Rate-Adaptive LDPC-based Key Reconciliation for High Performance Quantum Key Distribution

Jesus Martinez-Mateo, Jose Luis Rosales, Vicente Martin[†]

Madrid Center for Computational Simulation, Universidad Politécnica de Madrid, 28660 Boadilla del Monte, Spain

[†] e-mail:vicente@fi.upm.es

ABSTRACT.— This contribution addresses the classical postprocessing part of Quantum Key Distribution. Although this part has been often neglected in favor of the quantum part, it is essential and has demonstrated to be a real bottleneck in high speed QKD. Because of the lack of speed of the older QKD generations, the study of key distillation protocols has been concentrated on typical information theoretical concepts such as efficiency, whereas the most practical aspects were left out. However, due to the speed of current devices now in the lab, but expected to debut in the market soon, practical aspects are starting to take a center stage position. In this work we investigate on the interplay between the most theoretically driven concepts and their practical implications. In particular, we concentrate on throughput as a measure that is of prime importance to the practical world and introduce magnitudes, like the frame error rate, that must be taken into account in QKD postprocessing.

The postprocessing or secret-key distillation process in quantum key distribution (QKD) mainly involves two well-known procedures: information reconciliation (IR) and privacy amplification (PA). Information or key reconciliation has been customarily studied in terms of **efficiency**. During this, some information needs to be disclosed for reconciling discrepancies in the exchanged keys. The leakage of information leak_{IR} is lower bounded by a theoretical limit, and it is usually parameterized by the reconciliation efficiency (or inefficiency), f_{IR}, i.e. the ratio of additional information disclosed over the Shannon limit, thus

$$\mathrm{leak}_{IR} = f_{IR} h(Q), \tag{1}$$

where Q is the quantum bit error rate, and $h(Q) = -Q\log_2(Q) - (1-Q)\log_2(1-Q)$ the binary Shannon entropy.

Most techniques for reconciling errors in QKD try to optimize this parameter. However, while an efficient reconciliation method improves the overall secret-key rate, it offers a biased view of the performance of real QKD devices where this must be measured in terms of secret key length per second (**throughput**) and take into account the bandwidth of every involved step. An original work that focus on the compromise between reconciliation efficiency and performance, and the impact of both parameters in the secret key throughput was presented in Ref. (1). Reconciliation and privacy amplification are then analyzed together, and a new parameter is considered, the performance or **frame error rate** (FER), i.e. ratio of keys that cannot be reconciled.

Let ε_{EC} denote the FER of a linear error correcting code, with coding rate R, used for reconciling discrepancies in the exchanged keys, a proper description for the ratio of information leakage is then given by

$$\mathrm{leak}_{IR} = (1-\varepsilon_{EC})(1-R) + \varepsilon_{EC}. \tag{2}$$

RESULTS.— Figs. 1 and 2 summarize the results presented in Ref. (1) using binary short block-length LDPC codes (quasi-cyclic) decoded over specialized HW (GPUs).

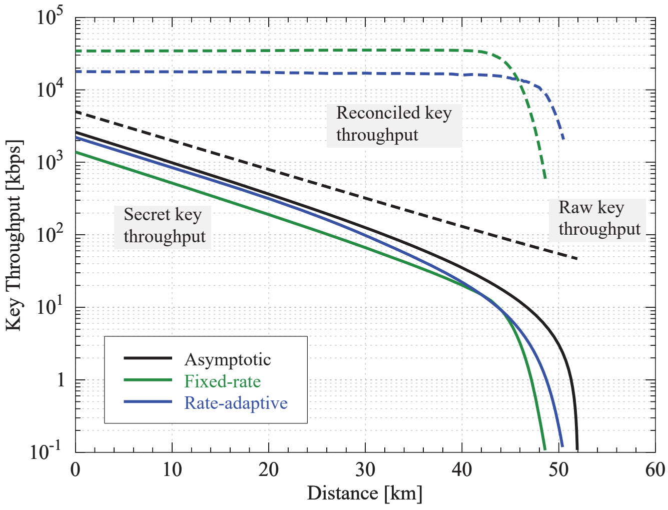

Fig. 1. Secret-key and reconciled key throughput for fixed-rate and rate-adaptive LDPC-based reconciliation.

Fig. 1 shows reconciled and secret-key throughput for fixed-rate and rate-adaptive reconciliation (as proposed in Ref. (2)) using a quasi-cyclic LDPC code of 2 kbits length and rate $R = 0.75$. In both cases, reconciliation is done with just one decoding procedure and thus only one message with the syndrome and information of punctured and shortened bits has to be exchanged. For the rate-adaptive approach, the proportion of punctured and shortened bits is chosen so that both, the modulated rate R and its computed FER, optimize the information leakage. The asymptotic key throughput for a perfect code is also shown. Note that, the amount of information published during reconciliation with a rate-adaptive code is smaller, hence its secret-key throughput is always higher and remarkably closer to the asymptotic case.

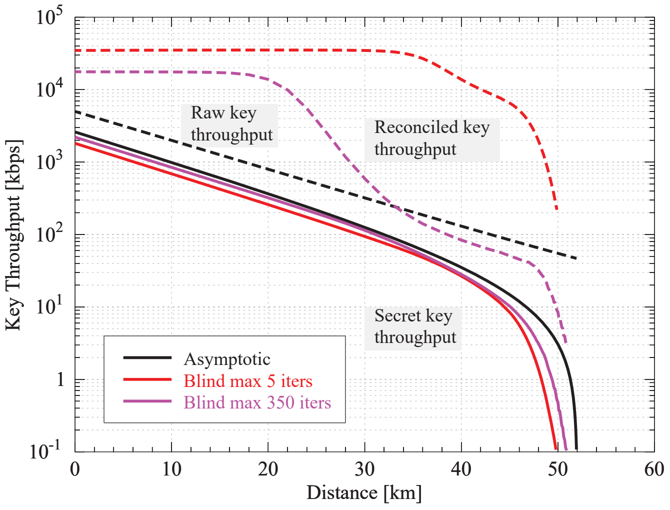

Fig. 2. Secret-key and reconciled key throughput for blind reconciliation.

Fig. 2 shows the performance of an interactive version of the rate-adaptive reconciliation, named blind reconciliation (as proposed in Ref. (3)), that adds feedback information to improve its performance. This allows to improve the average efficiency by repeating the decoding procedure with different proportions of punctured and shortened symbols, at the expense of the reconciliation throughput due to the interactivity of the algorithm. Two approaches with a maximum of 5 and 350 iterations are compared. For further details see Ref. (1).

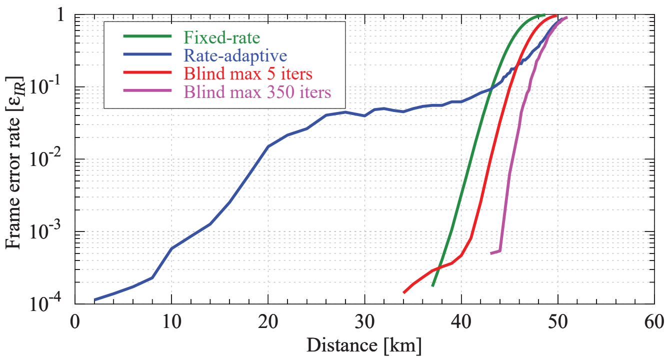

Fig. 3. Frame error rate for optimal secret-key rate.

Fig. 3 shows the FER that minimizes the information leakage according to Eq. (2) and thus maximizes the secret-key rate for those approaches considered in Figs. 1 and 2. As shown, at the point where FER values are above 90% the secret key rate drops.

ACKNOWLEDGMENTS.— Partially supported by the projects Hybrid Quantum Networks (HyQuNet), TEC2012-35673, funded by *Ministerio de Economía y Competitividad*, Spain, and Quantum Information Technologies Madrid+ (QUITEMAD+), S2013/ICE-2801, funded by *Comunidad Autónoma de Madrid*.

REFERENCES.

(1) J. Martinez-Mateo, D. Elkouss, and V. Martin, "Key Reconciliation for High Performance Quantum Key Distribution," *Sci. Rep.*, vol. 3, no. 1576, pp. 1–6, 2013.

(2) D. Elkouss, J. Martinez-Mateo, and V. Martin, "Information Reconciliation for Quantum Key Distribution," *Quantum Inform. Comput.*, vol. 11, no. 3&4, pp. 226–238, 2011.

(3) J. Martinez-Mateo, D. Elkouss, and V. Martin, "Blind Reconciliation," *Quantum Inform. Comput.*, vol. 12, no. 9&10, pp. 791–812, 2012.