Reconciliation with polar codes by Gaussian approximation for continuous-variable quantum key distribution

Yongseen Kim, Changho Suh, and June-Koo Kevin Rhee
School of Electrical Engineering, KAIST, Daejeon, South Korea
{chunday2, chsuh, rhee.jk}@kaist.ac.kr

In quantum key distribution, reconciliation refers to a post process that extracts two equal binary strings from quantum raw keys between two authenticated parties before distillation of secret keys via privacy amplification. In continuous-variable quantum key distribution (CV-QKD) where coherent states of light are used instead of single photons [1], this is important because it is harder for them to extract and share the same binary strings from continuous variables relative to an eavesdropper. To quantify its performance, reconciliation efficiency is defined as $\beta = \frac{R}{C}$, where R denotes code rate and C indicates Shannon's channel capacity. Reconciliation efficiency close to unity at the low signal-to-noise ratio (SNR) regime is a necessary condition to increase the transmission distance of secret keys.

The early reconciliation scheme, called sliced error correction [2], relies on quantization to extract discrete information. A challenge arises in the scheme: it suffers from reduction of β in the low-SNR regime. It had been one of main bottlenecks against transmission distance of CV-QKD. To cope with it, multi-dimensional reconciliation (MR) was introduced [3]. It approximates reconciliation to a channel coding problem on additive white Gaussian noise (AWGN) channel. It is reported that the combination of MR and multi-edge type low density parity check (MET-LDPC) codes can reach beyond 95% at certain, yet very small SNRs [4].

A natural question that one can ask in this context is it could be improved more. This is a meaningful question since transmission distance depends significantly on β. MET-LDPC codes are already optimized for low-rate applications. We believe that polar codes [5] can be a better option due to its capacity-achieving property shown for a class of discrete memory channels [5]. In fact, this is not the only work to apply polar codes on CV-QKD. The authors in [6] investigated its performance and concluded that codewords should be longer than MET-LDPC codes to achieve competitive performance. On the other hand, there are various polar code construction algorithms on the AWGN channel.

To design polar codes, the precise information on the status of bit channels is required to carry keys on good channels. Fixed bits are delivered via bad channels and used for decoding. However, it is too expensive to compute the exact information of all bit channels on the AWGN channel. The evolution of bounds on Bhattacharyya parameters of bit channels was used heuristically [7], but the equality of bounds holds only for binary erasure channel, which causes inaccurate computation of bit-channel status on other channels. A Monte-Carlo simulation is possible for design with better precision [5]. However, its complexity is also concerned when it comes to CV-QKD application, which requires very long codewords for high β. Polar codes tested in [6] were constructed by the algorithm, called density evolution, which analyzes how the distribution of the log likelihood ratio of a bit channel evolves to compute bounds on the probability of error. Although it can achieve high accuracy, it comes with significant computational complexity for tracking all distributions. This is problematic to CV-QKD due to its necessity of very long codewords.

We propose a new reconciliation protocol that is computationally much less expensive without critical loss of precision by Gaussian approximation(GA). This is possible because it is enough to track only mean of LLR distributions under GA. In our protocol, N independent virtual AWGN channels consist of multiple blocks of MR phase. Then, polar codes designed by GA are applied. However, there still exists a complicated integration function in GA. Previous algorithms with GA [8, 9] just applied approximated function developed for LDPC codes [10]. This heuristic method degrades performance a lot because the function [10] breaks polar codes as the length increases. To resolve this issue, multi-segment GA was

introduced [11] and used in our protocol.

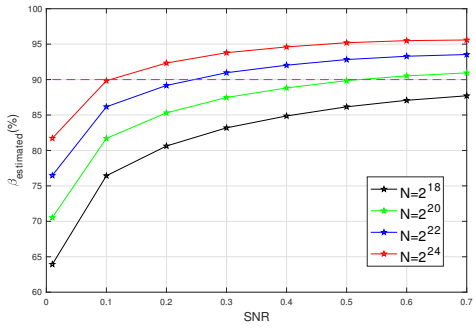

Figure 1: Estimated reconciliation efficiency of the proposed protocol with block error rate $BLER = 0.1$ and different lengths N

Another advantage of GA is that it can estimate block error rate (BLER). Hence, β can be evaluated before actually measured by decoders. The estimated reconciliation efficiencies are shown in Figure 1 with various lengths and $BLER = 0.1$. There is a wide region where reconciliation efficiency is greater than 90%, which enables long-distance CV-QKD, and the region is wider than the one in [6] when the length is equal. Figure 2 shows measured reconciliation efficiencies of the proposed protocol with recent work [12] when the length is 2^{10}. Polar codes with $R = 0.375$ were used in [12]. The proposed protocol achieves higher performance compared to [12] at SNRs less than 1, and this is a positive sign that our protocol can work well at low SNRs.

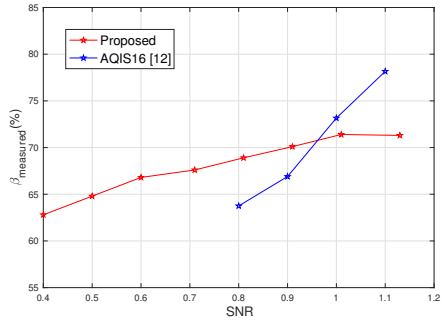

Figure 2: Measured reconciliation efficiency of the proposed protocol and previous work [12] with the length of $N = 2^{10}$

Acknowledgment

This work was supported by the ICT R&D program of MSIP/IITP [1711028311, Reliable cryptosystem standards and core technology development for secure quantum key distribution network] and by the MSIP(Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2017-2015-0-00385) supervised by the IITP(Institute for Information & communications Technology Promotion)

References

[1] F. Grosshans and et al., "Quantum key distribution using gaussian-modulated coherent states," *Nature*, pp. 238–241, 2003.

[2] J.Lodewyck and et al., "Quantum key distribution over 25km with an all-fiber continuous-variable system," *Phys. Rev. A*, 2007.

[3] A. Leverrier and et al., "Multidimensional reconciliation for continuous-variable quantum key distribution," *Phys. Rev. A*, 2008.

[4] P. Jouguet and et al., "Long-distance continuous-variable quantum key distribution with a gaussian modulation," *Phys. Rev. A*, 2011.

[5] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, 2009.

[6] P. Jouguet and et al., "High performance error correction quantum key distribution using polar codes," *arXiv preprint*, no. arXiv: 1204 5882, 2012.

[7] E. Arikan, "A performance comparison of polar codes and reed-muller codes," *IEEE Comm. Lett.*, vol. 12, no. 6, 2008.

[8] H. Li and J. Yuan, "A practical construction method for polar codes in awgn channels," *TENCON Spring Conference*, 2013.

[9] D. Wu and et al., "Construction and block error rate analysis of polar codes over awgn channel based on gaussian approximation," *IEEE Comm. Lett.*, vol. 18, no. 7, 2014.

[10] S.-Y. Chung and et al., "Analysis of sum-product decoding of low-density parity-check codes using a gaussian approximation," *IEEE Trans. Inf. Theory*, vol. 47, no. 2, 2001.

[11] D. Jincheng and et al., "Does gaussian approximation work well for the long-length polar code construction?" *IEEE Access*, 2017.

[12] S. Zhao and et al., "A reconciliation protocol based on polar codes for cvqkd," *Asian Quantum Information Science Conference*, 2016.