Open-Source LDPC Error Correction for QKD

Adomas Baliuka[2,3], Elsa Dupraz[1], Rengaraj Govindaraj[2,3], Michael Auer[2,3,5], Peter Freiwang[2,3], Lukas Knips[2,3,4] and Harald Weinfurter[2,3,4]

1. IMT Atlantique, Lab-STICC, UMR CNRS 6285, F-29238, France
2. Ludwig-Maximilian-University (LMU), Munich, Germany
3. Munich Center for Quantum Science and Technology (MCQST), Munich, Germany
4. Max Planck Institute of Quantum Optics (MPQ), Garching, Germany
5. Universität der Bundeswehr München, Neubiberg, Germany

Abstract

Error correction is an essential step in the classical post-processing of all quantum key distribution (QKD) protocols. We present error correction methods optimized for discrete variable (DV) QKD and make them freely available as an ongoing open-source project (`github.com/XQP-Munich/LDPC4QKD`). Our methods are based on irregular quasi-cyclic (QC) low density parity check (LDPC) codes and state-of-the-art rate adaption techniques [1].

LDPC codes are the subject of active research with many applications, such as for Wi-Fi and digital television. They have been used for QKD error correction for decades, together with methods such as Cascade [2].

A single LDPC code operates on a fixed number of symbols and is optimized for a specific noise level of the quantum channel. In practice, the quality of the quantum channel fluctuates over time and across applications of a single QKD system. To achieve efficient error correction would thus require a large set of LDPC codes. However, storing, selecting and using hundreds or even thousands of different codes is not feasible in practice. Rate adaption solves this issue by modifying a single LDPC code, thus adjusting it to the current channel.

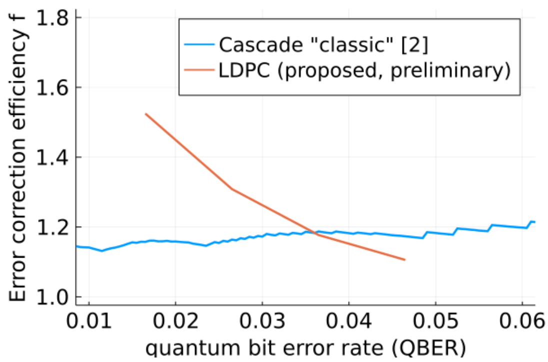

Figure 1: Error correction efficiency $f = r/h_2(\mathrm{QBER})$, where r is the rate of information leakage, and h_2 is binary entropy.

Error correction in QKD is a special case of Slepian-Wolf coding [3]. So far, the QKD community has been using rate adaption methods tailored to forward error correction, such as puncturing and shortening, which are sub-optimal for Slepian-Wolf coding [4]. Recently, more efficient rate adaption methods specialized for Slepian-Wolf coding have been developed [1, 3, 4]. Error correction in QKD can benefit from these insights to achieve better efficiency.

Due to the flexible nature of the proposed rate adaption, our coding scheme can be used not only for one-way error correction, but also for interactive protocols, which can achieve higher efficiency, *i.e.*, less leaked information, at the cost of more classical communication. Furthermore, while our current codes are optimized for DV-QKD, our construction and rate adaption methods can be applied more generally. We invite contributions from the research community and plan to add support for more protocols, such as CV-QKD, in the future, incorporating further developments in QKD and channel coding. We hope that the proposed methods will enable simpler, efficient and practical implementations of error correction for QKD post-processing.

References

[1] F. Ye, E. Dupraz, Z. Mheich, K. Amis, *IEEE Transactions on Communications* **67**, 3879 (2019).

[2] J. Martinez-Mateo, *et al.*, *Quantum Info. Comput.* **15**, 453–477 (2015).

[3] A. Liveris, Z. Xiong, C. Georghiades, *IEEE Communications Letters* **6**, 440 (2002).

[4] D. Varodayan, A. Aaron, B. Girod, *Signal Processing* **86**, 3123 (2006).