On the problem of non-zero word error rates for fixed-rate error correction codes in CVQKD

S. Johnson(1), A. Lance(2), L. Ong(1), M. Shirvanimoghaddam(1), T.C. Ralph(3) and T. Symul(2)

Poster presented at: QCrypt 7th International Conference on Quantum Cryptography, 2017 Sep. 18-22, Cambridge UK

(1) School of Electrical Engineering and Computer Science, The University of NewCastle, Australia
(2) QuintessenceLabs Pty. Ltd., Canberra, Australia
(3) Centre for Quantum Computation and Communication Technology, School of Mathematics
and Physics, University of Queensland, Brisbane, Australia

Overview

The maximum operation range of continuous variable quantum key distribution systems is constrained by the efficiency of the forward error correction post-processing step. We show that the current definition of this forward error correction efficiency can exceed unity when employing fixed-rate error correction codes operating at high word error rates, which in turn would lead to achieving positive secret key over an entanglement breaking channel. We propose a new bound for the secure key rate equation and show new optimisation strategies for forward error correction codes.

Background

Continuous variable quantum key distribution has been demonstrated for distances up to 100 km in optical fibers[1,2]. One of the main technological difficulty to achieve a positive key over large distances is to design Forward Error Correction (FEC) codes that achieve high efficiency at low Signal to Noise Ratio (SNR). The efficiency β of a FEC is defined as:

$$\beta_{FEC} = R / I_{AB}$$

Where I_{AB} is the theoretical channel capacity achievable for a given SNR, and R is the actual rate of the FEC code achieving perfect decoding for that SNR.

LDPC - a First Pass

Multi Edge Low Density Parity Codes (ME-LDPC) can achieve high efficiency at low SNR[3]. In this regime, however, practical ME-LDPC codes exhibit a non zero Word Error Rate (WER), meaning they have a probability p_{fail} to fail to decode a codeword.

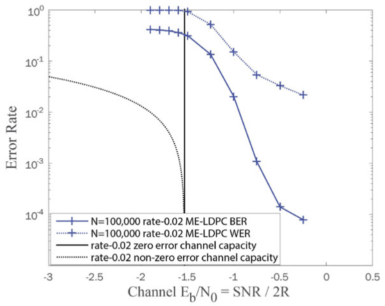
In order to take into account both the efficiency and WER of the ME-LDPC a new formulation of the key rate has been proposed[4]:

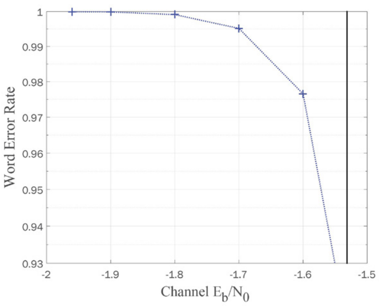
$$\Delta I = (\beta I_{AB} - I_E) (1 - p_{fail})$$

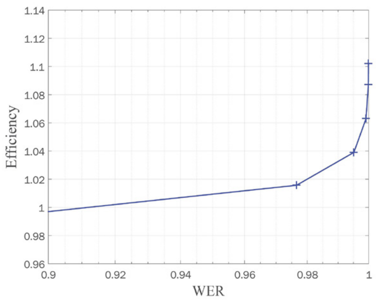
LDPC - a Closer Look

The theoretical asymptotical (WER=0) efficiency of a ME-LDPC can be estimated using the density evolution formalism. In practice ME-LDPC decoders accept codewords of finite length and therefore can function with an efficiency greater than unity.

The following figures show the WER and efficiency of a rate 0.02 ME-LDPC working on a codeword of size N=100,000.







The Issue

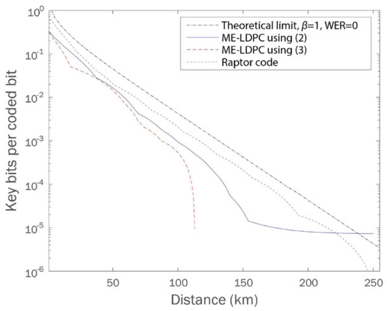
In the accepted formalism ME-LDPC codes working with an efficiency greater than unity allow establishment of a positive key over an entanglement breaking channel.

Another Approach

The non zero WER of the ME-LDPC can be interpreted as a post-selection step. A lower bound for the key rate can therefore be derived as follow:

$$\Delta I = (1 - p_{fail}) \beta I_{AB} - I_E$$

Although the previous bound is not tight, positive key rate can still be achieved: It is possible to keep using these ME-LDPC codes with a noticeable drop of performance only in the high loss regime. Alternatively rateless codes with zero WER such as the Raptor codes should be considered[6].



References

[1] P. Jouguet et al., Nature Photon. 7, p. 378 (2013)
[2] D. L. Huang et al., Scientific Rep. 6, 19201 (2016)
[3] T. J. Richardson et al., IEEE Trans. Inform. Theory, 47, 2, p. 619, (2001)
[4] J. Lodewyck et al., Phys. Rev. A 76, p. 042305 (2007)
[5] J. P. Aldis, Electronics Letters, 28, 13, p. 1252 (1992)
[6] M. Shirvanimoghaddam et al., IEEE International Conf. on Comm., (2016)
This paper: New Journal of Physics, Volume 19, February 2017