European Conference on Optical Communication (ECOC) 2022 © Optica Publishing Group 2022

A Multi-threshold Quantization Scheme for Physical Layer Key Distribution

Xiangyu Liu, Kongni Zhu, Yajie Li, Xiaosong Yu, Yongli Zhao, Jie Zhang

State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing, 100876, P. R. China, jie.zhang@bupt.end.cn

Abstract *A multi-threshold quantization scheme is proposed in this paper and compared with the traditional two-threshold quantization scheme. When the correlation coefficient is around 0.95 and above, the use of this scheme is better than two-threshold quantization.*

Introduction

With the advent of quantum computers, the security risks of key distribution schemes based on mathematical puzzles have become increasingly prominent [1]. The physical layer key distribution provides an alternative solution.

In the classical or quantum key distribution schemes, the final key is a binary sequence. Key post-processing is the process of converting physical features into the security key, which consists of three parts: quantification, information reconciliation (IR), and privacy amplification (PA) [2]. In the field of physical layer key distribution, the efficient quantization method has a great influence on key generation rate (KGR) and key error rate (KER).

In classical key distribution schemes, the extracted physical features with high correlations include the polarization state of optical signal (SOP) [1, 3 ,4], polarization mode dispersion (PMD) [5], phase [6], bit error rate (BER) [7, 8], and so on. In these schemes, physical features are quantized by two-threshold. In continuous variables quantum key distribution, the Slice reconciliation is a common method and first proposed in [9]. Slice reconciliation includes quantization and IR. High-efficiency multi-level coding and decoding coordination can be implemented by using Slice reconciliation [10].

In this paper, a new multi-threshold quantization scheme is proposed for seeking excellent KER and KGR, which combines the two-threshold quantization with the Slice quantization. Cascade protocol is employed for IR and the hash function is utilized for PA. Compared with the two-threshold quantization, the results show that the proposed scheme generates the error-free key with a higher KGR when the correlation coefficient (CC) of extracted physical features is greater than 0.95.

Principle

Fig. 1 shows the physical layer key distribution where Alice and Bob are legal participants. Physical layer key distribution is mainly divided into two steps. First, Alice and Bob both extract physical features, and they obtain two sets of physical feature values with high CC. Then, the values need to be further processed to make it completely consistent and security, which is the key post-processing. The quantization is to convert physical features into binary sequences as the initial key. However, the initial keys are not the same exactly, so IR is required. In PA, the leaked information will be removed to ensure the security of the key.

We put forward a new quantization method, i.e., the multi-threshold quantization. We compare the key retention initial rate (KRIR) of the proposed scheme with it the two-threshold quantization scheme after quantization. KRIR can be calculated with Eq. (1).

$$\mathrm{KRIR} = \frac{B}{L} \tag{1}$$

where B is the total number of the initial key after quantization, and L is the total number of physical

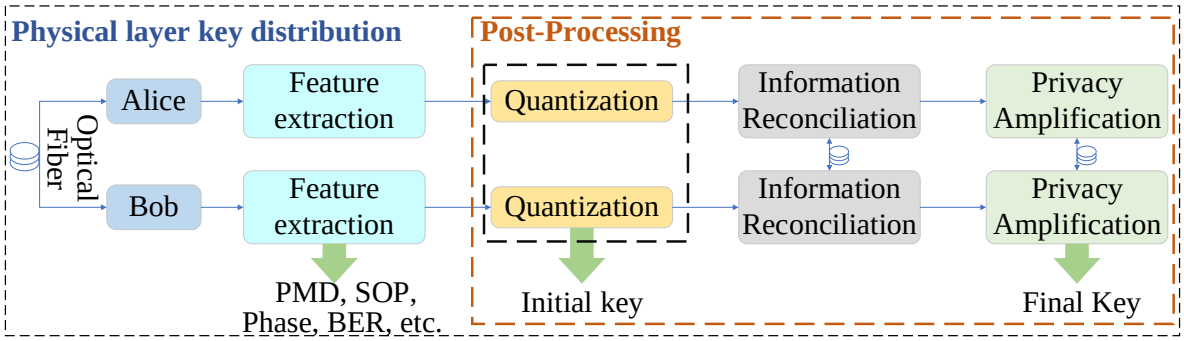

Fig. 1: A typical physical layer key distribution model diagram. The quantization part will be the core of this paper.

feature values.

Then, we compare the KRFR after IR and PA by using the final key. KRFR is calculated with Eq. (2).

$$\mathrm{KRFR} = \frac{R}{L} \tag{2}$$

where *R* is the total number of the final key, and *L* is the total number of physical feature values. Higher KRFR means a higher KGR.

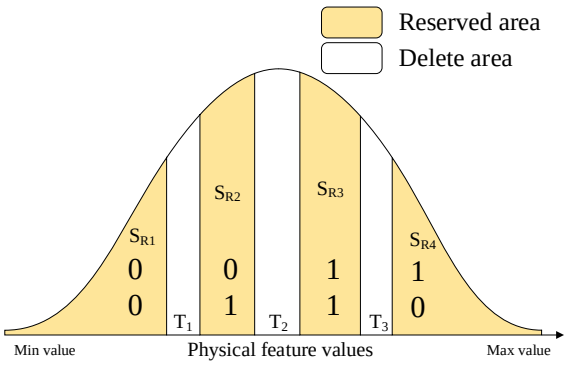

Fig. 2: The principle of multi-threshold quantization.

At the physical layer, the extracted physical features are generally Gaussian distribution or Gaussian-like distribution. Fig. 2 shows the rationale for multi-threshold quantization, which is also a graph of the probability distribution of Gaussian-like. It is a quantization schematic with a quantization order of two. Of course, there are other orders of multi-threshold quantization. If an order of two is chosen during initial key quantization, then a BER value will be encoded as two bits (00, 01, 11, 10). Each reserved area represents the total number of physical features that are ultimately used in this area. Each deleted area represents the total number of unused physical features that fall into this area.

Fig. 3 is the flow chart of this quantization scheme. For the convenience of description, the extracted features are taken as the BER as an example [7, 8]. BER is the physical feature of this scheme. This quantization scheme firstly takes ten percent of the BER or called samples. Using this ten percent of the samples, the CC of Alice and Bob's BER is estimated. According to CC, α will be selected, which controls the ratio of the reserved area to the deleted area. After that, the remaining BER will be sorted sequentially. Then the equation for thresholds is

$$\mathrm{T}_i^- = \frac{(1-\alpha)L}{2^n} + (i-1)\frac{\alpha L}{2^n - 1} + \Delta_i \tag{3}$$

$$\mathrm{T}_i^+ = \frac{(1-\alpha)L}{2^n} + i\frac{\alpha L}{2^n - 1} + \Delta_i \tag{4}$$

Where $i = 1,2,\cdots,2^n - 1$ and T_i^- is the left threshold value of T_i. T_i^+ is the right threshold value of T_i. Quantization order will be described by n. In this paper, n is taken as two. The boundary offset is denoted by Δ_i. Value of Δ_i needs to be determined iteratively according to the number of physical features falling in the reserved area we count.

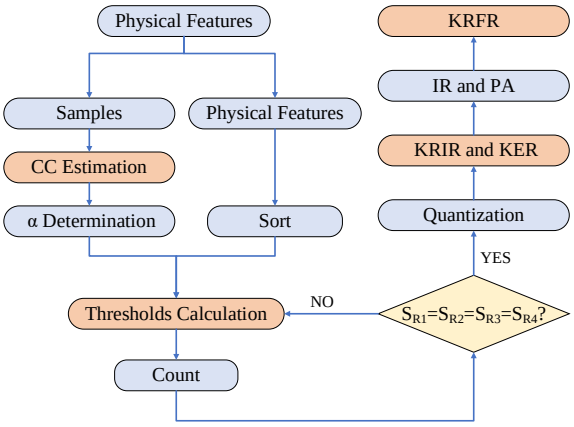

Fig. 3: Multi-threshold quantization flow chart.

It is worth noting that compared with the Slice quantization scheme, the encoding method of this quantization scheme adopts Gray Code encoding, while the Slice quantization scheme adopts the sequential encoding method. Its main purpose is to reduce the KER of Alice and Bob quantization. Suppose a value of Alice's BER falls within the second reserved area, coded as (01). Since the BER of Alice and Bob have a high CC, the BER of Bob will most likely fall in the second area or an area adjacent to it. If it falls in the second area, the number of wrong bits is zero and coded as (01), and if it falls in the adjacent region, (00 or 11) is coded. It guarantees that the number of bits is only wrong by one. Ultimately, the quantized key is guaranteed to have a lower KER and high KRIR. Finally, the Cascade protocol and hash are used to make the keys of Alice and Bob completely consistent and secure.

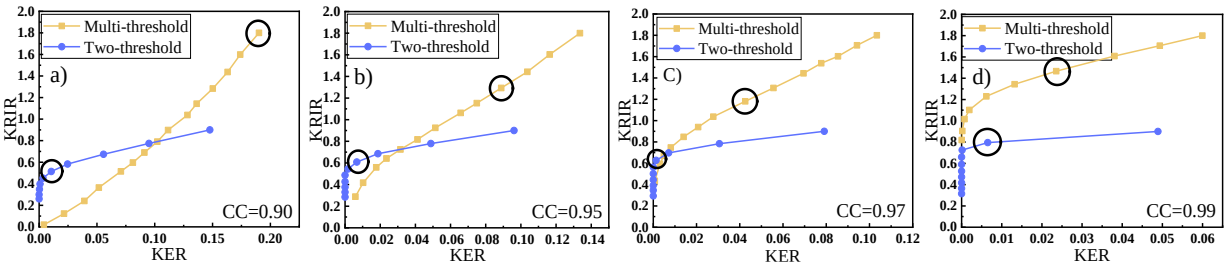

Fig. 4: KRIRs of multi-threshold quantization and two-threshold quantization under different KERs.

Simulation results

Fig. 4 shows the KRIR comparison of two-threshold quantization and multi-threshold quantization under different KER after physical feature quantization. It can be seen from the figure that if the multi-threshold quantization KER is greater than the KER at the boundary between the two-threshold and multi-threshold, the KRIR of the multi-threshold quantization is greater than the two-threshold. Multi-threshold quantization may generate more keys than two-threshold quantization after IR and PA, that is, the KRFR is relatively high. The transition from two-threshold to multi-threshold generally results in an increase in KER and KRIR. So, the two-threshold KER will not exceed the multi-threshold KER. KER varies with α, the optimal α has been circled in Fig. 4. If α is determined, you will get the result of Fig. 5.

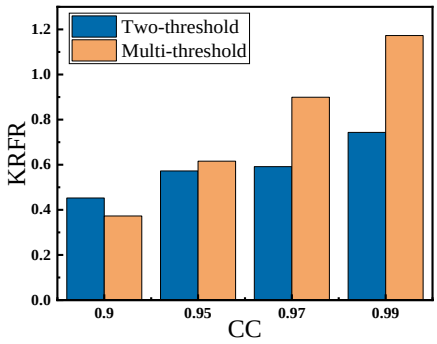

Fig. 5: KRFR under different CC.

Fig. 5 is the result after Cascade protocol and hash, which represents the KRFR when KER is reduced to zero. It can be seen from Fig. 5 that when the CC is around 0.95 and above, the KRR of multi-threshold quantization is better than two-threshold quantization.

Conclusions

We introduce the steps of physical layer key distribution and propose a multi-threshold quantization scheme. According to the simulation results, the KRFR is obviously better than that of the two-threshold quantization when the CC is greater than 0.95. That is to say, the KGR using multi-threshold quantization is higher than that of the two-threshold in this case. As the CC increases, this advantage becomes more pronounced. However, the multi-threshold quantization method with low CC is still under exploration.

References

[1] L. Zhang, A. A. E. Hajomer, W. Hu and X. Yang, "2.7 Gb/s Secure Key Generation and Distribution Using Bidirectional Polarization Scrambler in Fiber," IEEE Photonics Technology Letters, vol. 33, no. 6, pp. 289-292, 2021, DOI:10.1109/LPT.2021.3058118

[2] A. A. E. Hajomer, L. Zhang, X. Yang and W. Hu, "Post-Processing Protocol for Physical-Layer Key Generation and Distribution in Fiber Networks," IEEE Photonics Technology Letters, vol. 32, no. 15, pp. 901-904, 2020, DOI: 10.1109/LPT.2020.3004345

[3] Liuming Zhang, Xinran Huang, Weisheng Hu, and Xuelin Yang, "Point to multi-point physical-layer key generation and distribution in passive optical networks," Optics Letters, vol. 46, no. 13, pp. 3223-3226 2021. DOI: 10.1364/OL.428216

[4] Adnan A. E. Hajomer, Liuming Zhang, Xuelin Yang, and Weisheng Hu, "284.8-Mb/s Physical-Layer Cryptographic Key Generation and Distribution in Fiber Networks," Journal of Lightwave Technology. vol. 39, no. 6, pp. 1595-1601 2021. https://opg.optica.org/jlt/abstract.cfm?uri=jlt-39-6-1595

[5] I. U. Zaman, A. B. Lopez, M. A. A. Faruque and O. Boyraz, "Physical Layer Cryptographic Key Generation by Exploiting PMD of an Optical Fiber Link," Journal of Lightwave Technology, vol. 36, no. 24, pp. 5903-5911, 2018, DOI: 10.1109/JLT.2018.2880957

[6] A. A. E. Hajomer, X. Yang, A. Sultan and W. Hu, "Key Distribution Based on Phase Fluctuation Between Polarization Modes in Optical Channel," *IEEE Photonics Technology Letters*, vol. 30, no. 8, pp. 704-707, 2018, DOI: 10.1109/LPT.2018.2812832

[7] X. Wang, J. Zhang, Y. Li, Y. Zhao and X. Yang, "Secure Key Distribution System Based on Optical Channel Physical Features," IEEE Photonics Journal, vol. 11, no. 6, pp. 1-11, 2019, DOI: 10.1109/JPHOT.2019.2953783

[8] C Lei, J Zhang, Y Li, Y Zhao, B Wang, H Gao, J Li, and M Zhang, "Long-Haul and High-Speed Key Distribution Based on One-Way Non-Dual Arbitrary Basis Transformation in Optical Fiber Link," 2020 Optical Fiber Communications Conference and Exhibition (OFC), pp. 1-3, 2020. DOI: 10.1364/OFC.2020.W2A.51

[9] G. Van Assche, J. Cardinal, N. J. Cerf, "Reconciliation of a quantum-distributed Gaussian key," IEEE Transactions on Information Theory, vol. 50, no. 2, pp. 394-400, 2004, DOI: 10.1109/TIT.2003.822618

[10] Z Bai., X Wang., S Yang. Y Li. “High-efficiency Gaussian key reconciliation in continuous variable quantum key distribution,” Science China Physics, Mechanics & Astronomy. vol. 59, 2016. DOI:10.1007/s11433-015-5702-7