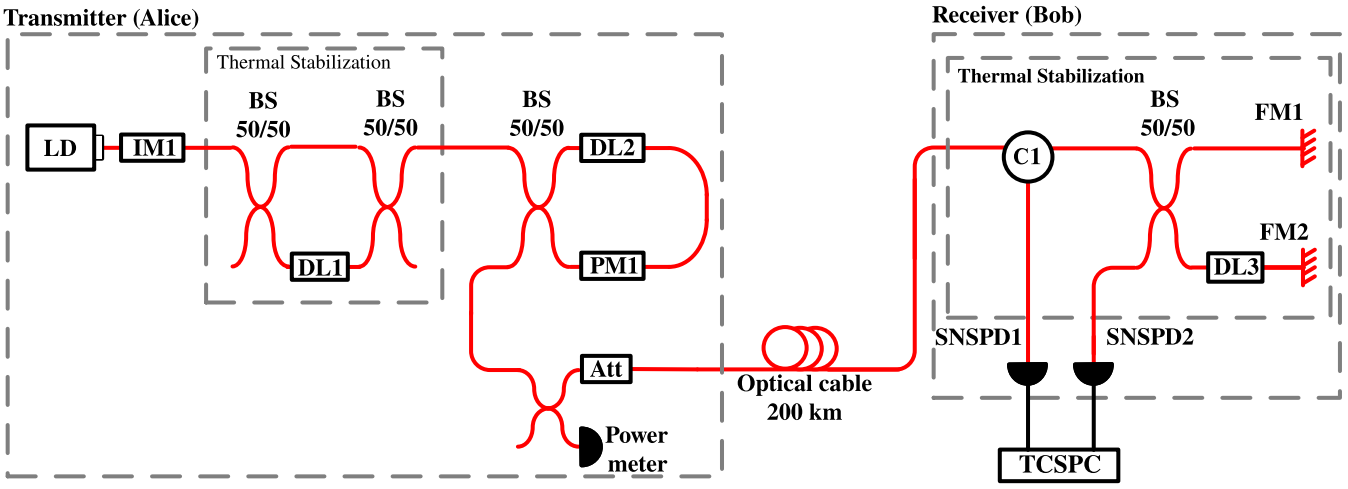


FIGURE 1. Optical scheme QKD system over 200 km. LD — laser, DL1 and DL3 — delay lines 5 ns, DL2 — delay lines 10 ns, BS 50/50 — beamsplitter 50:50, PM1 — phase modulator, IM1 — intensity modulator, C1 — circulator, SNSPD1 and SNSPD2 — superconducting single-photon detectors, FM1 and FM2 — Faraday mirror.

Upon measurement by the receiver, the temporal modes of a quantum state are transformed. On the receiver side, the shape of the transformed temporal mode depends on the received quantum state and a detector number. Bob measures the qubits in the Z or X basis with the same probabilities.

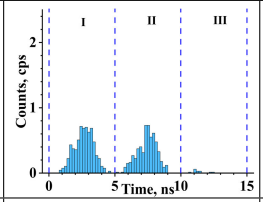
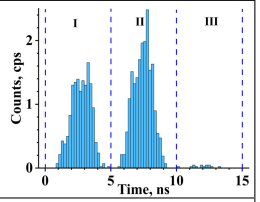
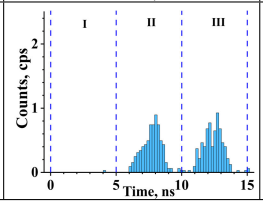
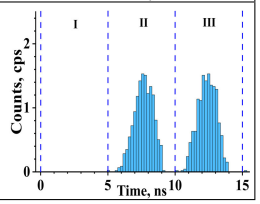
The receiver's optical scheme is designed for passive basis choice during the measurement of a photon's quantum state. Assume Alice transmits the quantum state $|\psi_0\rangle$, with its temporal mode occupying the first time interval. The measurement is performed by an unbalanced Michelson interferometer at the receiver, featuring an arm delay of 2.5 ns. Within the interferometer, the input optical pulse is divided into two pulses with this specific delay. Consequently, at each output of the interferometer, the shape of the quantum state's temporal mode is transformed, as shown in Table 1. Bob measures the arrival time of the photon for the Z basis, and the value of the bit does not depend on a detector number. The X basis is measured by the arrival time of the photon and the number of a detector. On the receiver side the rule is used: If a photon was registered in time bin I by detectors SNSPD1 or SNSPD2, we assign the state $|\psi_0\rangle$, corresponding to bit value "0". If registered in time bin III by SNSPD1 or SNSPD2, we assign state $|\psi_1\rangle$, corresponding to bit value "1". If registered in time bin II by SNSPD1, we assign state $|\psi_+\rangle$, corresponding to bit value "0". If registered in time bin II by SNSPD2, we assign state $|\psi_-\rangle$, corresponding to bit value "1". Thus, for quantum state $|\psi_0\rangle$ Bob can choose the Z basis or the X basis, because SNSPD1 or SNSPD2 can detect a photon in the first or second bin, i.e., the passive basis choice is independent of the input quantum state.

Of course, ideally, the shapes and amplitudes of the temporal modes for each time bin should be identical. However, in practice, due to deviations from the ideal 50:50 beamsplitter ratio and differential optical losses in the interferometer arms, the temporal modes cannot be perfectly identical in shape and amplitude. As a result, the photon detection probability differs between the both time bins, meaning the probabilities for choosing a measurement basis will differ. An analogous situation occurs for the second quantum state, $|\psi_1\rangle$. These imperfections in the receiver's optics and the transmitted pulses can raise concerns regarding the security of the QKD system. It is important to note that standard security proofs using complementarity, as well as those based on entropic uncertainty relations, are directly applicable to the passive protocol only under the condition of a balanced basis choice [48]. The work by [49] presents a security proof for the BB84 protocol with decoy states and passive basis choice against coherent attacks in the asymptotic regime. This proof is based on a complementarity approach [50].

In our work, the use of only the Z-basis ($|\psi_0\rangle$, $|\psi_1\rangle$) is sufficient. The transmitter sends a sequence of photons, each prepared strictly in the quantum state $|\psi_0\rangle$ or $|\psi_1\rangle$. The key generation time for each state was approximately 24 hours. The quantum state $|\psi_0\rangle$ corresponds to photon time bins in the first and second bins, while state $|\psi_1\rangle$ corresponds to bins in the second and third bins.

Quantum state determination followed this rule: If a photon was registered in time bin I by detectors SNSPD1 or SNSPD2, we assign the state $|\psi_0\rangle$, corresponding to bit value "0". If registered in time bin III by SNSPD1 or SNSPD2, we assign state $|\psi_1\rangle$, corresponding to bit value "1." Photons registered by SNSPD1 or SNSPD2 in the second time bin yield an undefined measured quantum state; these events are subsequently discarded during key formation. Events in the second time bin indicate quantum state uncertainty; such data are excluded from the generated sifted key.

TABLE 2. Photocount histograms for measured quantum states.

Quantum state	Photocount histogram for SNSPD1	Photocount histogram for SNSPD2
$\|\psi_0\rangle$		
$\|\psi_1\rangle$		

B. MEASURING OF STATISTICAL CHARACTERISTICS OF QUANTUM CHANNEL

The key hardware property investigated in this work is the asymmetry of bit-flipping errors observed when measuring bits with detectors SNSPD1 and SNSPD2. To measure the error rate for each "bit-detector" combination, the following procedure was performed.

During the first stage, only bits with value "0" were transmitted over the quantum channel for an extended period. On the receiver side, the value and detector number registering each received bit were recorded. The photocount histograms for states $|\psi_0\rangle$ and $|\psi_1\rangle$ are presented in Table 2. Thus, a total of n bits were received during the entire measurement period. These bits were then divided into two groups of approximately $n/2$ bits each: a group of bits detected by SNSPD1 and a group detected by SNSPD2. For these groups, the bit-flipping error rates (QBER) for the transmitted "0" bit and corresponding detector were calculated: e_{01} and e_{02}, respectively. The error rate notations adopted in this work are presented in Table 3.

Each error rate was calculated as the ratio of erroneously received bits in the group (i.e., those measured as "1" at the receiver) to the total number of bits in the group.

During the second stage, only bits with value "1" were transmitted analogously over the quantum channel. Their QBER values were similarly calculated: e_{11} and e_{12}.

Critically, unlike a binary symmetric channel, in our case $e_{01} \neq e_{02} \neq e_{11} \neq e_{12}$. Thus, we can consider our channel as consisting of 4 parallel sub-channels, formed by the 4 different combinations of the bit value and the detector number. In the works [43], [44], channels with such properties are proposed to be called non-uniform channels. Following this notation, we refer to our channel as a non-uniform binary channel — NUBC (by analogy with the binary symmetric channel — BSC), to emphasize its distinction from non-uniform channels with additive white Gaussian noise.

Generally, the QBER cannot be identical for each quantum state (bit). Numerous factors influence QBER magnitude, classifiable as internal and external. External factors include background radiation — external light penetrating the optical fiber from free space. A key characteristic of background radiation is its non-stationary nature, determined by the properties and behavior of external light sources. Internal factors affecting QBER are significantly more numerous. These include intrinsic detector noise (dark counts) and imperfections in the optical circuits of the transmitter and receiver in the QKD system. Detector noise levels can be substantially reduced to ≤ 0.5 cps using low-noise detectors such as SNSPDs.

The concept of optical circuit "imperfection" is broad and encompasses many influences. We identify several key parameters affecting QBER:

1) Optical losses in the fiber, caused by absorption and scattering of photons, lead to a decrease in the optical signal power as it propagates. For the single-mode fiber used in this work at a wavelength of 1550 nm, the attenuation coefficient is approximately 0.174 dB/km. The fraction of photons registered by the receiver, and consequently, the sifted key rate, decreases exponentially with distance: $\approx e^{-\alpha L}$, where α is the attenuation coefficient. Meanwhile, the detector's dark count rate remains constant. As a result, the signal-to-noise ratio decreases over long distances.
Since dark counts of a detector are random and, with a 50% probability, lead to the selection of an incorrect basis (and thus an erroneous bit). They directly contribute to the QBER. In our work, to estimate the contribution to the QBER from detector dark counts, we employed low-noise superconducting single-photon detectors with a dark count rate of 0.5 cps. Its contribution to the QBER can be calculated using formula: $QBER = \frac{\Delta t \cdot f \cdot \mathrm{DCR}}{r_{\mathrm{sift}} + 2\Delta t \cdot f \cdot \mathrm{DCR}}$. Where Δt is the time bin width 5 ns, the sifted key rate is $r_{\mathrm{sift}} \approx$ 30 bit/s, DCR is the dark count rate 0.5 cps, and f is the repetition rate 5 MHz. The theoretical value for the noise contribution to the QBER is 0.00042. As the length of the optical channel increases, the contribution of detector noise to the QBER grows. However, at the distance of 200 km used in this experiment, this contribution is minimal and does not have a decisive impact on the total QBER.
There is another parameter that can potentially influence the QBER over long distances. Single-mode optical fiber exhibits dispersion, which causes the spectral components of an optical pulse to travel at different velocities, leading to pulse broadening. The magnitude of pulse broadening is proportional to the fiber length L (for chromatic dispersion) and to $\sqrt{L}$ (for broadening related to polarization mode dispersion). When propagating over long distances through an optical fiber, the broadened pulses become larger than

the time bin width and begin to overlap with each other. Furthermore, in the time-bin protocol, this degrades the interference visibility, which also increases the QBER. However, no significant pulse broadening was observed in the presented work.

2) Back-reflections at high-reflection-point inhomogeneities in the optical path (fiber connections, active elements, etc.). Back-reflections become impactful if they fall within the first three time bins, which is particularly critical.
3) Imperfect optical pulse shaping in the transmitter. Pulses are generated using a 1550 nm continuous-wave laser and a high-speed fiber-optic intensity modulator (IM). The IM's maximum modulation depth is approximately 35 dB. However, in practice, due to device specifics, the modulation depth does not exceed 30 dB. Furthermore, optical pulse distortion can be caused by impedance mismatch in the RF electrical path between the intensity modulator and driving generator. This mismatch distorts the driving electrical pulse shape, which in turn produces a more complex optical pulse waveform and may cause afterpulsing. Such pulses can exceed the time bin boundaries and cause bit inversion errors. This effect can explain the QBER difference between the two quantum states ("0" and "1"). It should also be noted that the intensity modulator is a Mach-Zehnder interferometer (MZI) whose phase stability is highly temperature-dependent. Therefore, a bias controller with DC feedback is used for phase stabilization.
4) Generation of two coherent pulses at the output of an unbalanced Mach-Zehnder interferometer. Although the temporal separation between pulses is 2.5 ns, pulse overlap (interference) creates an interference pattern that varies over time. A similar effect occurs at the receiver side, where the interference pattern becomes more complex, leading to intricate QBER dynamics.

TABLE 3. Bit inversion and LLR calculation rules.

Bit value x_i	SNSPD number d_i	Inversion probability	LLR value
0	1	e_{01}	$\log((1-e_{01})/e_{11})$
0	2	e_{02}	$\log((1-e_{02})/e_{12})$
1	1	e_{11}	$\log(e_{01}/(1-e_{11}))$
1	2	e_{12}	$\log(e_{02}/(1-e_{12}))$

IV. METHODOLOGY FOR ASSESSING ERROR-CORRECTING CODE PERFORMANCE IN NON-UNIFORM BINARY QUANTUM CHANNELS

To demonstrate the performance improvement of ECC when accounting for different QBER, a mathematical simulation was performed using a simulation model of a QKD system.

The QKD simulation model is a software tool that allows for modeling the transmission of randomly generated quantum states through a noisy channel, their equiprobable detection, and the error correction process. The software implementation of the model enables saving the results of each simulation for subsequent statistical analysis. Moreover, the simulator allows switching between binary symmetric and non-uniform binary models of quantum channels. All parameters of the simulation model correspond to those of the experimental setup.

Within the simulation model, two quantum states were transmitted and detected by two single-photon detectors. Thus, for each detector, two QBERs are obtained, corresponding to the two detected quantum states.

The bit sequence generated at each iteration of the following experiment was processed in two methods. In the first method, the data transmission channel was considered a binary symmetric channel. For this purpose, the average QBER $e = (e_{01} + e_{02} + e_{11} + e_{12})/4$ was used in the calculations, and the Frame Error Rate (FER) was computed. FER is defined as the fraction of error correction attempts in which the decoder fails. In the second method, the data transmission channel was treated as a non-uniform binary channel. Each received bit was associated with one of the four QBERs, depending on the bit value and the detector that registered the state carrying this bit. During the error correction process, one QBER was selected as a variable parameter, while the others were fixed. The variable level was then adjusted within specified limits with a given step size, and the FER was calculated for each of its values.

Prior to the calculations, the following constants were fixed:

- $a_{\max}$ — the maximum number of decoding attempts after which FER is calculated.
- $f_{\max}$ — the maximum number of decoding failures after which FER is calculated.
- I — the number of calculation repetitions with the same QBER value to obtain a statistically significant dataset.
- i and j — the bit value and detector number for which the QBER value is varied, where $i \in \{0, 1\}, j \in \{1, 2\}$.
- e_{first}, e_{last} — the initial and final values of the variable QBER, respectively.
- e_{step} — the step size for varying the QBER.

The algorithm for FER calculation is presented in the following pseudocode:

$e_{ij} \leftarrow e_{\text{first}}$
while $e_{ij} < e_{\text{last}}$ **do**
  for iter $\leftarrow 0$ to I **do**
    $f \leftarrow 0$ {Number of failed decoding attempts}
    $a \leftarrow 0$ {Total number of decoding attempts}
    while $f \neq f_{\max}$ **and** $a \neq a_{\max}$ **do**
      $\mathbf{x} \leftarrow (x_1, x_2, \ldots, x_n) | \forall k = \overline{1, n} : P(x_k = 0) = P(x_k = 1) = 0.5$
      $\mathbf{d} \leftarrow (d_1, d_2, \ldots, d_n) | \forall k = \overline{1, n} : P(d_k = 1) = P(d_k = 2) = 0.5$
      $\mathbf{y} \leftarrow \text{rinv}(\mathbf{x}, \mathbf{d})$
      $\mathbf{s} \leftarrow \mathbf{x}\mathbf{H}^T$ {LDPC-code syndrome}

11: $\mathbf{l} \leftarrow (l_1, l_2, \ldots, l_n) | \forall k = \overline{1,n} : l_k = \log\frac{P(x_k=0|y_k)}{P(x_k=1|y_k)}$ {LLR values from Table 3}
12: result $\leftarrow$ msdecode($\mathbf{l}$, $\mathbf{s}$, $\mathbf{H}$)
13: **if** result = FAIL **then**
14: $f \leftarrow f + 1$
15: **end if**
16: $a \leftarrow a + 1$
17: **end while**
18: $\mathrm{FER}_{\mathrm{iter}}(e) \leftarrow f/a$
19: **end for**
20: $\mathrm{FER}(e) \leftarrow \mathrm{avg}(\mathrm{FER}_1(e), \mathrm{FER}_2(e), \ldots, \mathrm{FER}_I(e))$
21: $e_{ij} \leftarrow e_{ij} + e_{\mathrm{step}}$
22: **end while**

Here:

- rinv : $\{1,0\}^n \times \{1,2\}^n \to \{1,0\}^n$ — function that inverts every bit of input sequence with probability chosen according to the Table 3;
- msdecode : $\mathbb{R}^n \times \{1,0\}^m \times \{1,0\}^{m\times n} \to \{\mathrm{SUCCESS}, \mathrm{FAIL}\}$ — LDPC-code decoding function using the algorithm Min-Sum [51] corrected according to [52] (see algorithm below);
- avg : $\mathbb{R}^I \to \mathbb{R}$ — function computing average value of input sequence.

The LDPC decoding algorithm takes as input the vector $\mathbf{R}$ of LLRs of Bob's received message, Alice's syndrome $\mathbf{s}$, and the maximum number of iterations $\mathbb{I}$. Decoding then proceeds as follows:

Step 1. Initialization. Matrices $\mathbf{M}$ and $\mathbf{E}$ are created, with dimensions matching those of matrix $\mathbf{H}$. Matrix $\mathbf{M}$ is initialized as follows:

$$\forall i,j : H_{ji} \neq 0 \Rightarrow M_{ji} = R_i. \tag{1}$$

Step 2. Parity-check LLR computing. Matrix $\mathbf{E}$ is computed using the formula:

$$\forall i,j : \; H_{ji} \neq 0 \Rightarrow E_{ji} = (-1)^{s_j} \prod_{i' \neq i} \mathrm{sgn}(M_{ji'}) \min_{i' \neq i} |M_{ji'}|, \tag{2}$$

where sgn is the sign function and $|\cdot|$ is the absolute value operator.

Step 3. Re-evaluating LLR from Bob's message. A vector $\mathbf{L}$ of length n is created:

$$\forall i,j : H_{ji} \neq 0 \Rightarrow L_i = \sum_j E_{ji} + R_i. \tag{3}$$

Step 4. Re-evaluating bits from Bob's message. A vector $\hat{\mathbf{y}}$ of length n is created and is filled by the formula

$$\hat{y}_i = \begin{cases} 0, \text{ if } L_i > 0, \\ 1, \text{ otherwise.} \end{cases} \tag{4}$$

Step 5. Termination check. If $\hat{\mathbf{y}}\mathbf{H}^T = \mathbf{s}$, decoding terminates successfully. Else, if the current iteration number equals $\mathbb{I}$, a decoding failure is declared. Otherwise, execution continues.

Step 6. Message LLR Update. $\forall i,j : H_{ji} \neq 0 \Rightarrow M_{ji} = \sum_{j' \neq j} E_{j'i} + R_i$. Return to Step 2.

V. RESULTS

The simulation was conducted for all possible combinations of values i and j, resulting in four distinct cases. Additionally, to evaluate the decoding performance, a similar simulation was performed for each of the four cases where all e_{ij} values were replaced by the average value $e = (e_{01} + e_{02} + e_{11} + e_{12})/4$, corresponding to the use of a binary symmetric channel.

From the physical experiment (see Section III-B), the following QBER levels were obtained for each combination of the bit value and the detector that received it:

- $e_{01} = 0.0234507193$;
- $e_{02} = 0.02230361404$;
- $e_{11} = 0.009339003745$;
- $e_{12} = 0.009107093633$.

The following parameters were selected for the simulation (see Subsection IV):

- $a_{\max} = 10^9$;
- $f_{\max} = 300$;
- $I = 100$;
- $e_{\mathrm{first}} = 0.001$;
- $e_{\mathrm{last}} = 0.44 - e_{02} - e_{11} - e_{12}$ (chosen so that the maximum average QBER achievable within the simulation would be 0.11);
- $e_{\mathrm{step}} = 0.001$.

The parity-check matrix for the LDPC code was selected as Base graph 1 from the 5G standard [53], corresponding to a code rate of 2/3 ($m = 11, n = 33$) with an expansion factor $Z_C = 16$.

Moreover, to demonstrate the advantage of the proposed method, we performed a similar simulation with the classical information reconciliation protocol Cascade [31]. To ensure equal experimental conditions for all protocols, we limited the number of bits that could be disclosed during the execution of the Cascade protocol to the value $mZ_C = 11 \cdot 16 = 176$. The QBER value for calculating the initial block size was computed as the average of e_{01}, e_{02}, e_{11}, and e_{12}.

Fig. 2 and 3 present the results of simulations where the values e_{01} and e_{11} were varied, respectively.

In Fig. 2–3, the line with triangle symbols represents the LDPC-based protocol treating the channel as binary symmetric, the line with square symbols represents the LDPC-based protocol accounting for individual e_{ij} values in the LLR (Log-Likelihood Ratio), and the line with circle symbols represents the Cascade protocol.

As the average QBER value approaches its limit, the distance between the graphs decreases. This arrangement of the curves is explained by the fact that, due to the higher efficiency of the proposed approach, the non-convergence region (the range of QBER values where the FER is close to 1, rendering the selected code practically unsuitable for

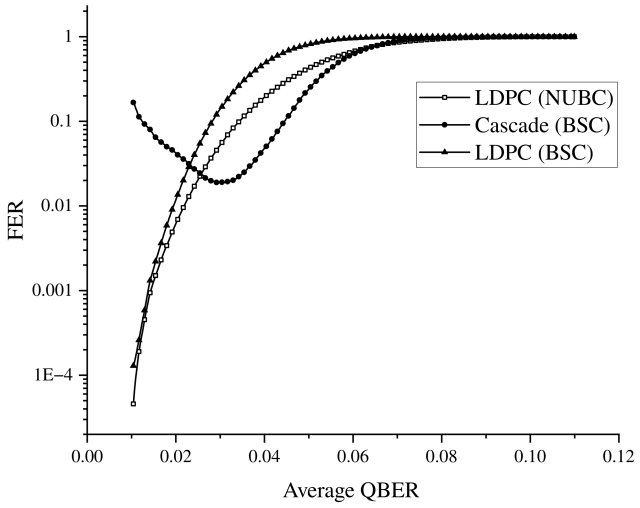


FIGURE 2. Results of the simulation with varying e_{01}.

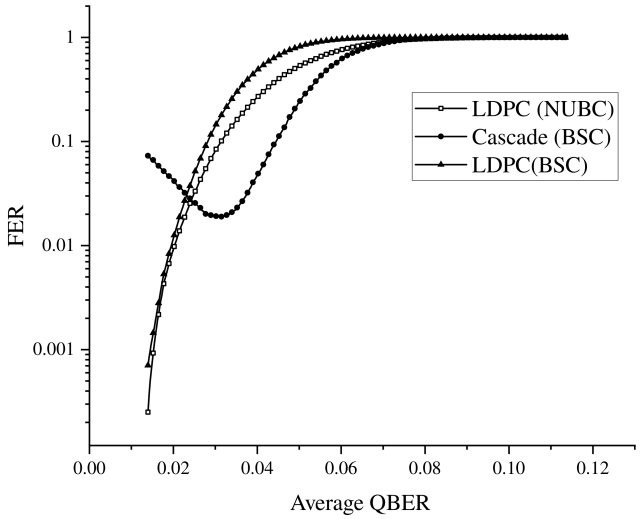


FIGURE 3. Results of the simulation with varying e_{11}.

error correction) for the chosen code begins at higher QBER values compared to the classical approach.

Simulations for QBERs e_{01} and e_{11} are approximately the same as for e_{02} and e_{12}.

To demonstrate the achieved improvements, the ratio of the values on the presented graphs is of greater interest. To display this ratio, another pair of graphs was constructed, shown in Fig. 4 and 5.

In Fig. 4-5, the ordinate axis shows the ratio of the FER value from the simulation where the channel was treated as binary symmetric to the FER value from the simulation where differences in QBER levels were accounted for. The line marked with square symbols corresponds to the improvements relative to the LDPC-based protocol, while the line with circle symbols corresponds to the improvements relative to the Cascade protocol.

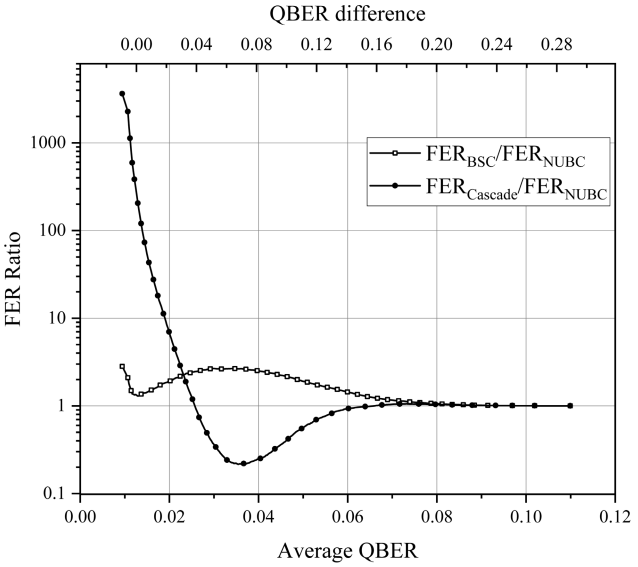


FIGURE 4. Dependence of the FER ratio on the average QBER (simulation with varying e_{01}).

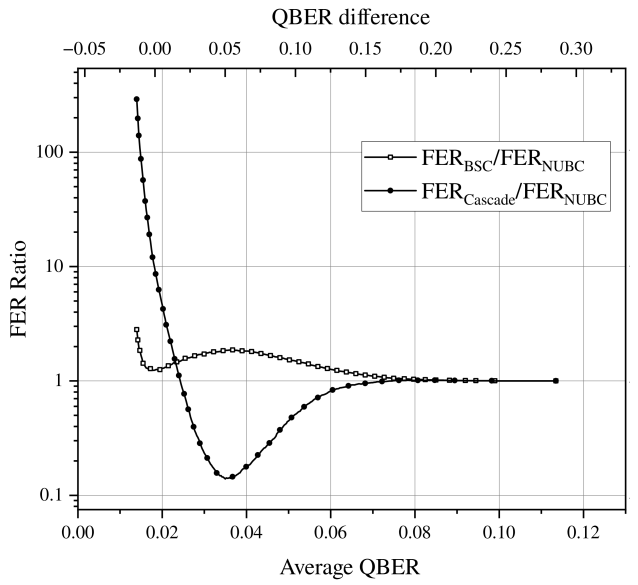


FIGURE 5. Dependence of the FER ratio on the average QBER (simulation with varying e_{11}).

This ratio illustrates the degree of improvement introduced by the proposed approach. As can be seen, outside the non-convergence region, the smallest improvement relative to the LDPC-based protocol is observed between average QBER values of 0.011 and 0.016 for the simulation with varying e_{01}, and between values of 0.017 and 0.022 for the simulation with varying e_{11}.

To show the reason for the reduction in the proposed approach's effectiveness within these ranges, an additional scale was added to the graphs, displaying the difference

between the varying QBER level and the average QBER level (top abscissa axis).

Regarding the Cascade protocol, Fig. 4–5 show that it is significantly inferior in error correction performance to the proposed approach at low QBER values. However, as the QBER values increase, the performance gap narrows. When the QBER values reach approximately 0.027 in both experiments, the Cascade protocol demonstrates higher performance, surpassing that of the proposed approach by up to 5 times in the experiment with varying e_{01} and by up to 7 times in the experiment with varying e_{11}. These results confirm the efficiency of the Cascade protocol for high QBER levels, noted, for example, in [42].

As evident from Fig. 4-5, the proposed approach provides the least improvement compared to the classical LDPC-based one when the varying QBER differs the least from the average QBER value, i.e., in a situation where the channel model is closest to binary symmetric. The subsequent increase in the graph values shows that as the difference between the set and average QBER levels grows, the proposed approach yields better results. The subsequent decline, when the average QBER reaches values above 0.04, is caused by the values approaching the non-convergence region for the selected code, which is clearly visible in Fig. 2-3.

It is important to note that even at the minimum values of the difference between the varying and average QBER, outside the non-convergence region, the QBER ratio between proposed and classical LDPC-based protocols never reached values less than or equal to 1. This means that, regardless of the set QBER level, the proposed approach consistently provided some improvement in decoding quality.

Thus, it can be concluded that the decoding approach accounting for different QBER levels caused by hardware specifics of the QKD system allows for the correction of a significantly greater number of errors compared to the classical LDPC-based approach. This is particularly relevant in situations where significant discrepancies exist between the average QBER value and the values of its individual components observed for each bit-detector combination.

Regarding the computational complexity of the proposed error correction approach, it does not change the asymptotic complexity of the protocol as a whole, as it is expressed only in a constant number (namely, 3) of additional real-number computations when recalculating the LLR according to Table 3. Furthermore, it is important to note that this computational overhead is incurred only a single time after the QBER estimation phase. The computed values are then stored and utilized in all following decoding procedures, minimizing the practical impact on the protocol's runtime.

The real-time performance metrics of the proposed approach compared to the classical LDPC-based protocol and the Cascade protocol for various hardware characteristics are presented in Table 4. As can be seen, the channel model used (BSC or NUBC) does not affect the average error correction time for either of the two LDPC-based error correction approaches.

TABLE 4. Average error correction time per bit vector for the investigated protocols (microseconds).

CPU model	LDPC (BSC)	LDPC (NUBC)	Cascade
AMD Ryzen 9 7950X	410	410	280
AMD Ryzen 5 4600H	720	720	400
1 core of Intel Xeon Gold 6248R	840	840	620

VI. CONCLUSION

Thus, during experiments with a QKD prototype system, which uses time-bin protocol, estimates of QBER levels characteristic for the transmission of logical "0" and logical "1" in the Z-basis were obtained. The levels were approximately 0.02 and 0.009, respectively. Moreover, it was established that the detector number receiving a particular quantum state has a less significant impact on the QBER level for that state.

At the next stage, a methodology was developed to assess the degree of influence that accounting for differences in QBER levels during decoding has on error correction efficiency. The results of further simulations showed that QKD efficiency can be improved by considering the quantum channel as a non-uniform binary channel. This can be done by estimating QBER separately for each combination of transmitted bit and the detector receiving it. In particular, at low QBER levels, the proposed method achieves an approximately 2.7-fold reduction in the output FER compared to the classical LDPC-based protocol. This corresponds to an increase in reconciliation efficiency of approximately 0.605.

However, it must be taken into account that in this case, to compensate for QBER fluctuations arising during the operation of the QKD system, it will be necessary to disclose 4 times more key information for QBER estimation when using the bit disclosure approach. Consequently, developers of the QKD system should find a tradeoff between the volume of disclosed bits and the accuracy of the obtained QBER estimates.

Studying the applicability of syndrome-based QBER estimation in conjunction with the described method is a topic for future research.

ACKNOWLEDGMENT

This research was supported in part through computational resources of HPC facilities at HSE University.

REFERENCES

[1] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.
[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.
[3] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.
[4] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.
[5] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," *Appl. Phys. Lett.*, vol. 87, no. 19, Nov. 2005, Art. no. 194108.

[6] H. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, no. 13, Mar. 2012, Art. no. 130503.

[7] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, no. 2, pp. 441–444, Jul. 2000.

[8] K. Inoue, E. Waks, and Y. Yamamoto, "Differential-phase-shift quantum key distribution using coherent light," *Phys. Rev. A, Gen. Phys.*, vol. 68, no. 2, Aug. 2003, Art. no. 022317.

[9] Y.-L. Tang et al., "Time-bin phase-encoding quantum key distribution using Sagnac-based optics and compatible electronics," *Opt. Exp.*, vol. 31, no. 16, pp. 26335–26343, Jul. 2023.

[10] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," *Sci. Adv.*, vol. 3, no. 11, Nov. 2017, Art. no. 1701491.

[11] C. Agnesi, M. Avesani, A. Stanco, P. Villoresi, and G. Vallone, "All-fiber self-compensating polarization encoder for quantum key distribution," *Opt. Lett.*, vol. 44, no. 10, p. 2398, May 2019.

[12] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, "Micius quantum experiments in space," *Rev. Modern Phys.*, vol. 94, no. 3, Jul. 2022, Art. no. 035001.

[13] S. Liao et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Sep. 2017.

[14] Y. Li et al., "Microsatellite-based real-time quantum key distribution," *Nature*, vol. 640, no. 8057, pp. 47–54, Apr. 2025.

[15] A. Boaron, B. Korzh, R. Houlmann, G. Boso, D. Rusca, S. Gray, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Simple 2.5 GHz time-bin quantum key distribution," *Appl. Phys. Lett.*, vol. 112, no. 17, Apr. 2018, Art. no. 171108.

[16] I. V. Sinil'shchikov and S. N. Molotkov, "Decoy states and low-density parity-check error-correcting codes in quantum cryptography with phase-time coding," *J. Experim. Theor. Phys.*, vol. 129, no. 2, pp. 168–196, Aug. 2019.

[17] S. I. Nefedov, "Challenges of creating a quantum key distribution system for long-distance trunk line," *Nanoindustry*, vol. 17, no. 128, pp. 553–558, 2024.

[18] V. I. Morozov, O. O. Evsyutin, and S. I. Nefedov, "Study of a quantum key distribution protocol with phase-time coding using simulation modeling," *Problems Inf. Transmiss.*, vol. 61, no. 1, pp. 8–26, Apr. 2025.

[19] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. A. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

[20] H. Bechmann-Pasquinucci and N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography," *Phys. Rev. A, Gen. Phys.*, vol. 59, no. 6, pp. 4238–4248, Jun. 1999.

[21] R. G. Gallager, "Low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. IT-8, no. 1, pp. 21–28, Jan. 1962.

[22] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009.

[23] Z. Liu, Z. Wu, and A. Huang, "Blind information reconciliation with variable step sizes for quantum key distribution," *Sci. Rep.*, vol. 10, no. 1, p. 171, Jan. 2020.

[24] G. Limei, R. Qi, J. Di, and H. Duan, "QKD iterative information reconciliation based on LDPC codes," *Int. J. Theor. Phys.*, vol. 59, no. 6, pp. 1717–1729, Jun. 2020.

[25] E. O. Kiktenko, A. O. Malyshev, and A. K. Fedorov, "Blind information reconciliation with polar codes for quantum key distribution," *IEEE Commun. Lett.*, vol. 25, no. 1, pp. 79–83, Jan. 2021.

[26] J. Zhang, H. Jin, H. Xu, and J. Feng, "A rate compatible LDPC scheme in the quantum key distribution system," in *Proc. 3rd Int. Conf. Inf. Commun. Softw. Eng. (ICICSE)*, Apr. 2023, pp. 51–55.

[27] J. Ha, J. Kim, and S. W. McLaughlin, "Rate-compatible puncturing of low-density parity-check codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 11, pp. 2824–2836, Nov. 2004.

[28] T. Tian and C. R. Jones, "Construction of rate-compatible LDPC codes utilizing information shortening and parity puncturing," *EURASIP J. Wireless Commun. Netw.*, vol. 2005, no. 5, Dec. 2005, Art. no. 692121.

[29] N. Borisov, I. Petrov, and A. Tayduganov, "Asymmetric adaptive LDPC-based information reconciliation for industrial quantum key distribution," *Entropy*, vol. 25, no. 1, p. 31, Dec. 2022.

[30] P. Treeviriyanupab and C.-M. Zhang, "Efficient integration of rate-adaptive reconciliation with syndrome-based error estimation and sub-block confirmation for quantum key distribution," *Entropy*, vol. 26, no. 1, p. 53, Jan. 2024.

[31] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology EUROCRYPT*. Berlin, Germany: Springer, 1994, pp. 410–423.

[32] M. Toyran, "More efficient implementations of CASCADE information reconciliation protocol," in *Proc. 24th Signal Process. Commun. Appl. Conf. (SIU)*, May 2016, pp. 161–164.

[33] D. Mayers, "Unconditional security in quantum cryptography," *J. ACM*, vol. 48, no. 3, pp. 351–406, May 2001.

[34] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, "A proof of the security of quantum key distribution," *J. Cryptol.*, vol. 19, no. 4, pp. 381–439, Oct. 2006.

[35] L. Yang, L.-A. Wu, and S.-H. Liu, "On the breidbart eavesdropping problem of the extended BB84 QKD protocol," *Acta Phys. Sinica*, vol. 51, no. 5, pp. 961–965, 2002.

[36] L. Yang, H. Dong, and Z. Li, "One-way information reconciliation schemes of quantum key distribution," *Cybersecurity*, vol. 2, no. 1, p. 16, Dec. 2019.

[37] B. Bilash, B. K. Park, C. Hoon Park, and S.-W. Han, "Error-correction method based on LDPC for quantum key distribution systems," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2020, pp. 151–153.

[38] B.-Y. Tang, B. Liu, W.-R. Yu, and C.-Q. Wu, "Shannon-limit approached information reconciliation for quantum key distribution," *Quantum Inf. Process.*, vol. 20, no. 3, p. 113, Mar. 2021.

[39] H. Mao, Q. Li, Q. Han, and H. Guo, "High-throughput and low-cost LDPC reconciliation for quantum key distribution," *Quantum Inf. Process.*, vol. 18, no. 7, p. 232, Jul. 2019.

[40] R. Mueller, D. Ribezzo, M. Zahidy, L. K. Oxenløwe, D. Bacco, and S. Forchhammer, "Efficient information reconciliation for high-dimensional quantum key distribution," *Quantum Inf. Process.*, vol. 23, no. 5, p. 195, May 2024.

[41] R. Müller, D. Bacco, L. K. Oxenløwe, and S. Forchhammer, "Information reconciliation for high-dimensional quantum key distribution using nonbinary LDPC codes," in *Proc. 12th Int. Symp. Topics Coding (ISTC)*, Sep. 2023, pp. 1–5.

[42] Y. Luo, X. Cheng, H.-K. Mao, and Q. Li, "An overview of postprocessing in quantum key distribution," *Mathematics*, vol. 12, no. 14, p. 2243, Jul. 2024.

[43] A. Sanaei and M. Ardakani, "LDPC code design considerations for non-uniform channels," *IEEE Trans. Commun.*, vol. 58, no. 1, pp. 101–109, Jan. 2010.

[44] H.-B. Lee and J.-W. Kim, "Modified CC-PEG algorithm for protograph-based QC-LDPC codes over non-uniform channel," *IEEE Access*, vol. 12, pp. 173660–173669, 2024.

[45] L. Guo, H.-C. Wu, and D. Huang, "Novel intelligent blind information reconciliation for LDPC codes in quantum key distribution systems," *Phys. Commun.*, vol. 64, Jun. 2024, Art. no. 102348.

[46] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," *Phys. Rev. Lett.*, vol. 94, no. 23, Jun. 2005, Art. no. 230503.

[47] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," *Phys. Rev. A, Gen. Phys.*, vol. 72, no. 1, Jul. 2005, Art. no. 012326.

[48] D. Tupkary, E. Y.-Z. Tan, S. Nahar, L. Kamin, and N. Lütkenhaus, "QKD security proofs for decoy-state BB84: Protocol variations, proof techniques, gaps and limitations," 2025, *arXiv:2502.10340*.

[49] S. Kawakami, A. Taniguchi, Y. Tonomura, K. Takasugi, and K. Azuma, "Security of the BB84 protocol with passive biased basis choice by the receiver," 2025, *arXiv:2507.04248*.

[50] M. Koashi, "Simple security proof of quantum key distribution based on complementarity," *New J. Phys.*, vol. 11, no. 4, Apr. 2009, Art. no. 045018.

[51] M. P. C. Fossorier, M. Mihaljevic, and H. Imai, "Reduced complexity iterative decoding of low-density parity check codes based on belief propagation," *IEEE Trans. Commun.*, vol. 47, no. 5, pp. 673–680, May 1999.

[52] A. D. Liveris, Z. Xiong, and C. N. Georghiades, "Compression of binary sources with side information at the decoder using LDPC codes," *IEEE Commun. Lett.*, vol. 6, no. 10, pp. 440–442, Oct. 2002.
[53] *5G; NR; Multiplexing and Channel Coding (3GPP TS 38.212 Version 19.1.0 Release 19)*, document TS 138 212, 3GPP, Sep. 2025.

VLADIMIR I. MOROZOV received the Specialist degree from Tomsk State University of Control Systems and Radioelectronics, Tomsk, in 2021.

From 2021 to 2023, he was a Junior Research Fellow and an Assistant Professor with the Department of Cyber-Physical Systems Information Security, National Research University Higher School of Economics, Moscow, Russia. Since 2024, he has been a Senior Lecturer with the Department of Cyber-Physical Systems Information Security, National Research University Higher School of Economics. His current research interests include information security, algorithms, information and coding theory, and quantum key distribution.

MIKHAIL S. ELEZOV received the M.S. degree in physics and information technology from Vyatka State Pedagogical University, Kirov, Russia, in 2005, and the master's degree from Moscow State Pedagogical University (MSPU), Moscow, Russia, in 2008.

He is currently a Researcher with the Laboratory of Quantum Detectors, MSPU. Also, he is an Instructor with the National Research University Higher School of Economics (HSE), Moscow. His scientific research interests include superconductivity, single-photon detection, OTDR, quantum optics, and quantum-integrated optics.

OLEG O. EVSUTIN received the Specialist degree from Tomsk State University of Control Systems and Radioelectronics, Tomsk, Russia, in 2009, and the Engineering degree from Tomsk State University, Tomsk, in 2012.

He is currently the Head of the Department of Cyber-Physical Systems Information Security, National Research University Higher School of Economics, Moscow, Russia. His current research interests include information security, steganography, digital watermarking, metaheuristics, and quantum key distribution.

Prof. Evsutin became the Laureate of the Russian Federation Government Prize in Science and Technology for Young Scientists, in 2018.

ROMAN V. OZHEGOV received the Specialist degree from Vyatka's State University, Kirov, Russia, in 2002, and the degree in physical and mathematical science from Moscow State Pedagogical University, Moscow, Russia, in 2011.

He is currently the Director of the NTI Quantum Communication Center, University of Science and Technology MISIS, Moscow; the Head of the Electronics Group, JSC Superconducting Nanotechnology (Scontel), Moscow; and an Associate Professor with the National Research University Higher School of Economics, Moscow. His current research interests include superconductivity, radiophysics, quantum cryptography, quantum sensors, and single-photon detectors.