Efficient Rate-Adaptive Reconciliation in Quantum Key Distribution

Patcharapong Treeviriyanupab [1], Tharathorn Phromsa-ard [2], Jutaphet Wetcharungsri [3], Paramin Sangwongngam [3], Chun-Mei Zhang [4], Mo Li [4], Wei Chen [4], and Zheng-Fu Han [4]
[1] Department of Computer Science, Faculty of Science and Technology,
Phranakhon Rajabhat University (PNRU), Bangkok, Thailand.
patcharapong@pnru.ac.th
[2] Department of Electrical Engineering, Faculty of Engineering,
Chulalongkorn University, Bangkok, Thailand.
[3] National Electronics and Computer Technology Center (NECTEC),
National Science and Technology Development Agency (NSTDA), Pathum Thani, Thailand.
[4] Key Laboratory of Quantum Information, Chinese Academy of Sciences (CAS),
University of Science and Technology of China (USTC), Hefei, China.

***Abstract*—The purpose of reconciliation, one of classical aspects of quantum key distribution (QKD) protocol, is to mitigate errors after the distribution of quantum information over a quantum channel. In this work, a rate-adaptive method is proposed by means of a channel coding scheme where specific low-density parity-check (LDPC) codes are adapted in the Slepian-Wolf coding system. In order to estimate QBER, this method utilizes the properties of a maximum likelihood estimator based on the syndrome information instead of using the traditional key sampling. Evidently, numerical results confirm an improvement in the achievable secret key throughput in the current state-of-the-art QKD system.**

I. Introduction

Quantum key distribution (QKD) was first proposed in 1984 [1]. It is one of the quantum information processing technologies which employs properties of quantum mechanics to guarantee the secure key exchange for cryptographic purposes. Since the first publication of QKD prototype in 1992 [2], the QKD protocol has been developed into a competitive industry with commercial QKD products [3–5]. However, its applicability is still obstructed by the low key rates, which depend on both the detection facilitates of the quantum state at the optical hardware and the efficiency of purely classical information processing, known as *QKD post-processing*. In fact, the critical step of the post-processing is key reconciliation. For this reason, one promising way to increase the secret key rates is the invention of the highly efficient reconciliation protocol.

Previously, the most widely used reconciliation protocol, such as the well-known Cascade [6], has applied the interactive error correction based on binary searching. Although it is a simple method with proven efficiency, its speed is fundamentally limited by the network latency in the high interactivity that is not suitable for the high-speed QKD applications. Several applications for coding schemes have been proposed in [7–10]. These methods require the waste of using sample keys in order to estimate quantum bit error rate (QBER), and then to optimize their coding rate. Furthermore, there is an interactive reconciliation based on LDPC codes that works without a priori estimation of QBER, called Blind reconciliation [11]. It commonly uses the incremental redundancy with a hybrid automatic repeat request (HARQ) scheme by requiring round-trip communications until the feedback of successful decoding is declared. In [12] the analysis of a rate-adaptive reconciliation protocol has been presented by considering the effect of information leakage. Its results can increase the amount of a distillable secret key, but the design of the specific code has not been mentioned for the practical method.

The goal of this work is to propose a rate-adaptive reconciliation using LDPC codes to achieve higher system efficiency. Puncturing and shortening techniques are adapted to optimize coding rates in the lower bound of Slepian-Wolf coding where the cross-over probability distribution obviously corresponds to the various error rates in the QKD system. That is accomplished according to the estimated QBER, which is purely obtained from the LDPC code's syndromes by using the maximum-likelihood (ML) estimator. Its objective is to skip the step of traditional key sampling, and to get the longer secret key length after the QKD post-processing. Eventually, it impacts significantly on the achievable secret key generation rate responding to the high-speed QKD applications.

II. Slepian-Wolf Coding and Its Application to Reconciliation

Slepian-Wolf theorem deals with the lossless compression of two correlated sources, known as source coding with side information [13]. It is the main contribution for solving the key reconciliation problem based on the channel coding scheme as illustrated in Fig. 1. In this scheme, *Alice* and *Bob* have sifted keys modeled by binary random variables X and Y respectively, and it can be described by following two major steps:

1) Encoding: Alice encodes X and communicates the resulting stream $|M|$ to *Bob* over the public classical channel.

2) Decoding: Then, Y and $|M|$ are both fed into the channel decoder. Finally, *Bob* has the reconciled keys that will eventually become X'. It should be noted that the minimum information needed by *Bob* is under the condition of the Slepian-Wolf lower bound as $R_S \geq H(X|Y)$.

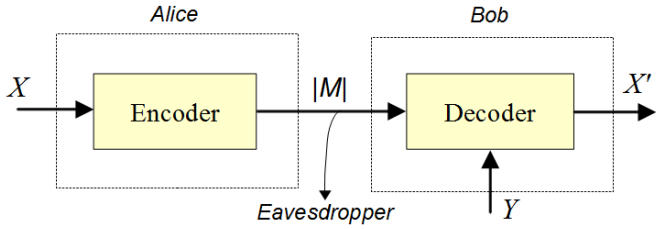

Fig. 1. Reconciliation as Slepian-Wolf coding scheme

The objective of this scheme is to transform X and Y into a pair of fully correlated variables, where the $Pr[X'=X]$ is equal to one. Since the communications of $|M|$ are sent over the public classical channel, eavesdropper (*Eve*) can obtain the information of the secret keys whenever this channel is insecure. Therefore, its efficiency must depend on the leakage of reconciliation $|M|$ that corresponds to the compression rate R_S.

Generally, the channel coding scheme can be applied to the Slepian-Wolf system for various applications such as distributed source coding for wireless sensor networks and multimedia applications. In fact, the Slepian-Wolf coding is closely related to the channel coding. For this reason, X and Y can be viewed as the input and the output over GF(2) of a binary symmetric channel (BSC) respectively. Let C be a linear block code which has a parity check matrix $\mathbf{H}$ of size $M \times N$. In the Slepian-Wolf scheme, the syndrome S can be calculated by compression of main information X^N, where $S = X^N\mathbf{H}^T$. Correspondingly in Slepian-Wolf coding, the compression rate R_S is the rate of syndrome denoted as $\frac{M}{N}$. It is equivalent to the channel coding rate (R_C) of linear code C, where R_C is $\frac{N-M}{N}$. Therefore, the relationship between Slepian-Wolf compression rate and channel coding rate can be expressed as

$$R_S = 1 - R_C. \tag{1}$$

For an efficient reconciliation, the channel coding rate R_C must be optimized to the Slepian-Wolf lower bound. Then, it can be rewritten as

$$1 - R_C \geq H(X|Y) \tag{2}$$

$$\geq H(e),$$

where e is the cross-over probability distribution among X and Y. In the case of a QKD system, e is equivalent to QBER which indicates the joint probability distribution among correlated information from *Alice*, and *Bob*, as well as *Eve*.

III. Rate-Adaptive Reconciliation with LDPC Codes Based on Slepian-Wolf System

In this section, a rate-adaptive reconciliation with the maximum-likelihood (ML) estimator is presented by means of a channel coding scheme where irregular LDPC codes are adapted for the Slepian-Wolf coding system. LDPC codes [14] are binary linear block code which can be described by a sparse (low-density) parity-check matrix $\mathbf{H}$. Let $\mathbf{H}$ has a dimension $(n - k) \times n$, where n is the block length, and k is the number of information bits. It allows to adapt the coding rate by puncturing the p symbols, and shortening the s symbols, which are denoted by $C(n - p - s, k - s)$. The proportion of punctured and shortened symbols is $d = p + s$.

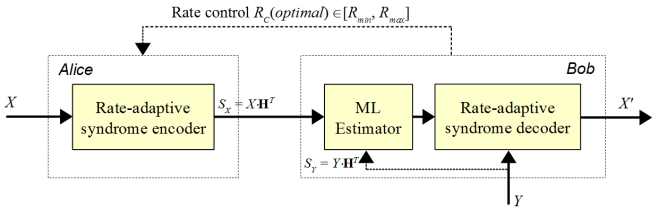

Fig. 2. Rate-adaptive reconciliation as a Slepian-Wolf coding scheme.

The proposed method can be constructed adaptively on its rate by using the Slepian-Wolf coding scheme as illustrated in Fig. 2. It is formed and described in three steps as:

Step 1) Syndrome encoding: Alice first calculates her syndrome S_X with a high code rate R_{max} ($p = d$, $s = 0$), and sends it to *Bob* over the public classical authenticated channel.

Step 2) QBER estimation: At *Bob*'s side, S_Y is also calculated by R_{max}. Then, the cross-over probability e of the correlated sources (*i.e.*, QBER of the QKD system) is computed using the ML estimator from syndrome matching S_{diff} [15–16]. This can be defined as the binomial distribution of $q(e)$ given by

$$q(e) = \sum_{i=1;\ i\ odd}^{d_c} \binom{d_c}{i} e^i (1-e)^{d_c - i}, \tag{3}$$

where d_c is the number of ones per row of parity check matrix $\mathbf{H}$. Then, the ML estimator for e with respect to S_{diff} is the inverse function of (3) as

$$\hat{e}(S_{diff}) = f^{-1}(\hat{q}(S_{diff})) = -\frac{\left(1 - 2\hat{q}(S_{diff})\right)^{\frac{1}{d_c}} - 1}{2}, \tag{4}$$

where $\hat{q}(S_{diff}) = \frac{1}{n-k}\sum_{m=1}^{n-k} S_{diff}$, and $S_{diff} = S_X \oplus S_Y$.

After this step, the knowledge of e can be utilized to optimize the channel coding rate $R_C(optimal)$, which is constrained with the density evolution threshold [17]. If $R_C(optimal) < R_{max}$, they then return to Step 1 in order to vary a number of p and s symbols closer to the Slepian-Wolf lower bound in

$$1 - R_C(optimal) = \frac{n-k-p}{n-s-p} \geq H(X|Y) \tag{5}$$

$$\geq H(e)$$

where $H(e)$ is the binary entropy function of QBER.

Step 3) Syndrome decoding: Bob decodes his sequences Y, which is constructed from the corresponding p and s symbols in (5). The advantage of syndrome decoding is to determine whether LDPC decoder is a success or a failure. By convention, this method is successfully concluded when *Bob* can produce his new syndrome ($S_{X'}$) that matches the syndrome received from *Alice* ($S_{X'} = S_X$), where $\Pr(X' = X)$ equals to one. Otherwise, the feedback of decoding failure is announced for re-estimation of QBER by returning to Step 2.

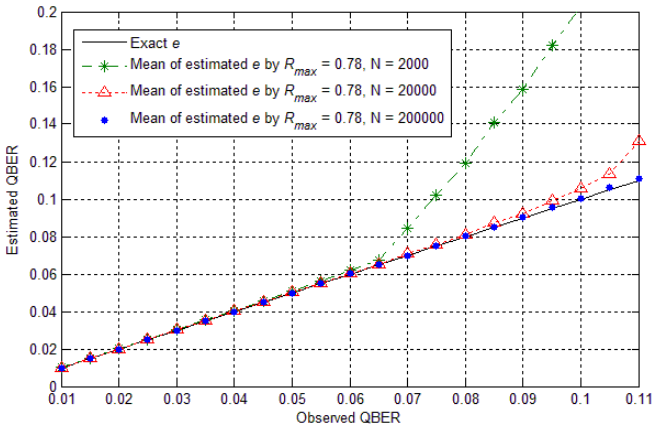

Fig. 3. Estimated bit error rate e by the ML estimator as a function of observed QBER.

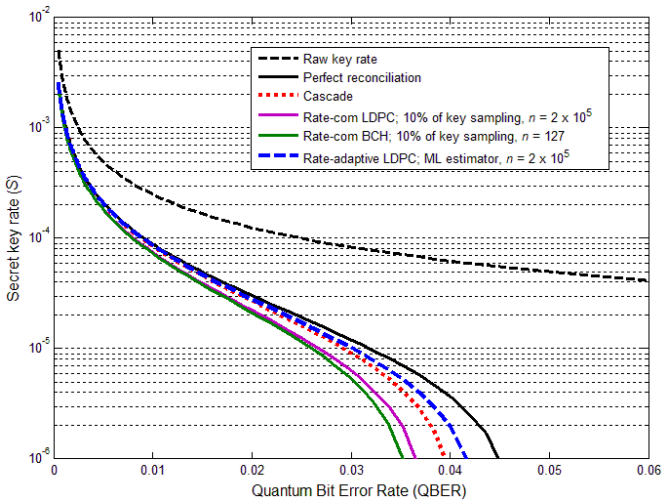

Fig. 4. Secret key rate S as a function of QBER. This simulation is calculated by α = 0.2 dB/km losses in optical fiber, a detection efficiency of η = 0.1, a dark counts probability of $p_d = 10^{-5}$, and q = 0.5.

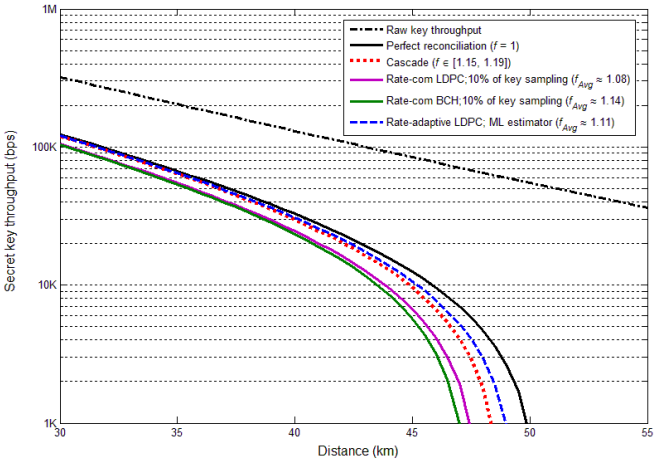

Fig. 5. Secret key throughput as a function of distance. This simulation is calculated by 1 GHz clock rate of the source over α = 0.2 dB/km, η = 0.1, $p_d = 10^{-5}$, and q = 0.5.

IV. Numerical Results and Discussion

Fig. 3 presents the mean of estimated bit error rate e (estimated QBER) considered by the high code rate R_{max} = 0.78 (modulated by $d = 2 \times 10^4$) of three LDPC codes from short to long block lengths, $N = 2 \times 10^3$, 2×10^4, and 2×10^5 bits. As illustrated in Fig. 3, the performance of the ML estimator is interpreted as that limitations for different block lengths $N = 2 \times 10^3$, 2×10^4, and 2×10^5 bits are achieved approximately with QBER $\in$ [0, 0.06], [0, 0.08], and [0, 0.11] respectively. Consequently, the efficient estimation of the LDPC codes with block length $N = 2 \times 10^5$ can cover the whole range of QKD (QBER: 1% – 11%) that is suitable for the rate-adaptive reconciliation method.

Next, the secret key rate S is evaluated in the view of the real inherent parameter in BB84 QKD systems [18], defined by

$$S = p_{\text{exp}} \cdot q \cdot r \,, \tag{6}$$

where p_{exp} is the total detection rate for the events when photons are sent from *Alice* to *Bob*, q is the protocol efficiency, and r is the secure secret key. The expression for r can be defined in terms of only the simple entropic quantities by

$$r = H(X \mid Z) - f \cdot H(X \mid Y) \,, \tag{7}$$

where f is the parameter of reconciliation efficiency defined by the ratio of disclosed information during the reconciliation step ($leak_{recon}$) and the limit of Slepian-Wolf bound $H(X|Y)$,

$$f = \frac{leak_{recon}}{H(X \mid Y)} = \frac{1 - R_C(optimal)}{H(e)} = \frac{n - k - p}{(n - s - p) \cdot H(e)} \,. \tag{8}$$

In the perfect reconciliation scheme, f is equal to one, and the maximum QBER acceptable to guarantee the security for any QKD system is 11%, which obtains a positive value of r.

In Fig. 4 and 5, the results are calculated with the real inherent factors of the single photon source and detection for BB84 QKD protocol. This significantly ensures the system practicality, when the reconciliation schemes are considered, especially in the case of high-speed QKD devices. As illustrated in Fig. 4 and 5, the proposed rate-adaptive LDPC codes (blue line) uses a mother code's rate R_C = 0.7 (modulated by $d = 2 \times 10^4$ between R_{min} = 0.67 and R_{max} = 0.78). It achieves the secret key rate (Fig. 4) and throughput (Fig. 5) closer to the theoretical limit on the perfect reconciliation (black line) than that of Cascade (red line), and the rate-compatible reconciliation with estimated QBER by wasting 10% of the traditional key sampling such as LDPC (purple line) and BCH codes [9] (green line). The advantage of the proposed rate-adaptive method significantly impacts the achievable secret key generation over the longest distance for the high QKD throughput applications such as real-time video conferences. However, the computation and communication times are also the main argument for reconciliation improvement in case of a practical realization. In the future work, the rate-adaptive methods with low complexity would be proposed to implement as the software integrated in the commercial QKD devices.

REFERENCES

[1] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175–179, 1984.

[2] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. “Experimental quantum cryptography,” *J. Cryptol*, vol 5, no 1, pp 3–28, 1992.

[3] ID Quantique SA. A fast and secure solution: high speed encryption combined with quantum key distribution [Online]. Viewed February 12, 2015. Available: http://www.idquantique.com

[4] Anhui Qasky Quantum Science and Technology Co. Ltd. [Online]. Viewed February 12, 2015. Available: http://www.qasky.com

[5] SeQureNet SARL. Cygnus: State-of-the-art CVQKD module [Online]. Viewed February 12, 2015. Available: http://www.sequrenet.com

[6] G. Brassard and L. Salvail, “Secret-Key Reconciliation by public discussion,” *Advance in Cryptology (EUROCRYPT’93*), pp. 410–423, 1994.

[7] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, “Efficient reconciliation protocol for discrete-variable quantum key distribution,” *in Proc. 2009 IEEE International Symposium on Information Theory*, pp. 1879–1883, July 2009.

[8] K. Kasai, T. Tsujimoto, R. Matsumoto, and K. Sakaniwa, “Information reconciliation for QKD with rate-compatible non-binary LDPC codes,” *the International Symposium on Information Theory and Its Applications (ISITA2010)*, pp 922–927, Oct. 2010.

[9] P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, and O. Sangaroon, “BCH-Based Slepian-Wolf Coding with Feedback Syndrome Decoding for Quantum Key Reconciliation,” *International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON 2012)*, Thailand, May 16-18, 2012.

[10] N. Benletaief, H.a Rezig, A. Bouallegue, “Toward efficient quantum key distribution reconciliation,” *Journal of Quantum Information Science*, vol.4, no.2, pp. 117–128, 2014.

[11] J. Martinez-Mateo, D. Elkouss, V. Martin, “Blind reconciliation,” *Quantum Information and Computation*, pp. 791–812, vol 12, 2012.

[12] D. Elkouss, J. Martinez-Mateo, V. Martin, "Analysis of a rate-adaptive reconciliation protocol and the effect of the leakage on the secret key rate," *Physical Review A*, vol. 87, no. 4, p. 042334, 2013.

[13] D. Slepian and J. K. Wolf, “Noiseless coding of correlated information sources,” *IEEE Transactions on Information Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[14] R. Gallager, “Low-density parity-check codes,” PhD thesis, Massachusetts Institute of Technology, 1963.

[15] V. Toto-Zarasoa, A. Roumy, C. Guillemot, "Maximum likelihood BSC parameter estimation for the Slepian-Wolf problem," *IEEE Communications Letters*, pp 232–234, vol 15, 2011.

[16] G. Lechner and C. Pacher, “Estimating channel parameters from the syndrome of a linear code, *IEEE Communications Letters*, vol. 17, issue 11, pp. 2148–2151, 2013.

[17] T. Tian, C. R. Jones, “Construction of rate-compatible LDPC codes utilizing information shortening and parity puncturing,” *EURASIP Journal on Wireless Communications and Networking*, pp. 789–795, vol 5, 2005.

[18] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” *Reviews of Modern Physics*, vol 81, pp. 1301–1350, 2009.