INFORMATION RECONCILIATION FOR QUANTUM KEY DISTRIBUTION

D. Elkouss, J. Martinez-Mateo, D. Lancho, V. Martin*

Research group on Quantum Information and Computation.

Facultad de Informática, Universidad Politécnica de Madrid, Campus de Montegancedo, Madrid 28660, Spain

Introduction: Secret-key agreement, a well-known problem in cryptography, allows two parties holding correlated sequences to agree on a secret key communicating over a public channel. Secret-key agreement is usually divided into three different procedures: advantage distillation, information reconciliation and privacy amplification. The efficiency of each one of these procedures is needed if a positive key rate is to be attained from the legitimate parties' correlated sequences.

Quantum key distribution (QKD) allows the two parties to obtain correlated sequences, provided that they have access to an authentic channel. The new generation of QKD devices is able to work at higher speeds and in noisier or more absorbing environments. This exposes the weaknesses of current information reconciliation protocols, a key component to their performance. Here we present a new protocol based in Low Density Parity-Check codes that presents the advantages of low interactivity, rate adaptability and high efficiency, characteristics that make it highly suitable for next generation QKD devices.

Information reconciliation: Modern coding theory provides techniques that can be used within the QKD context in order to improve the efficiency of current procedures used for reconciliation. In this poster we propose the use of low-density parity-check (LDPC) codes [1] adapted for the information reconciliation problem in QKD. For this purpose, several families of LDPC codes were optimized for different information rates in the binary symmetric channel (BSC) [2]. Improved codes were then constructed by modifying the progressive edge-growth algorithm, in order to construct codes with irregular check-node degree distributions [3].

A new protocol was proposed to adapt the information rate of these codes [4], thus reducing the amount of information to be published during the reconciliation process (i.e. increasing the efficiency). Rate modulation is performed using puncturing and shortening, with asymptotic behaviour analyzed using the *density evolution* algorithm. Both techniques allow to adapt LDPC codes in real time with a small efficiency loss (see Fig. 1). The proposed protocol can be modified to improve the average efficiency by running an interactive communication session. In the modified protocol, punctured symbols are revealed in an incremental way [5]. With each additional step, the information rate is reduced until successful decoding is achieved.

Simulation results: Fig. 1 shows the experimental efficiency for *Cascade* [6], the *de facto* standard in information reconciliation for QKD, and several LDPC codes designed and constructed for different coding rates. Simulations have been computed for a target key length of 2×10^5 bits. This length is reduced by a 10% when the proposed rate-adaptive protocol is used ($\delta = 0.1$). Two different strategies have been simulated when using LDPC codes: (i) direct reconciliation without rate modulation, and (ii) a reconciliation procedure according the proposed information reconciliation protocol.

The blue and green lines show that the achieved efficiencies are closer to the theoretical limits than *Cascade* while the grey line shows that in the asymptotic case, if long enough codes are available, the efficiency would be close to optimal.

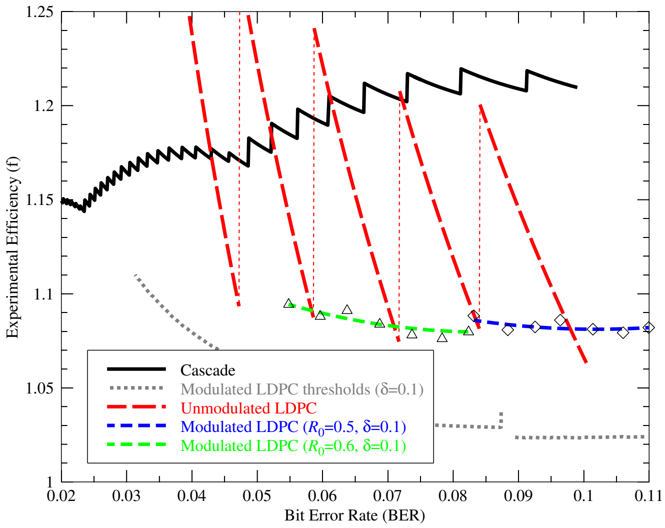

Fig. 1: Experimental efficiency for *Cascade*, and LDPC codes.

Conclusions: Modern coding theory provides the necessary tools to improve the efficiency of the information reconciliation process in the secret-key agreement context.

References

[1] T.J. Richardson and R.L. Urbanke, *The capacity of low-density parity-check codes under message-passing decoding*, IEEE Trans. Inf. Theory, Vol. 47, No. 2, pp. 599-618 (2001).

[2] D. Elkouss, A. Leverrier, R. Alleaume and J.J. Boutros, *Efficient reconciliation protocol for discrete-variable quantum key distribution*, in IEEE Int. Symposium on Inf. Theory, pp. 1879-1883 (2009).

[3] J. Martinez-Mateo, D. Elkouss and V. Martin, *Improved construction of irregular progressive edge-growth Tanner graphs in the waterfall region* (2010). To be published.

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

[5] J. Martinez-Mateo, D. Elkouss and V. Martin, *Interactive Reconciliation with Low-Density Parity-Check Codes*, in 6th Int. Symposium on Turbo Codes & Iterative Information Processing (2010). To appear.

[6] G. Brassard and L. Salvail, *Secret-Key Reconciliation by Public Discussion*, Lecture Notes in Computer Science, Vol. 765, pp. 410-423 (1994).

*vicente@fi.upm.es