Blind Reconciliation with Protograph LDPC Code Extension for FSO-based Satellite QKD Systems

Cuong T. Nguyen*, Hoang D. Le*, Vuong V. Mai†, Phuc V. Trinh‡, and Anh T. Pham*
* Computer Communications Laboratory, The University of Aizu, Aizuwakamatsu 965-8580, Japan
† Bradford-Renduchintala Centre for Space AI, University of Bradford, BD7 1DP Bradford, U.K.
‡ Communications and Signal Processing Laboratory, The University of Tokyo, Tokyo, Japan

***Abstract*—A significant breakthrough in space-based quantum key distribution (QKD) inaugurated by the Micius satellite has brought us closer to the era of global QKD networks. An essential step in the post-processing QKD is key reconciliation (KR), which eliminates the mismatch in the raw keys between two legitimate users. However, the fluctuation in the quantum bit-error rate (QBER) caused by the free-space optical (FSO) turbulence channels poses various challenges for the KR design. This paper addresses the design of blind KR schemes for FSO-based low Earth orbit (LEO) satellite QKD systems, which allow operating without a prior QBER estimation. Specifically, we present a novel blind KR scheme with a protograph low-density parity check (LDPC) code extension. The proposed LDPC structure is constructed by gradually extending and exhaustively searching among all possible solutions. The proposed design is evaluated in terms of the final key rate performance over the QKD systems using a dual-threshold/direct detection (DT/DD) scheme. Simulation results confirm the effectiveness of our proposed design compared to the state-of-the-art design in different turbulence channel conditions.**

***Index Terms*—Quantum key distribution, key reconciliation, LEO satellite, LDPC codes, protograph codes.**

I. Introduction

Quantum key distribution (QKD) is a technology that allows the sharing of secret keys between legitimate users. QKD exploits the laws of quantum physics to achieve unconditional security against recent advances in quantum computers [1]. The feasibility of QKD has been widely demonstrated over optical fiber [2] and terrestrial free-space optical (FSO) systems [3]. In addition, to enable global/seamless QKD networks for wireless applications, e.g., secure Internet of Vehicles (IoV), a viable solution is the deployment of satellite-based FSO/QKD systems. In 2016, the Micius QKD satellite achieved a non-zero key rate over 1200 km of the FSO link [4]. This milestone was the first proof-of-principle space-based QKD implementation, taking us closer to global quantum networks.

The operation of QKD has two phases: shared key establishment (i.e., quantum raw key exchange) and classical post-processing. The raw key shared between legitimate users (Alice and Bob) may contain errors due to quantum channel noise and/or eavesdropper attacks. This becomes particularly critical over the uncertainty of FSO turbulence channels experiencing high fluctuation in quantum bit error rate (QBER) [5]. As a result, a pressing concern on satellite-based FSO/QKD systems is an effective design of key reconciliation (KR). It is essential in the post-processing step to reconcile the sifted keys between Alice and Bob via a classical channel [6]. A common KR approach relies on syndrome-based error correction codes, in which Alice or Bob can correct the key based on the other user's key. Low-density parity check (LDPC) codes have been widely considered for KR protocols thanks to their close-to-capacity performance and low decoding complexity.

Two main methods for syndrome-based KR that use LDPC codes include adaptive-rate [7], [8] and blind reconciliation [9]. The former necessitates an accurately estimated QBER to properly adjust the coding rates adopted from an LDPC family. For time-varying FSO-based satellite channels with high QBER fluctuation, a significant portion of the sifted key information may need to be disclosed for accurate QBER estimation. This, in turn, substantially deteriorates the final key rate performance. The blind reconciliation, nevertheless, does not require the estimation of QBER beforehand, which is a potential solution for such systems [9]. When a decoding attempt fails, Alice[1] reveals more information via the classical channel so that Bob can reconcile the key with a higher probability of success.

An early design of the blind KR was presented in [9], which considered a set of the rate-compatible LDPC code family based on puncturing and shortening bits. Alice adjusts the code rates after each communication round until Bob successfully corrects his key. Following this potential proposal, significant efforts have been devoted to the design of blind KR schemes, e.g., [10]–[14]. Particularly, Kiktenko *et al.* proposed an improvement of blind reconciliation by introducing symmetric interaction between two legitimate users [10]. In [11], the authors focused on reducing the processing time by gradually increasing the number of revealing bits in each communication round. A design of blind KR based on polar code was investigated in [12]. In [13], a technique to reduce information leakage for blind KR by reusing syndrome bits was investigated. Most recently, Tarable *et al.* considered the rateless protograph LDPC code families for blind KR [14].

This paper proposes a novel blind reconciliation design with protograph LDPC code extension for FSO-based satellite QKD systems. The motivation and key idea of the proposed design are twofold. *Firstly*, conventional blind reconciliation [10], [11], [13] considered random-based methods to construct

[1]Without loss of generality, we assume that Alice is the one who sends the side information.

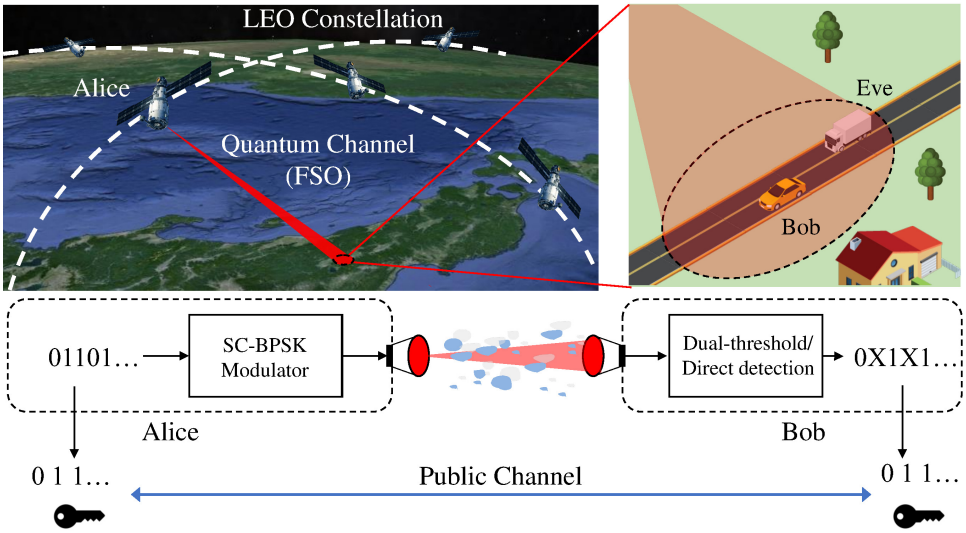

Fig. 1. The considered scenario of LEO satellite-based FSO/QKD-assisted secure Internet of Vehicles (IoV).

LDPC codes, implying that their parity check matrices possess little structure. This often requires high complexity in terms of hardware implementation, preventing them from being used in practical systems. *Instead, our proposed design is constructed using protographs, which are small graph prototypes used to construct larger parity check matrices. LDPC codes constructed in this way inherit the structure from the protograph and can facilitate parallel decoding on hardware [15]. Secondly*, while the design in [14] also addressed the protograph LDPC code, the authors derive lower code rates by splitting a check node into two. However, this check-splitting method may miss good codes due to the lack of comprehensive search. *In our design, we obtain the protographs by extending and exhaustively searching for good nested codes.* Moreover, to comprehensively investigate the performance of the proposed design, we consider a satellite-based FSO/QKD system using the dual-threshold/direct detection (DT/DD) [16]. The final key rate performance is investigated over different channel conditions, and a case study is conducted involving Starlink's satellites.

II. System and Proposed Blind Reconciliation

A. System Model

Figure 1 depicts the LEO satellite-based FSO/QKD-assisted secure IoV applications. Particularly, an LEO satellite (Alice) distributes secret keys to a self-driving car (Bob) via FSO channels. Also, we assume that Alice will perform the post-processing phase over the public channel with Bob. In addition, we investigate the case that an Eavesdropper (Eve) is able to compromise the system by attempting an unauthorized receiver attack (URA). Eve, which is a moving car, attempts to tap the transmitted signals from Alice by locating its receiver within the beam footprint near Bob. Here, we adopt a simpler and low-cost version of BB84 QKD protocol using the DT/DD scheme [16]. In this protocol, Alice transmits sub-carrier binary phase shift keying (SC-BPSK) modulated signals, representing binary random bits over the FSO channel. At the receiver, Bob directly detects the received signal using a PIN photodiode before passing it through a demodulator with dual thresholds. More details regarding this method can be found in [16].

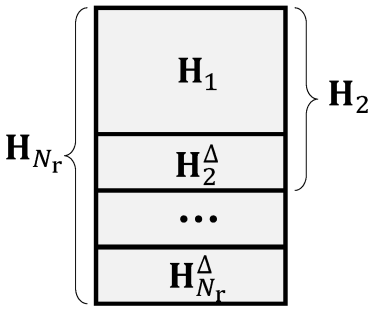

Fig. 2. An example of nested code structure for syndrome-based blind KR.

B. Proposed Blind Reconciliation

In our study, we focus on information reconciliation, which is an essential step in the QKD post-processing. Specifically, we consider the blind reconciliation with the rate-compatible (RC) LDPC code family, whose structure is shown in Fig. 2. Here, we denote N_r and $\mathbf{H}_i$ as the total number of code rates in the family and the parity check matrix of the code rate C_i, $(1 \leq i \leq N_\mathrm{r})$, respectively. It is noted that $C_1 > C_2 > ... > C_{N_\mathrm{r}}$. The parity check matrix $\mathbf{H}_{i+1}$ of an arbitrary rate C_{i+1} in the family can be constructed by appending a certain number of rows, denoted as $\mathbf{H}_{i+1}^{\Delta}$, to a higher-rate matrix $\mathbf{H}_i$. The parity check matrices of higher-rate codes are nested in that of lower-rate ones. Therefore, syndromes of low-code rates can be constructed by appending additional bits to that of

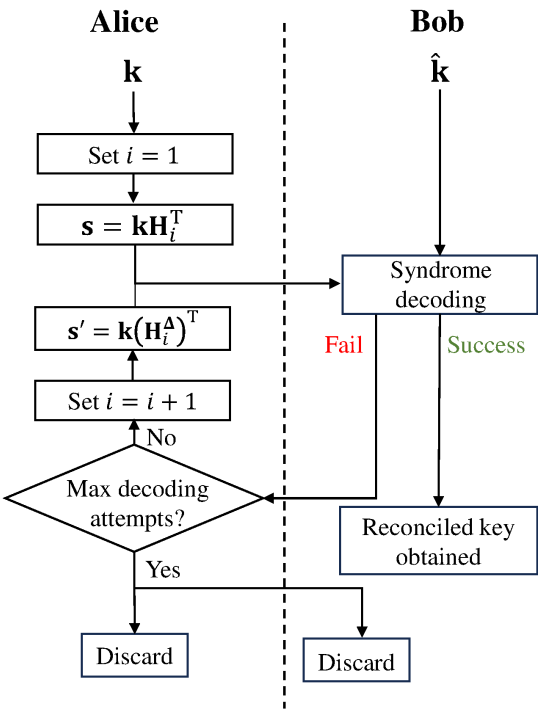

Fig. 3. Flow chart of the proposed blind reconciliation.

higher-code rates, facilitating incremental information for the syndrome decoding.

The flowchart of the proposed blind reconciliation is depicted in Fig. 3. Let $\mathbf{k}$ and $\hat{\mathbf{k}}$ be the row vector presenting the sifted key at Alice and Bob's side, respectively. We also set the maximum number of communication rounds as N_{r} and $i = 1$ at initial. The details of the protocol are as follows:

1) Alice encodes the sifted key into syndrome $\mathbf{s} = \mathbf{k}\mathbf{H}_i^{\mathrm{T}}$ and sends it to Bob via the classical channel.
2) Bob performs the syndrome decoding to reconcile his sifted key [17]. In the case of successful decoding, Bob announces Alice, and they keep the reconciled key. Otherwise, they move to step 3.
3) Alice checks whether the maximum number of decoding attempts is reached. If $i = N_{\mathrm{r}}$, both parties discard their sifted keys. Otherwise, she increases $i = i+1$, computes the incremental syndrome $\mathbf{s'} = \mathbf{k}\left(\mathbf{H}_i^{\Delta}\right)^{\mathrm{T}}$ and sends it to Bob.
4) Bob sets $\mathbf{s} = [\mathbf{s} \quad \mathbf{s'}]$ and tries another decoding attempt based on the newly obtained syndrome. If the decoding attempt is successful, both users obtain the reconciled keys. Otherwise, they go back to step 3.

III. Design of LDPC Code Extension Family

A. Protograph LDPC Code Extension

To construct the RC-LDPC code family with the proposed design, we consider the LDPC codes constructed by protograph. Protograph is a small bipartite graph that serves as a template for constructing parity check matrices of LDPC codes [15]. A protograph can be equivalently represented by

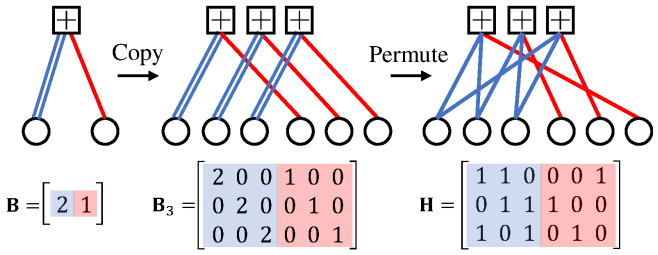

Fig. 4. A simple example of constructing a parity check matrix by lifting a protograph.

a protomatrix whose each row and column correspond to a check node (CN) and a variable node (VN) of the protograph. Each element in the protomatrix denoted the number of edges connecting a type of CN to a type of VN. As depicted in Fig. 4, the parity check matrix of an LDPC code is constructed by lifting the protograph a number of times, denoted as the lifting factor, and then permuting edges among the same node type.

One advantage of protograph LDPC codes is that the edge property of the protograph is conserved during the lifting process. This means the performance of an LDPC code can be investigated and optimized faster on the protograph level [18], [19]. Taking this advantage, a design method for the considered structure can be conducted using the code extension and exhaustive search [19]. Specifically, we will start from a high-rate protomatrix and gradually add new rows to it. The protomatrix with the lowest decoding threshold among all possible solutions will be selected. To analyze the decoding convergence of protographs, we use the protograph extrinsic information transfer (PEXIT) algorithm [20].

B. Example of Construction

Let's consider the following example, where we construct a set of LDPC code rates for blind reconciliation protocol. We start from a high code rate, i.e., 9/10, whose protomatrix is given as follows

$$\mathbf{B}_{9/10} = \begin{pmatrix} 1 & 3 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 2 & 2 \end{pmatrix}. \tag{1}$$

The protomatrix has the size of 2×20 and is constructed using the lengthening method in [19]. The first and second columns correspond to the 1-degree VN and the highest-degree VN, respectively. This is due to the fact that including some degree-1 VNs and a very high degree VN can improve the decoding threshold [15]. To construct lower code rates, we will extend the protomatrix by one row each step and exhaustively search for the best code. The possible constructed code rates range from $\frac{9}{10}$ to $\frac{20-(n_{\mathrm{step}}+2)}{20}$ where n_{step} denotes the number of conducted step. To reduce the search space, we constrain the number of edges from the new check node to the old variable nodes. In particular, the possible values for the first column are $\{0\}$, for the second column are $\{1, 2\}$, and for

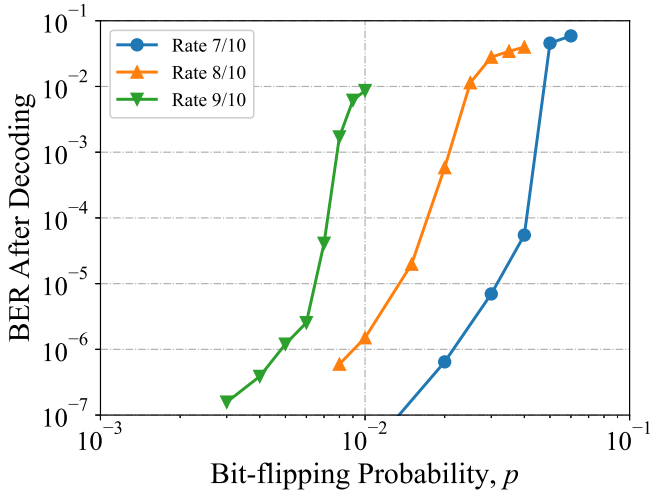

Fig. 5. Bit-error rate after syndrome decoding with different bit-flipping probabilities of the BSC. The block length is 40k.

other nodes are $\{0, 1\}$. After a few steps of extending, we derive the protomatrix for the code rate 7/10 as

$$\mathbf{B}_{7/10} = \begin{pmatrix} 1 & 3 & 1 & 1 & 1 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 1 & 1 & 2 & 2 \\ 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 2 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}. \tag{2}$$

From the initial protomatrix $\mathbf{B}_{9/10}$, we now obtained the protomatrices of lower code rates, i.e., $\{0.85, 0.8, 0.75, 0.7\}$, corresponding to each extended row. It should be noted that lower code rates can still be constructed by extending the protomatrix $\mathbf{B}_{7/10}$.

In the next step, we will construct the parity check matrix of the LDPC code family by conducting two-step lifting on the derived protomatrix $\mathbf{B}_{7/10}$ [21]. The lifting factors of the first and second steps are, respectively, 8 and 250, giving the block length of 40,000 bits. The parity check matrices of higher-rate codes are obtained by removing columns of the lifted matrix. Now, we investigate the performance of code rates in the family over the binary symmetric channel (BSC). Fig. 5 illustrates the bit-error rate after syndrome decoding of rates 0.7, 0.8, and 0.9 with different bit-flipping probabilities, p, of the BSC. A sum-product decoder modified for syndrome decoding is used [17]. The maximum number of iterations is 100. It is observed that the code family can correct up to $p = 0.04$.

IV. Signal and Channel Models

A. Signal Model for DT/DD

According to [16], the demodulated signal at receiver is

$$r(t) = \begin{cases} i_0 = -\frac{1}{4}\Re\delta P_{\mathrm{t}} h(t) + n(t), \\ i_1 = \frac{1}{4}\Re\delta P_{\mathrm{t}} h(t) + n(t), \end{cases} \tag{3}$$

where i_0 and i_1 are the received signal corresponding to bit "0" and bit "1", respectively; $\Re$ is the responsivity of the detector; δ is the modulation depth; P_{t} denotes the peak transmitted power, $h(t)$ is the channel coefficient; $n(t)$ is the received noise.

The received noise, including thermal noise, shot noise, and background noise, can be modeled as zero-mean additive white Gaussian (AWGN) noise. Thus, the variance of $n(t)$ is $\sigma_{\mathrm{n}}^2 = \sigma_{\mathrm{sh}}^2 + \sigma_{\mathrm{bg}}^2 + \sigma_{\mathrm{th}}^2$, where σ_{sh}^2, σ_{bg}^2, and σ_{th}^2 are respectively the variances of the shot noise, background noise, and thermal noise [16]. These variances are expressed as $\sigma_{\mathrm{sh}}^2 = 2q\Re\left(\frac{1}{4}P_{\mathrm{t}}\delta h\right)\Delta f$, $\sigma_{\mathrm{bg}}^2 = 2q\Re P_{\mathrm{b}}\Delta f$, $\sigma_{\mathrm{th}}^2 = \frac{4k_{\mathrm{B}}TF_{\mathrm{n}}}{R_{\mathrm{L}}}\Delta f$, where $P_{\mathrm{b}} = \Omega\pi r_{\mathrm{a}}^2 \frac{B_0\lambda^2}{c}$ is the average received background radiation power, Ω is the Sun's spectral irradiance above the atmosphere, r_{a} is the receiver aperture radius, B_0 is the optical bandwidth, λ is the optical wavelength, c is the speed of light. Moreover, $\Delta f = \frac{R_{\mathrm{b}}}{2}$ is the effective noise bandwidth, R_{b} is the satellite's data rate, k_{B} is the Boltzmann constant, T is the receiver temperature in Kelvin degree, F_{n} represents the amplified noise figure, and R_{L} denotes the load resistance.

Bob detects the received signal using dual thresholds (DT) d_0 and d_1 as follows

$$b(t) = \begin{cases} 0 & \text{if } r(t) \le d_0, \\ 1 & \text{if } r(t) \ge d_1, \\ \mathrm{X} & \text{otherwise}, \end{cases} \tag{4}$$

where $b(t)$ represents the detected bit at time t, 'X' is the case that Bob can not detect the bit. The DTs are written as [16]

$$d_0 = \mathbb{E}[i_0] - \zeta\sigma_{\mathrm{n}}, \text{ and } d_1 = \mathbb{E}[i_1] + \zeta\sigma_{\mathrm{n}}, \tag{5}$$

where ζ is the DT scale coefficient, $\mathbb{E}[i_0]$ and $\mathbb{E}[i_1]$ are mean values of i_0 and i_1, respectively.

B. FSO Channel Model

We consider three major impairments for the FSO channel model, which are cloud attenuation h_{c}, atmospheric turbulence h_{t}, and beam-spreading loss h_{p}. The composite channel coefficient is then determined as $h = h_{\mathrm{c}}h_{\mathrm{t}}h_{\mathrm{p}}$.

Regarding the cloud attenuation, it is computed as $h_{\mathrm{c}} = \exp[-\sigma H_{\mathrm{c}} \sec(\xi)]$, where ξ is the zenith angle, H_{c} is the vertical extent of clouds, and σ is the attenuation coefficient and can be computed by the visibility, V, and the wavelength λ [22, (12)]. The visibility is expressed as [22]

$$V = \frac{1.002}{\left(N_{\mathrm{c}}[\mathrm{cm}^{-3}] \times M_{\mathrm{c}}[\mathrm{g/m}^{-3}]\right)^{0.6473}}, \tag{6}$$

where M_{c} is the cloud liquid water content (CLWC), and N_{c} is the cloud droplet number concentration.

For the atmospheric turbulence, we consider the Gamma-Gamma distribution to model a wide range of turbulence conditions. As a result, the probability density function of h_t is written as [23]

$$f_{h_{\mathrm{t}}}\left(h_{\mathrm{t}}\right)=\frac{2\left(\alpha\beta\right)^{\frac{\alpha+\beta}{2}}}{\Gamma\left(\alpha\right)\Gamma\left(\beta\right)}h_{\mathrm{t}}^{\frac{\alpha+\beta}{2}-1}K_{\alpha-\beta}\left(2\sqrt{\alpha\beta h_{\mathrm{t}}}\right), \quad (7)$$

where $\Gamma\left(.\right)$ is the Gamma function, $K_{\alpha-\beta}\left(.\right)$ is the modified Bessel function of the second kind of order $\alpha-\beta$. The shaping parameters α and β are computed as functions of the Rytov variance σ_{R}^2, which can be found on [22, (15)].

As for the beam-spreading loss, the proportion of receiver power at the detector is approximated as [24]

$$h_{\mathrm{p}}\approx A_0\exp\left(-\frac{2\rho^2}{w_{L_{\mathrm{eq}}}^2}\right), \quad (8)$$

where ρ is the radial displacement between the centers of the beam footprint and that of the vehicle detector, $A_0=\left[\mathrm{erf}\left(v\right)\right]^2$ is the fraction of the collected power at $\rho=0$ with $v=\left(\sqrt{\pi}r_{\mathrm{a}}\right)/\left(\sqrt{2}w_{L,\mathrm{eff}}\right)$, $\mathrm{erf}\left(\cdot\right)$ is the error function, $w_{L_{\mathrm{eq}}}$ is the equivalent beam width and can be expressed as $w_{L_{\mathrm{eq}}}^2=w_{L,\mathrm{eff}}^2\frac{\sqrt{\pi}\mathrm{erf}(v)}{2v\exp(-v^2)}$. Also, $w_{L,\mathrm{eff}}$ is the effective beam width and approximated as $w_{L,\mathrm{eff}}\approx w_0\sqrt{\left(1-\frac{L}{F_0}\right)^2+\left(\frac{2L}{k_{\mathrm{wave}}w_0^2}\right)^2}$ [23], where F_0 is the phase font radius of curvature, $k_{\mathrm{wave}}=2\pi/\lambda$, $w_0=\frac{\lambda}{\pi\theta}$, θ is the divergence half-angle.

V. Simulation Results

This section presents and discusses the performance of our proposed blind reconciliation using Monte Carlo simulations. An LDPC code family with a set of code rates of $(7/10, 8/10, 9/10)$ is considered for the blind KR scheme. To evaluate the performance of the proposed design, we analyze the final key rate, which is calculated as [16]

$$\mathrm{KR}=R_{\mathrm{b}}P_{\mathrm{sift}}\sum_{i=1}^{N_{\mathrm{r}}}P_{\mathrm{succ}}^{(i)}\left(\beta_i I_{\mathrm{AB}}-I_{\mathrm{E}}\right), \quad (9)$$

where R_{b} is the satellite's data rate, P_{sift} denotes the sift probability, N_{r} denotes the maximum number of code rates in the family, $P_{\mathrm{succ}}^{(i)}$ is the percentage of simulated frames corrected by i-th code rate. Moreover, I_{AB} represents the mutual information between the sifted key of Alice and that of Bob, I_{E} is the upper bound on the information that the eavesdropper can obtain over the quantum channel, $\beta_i=\frac{C_i}{I_{\mathrm{AB}}}$ is the reconciliation efficiency, and C_i is the i-th code rate.

A. Parameter Settings

The parameters used for the simulations are as follows. *At the LEO satellite (Alice):* transmitted power $P_{\mathrm{t}}=25$ dBm, divergence half-angle $\theta=25$ μrad, zenith angle $\xi=60°$, satellite altitude $H_{\mathrm{s}}=500$ km, data rate $R_{\mathrm{b}}=1$ Gbps, modulation depth $\delta=0.4$, $F_0=\infty$ (collimated Gaussian beam), and optical wavelength $\lambda=1.55$ μm. *At the ground vehicle (Bob and Eve):* receiver aperture radius $r_{\mathrm{a}}=5$ cm, optical bandwidth $B_0=250$ GHz, responsivity $\Re=0.9$ A/W, load resistor $R_{\mathrm{L}}=1$ $k\Omega$, amplified noise figure $F_{\mathrm{n}}=2$, and receiver temperature $T=298$ K. The DT scale coefficient of Bob is $\zeta=1.5$, and the minimum distance between him and Eve $d_{\mathrm{E}}=10$ m. *Regarding the FSO channel:* ground turbulence level $C_0^2\left(n\right)=10^{-14}$ $\mathrm{m}^{-2/3}$, atmospheric altitude $H_{\mathrm{a}}=20$ km, channel coherence time $t_{\mathrm{slot}}=1$ ms, sun's spectral irradiance $\Omega=0.1$ W/cm$^2\cdot\mu$m, vertical extent of clouds $H_{\mathrm{c}}=2$ km, rms wind speed $v_{\mathrm{wind}}=21$ m/s, $M_{\mathrm{c}}=5$ mg/m^3, and $N_{\mathrm{c}}=250$ cm^{-3}.

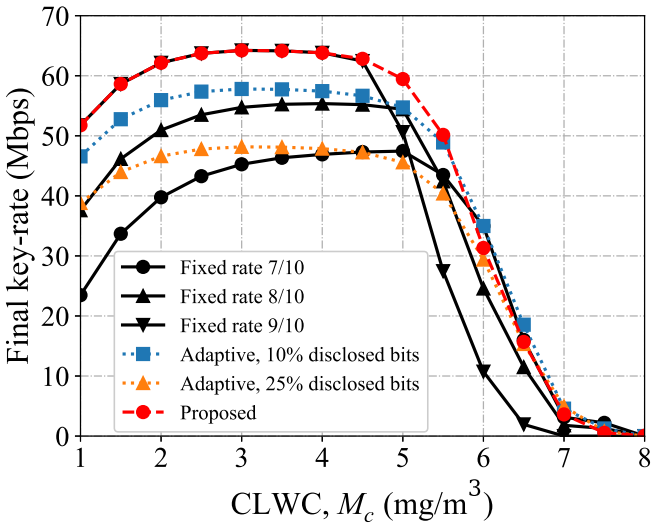

Fig. 6. Final key rate performance of the proposed design and existing reconciliation schemes with different CLWC values.

B. Performance Evaluation

Firstly, we quantitatively compare the performance of the proposed design with state-of-the-art KR schemes, including the fixed-rate and adaptive-rate methods, as shown in Fig. 6. Also, different cloud conditions indicated by CLWC values are considered. Here, the fixed-rate and adaptive-rate KR schemes are analyzed from the theoretical bounds. As expected, the proposed design outperforms the existing solutions in a wide range of CLWC values. It is because when a decoding attempt fails, Alice sends additional syndrome bits to form a lower code rate for decoding. Alice can always choose the most suitable code rate in the family to reconcile, avoiding failed decoding or leaking too much information. It is noted that the adaptive rate method can also adapt the code rate according to the estimated QBER. However, it must disclose a portion of sifted bits, which, in turn, reduces the overall final key rate.

Next, we investigate in Fig. 7 the performance of the proposed design in a satellite pass duration. We select the LEO satellite's transmitted power as $P_{\mathrm{t}}=30$ dBm. Also, different values of Bob's DT scale coefficients are considered. Here, we study a scenario where Alice is the Starlink-1293 flying over Japan on 23 December 2021, and Bob is the vehicle moving in Aizuwakamatsu. The time we start tracking the satellite $t=0$ corresponds to 16:09:20:00 (UTC+9). It is worth noting that due to the low operating altitude, the LEO

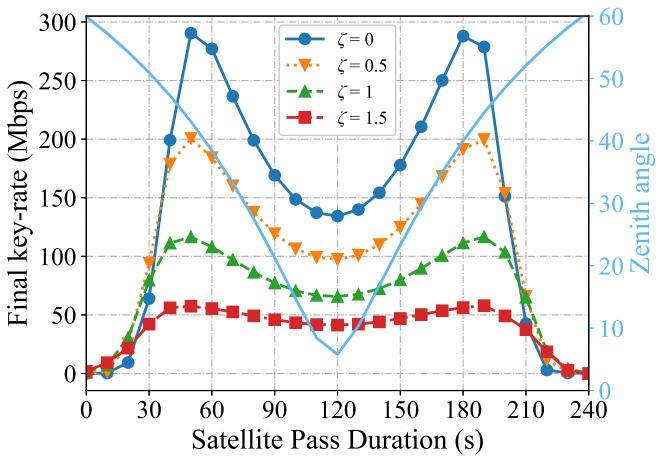

Fig. 7. Final key-rate performance of the proposed design over a satellite pass duration with different values of DT scale coefficients.

satellite's position is not fixed relative to Earth. This results in the changing of the slant path and zenith angle over the satellite pass duration. Therefore, we recompute these values for each simulation point [25].

It is observed that a high final key rate performance can be achieved with a low value of ζ due to the increase of the sift probability. However, the system with a low value of ζ also experiences high QBER, especially for large zenith angle values ($\xi \geq 50°$), which results in a low achievable final key rate. Using this figure, Bob can adjust the DT coefficient over the satellite pass duration to maximize the key rate performance. For instance, Bob can select the DT scale coefficient as $\zeta = 0.5$ when $t \in [0, 30]$ and $t \in [210, 240]$; $\zeta = 0$ when $t \in [210, 240]$.

VI. Conclusion

In this paper, we proposed the blind key reconciliation scheme with protograph LDPC code extension for FSO-based satellite QKD systems. The parity check matrices of LDPC codes were constructed by extending and optimizing the protograph level. The performance of the QKD-based DT/DD systems using the proposed design is analyzed in terms of the final key rate. The Monte Carlo simulation showed that our proposed design outperformed conventional approaches over the considered range of CLWC values. Moreover, we investigated the final key rate performance of our design in a case study involving an LEO satellite from Starlink's network and a moving vehicle at Aizuwakamatsu.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Modern Phys.*, vol. 81, no. 3, p. 1301, Sept. 2009.

[2] A. Boaron *et al.*, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, p. 190502, Nov. 2018.

[3] Schmitt-Manderbachand *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," *Phys. Rev. Lett.*, vol. 98, no. 1, p. 010504, Jan. 2007.

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

[5] I. Capraro, *et al.*, "Impact of turbulence in long range quantum and classical communications," *Phys. Rev. Lett.*, vol. 109, no. 20, p. 200502, Nov. 2012.

[6] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology-Eurocrypt'93*. Springer, 1993, pp. 410–423.

[7] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in *Proc. IEEE Int. Symp. Inf. Theory,*. IEEE, 2009, pp. 1879–1883.

[8] D. Elkouss, J. Martinez, D. Lancho, and V. Martin, "Rate compatible protocol for information reconciliation: An application to QKD," in *Proc. IEEE Inf. Theory Workshop*. IEEE, 2010, pp. 1–5.

[9] J. Martinez Mateo, D. Elkouss Coronas, and V. Martín Ayuso, "Blind reconiliation," *Quantum Inf. Comp.*, vol. 12, no. 9&10, pp. 791–812, May 2012.

[10] E. O. Kiktenko, A. S. Trushechkin, C. C. W. Lim, Y. V. Kurochkin, and A. K. Fedorov, "Symmetric blind information reconciliation for quantum key distribution," *Phys. Rev. Appl.*, vol. 8, no. 4, p. 044017, Oct. 2017.

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

[12] 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.

[13] H.-K. Mao, Y.-C. Qiao, and Q. Li, "High-efficient syndrome-based LDPC reconciliation for quantum key distribution," *Entropy*, vol. 23, no. 11, p. 1440, Nov. 2021.

[14] A. Tarable, R. P. Paganelli, and M. Ferrari, "Rateless protograph LDPC codes for quantum key distribution," *IEEE Trans. Quantum Eng.*, Feb. 2024.

[15] D. Divsalar, S. Dolinar, C. R. Jones, and K. Andrews, "Capacity-approaching protograph codes," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 6, pp. 876–888, Aug. 2009.

[16] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng, and A. T. Pham, "Design and security analysis of quantum key distribution protocol over free-space optics using dual-threshold direct-detection receiver," *IEEE Access*, vol. 6, pp. 4159–4175, Jan. 2018.

[17] 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.

[18] M. El-Khamy, J. Hou, and N. Bhushan, "Design of rate-compatible structured LDPC codes for hybrid ARQ applications," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 6, pp. 965–973, Aug. 2009.

[19] T. Van Nguyen, A. Nosratinia, and D. Divsalar, "The design of rate-compatible protograph LDPC codes," *IEEE Trans. Commun.*, vol. 60, no. 10, pp. 2841–2850, Oct. 2012.

[20] G. Liva and M. Chiani, "Protograph LDPC codes design based on EXIT analysis," in *Proc. IEEE GLOBECOM*, Nov. 2007, pp. 3250–3254.

[21] C. T. Nguyen, H. D. Le, and A. T. Pham, "Performance of IR-HARQ-based RC-LDPC code extension in optical satellite systems," in *Proc. IEEE VTS Asia–Pacific Wireless Commun. Symp. (APWCS)*, Aug. 2023, pp. 1–6.

[22] H. D. Le, H. D. Nguyen, C. T. Nguyen, and A. T. Pham, "FSO-based space-air-ground integrated vehicular networks: Cooperative HARQ with rate adaptation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 59, no. 4, pp. 4076–4091, Aug. 2023.

[23] L. C. Andrews and R. L. Phillips, *Laser beam propagation through random media*. Washington, USA: SPIE Press, 2005.

[24] A. A. Farid and S. Hranilovic, "Outage capacity optimization for free-space optical links with pointing errors," *IEEE/OSA J. Lightwave Technol.*, vol. 25, no. 7, pp. 1702–1710, July 2007.

[25] W. L. Pritchard, H. G. Suyderhoud, and R. A. Nelson, *Satellite Communications Systems Engineering*, 2nd ed. Pearson Education India, 1993.