Adaptive Multi-level Phase Quantization for Secret Key Generation

Meixiang Zhang[1,2], Sooyoung Kim[2]

[1]Yangzhou University, [2]Jeonbuk National University

[1,2]maehyang@foxmail.com, [2]sookim@jbnu.ac.kr

비밀 키 생성을 위한 적응적 다중 단계 위상 양자화 기법

장매향[1,2], 김수영[2]

[1,2]양주대학교, [2]전북대학교

Abstract

To meet the requirements of a high secret key generation rate and low bit mismatch rate, this paper proposes to adaptively quantize the phase information of the channel measurements using two alternative Gray mappings. Specifically, two Gray mapping codewords are assigned to each quantization region, which is further divided into four cells. Then, a Gray mapping codeword with the lowest disagreement probability is selected as the quantized bits. Simulation results demonstrated that the proposed method outperforms the conventional methods without discarding any channel measurements.

Ⅰ. Introduction

The physical layer secret key generation (SKG) exploits the inherent randomness contained in the time-varying channel measurements to generate secret keys without any third-party assistance. Generally, SKG consists of channel probing, quantization, information reconciliation (IR), and privacy amplification.

The goals of quantization are maximizing the secret key rate (SKR) while minimizing the bit mismatch rate (BMR) between legitimate parties. Binary quantization methods typically offer the lowest BMR, while limited in terms of the SKR [1]. To increase the SKR, multi-level quantization methods were proposed [2]. However, the probability that the channel measurements cross the threshold increases with the increasing number of quantization regions, resulting in a higher BMR.

To reduce the BMR, the channel quantization with guard-band (CQG) uses a guardband to filter out channel measurements falling near the thresholds [2]. Nevertheless, the drawbacks of this method lie in discarding many channel measurements. As an alternative approach to reducing the BMR, channel measurements, rather than relying on a fixed guardband. The multiple-bit adaptive quantization was introduced by partitioning each quantization region into four cells and selecting the quantization mapping that minimizes the disagreement probability [3].

This paper applies the concept of dynamically selecting between two alternative quantization mappings to the phase quantization of the channel measurements. We simulated the proposed method to verify its performance. The remainder of the paper is organized as follows. In section II, the system is introduced. Section III describes the proposed methods. The simulation results are shown in Section IV, and conclusions are drawn in Section V.

Ⅱ. System model

We consider a wireless communication system with two legitimate users, Alice and Bob, and a passive eavesdropper, Eve, where each user works in time-division duplex mode. Assuming that Eve stays far away from the legitimate users, Eve's channel measurements are completely uncorrelated with those of Alice and Bob. The estimated channel state information (CSI) at Alice is highly correlated with that at Bob, and they are represented as follows.

$$h_A = h + n_A, \quad (1)$$

$$h_B = h + n_B, \quad (2)$$

where h follows Rayleigh fading, $n_A \sim CN(0,\sigma^2)$ and $n_B \sim CN(0,\sigma^2)$ denote the channel estimation errors with Gaussian distribution at Alice and Bob, respectively.

Ⅲ. Proposed methods

We divide each quantization region for 2^m into 4 cells. That is, we, divide the total phase space into $M=2^m \times 4$ equally likely quantization regions, and the qth quantization region is represented by $[\eta_q, \eta_{q+1})$, where η_q denotes the qth threshold and can be formulated as:

$$\eta_q = q \times 2\pi/M, \quad q=0, 1, 2, \ldots, M-1. \tag{3}$$

Next, we assign two pre-determined codewords of the Gray mapping and an indicator bit to represent which mapping should be used as follows.

1. Create a list of 2^m possible Gray codewords with m bits.
2. Define $\mathbf{d_1}(q)$ to be equal to the $q//4$-th Gray codeword, where // represents the integer division.
3. Define $\mathbf{d_0}(q)$ to be equal to the $(q+2)//4$-th Gray codeword.
4. Define the indicator bit $e(q)$ as 0 if $q \% s = 0$ or 3, while as 1 if $q \% s = 1$ or 2.

Using the procedures above, examples for 2^m -PQ can be designed. Table I shows the designed examples for 2^1 and 2^2 -PQ.

Table I Examples for 2^1- and 2^2 -PQ

2^1- PQ					2^2 -PQ				
q	$\mathbf{d_1}$	$\mathbf{d_0}$	e	$[\eta_q, \eta_{q+1})$	q	$\mathbf{d_1}$	$\mathbf{d_0}$	e	$[\eta_q, \eta_{q+1})$
0	0	0	0	$[\eta_0, \eta_1)$	0	00	00	0	$[\eta_0, \eta_1)$
1	0	0	1	$[\eta_1, \eta_2)$	1	00	00	1	$[\eta_1, \eta_2)$
2	0	1	1	$[\eta_2, \eta_3)$	4	00	01	1	$[\eta_2, \eta_3)$
3	0	1	0	$[\eta_3, \eta_4)$	3	00	01	0	$[\eta_3, \eta_4)$
4	1	1	0	$[\eta_4, \eta_5)$	4	01	01	0	$[\eta_4, \eta_5)$
5	1	1	1	$[\eta_4, \eta_5)$	5	01	01	1	$[\eta_4, \eta_5)$
6	1	0	1	$[\eta_6, \eta_7)$	6	01	11	1	$[\eta_6, \eta_7)$
7	1	0	0	$[\eta_7, \eta_8)$	7	01	11	0	$[\eta_7, \eta_8)$
					8	11	11	0	$[\eta_8, \eta_9)$
					9	11	11	1	$[\eta_9, \eta_{10})$
					10	11	10	1	$[\eta_{10}, \eta_{11})$
					11	11	10	0	$[\eta_{11}, \eta_{12})$
					12	10	10	0	$[\eta_{12}, \eta_{13})$
					13	10	10	1	$[\eta_{13}, \eta_{14})$
					14	10	00	1	$[\eta_{14}, \eta_{15})$
					15	10	00	0	$[\eta_{15}, \eta_{16})$

Ⅲ. Simulation results

We evaluate the performance of the proposed method in terms of the BMR according to channel SNR, compared with various quantization methods, as shown in Fig. 1. The CQG methods outperform the conventional PQ method, and the proposed MPQ method outperforms the CQG with reduced complexity, because it does not discard any the channel measurements when generate the secret keys.

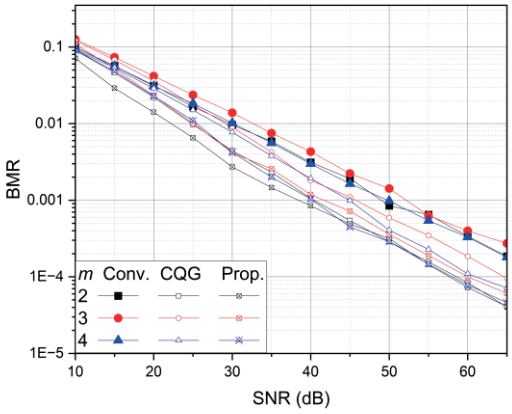

Fig. 1 BMR comparisons between various m and various quantization methods

Ⅲ. Conclusion

We proposed an adaptive multi-level phase quantization method by dividing each quantization into 4 cells. Simulation results demonstrated that the proposed methods achieve the best BMR performance, compared to the conventional methods.

ACKNOWLEDGMENT

This research was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (RS-2024-00459799).

REFERENCES

[1] Y. S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Transactions on Information Forensics and Security*, vol. 5, no.2, pp. 240-254, June 2010.

[2] J. W. Wallace and R. K. Sharma, "Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis," *IEEE Transactions on Information Forensics and Security*, vol. 5, no. 3, pp. 381- 392, Sep. 2010

[3] N . Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on. Mobile Computing*, vol. 9, no. 1, Jan. 2010.