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

Jesus Martinez-Mateo, Jose Luis Rosales, Vicente Martin
Universidad Politécnica de Madrid (UPM)
Campus de Montegancedo, 28660 Boadilla del Monte, Madrid, Spain

The postprocessing or secret-key distillation process in quantum key distribution (QKD) mainly involves two well-known procedures: information reconciliation and privacy amplification. 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 is lower bounded by a theoretical limit, and is usually parameterized by the reconciliation efficiency (or inefficiency), i.e. the ratio of additional information disclosed over the Shannon limit. Most techniques for reconciling errors in QKD try to optimize this parameter. For instance, the well-known Cascade (probably the most widely used procedure for reconciling errors in QKD) was recently shown to have an average efficiency of 1.05 [1] at the cost of a high interactivity (number of exchanged messages). Modern coding techniques, such as rate-adaptive low-density parity-check (LDPC) codes were also shown to achieve similar efficiency values exchanging only one message [2], [3], or even better values with few interactivity and shorter block-length codes [4].

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 [5]. 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. Figs. 1 and 2 summarize the results presented in [5] using short block-length LDPC codes (quasi-cyclic) decoded over specialized HW (GPUs).

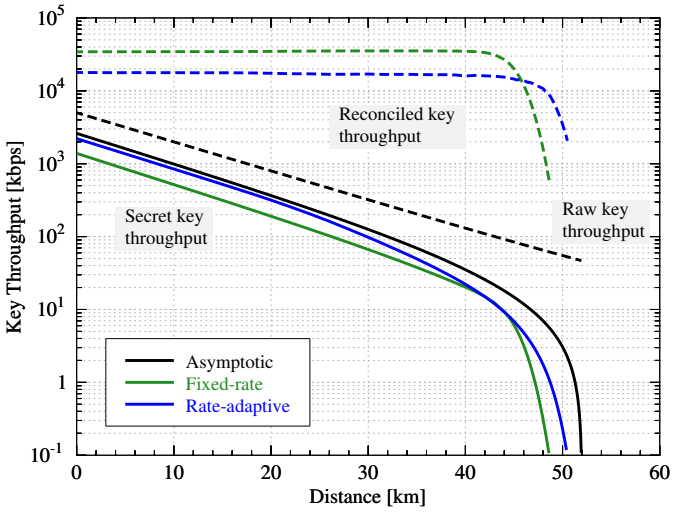

Fig. 1. Secret-key and reconciled key throughput for fixed-rate and rate-adaptive LDPC-based reconciliation.

Fig. 1 shows reconciled and secret-key throughput for fixed-rate and rate-adaptive reconciliation 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. The asymptotic key throughput for a perfect code is also shown. 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.

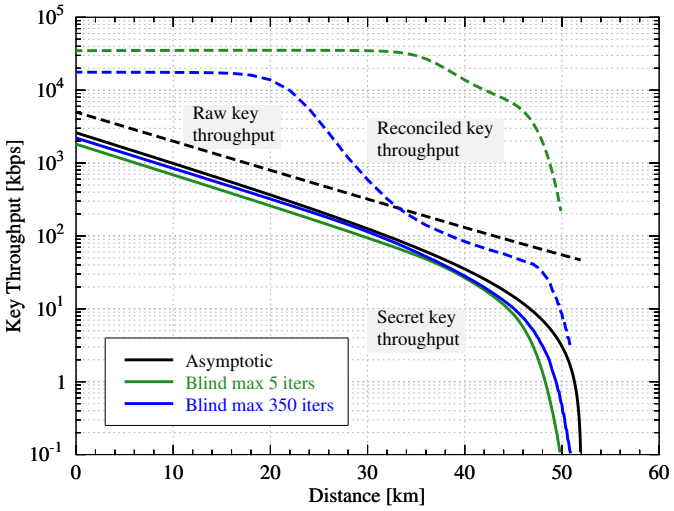

Fig. 2. Secret-key and reconciled key throughput for blind reconciliation.

Fig. 2 shows the performance of an interactive version of the rate-adaptive reconciliation, named blind reconciliation [4], 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, refer to [5].

References

[1] J. Martinez-Mateo, C. Pacher, M. Peev, A. Ciurana, and V. Martin, "Demystifying the information reconciliation protocol Cascade," *Quantum Inform. Comput.*, vol. 15, no. 5&6, pp. 453–477, 2015.

[2] D. Elkouss, J. Martinez, D. Lancho, and V. Martin, "Rate Compatible Protocol for Information Reconciliation: An application to QKD," in *IEEE Information Theory Workshop*, 2010, pp. 145–149.

[3] 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.

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

[5] ——, "Key Reconciliation for High Performance Quantum Key Distribution," *Sci. Rep.*, vol. 3, no. 1576, pp. 1–6, 2013.