Design of the Bhattacharyya Parameter of Polar Codes for Quantum Key Distribution

Tianjian He[1,2], Gan Wang[3,2], Zhengyu Li[3], Yaxiong Liu[1], Tian Liu[1], Xiang Peng[3] and Hong Guo[3*]

[1] *Key Laboratory of High Confidence Software Technologies, Ministry of Education, Peking University, Beijing 100871, China.*

[2] *Science and Technology on Security Communication Laboratory, Institute of Southwestern Communication, Chengdu 610041, China.*

[3] *State Key Laboratory of Advanced Optical Communication System and Network, School of Electronics Engineering and Computer Science, and Center for Quantum Information Technology, Peking University, Beijing 100871, China.*

[*] *Corresponding author: hongguo@pku.edu.cn*

Abstract: We propose a Bhattacharyya parameter formula of Polar codes for binary symmetric channel using the linear combination of its upper and lower bound. The optimized reconciliation efficiency is suitable for quantum key distribution.

1. Introduction

Polar codes [1] have the remarkable properties of low decoding complexity, and thus can be applied in the high-speed quantum key distribution (QKD) system, especially in the short-range condition. Polar codes take advantages of channel polarization to transmit information in some channels, while other channels are populated with pre-agreed values (the so-called frozen bits) which is usually decided by the Bhattacharyya parameter (Z-value for short). [1] gave the recursive formula of Z-value, which are $Z\left(W_N^{(i)}\right) \leq Z\left(W_{2N}^{(2i-1)}\right) \leq 2Z\left(W_N^{(i)}\right) - Z\left(W_N^{(i)}\right)^2$ and $Z\left(W_{2N}^{(2i)}\right) = Z\left(W_N^{(i)}\right)^2$. The explicit formula of the Z-value for the odd index depends on the channel type, and it is unknown for a binary symmetric channel (BSC), which plays a key role in QKD.

The performance of three types of the Z-value, which are the upper bound (I), lower bound (II) and the mean of the two bounds (III), are compared in [2]. Later, the simulation method [3] to select the frozen bits is proposed, which outperforms all the three types of Z-value method. However, the simulation method will consume a long design time especially for the large block size. Therefore, a hybrid method which uses both Z-value and the simulation to decide the frozen bits is proposed.

Here we propose to use the linear combination of the upper bound and the lower bound of the Z-value, which is formally presented as:

$$Z\left(W_{2N}^{(2i-1)}\right) = (1-\alpha) \times \left[2Z\left(W_N^{(i)}\right) - Z\left(W_N^{(i)}\right)^2\right] + \alpha \times Z\left(W_N^{(i)}\right) \tag{1}$$

We carry a comprehensive experiment under different block length and different QBER, which verifies that when the value of α changes, the performance of corresponding polar codes will change. Moreover, we successfully apply this method to the hybrid method to optimize the reconciliation efficiency.

2. Experiment and Result

We implement our experiment with three QBER values: 0.02, 0.05 and 0.08. Under each QBER value, we fix the proportion of frozen bits. We traverse α from 0 to 1 with 0.01 step value, which means 101 test batches. Under each batch we compute the Z-value of each channel using the corresponding recursive formula. Then we test 500 groups of data to get the frame error rate (FER) of each batch. The results of our experiments are shown in figure 1.

As depicted in the figure, one can find that: First, the coefficient α_{opt} that yields the best performance is not 0, 0.5 or 1. Generally, α_{opt} lies in the range $[0.1, 0.35]$, which is closer to 0, and thats why [2] obtains the conclusion that the upper bound has the best performance. Second, α_{opt} is not always the same under different circumstance, and it is

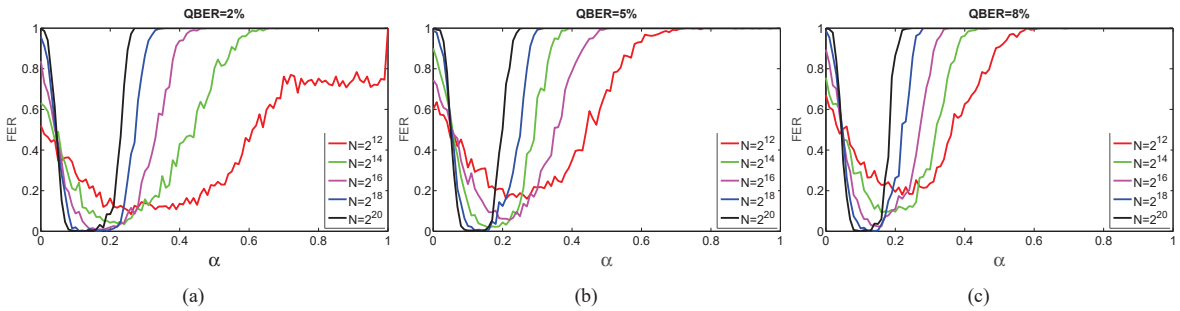

Fig. 1. The QBER and the proportion of frozen bits of (a), (b) and (c) are: 0.02, 0.05 and 0.08; 0.26, 0.41 and 0.52, respectively. N is the block size.

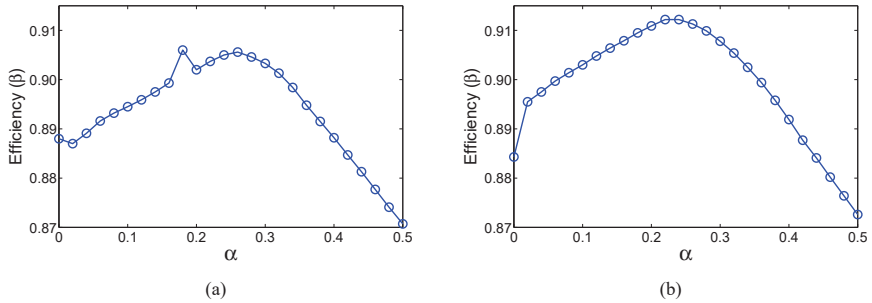

Fig. 2. The block length is (a) 2^{18} and (b) 2^{20}, the QBER is 0.05 and the FER is guaranteed under 0.1. As for other parameters, we set them the same as [3].

shown that when QBER is fixed, the longer the block length is, the lower α_{opt} is. Third, although the exact value of α_{opt} may vary with different conditions, the trend of the curve is the same: decrease first and then increase, which can help us to find α_{opt} quickly.

3. Application to the hybrid method

The application potential of Polar codes to QKD environment is discussed in [3, 4]. A hybrid method is proposed to design well-performed polar codes, which uses the Z-value to decide the first m frozen bits and then use the simulation to decide the rest. Generally, larger m saves more time of finishing the design of polar codes, which also means worse reconciliation efficiency. By using our proposed linear combination Z-value, the reconciliation can be optimized to be close to the only-simulation case.

We test the reconciliation efficiency over different α, see Figure 2. Comparing to the type I and II Z-value, the optimized α will improve the reconciliation efficiency significantly. Although the highest efficiency of 2^{20} block size is 91.2%, only close to 93.8% reached by the only simulation method, the m used here will save more than 70% time comparing to the only simulation method.

In summary, we propose a formula of the Bhattacharyya parameter of polar codes which uses the linear combination of its upper and lower bounds. The performance of the polar code can be optimized by traversing the coefficient α, which saves the code design time and still approaches a reconciliation efficiency suitable for quantum key distribution.

Acknowledgement

This work is supported by the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003), the State Key Project of National Natural Science Foundation of China (Grant No. 61531003) and the Foundation of Science and Technology on Security Communication Laboratory (Grant No. 9140C110101150C11048).

References

1. E. Arikan, “Channel Polarization: A method for constructing capacity-achieving codes for symmetric bianry-input memoryless channels,” IEEE Trans. Inf. Theory 55, 3051 (2009).
2. S. M. Zhao, P. Shi, and B. Wang, “Designs of Bhattacharyya Parameter in the Construction of Polar Codes,” in Proc. of 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), pp. 1-4 (2011).
3. A. Nakassis and A. Mink, “Polar codes in a QKD environment,” In Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, Vol. 9123, pp. 05 (2014).
4. P. Jouguet and S. Kunz-Jacques, “High Performance Error Correction for Quantum Key Distribution using Polar Codes,” Quantum Inf. Comput. 14 329 (2012).