Application of Adaptive Polar Code based CV-QKD Scheme for LEO Satellite Systems

Qiang Wang*, Thara Son†, Meixiang Zhang*, and Sooyoung Kim†
*Yangzhou University, China
†IT Convergence Research Center, Div. of Elec. Eng., Jeonbuk National University, Korea

***Abstract*—The information reconciliation protocol plays a crucial role in achieving a high secret key rate in continuous variable quantum key distribution (CV-QKD) systems. It is closely intertwined with a forward error correction scheme. In systems that operate under dynamic channel conditions, such as low earth orbit (LEO) satellite systems, the utilization of an adaptive reconciliation protocol becomes essential to ensure efficiency. This necessity calls for an efficient rate-adaptive forward error correction scheme, encompassing a single encoder and decoder. This paper provides a comprehensive review of adaptive information reconciliation schemes utilizing polar codes. It also explores their application to LEO satellite systems.**

***Index Terms*—CV-QKD, LEO, satellite, polar codes, information reconciliation**

I. Introduction

Quantum Key Distribution (QKD) protocol is a revolutionary cryptographic technique that leverages the principles of quantum mechanics to establish secure communications. QKD allows two legitimate parties, Alice and Bob to share secret keys in the presence of an illegal eavesdropper, Eve [1]. In the QKD process, Alice is responsible for preparing quantum states, which are then transmitted through a quantum channel to Bob. Subsequently, Bob performs measurements on the received quantum states, leading to the establishment of correlated data between the two trusted parties.

QKD is categorized into discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD) systems according to the quantum states.In DV-QKD, the quantum states used for encoding information are discrete, typically based on the polarization or spin of individual photons. On the other hand, the quantum states used for encoding information are continuous variables in CV-QKD, typically related to the properties of photons, such as their amplitude and phase. Continuous variable states can be produced and detected utilizing readily available optical equipment [2], and thus CV-QKD is particularly effective for transmitting quantum information via mediums such as lasers. Typically, information is encoded in the quadrature variables of the optical field, which collectively define an infinite-dimensional Hilbert space [2].

Owing to the above mentioned advantages of the CV-QKD, CV-QKD has been intensively researched and applied to a variety of scenarios such as commercial fibre-optic networks [3], free-space optical communications [4] and satellite communications [5]. Specifically, quantum communication through satellites has become a tangible reality, and thus QKD can be globally implemented using modern satellite technologies.

One of the important processes of CV-QKD is error detection and correction which is called information reconciliation (IR). In this process, Alice and Bob communicate openly over a public channel, comparing a subset of their quantum information to detect any discrepancies. They also use error correction schemes to recover error-contaminated information into a secure key. Since the communication environment of a satellite system is largely different from that of a terrestrial system, the selection of a proper error correction scheme for a target application plays an important role in determining efficiency of the system.

This paper reviews and investigates the applicability of polar codes as a means of IR for CV-QKD in the low-earth orbit (LEO) satellite systems. The rest of this paper is organized as follows. Section II and III review the basics on IR of CV-QKD and its application to satellite systems, respectively. Section IV investigates the rate-adaptive reconciliation protocols using polar codes which are suitable for dynamic LEO satellite systems, and presents a few simulation results. Finally, Section V draws conclusion and suggests future works.

II. CV-QKD and its reconciliation protocol

A. CV-QKD and post-processing procedures

Unlike DV-QKD systems, which rely on single-photon-based approaches, CV-QKD systems utilize homodyne (or heterodyne) detection to map key information onto the quadrature variables of the optical field and can be implemented using off-the-shelf optical hardware [6–8]. Quantum state transmission provides raw data but does not constitute the final key itself. Therefore, additional processing, known as post-processing procedures, is essential. Post-processing procedures are employed on the raw data obtained in the quantum transmission between the involved parties. This process facilitates the extraction of a key that remains undisclosed to any potential eavesdroppers. The post-processing procedures extract information from the raw data, establish mutual understanding between the parties, and generate the ultimate key that ensures absolute security.

Figure 1 illustrates the post-processing in CV-QKD systems, inclduing information reconciliation and privacy amplification [9, 10]. To generate secret keys, Alice and Bob share correlated

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (NRF-2021R1A2C1003121) and Graduate Research and Innovation Projects of Jiangsu Province(SJCX22_1711).

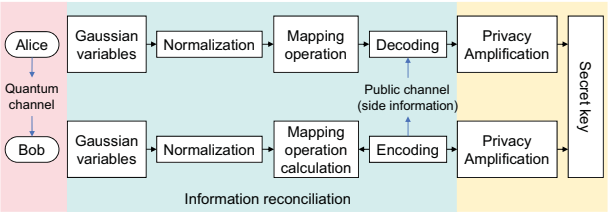

Fig. 1: Post-processing in CV-QKD.

Gaussian variables using the coherent states derived from the quantum process. Subsequently, they individually perform multidimensional reconciliation to rectify errors in their shared raw keys arising from inconsistencies in the correlated variables. Finally, Alice and Bob separately apply privacy amplification to their respective corrected shared keys, leading to the construction of the final secret keys. The ultimate goal of this process is to enhance secrete key rate and increase transmission distance, which can be estimated by the following measures.

First, the reconciliation efficiency β is defined as follows [11]:

$$\beta = \frac{R}{C}, \tag{1}$$

where R is the code rate of the employed the forward error correction (FEC) code, $C = \frac{1}{2}\log_2(1+\gamma)$ is the channel capacity, and γ is the signal-to-noise ratio (SNR) of the channel. This β directly affects the key rate and transmission distance.

Second, the ideal secret key rate R_{s0} of the CV-QKD system is theoretically defined as [11]:

$$R_{s0} = \beta I_{AB} - \chi_{BE}, \tag{2}$$

where I_{AB} is the mutual information between the Alice and Bob, and χ_{BE} is the Holevo bound on the information leaked to eavesdropper [11]. In practice, the secret key rate is scaled by the frame error rate (FER), since the entire frame with known errors must be discarded and it can not be used as secret keys. As a result, the practical secret key rate of a CV-QKD system, R_s is given by:

$$R_s = (1 - \text{FER})\left(\beta I_{AB} - \chi_{BE}\right). \tag{3}$$

The secret key rate increases as β increases and as FER decreases.

B. Information reconciliation of CV-QKD

The IR interfaces quantum communication with classical communication. The aim of the IR is to optimize the extraction of final secret key from the raw data shared between two legitimate parties, thereby enhancing secrete key rate and increasing transmission distance. There are two extraction methods for CV-QKD reconciliation, namely slice reconciliation [12] and multidimensional reconciliation [13]. Multidimensional reconciliation was generally known to achieve higher efficiency when SNR is low, typically γ is less than 1 dB [14], achieving higher key rate with a larger transmission range. However, it is noteworthy that its utility in low γ conditions necessitates the integration of FEC codes endowed with substantial error correction capabilities.

After receiving a quantum state, the reconciliation process is started by using a FEC code. The reverse multidimensional reconciliation can be adopted to extract the final key at Bob and sends additional side information back to Alice through the classical channel. Upon the completion of data encoding to the codeword $\mathbf{c}$ at Bob, $\mathbf{c}$ is converted to a binary spherical sequence $\mathbf{c}'$ in order to enable the following mapping [13]:

$$\mathbf{M}(\mathbf{y}', \mathbf{c}') = \sum_{1,2\cdots,d} \alpha_i(\mathbf{y}', \mathbf{c}')\mathbf{A}_d, \tag{4}$$

where $\mathbf{y}'$ is the normalized coherent state modulated by Gaussian modulation, $\alpha_i(\mathbf{y}', \mathbf{c}') = (\mathbf{A}_d\mathbf{y}'|\mathbf{c}')$ and $\mathbf{A}_d$ is a family of d orthogonal matrices [13]. Then, Bob share $\mathbf{M}(\mathbf{y}', \mathbf{c}')$ with Alice over the public channel, for her error correction.

Once the information reconciliation protocol is determined, the important factor in enhancing efficiency and minimizing FER lies in the selection of a FEC code. In CV-QKD, FEC codes are employed to ensure that the final keys generated by Alice and Bob are consistent, thus enhancing the reliability of the quantum key exchange process. There are several FEC codes that have been investigated and adapted for use in CV-QKD reconciliation protocols, including low-density parity-check LDPC codes, polar codes, raptor codes, and other codes.

III. CV-QKD for satellite systems

A. Application of CV-QKD for satellite systems

An increasing body of research indicates the promise of integrating satellite systems into QKD deployments, owing to their capability to enable quantum communications at a global level [15], and satellite-based QKD has been verified in various scenarios [16–18]. For example, China luanched a quantum satellite, dubbed Micius which demonstrated remarkable progress within the realm of quantum communications through satellite mediums [19]. However, the performance of DV-QKD is constrained in satellite communications, mainly because of the intricate nature of preparing individual photons. In contrast, CV-QKD can be implemented by modulating both the amplitude and phase quadratures of a coherent laser, detectable with efficient homodyne detectors. This surpasses single-photon detectors in speed and efficacy [20].

A comprehensive exploration of satellite-based CV quantum communications in both Gaussian and non-Gaussian entanglement distribution environments, along with their applicability in CV-QKD, has been meticulously examined in [21]. Significantly, an experiment of considerable significance has been conducted, predicated upon the principle of homodyne detection of optical signals transmitted from a geostationary satellite [22], with reception transpiring at a terrestrial ground station.

Figure 2 shows an example of CV-QKD system for LEO satellite systems. Alice transmits the quantum states to Bob via a satellite-to-ground channel. Then, Alice and Bob possess

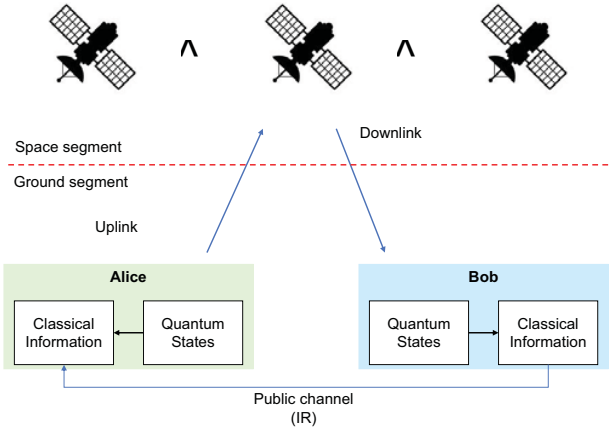

Fig. 2: CV-QKD system for LEO satellite.

two identical and secure key strings by performing IR and privacy amplification. This QKD protocol remains operational throughout the visibility period of the LEO satellite, concluding as the satellite moves beyond the line of sight [19]. It was reported that an average secure key rate of 1.1 kbps could be achieved from a LEO satellite at an altitude of 1200 km, and a higher key rate could be achieved as the satellite moves closer to the ground station [19].

The users of a CV-QKD system anticipate the capability to offer two consistent and secure keys within a confined temporal span. In scenarios such as LEO satellite-based implementations, the reconciliation process is anticipated to conclude while sustaining an uninterrupted line-of-sight connection with the ground station. For CV-QKD-equipped LEO satellites, it may mean the reconciliation need to be completed within minutes. This raises the issue that CV-QKD scheme for satellite systems needs to be as efficient as possible in terms of reconciliation efficiency and complexity.

B. Channel characteristics of LEO satellite systems

The primary advantage offered by satellite-based communication lies in its capability to facilitate extended communication ranges, surpassing the capacities of alternative methods. In addition, communication between two ground stations can be achieved even in the absence of a direct free-space line of sight (LoS) by using satellites, provided there are LoS paths from a satellite to both ground stations. These advantages stem from its immunity to the constraint of terrestrial horizon limitations and the attenuation of photon losses at elevated altitudes. It was noted that only a small fraction of the propagation path, less than 10 km, is through the atmosphere in satellite-based FSO communications. This implies that most of the propagation path experiences no absorption and no turbulence induced losses [5]. The utilisation of satellites also allows for fundamental studies on the impact of relativity on quantum communications [23]. However, the main drawback of the satellite based system is attributed to loss induced by atmospheric turbulence-induced.

In the LEO satellite system, the atmospheric turbulence layer mainly exerts its influence on both the uplink and downlink channels, and turbulence occurs only in proximity to the transmitting terminal during the uplink phase, and exclusively in the vicinity of the terrestrial receiver during the downlink phase. Propagation through the turbulent atmosphere causes beam roaming and diffraction, respectively [5].

IV. Adaptive reconciliation protocol for LEO satellites

A. Conventional approaches

A satellite channel has dynamic and time-varying characteristics. Specifically with regard to LEO satellites, γ is subject to rapid fluctuations over time, a phenomenon that arises as the satellite ascends above the horizon and subsequently recedes. When the practical γ differs from the designed optimal γ, the reconciliation efficiency highly degrades. Furthermore, LEO satellites exhibit short transit times, necessitating the minimization of complexity. As a strategy to achieve low-complexity CV-QKD through satellite-based systems, adaptive IR approach can be an effective means. In this context, the adoption of rate-adaptive approaches emerges as an attractive and well-suited method for implementing the IR process within these practical systems.

Elkouss et al. adopted the puncturing and shorted techniques used for QKD, effectively adjusting the code rate of LDPC codes to suit the desired requirements [24, 25]. Furthermore, blind IR was proposed to be used with puncturing and shorted techniques for rate adaptive protocol without an error rate estimate [26].

A previous study realized adaptive IR by introducing punctured bits and shortened bits into the Gaussian variables of both Alice and Bob [25]. This action is equivalent to adjusting the rate of the Multi-edge type LDPC code. Punctured bits serve to increase the code rate, while shortened bits contribute to decreasing the code rate. The change in code rate caused by the puncturing bit results from the elimination of certain variable nodes and check nodes. On the other hand, the shortening technique adjusts the code rate by removing specific variable nodes.

B. Proposed adaptive IR using polar codes

The polar code is a linear block code proposed by Erdal Arikan that can achieve channel capacity via channel polarization [27]. In contrast to LDPC codes and turbo codes, the utilization of polar codes in CV-QKD reconciliation offers two distinct advantages. First, polar codes exhibit a better performance when dealing with shorter block lengths. As a result, polar codes are more suitable for scenarios where a relatively low raw key rate is anticipated, such as LEO satellite systems [28]. Secondly, polar codes enable a faster reconciliation rate than LDPC codes to achieve a desired reconciliation efficiency [29]. This attribute makes polar codes particularly valuable in ensuring the real-time delivery of CV-QKD.

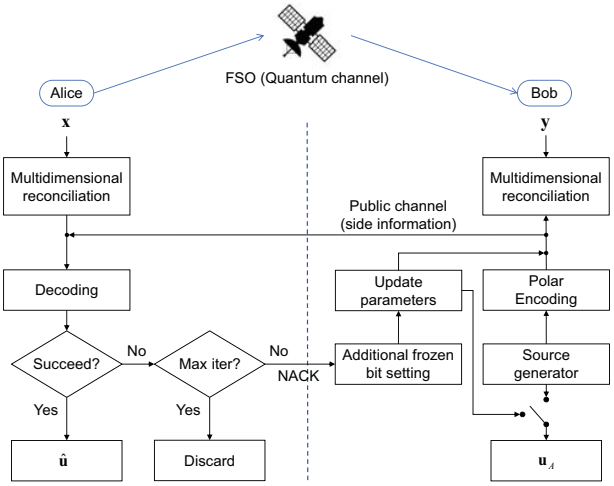

Fig. 3: Process of the rate-adaptive information reconciliation protocol.

The first proposal is to utilize rate-adaptive multidimensional IR protocol using a polar code [30], in order to enhance the reconciliation efficiency of the LEO satellite system. In this scheme, the code rate of the polar code is lowered by incrementally increasing fixed number of frozen bits with the lowest reliability when SNR becomes low, thereby the reconciliation success probability is enhanced. Furthermore, the inherent property of polar codes, i.e., known frozen bits does not reveal any information on information bits, guarantees the security of the proposed rate-adaptive information reconciliation protocol. We refer to this method as P1.

Specifically, Figure 3 shows the rate-adaptive IR protocol using a polar code. Initially, Alice and Bob normalize continuous random Gaussian variables $\mathbf{x}$ and $\mathbf{y}$. Afterwards, Bob calculates the maximum achievable code rate $R_{\max}$, and generates a binary sequence $\mathbf{u}$ of length N, which is then encoded into a polar code $\mathbf{c}$. Then Bob applies reverse multidimensional reconciliation with (4), and shares side information through the public channel with Alice. This side information contains the code rate, bit indices on the frozen bits which are required to perform decoding. Upon receiving side information, Alice Alice performs decoding to obtain $\hat{\mathbf{u}}$.

In scenarios where decoding process is unsuccessful, Alice transmits NACK to Bob. In this case, Bob allocates additional n_f bits as incremental frozen bits and updates the parameters of the code, and transmit the updated side side information to Alice via the public channel. Upon receiving this updates from Bob, Alice tries another decoding for successful retrieval of the raw key. This retransmission process is repeated until Alice achieves successful decoding or the maximum number of retransmission is reached. Ultimately, the final key is obtained by privacy amplification.

The P1 method could achieve higher efficiency and lower FER in low SNR range, and improve the robustness of CV-QKD systems. However, it requires too much number of retransmissions, especially in low SNR ranges mainly because the number of incremental frozen bits are fixed. In order to overcome this problem, our second proposal is to adopt time-varying number of incremental frozen bits and adaptive coding scheme from the initial transmission. The purpose of the second proposal is to reduce the computational complexity and the decoding delay, especially when the SNR exhibit rapid variations versus time as in LEO satellite-based communications [31]. To achieve this, we use a single polar code which can generate various code rates by regulating the number of frozen bits, and a look-up table is used to set the optimum code rate for a given SNR. We refer to this method as P2 in this paper.

Specifically, in the P2, Alice estimates the SNR information on the quantum channel, and this information is sent back to Bob via public channel. Then, Bob determines the optimal code rate based on the given codeword length N using a predetermined function, and thus the number of frozen bits is appropriately assigned to satisfy a target FER for the given channel condition. Afterwards, both Bob and Alice perform the rate-adaptive reconciliation process for the estimated γ. When decoding fails, the optimum number of additional frozen bits is determined, according to γ to achieve a target FER. By this way, the number of retransmissions required for successful decoding can be significantly reduced.

C. Performance evaluation

The performance of the proposed adaptive IR methods, P1 and P2 are compared by using the polar code with a length of 256 bits. For the performance comparison, we estimate the performance of a fixed method using the polar code with information length of 128 bits, having code rate of 1/2, without any retransmission. On the other hand, the PI and P2 method employ retransmission protocol to satisfy a target FER of 10^{-4}. The P1 method starts initial transmission with an information length of 250 bits, and additional 16 bits are converted to the frozen bits for every retransmission. Furthermore, the P2 methods determines the information length adaptively by γ from the initial transmission. For decoding, we utilize the successive cancellation decoding (SCD) algorithm, and we set the dimension of multidimensional reconciliation d to 8 and the maximum number of retransmissions to 10.

We first analyze the FER performance comparisons, and then analyze the computational complexity in terms of the average number of retransmissions. Figure 4 compares FER performance according to SNR. The figure clearly demonstrates that the P2 method satisfies the target FER across all the investigated SNR ranges. In contrast, the P1 method encounters challenges in achieving the target FER with SNR below 2 dB because of the limited number of retransmissions. Moreover, the fixed method could not achieve the target FER unless the SNR is sufficiently high. This enhancement stems from the advantageous error correction capabilities inherent to the adaptive protocol.

Figure 5 compares the number of retransmissions required to achieve a target FER of 10^{-4}. Although the fixed method

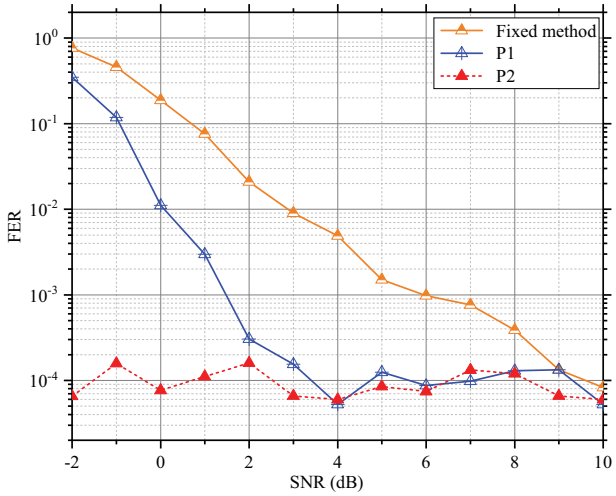

Fig. 4: The FER performance comparisons between IR protocols.

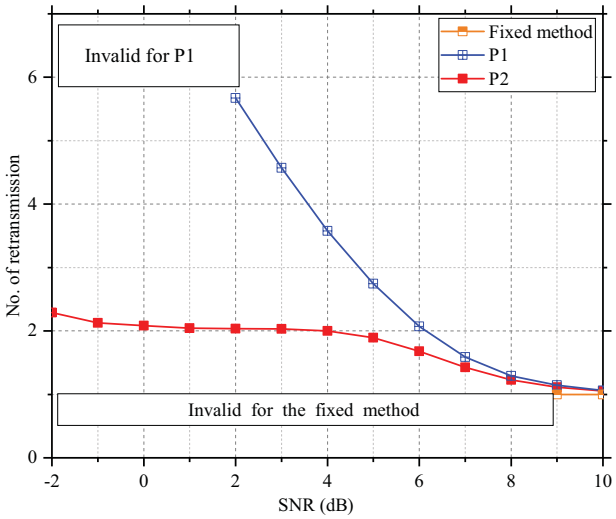

Fig. 5: The average number of the required retransmissions to achieve FER of 10^{-4}.

requires only one transmission, it can only achieve the target BER at high SNR range, greater than 9 dB, so this method is invalid for the other SNR range. The P1 method is valid when SNR is greater than 2 dB, but it still requires a quite large number of retransmissions in low SNR ranges. On the other hand, the P2 method is able to achieve the target FER only one to two transmissions, showing highly enhanced computational complexity.

V. Conclusion and Discussion

This paper reviewed adaptive reconciliation protocols for CV-QKD scheme with polar codes, especially their application to LEO satellite systems. The analysis showed that the development of an optimized adaptive reconciliation scheme, built on CV-QKD protocols, holds the potential to minimize FER while keeping a low complexity. This innovation is expected to find practical utility in LEO satellite applications. The simulation results demonstrated in the paper revealed that adaptive reconciliation protocols using polar codes could be an effective means for LEO satellite systems, where the channel exhibits dynamic. Future study may be directed to analyze the performance of the proposed methods in practical LEO satellite channels including various channel impairment effects, and find a more efficient methods.

References

[1] G. S. Vernam, "Cipher Printing Telegraph Systems: For Secret Wire and Radio Telegraphic Communications," *Journal of the American Institute of Electrical Engineers,* vol. 45, no. 2, pp. 109–115, 1926.

[2] T. C. Ralph, "Continuous Variable Quantum Cryptography," *Physical Review A*, vol. 61, Dec. 1999, Art. no. 010303(R)

[3] B. Korzh et al., "Provably Secure and Practical Quantum Key Distribution Over 307 Kilometers of Optical Fibre," *Nature Photonics*, vol. 9, 2015, Art.no. 163.

[4] S.-Y. Shen et al., "Free-Space Continuous-Variable Quantum Key Distribution of Unidimensional Gaussian Modulation Using Polarized Coherent States in an Urban Environment," *Physical Review A*, vol. 100, no. 1, Art. no.012325, 2019,

[5] N. Hosseinidehaj, Z. Babar, R. Malaney, S. X. Ng and L. Hanzo, "Satellite-Based Continuous-Variable Quantum Communications: State-of-the-Art and a Predictive Outlook," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 1, pp. 881-919, 2019.

[6] Bennett, Charles H, and Gilles Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of International Conference on Computers, Systems & Signal Processing,*, vol. 175, p8, New York, 1984.

[7] Gyongyosi L, "Singular Value Decomposition Assisted Multicarrier Continuous-variable Quantum Key Distribution," *Theoretical Computer Science*, vol. 801, pp. 35-63, New York, 2020.

[8] Grosshans, F., Grangier, P, "Continuous Variable Quantum Cryptography using Coherent States," *Physical review letters*, vol. 88, no. 5, pp. 057902, 2002.

[9] P. Jouguet, S. Kunz-Jacques and A. Leverrier, "Long-distance Continuous-variable Quantum Key Distribution with a Gaussian Modulation," *Physical review letters*, vol. 84, no. 6, 2011.

[10] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu and A. Sanpera, "Quantum Privacy Amplification and the Security of Quantum Cryptography over Noisy Channels," *Physical review letters*, vol. 77, no. 13, PP. 2818-2821, 1996.

[11] Milicevic, M., Feng, C., Zhang, L.M., Gulak, P.G, "Key Reconciliation with Low-density Parity-check Codes for Long-distance Quantum Cryptography," *npj Quantum Information*, vol. 4, no. 21, PP. 2018.

[12] Van Assche GCardinal JCerf N J, "Reconciliation of a Quantum-distributed Gaussian Key," *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 394-400, 2004.

[13] Leverrier, A., All eaume, R., Boutros, J., Z emor, G., Grangier, P, "Multidimensional Reconciliation for a Continuous-variable Quantum Key Distribution," *Physical Review A*, vol. 77, no. 4, pp. 042325, 2008.

[14] M. Bloch, A. Thangaraj, S. W. McLaughlin, and J.-M. Merolla, "LDPC Based Gaussian Key Reconciliation," *Proceedings of the IEEE Information Theory Workshop*, pp. 116–120, 2006.

[15] Bonato, Cristian, et al., "Feasibility of Satellite Quantum Key Distribution," *New Journal of Physics*, vol. 11, no. 4, pp. 045017, 2009.

[16] Nauerth, Sebastian, et al., "Air-to-ground Quantum Communication," *Nature Photonics*, vol. 7, no. 5, pp. 382-386, 2013.

[17] J.-Y. Wang et al.,"Direct and Full-scale Experimental Verifications Towards Ground-satellite Quantum Key Distribution," *Nature Photonics*, vol. 7, no. 5, pp. 387–393, 2013.

[18] J.-P. Bourgoin et al., "Free-space Quantum Key Distribution to a Moving Receiver," *Optics express*, vol. 23, no. 26, pp. 33437–33447, 2015.

[19] S.-K. Liao et al., "Satellite-to-ground Quantum Key Distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, 2017.

[20] S. Pirandola et al., "High-rate Measurement-device-independent Quantum Cryptography," *Nature Photonics*, vol. 9, pp. 397–402, May 2015.

[21] N. Hosseinidehaj and R. Malaney, "CV-QKD with Gaussian and Non-Gaussian Entangled States over Satellite-based Channels," *2016 IEEE Global Communications Conference (GLOBECOM)*, pp. 1-7, IEEE, 2016.

[22] K. Günthner et al, "Quantum-limited Measurements of Optical Signals from a Geostationary Satellite," *Optica*, vol. 4, no. 6, pp. 611–616, 2017.

[23] D. E. Bruschi, T. C. Ralph, I. Fuentes, T. Jennewein, and M. Razavi, "Spacetime Effects on Satellite-based Quantum Communications," *Physical Review A*, vol. 90, no. 4, 2014, Art. no. 045041.

[24] D. Elkouss, J. Martinez-Mateo, and V. Martin, "Secure Rate-adaptive Reconciliation," *The International Symposium on Information Theory and Its Applications (ISITA)*, pp. 179-184, 2010.

[25] X. Wang, Y. -C. Zhang, Z. Li, B. Xu, S. Yu, and H. Guo, "Efficient Rate-adaptive Reconciliation for Continuous-variable Quantum Key Distribution," *Quantum Information & Computation*, vol. 17, pp. 1123–1134, 2017.

[26] J. Mart´ınez-Mateo, D. Elkouss, "Blind Reconciliation," *Quantum Information & Computation*, vol. 12, pp. 791-812, 2012.

[27] Arikan, E, "Channel polarization: A Method for Constructing Capacity-achieving Codes for Symmetric Binary-input Memoryless Channels," *IEEE Transactions on information Theory*, vol. 55, no. 7, pp. 3051–3073, 2009.

[28] B. Tahir, S. Schwarz, and M. Rupp, "BER Comparison between Convolutional, turbo, LDPC, and polar codes," *2017 24th international conference on telecommunications (ICT)*, pp. 1–7, 2017.

[29] Jouguet, P., Kunz, J., S´ebastien, "High Performance Error Correction for Quantum Key Distribution using Polar Codes," *Quantum Information & Computation*, vol. 14, no. 3, 2012.

[30] M. Zhang, H. Hai, Y. Feng, and X. Jiang, "Rate-adaptive Reconciliation with Polar Coding for Continuous-variable Quantum Key Distribution," *Quantum Information Processing*, vol. 20, article no. 318, 2021.

[31] M. Zhang, Q. Wang, T. Son, and S. Kim, "Evaluation of Adaptive Reconciliation Protocols for CV-QKD using Systematic Polar Codes," submitted to *Quantum Information Processing* for review and posted at *Research square*, https://doi.org/10.21203/rs.3.rs-3244551/v1.