High effective efficiency LDPC codes for CV-QKD

T. Symul[1,†], S. Johnson[2] & A.M. Lance[1]

[1]QuintessenceLabs Pty. Ltd., Canberra ACT, Australia
[2]School of Engineering, The University of Newcastle, Australia
[†] Corresponding author: ts@quintessencelabs.com

Abstract

High efficiency error reconciliation, typically achieved by using Multi Edge Low Density Parity Codes (ME-LDPC), is necessary for CV-QKD to reach large transmission distance. The commonly accepted definition of the efficiency, however, is problematic as it does not take into account the Frame Error Rate (FER) of LDPC, and therefore is theoretically and provably unbounded (i.e. can tend to infinity), if one can accept increasingly larger FER. Here we report new ME-LDPC code construction allowing high efficiency ($>$0.91) with very low FER ($<$0.008), allowing for a large effective efficiency, over a large continuous range of SNR (between -20.5dB to -6dB).

Introduction

The advent of moderate to long distance Gaussian modulated CV-QKD has been made possible primarily through the combination of very efficient Gaussian to binary mapping methods [1] and ME-LDPC codes [2]. The reconciliation efficiency β of the reconciliation procedure is defined as:

$$\beta = \frac{R}{I_{AB}} \tag{1}$$

where R is the error correction code rate, and I_{AB} is the mutual information shared between Alice and Bob, and bounded by the Gaussian channel capacity $C = 0.5 \log_2(1 + \text{SNR})$, and where SNR is the signal to noise ratio of the Gaussian channel between Alice and Bob. From a theoretical perspective it is commonly understood that this efficiency is always less than 1 [3, 4, 5, 6].
It was discovered early on that in order to achieve high reconciliation efficiency $\beta > 0.95$ the error correction codes had to be operated in a regime where the Word Error Rate (WER), also referred as Frame Error Rate or FER in the literature, starts to deviate strongly from 0. The proposed solution to deal with a non-zero WER, and still in effect in most if not all of the reported experimental CV-QKD literature, has been to simply disregards the words that cannot be decoded, in effect expressing the asymptotic secret key rate as:

$$K = (1 - \text{WER})\,(\beta I_{AB} - \chi_E) \tag{2}$$

where χ_E is the Holevo bound of the amount of information that could have leaked to an Eve due to imperfections in the physical channel.
However, in 2017 [7] we demonstrated using real codes that the efficiency β as defined in 1 is not bounded by 1, and can actually tend to infinity at the cost of increasing WER. In particular we demonstrated that using $1/50$ codes from [2] with codeword length of 10^5 bits we could reach an efficiency $\beta > 1.05$. We therefore proposed that equations 1 and 2 were not correct, and that instead one had to use the 'true' asymptotic equations:

$$\beta_{eff} = (1 - \text{WER})\,\frac{R}{I_{AB}}, \text{ and} \tag{3}$$

$$K = \beta_{eff} I_{AB} - \chi_E \tag{4}$$

in order to make sure the asymptotic effective reconciliation efficiency never exceeds unity.

Since the publication of [7] it appears that all CV-QKD publications have kept using equations 1 and 2, meaning that the authors either:

- disagree with our results (in which case we are interested to discuss, and find out whether LDPC codes with efficiency $\beta > 1$ should be pursued);
- got discouraged by the relatively poor effective reconciliation efficiency achieved by known codes (in which case the results presented here might be of interest)

LDPC codes

Our proposed codes use the following degree distributions:

$$\boldsymbol{L} = \begin{bmatrix} 3 & 0 & 97 & 0 & 0 & 1 & 0.02 & 1 \\ 0 & 2 & 9 & 0 & 0 & 1 & 0.05 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0.93 & 1 \end{bmatrix}$$

$$\boldsymbol{R} = \begin{bmatrix} 1 & 2 & 0 & 0 & 0.04 \\ 2 & 2 & 0 & 0 & 0.01 \\ 0 & 0 & 2 & 1 & 0.4 \\ 0 & 0 & 3 & 1 & 0.53 \end{bmatrix}$$

Table 1: Rate 1/50 MELDPC

$$\boldsymbol{L} = \begin{bmatrix} 3 & 0 & 42 & 0 & 0 & 1 & 0.05 & 1 \\ 0 & 2 & 7 & 0 & 0 & 1 & 0.05 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0.9 & 1 \end{bmatrix}$$

$$\boldsymbol{R} = \begin{bmatrix} 3 & 2 & 0 & 0 & 0.05 \\ 0 & 0 & 2 & 1 & 0.25 \\ 0 & 0 & 3 & 1 & 0.65 \end{bmatrix}$$

Table 2: Rate 1/20 MELDPC

$$\boldsymbol{L} = \begin{bmatrix} 3 & 0 & 13 & 0 & 0 & 1 & 0.2 & 1 \\ 0 & 2 & 2 & 0 & 0 & 1 & 0.05 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0.75 & 1 \end{bmatrix}$$

$$\boldsymbol{R} = \begin{bmatrix} 12 & 2 & 0 & 0 & 0.05 \\ 0 & 0 & 3 & 1 & 0.3 \\ 0 & 0 & 4 & 1 & 0.45 \end{bmatrix}$$

Table 3: Rate 1/10 MELDPC

Where $\boldsymbol{L}$ and $\boldsymbol{R}$, are the variable nodes and constraint nodes distribution respectibvely of the Multi-Edge LDPC using the formalism developed in [8].

Decoding to the syndrome

Due to the presence of an error-less classical channel in CV-QKD, one can decode to an arbitrary syndrome:

1. Alice and Bob agree on a m(rows) $\times$ n(columns) LDPC matrix $\boldsymbol{H}$
2. Bob calculate the syndrome $\boldsymbol{s}$ (length m) of his binary codeword $\boldsymbol{u}$ (length n) with respect to $\boldsymbol{H}$ and transmits it to Alice.
$$\boldsymbol{s} = \boldsymbol{u} \cdot \boldsymbol{H}^\top \tag{5}$$
3. Alice uses a LDPC decoder for the code $\boldsymbol{H}$ to decode $\boldsymbol{v}$, which can be seen as a noisy version of $\boldsymbol{u}$, to the syndrome $\boldsymbol{s}$ rather than the typical approach of decoding $\boldsymbol{H}$ to obtain an all zero syndrome.

The code rate is given by:

$$R = \frac{n - m}{n} \tag{6}$$

Code extension

In order to obtain codes at lower rates, we extend the LDPC matrix. Starting from a base LDPC matrix $\boldsymbol{H}$, we construct the extended matrix $\boldsymbol{H}_{\text{ext}}$:

$$\boldsymbol{H}_{\text{ext}} = \begin{bmatrix} \boldsymbol{H} & \boldsymbol{0} \\ \boldsymbol{A} & \boldsymbol{I} \end{bmatrix}, \tag{7}$$

where $\boldsymbol{0}$ is a $m \times e$ all zero matrix, $\boldsymbol{I}$ is the $e \times e$ identity matrix and $\boldsymbol{A}$ is a $n \times e$ matrix with a single '1' per row placed at a random column position. The new rate R_{ext} is given by:

$$R_{\text{ext}} = \frac{n - m}{n + e}, \tag{8}$$

where n and m are the dimension of the base matrix $\boldsymbol{H}$, and e is the size of the extension.
There is no restriction on the extension size e, which can be larger than the original number of columns n.

Code puncturing

A well known method to improve the LDPC reconciliation efficiency at SNR higher than optimal is to perform puncturing. Puncturing is usually described as '*the process of removing some of the parity bits after encoding*'. However, in our case, as we are decoding to the syndrome, and all codewords bits have already been sent over the channel, a modified puncturing method needs to be implemented:

- Alice and Bob agree on a $n \times m$ LDPC matrix $\boldsymbol{H}$, and a puncturing size p, as well as the random position of the punctured bits.
- Bob construct a n bits codeword by using $n - p$ bits from his vector $\boldsymbol{u}$, and completing them with p random bits he draws at random using a QRNG.
- Bob sends the syndrome s to Alice.
- Alice set her first $n - p$ LLRs from her vector $\boldsymbol{v}$ and setting the remaining p LLRs to 0.
- Alice decodes her constructed LLR vector to the syndrome Bob has sent, leading her to decode p new bits that were never transmitted.

The code rate after puncturing is given by:

$$R_{\text{punc}} = \frac{n - m}{n - p}, \tag{9}$$

where n and m are the dimension of the base matrix $\boldsymbol{H}$, and p is the number of punctured bits. As expected, the number of punctured bits p cannot exceed the number of columns n of the base LDPC matrix $\boldsymbol{H}$.

Results

For the simulation results, base parity-check matrix have been pseudo-randomly constructed, to satisfy the three proposed degree distribution with a width of $n = 2 \times 10^6$ bits. We implemented an encoder and decoder for the proposed LDPC codes on NVidia GPUs. We used the multi-dimensional Gaussian to Binary transform from [1], and the efficiencies reported are with respect to the underlying GAWGN channel (i.e. Gaussian encoding). Due to the simplicity of the encoding we achieve an encoding bandwidth of 1.9×10^9 bits/s, whilst the decoder performance is captured in the Figure below.

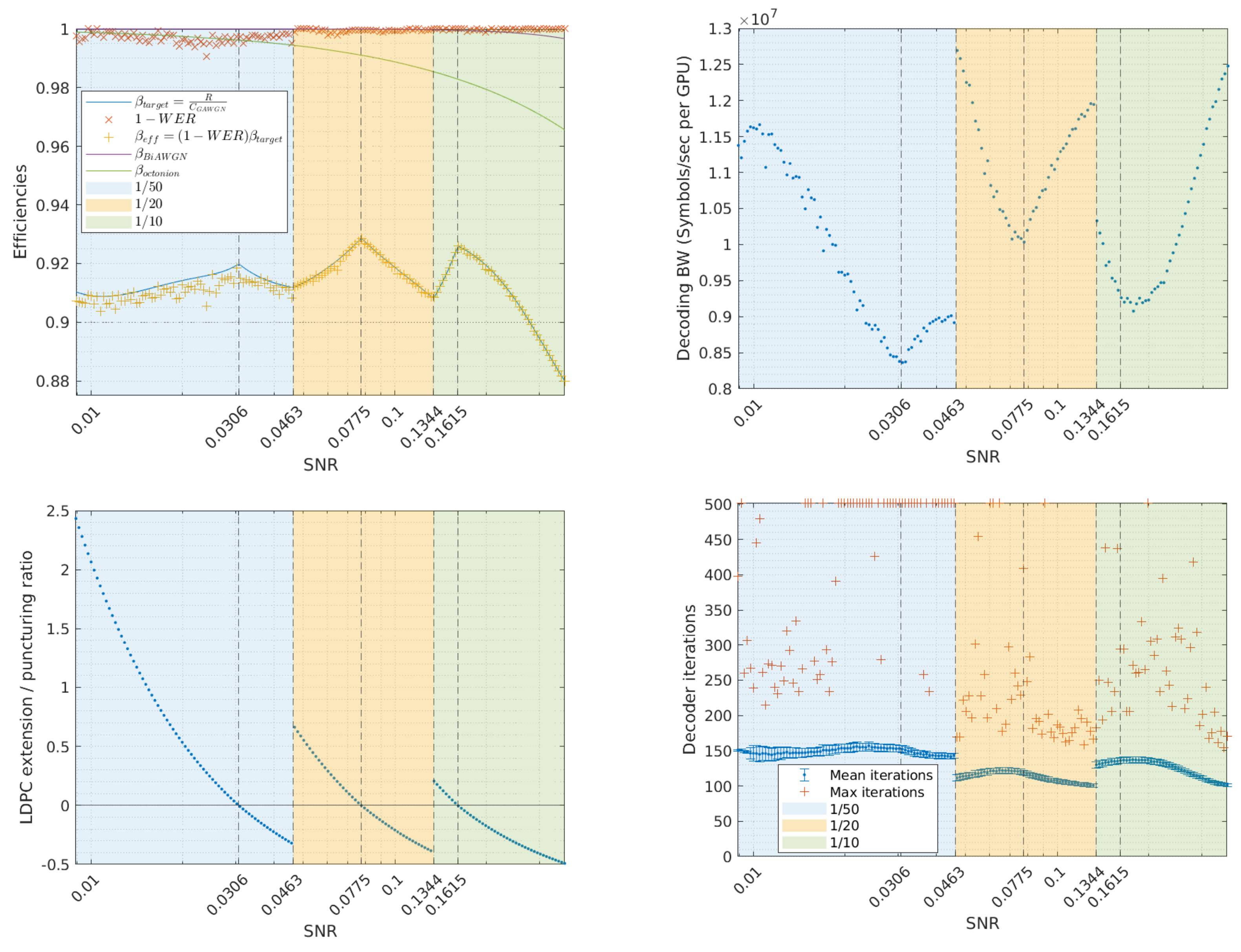

Figure 1: Efficiency (top left), Extension/puncturing ratio (bottom left), decoding bandwidth (top right), and decoding iterations statistics (bottom right) of the 1/50, 1/20 and 1/10 (word size $= 2 \times 10^6$ bits) with extension and puncturing. For each of the 162 SNR values a new simulation was performed over 6×10^9 symbols.

References

[1] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier, *'Multidimensional reconciliation for continuous-variable quantum key distribution'*, Phys. Rev. A, **77**, 042325, (2008).
[2] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, *'Long distance continuous-variable quantum-key-distribution protocols with a Gaussian modulation'*, Phys. Rev. A, **84**, 062317, (2011).
[3] F. Laudenbach, C.Pacher, C.-H. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hubel, *'Continuous-Variable Quantum Key Distribution with Gaussian Modulation - The Theory of Practical Implementations'*, Adv. Quantum Technol., 1800011, (2018).
[4] A. Denys, P. Brown, and A. Leverrier, *'Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation'*, arXiv:2103.13945v2, (2021).
[5] I. Derkach, V. C. Usenko, *'Applicability of Squeezed-and Coherent-State Continuous-Variable Quantum Key Distribution over Satellite Links'*, Entropy 2021, 23(1), 55(2021).
[6] A.G. Mountogiannakis, P. Papanastasiou, B. Braverman, and S. Pirandola, *'Composably-secure data-processing in continuous variable quantum key distribution'*, arXiv:2103.16589, (2021).
[7] S.J. Johnson, A.M. Lance, L. Ong, M. Shirvanimoghaddam, T.C. Ralph, and T. Symul, *'On the problem of non-zero word error rates for fixed-rate error correction codes in continuous variable quantum key distribution'*, NJP, **19**, 023003, (2017).
[8] T. Richardson and R. Urbanke, *'Mutli-Edge Type LDPC codes'* in Workshop honoring Prof. Bob McEliece on his 60th birthday, California Institute of Technology, Pasadena, California, (2002).