Iteration-Dependent Scaled Min-Sum Decoding for Low-Complexity Key Reconciliation in CV-QKD

Erdem Eray Cil* **and Laurent Schmalen**

Communications Engineering Lab, Karlsruhe Institute of Technology, Karlsruhe, Germany

*erdem.cil@kit.edu

Abstract: We introduce an iteration-dependent scaled min-sum decoding for low-rate LDPC codes in CV-QKD, achieving near-sum product algorithm performance with reduced complexity, and facilitating CV-QKD hardware implementation.

1. Introduction

Quantum computing has advanced remarkably in recent years, posing a significant threat to the current data encryption systems that rely on the computational hardness of the factoring problem [1]. Quantum key distribution (QKD) is a physical-layer security scheme that provides secure keys to be used with a symmetric encryption scheme. Continuous-variable quantum key distribution (CV-QKD) is a promising technique for secure communication over long distances, as demonstrated by the experimental achievement of a cryptographic key exchange over more than 200 km [2].

However, implementing CV-QKD in hardware remains a challenge, especially in the information reconciliation step, where the two parties need to generate a common raw key from their measurements. This step typically involves the use of multi-edge type (MET) low-density parity-check (LDPC) codes [3–5], which require large block lengths and high decoding iterations to achieve satisfactory performance [3]. These requirements result in a low decoder throughput, which reduces the secret key rate (SKR) compared to the achievable theoretical value. Therefore, low-complexity decoding algorithms are needed to optimize the system performance.

The scaled min-sum algorithm (MSA) is a frequently-used low-complexity decoding scheme, which approximates the sum-product algorithm (SPA) under the assumption of high signal reliability. This assumption holds for high-capacity channels, like optical channel, thus the performance gap between the MSA and the SPA is minimal. However, in the case of low-capacity channels such as quantum channels, this assumption is not met, leading to substantial deterioration in performance. Consequently, there is a need for a new low-complexity scheme tailored to CV-QKD operation.

In this work, we present a new method to compute the scaling coefficients for the scaled MSA that achieves near-SPA performance with lower complexity. We do this by rewriting the SPA check node (CN) update equation as a scaled MSA CN update equation and then estimating the scaling coefficients for each edge type and iteration. We evaluate the performance of our proposed iteration-dependent (ID) scaled MSA (ID-MSA) algorithm by decoding TBP LDPC codes with rates of $R = 0.01$ and $R = 0.1$ [3], which are suitable to be used in long-distance CV-QKD systems.

2. Check Node Update Approximation

In this section, we derive an approximation for the SPA CN update equation, which computes the output log-likelihood ratio (LLR) for each connected edge based on input LLRs received from its connected variable nodes (VNs).

The box-plus operator for input LLRs $L_1 = \alpha_1\beta_1$ and $L_2 = \alpha_2\beta_2$, where α_i and β_i represent the sign and the magnitude of the LLR respectively, can be expressed as [6, Ch. 5]

$$L_1 \boxplus L_2 = \alpha_1\alpha_2\left(\min(\beta_1,\beta_2) + \underbrace{\log\left(\frac{1+\exp\left(-|\beta_1+\beta_2|\right)}{1+\exp\left(-|\beta_1-\beta_2|\right)}\right)}_{:=\mathrm{s}(\beta_1,\beta_2)}\right). \tag{1}$$

To achieve the SPA performance with the MSA, we focus on the second term in (1), which represents the correction term of SPA over MSA. We denote this correction term as $\mathrm{s}(\beta_1,\beta_2)$. Without loss of generality, we assume that $\beta_1 \le \beta_2$ and $\beta_2 = a\beta_1$ for any $1 \le a \in \mathbb{R}$. Under this assumption, the correction term $\mathrm{s}(\beta_1,\beta_2)$ can be reformulated as follows:

$$\begin{aligned}
\mathrm{s}(\beta_1,\beta_2) &= \log\left(1+\exp\left(-(a+1)\beta_1\right)\right) - \log\left(1+\exp\left(-(a-1)\beta_1\right)\right) \\
&\overset{(i)}{=} \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k} \exp\left(-ka\beta_1\right)\left(\exp\left(-k\beta_1\right) - \exp\left(k\beta_1\right)\right) \\
&\overset{(ii)}{\approx} 2\sum_{k=1}^{\infty}(-1)^k \exp\left(-ka\beta_1\right)\beta_1 \overset{(iii)}{=} -\frac{2\,\beta_1}{1+\exp\left(a\beta_1\right)} = -\frac{2\,\beta_1}{1+\exp\left(\beta_2\right)}.
\end{aligned} \tag{2}$$

Here, step (i) involves expressing the logarithmic terms using the Taylor series. In step (ii), by assuming small values of $k\beta_1$, we employ $\exp(x) \approx 1+x$. This assumption is reasonable since the density of the degree-1 VNs in typical low-rate codes used in CV-QKD is high. To give an example, in the TBP-LDPC code of rate 0.01 [3], 98.9% of the CNs are connected to degree-1 VNs. It is important to note that this approximation holds for small values of $k\beta_1$, and the presence of $\exp(-ka\beta_1)$ aids in reducing the error between the actual function and its approximation for large values. In step (iii), we employ the geometric series $1/(1+x) = \sum_{k=0}^{\infty}(-1)^k x^k$.

Replacing the correction term in (1) with the approximate correction term in (2) yields

$$L_1 \boxplus L_2 \quad \approx \quad \alpha_1\alpha_2\left(\min(\beta_1,\beta_2) - \frac{2\,\min(\beta_1,\beta_2)}{1+\exp\left(\max(\beta_1,\beta_2)\right)}\right) = \alpha_1\alpha_2\min(\beta_1,\beta_2)\tanh\left(\frac{\max(\beta_1,\beta_2)}{2}\right). \quad (3)$$

Hence, the output LLR of the ith edge of CN j with VN connections $\mathcal{M}(j)$ can be written as:

$$L_i \approx \left(\prod_{k\in\mathcal{M}(j)/\{i\}} \alpha_k\right)\beta_m\left(\prod_{\ell\in\mathcal{M}(j)/\{i,m\}} \tanh\left(\frac{\beta_\ell}{2}\right)\right), \quad (4)$$

where m is the index of the minimum β. While we derived (4) for low-rate codes, the same expression can also be used for high rate codes with a small performance penalty [7].

3. Iteration-dependent Scaling for the MSA

In the previous section, we demonstrated that the SPA CN update equation can be effectively approximated using a scaled MSA CN update equation. The scaling factor, in this case, is determined by the product of hyperbolic tangent functions applied to the LLRs. Nonetheless, the computational demands of calculating this factor in real-time, involving hyperbolic tangent evaluations and multiplications, remain quite substantial. To mitigate this computational complexity, we introduce an alternative method: we propose using the expected value $\mathbb{E}\{\prod_\ell \tanh(\beta_\ell/2)\}$ for the MSA's scaling factor. This approach simplifies the method in [8] to calculate the scaling coefficients that depend on both decoding iterations and edge type.

In the context of a long-distance CV-QKD system, it becomes evident that fixed scaling coefficients as in [8], which do not consider the input LLR values, are not sufficient. This observation is corroborated by (4), where the second-smallest LLR value dominates the scaling term. Additionally, transmission over the quantum channel leads to LLR distributions with low mean and high variance. Consequently, it is imperative to consider the second-smallest LLR value in order to improve the scaling coefficients and approach performance levels close to the SPA. This approach enables us to express the CN update equation of the ID-MSA for the tth iteration as follows:

$$L_i^t = \left(\prod_{k\in\mathcal{M}(j)/\{i\}} \operatorname{sign}(L_k)\right)\beta_m \mathrm{c}_i^t(\beta_{m'}), \quad (5)$$

where m' is the index of the second smallest β. To obtain the ID scaling term $\mathrm{c}_i^t(\beta_{m'})$, we take the conditional expectation of the scaling factor in (4) given the second smallest β value and assume independent LLRs. The ID scaling term is then given by

$$\mathrm{c}_i^t(\beta_{m'}) = \mathbb{E}\left\{\prod_{\ell\in\mathcal{M}(j)/\{i,m\}} \tanh\left(\frac{\beta_\ell}{2}\right)\middle|\beta_{m'}\right\} = \tanh\left(\frac{\beta_{m'}}{2}\right)\prod_{\ell\in\mathcal{M}(j)/\{i,m,m'\}}\int_{x\in\mathbb{S}} \tanh\left(\frac{|x|}{2}\right) f_\ell^t(x)\mathrm{d}x, \quad (6)$$

where $\mathbb{S} = \{(-\infty,-\beta_{m'}]\cup[\beta_{m'},\infty)\}$ is the set of values that have a larger magnitude than the second minimum $\beta_{m'}$ and $f_\ell^t(x)$ is the probability density function of the LLR at iteration t for the edge type ℓ.

4. Results and Evaluation

In this section, we evaluate the performance of the ID-MSA to decode TBP-LDPC codes of rates $R = 0.01$ and $R = 0.1$ of block length N, as defined in [3]. All algorithms perform 500 decoding iterations on the output of the binary-input additive white Gaussian noise channel with noise power $\sigma_n^2 = N_0/2$.

To obtain the required statistics used in (6), we perform an extrinsic information transfer chart analysis using the code protograph [9]. Subsequently, we calculate look-up tables (LUTs) for $\mathrm{c}_i^t(\beta_{m'})$ for $t \in \{1,\ldots,500\}$, and $i \in \{1,\ldots,e\}$, where e is the number of different edge types in the code graph and equals 11 and 8 for the rates 0.01 and 0.1, respectively, and $\beta_{m'}$ is quantized to 32 values. Figure 1 shows how the mean scaling factor $\mathbb{E}_{\beta_{m'}}\{c_i^t(\beta_m')\}$ changes with the decoding iteration for each edge type for the code of rate $R = 0.01$. This figure clearly demonstrates the necessity of using multiple scaling factors in the MSA. To reduce the size and redundancy of the LUTs, we apply the K-means algorithm to obtain the final compressed LUT with 2600 entries for the decoding process.

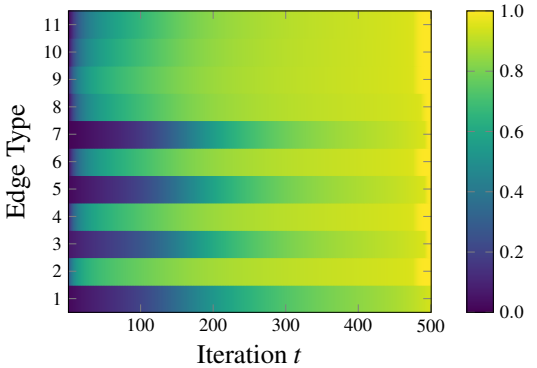
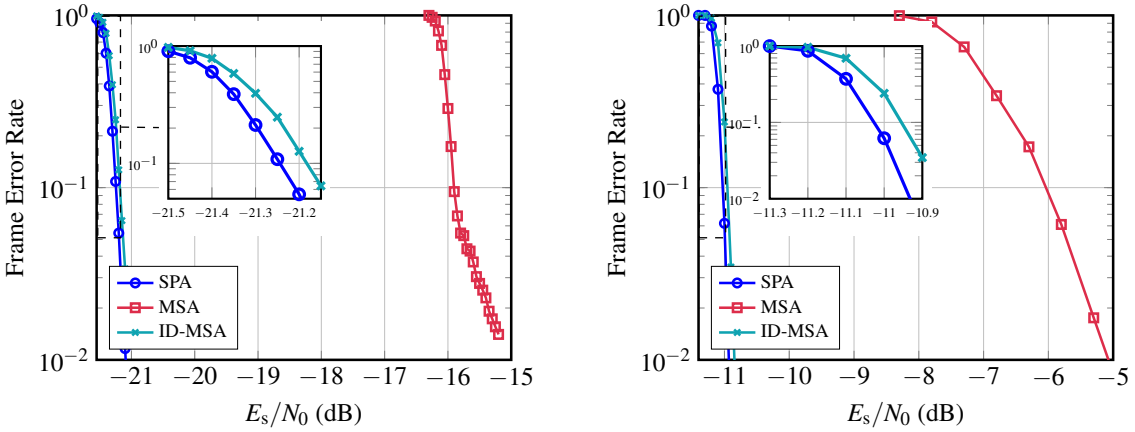


Fig. 1: Average values of $\mathrm{c}_i^t(\beta_{m'})$ for $R = 0.01$ TBP-LDPC code protograph [3]



(a) $R = 0.01$ TBP-LDPC code [3] with $N = 998400$ (b) $R = 0.1$ TBP-LDPC code [3] with $N = 128000$

Fig. 2: Performance comparison of sum-product algorithm (SPA), scaled min-sum algorithm with the factor 0.75 (MSA), and the proposed iteration-dependent MSA (ID-MSA)

We compare the performance of the algorithms at an FER of 0.1, since the secret key rate of the system is typically maximized at this value [2]. Fig. 2a shows that the SP algorithm outperforms the scaled MS algorithm by 5.2 dB for the $R = 0.01$ code. This large gap reduces the SKR significantly, making the MSA unsuitable for CV-QKD applications. However, by using iteration-dependent scaling coefficients, we can reduce this gap to only 0.059 dB, achieving a performance close to that of the SP algorithm. Similarly, Fig. 2b shows that the ID-MSA also performs close to the SP algorithm for the $R = 0.1$ code, with a gap of only 0.068 dB. Thus, the ID-MSA is a promising candidate for low-complexity key reconciliation in long-distance CV-QKD scenarios.

To compare the decoding complexity of ID-MSA with existing algorithms, we consider the CN update as described in [10], which employs (1) for the 3 LLRs with the smallest magnitudes to approach SPA performance. This algorithm requires two evaluations of (1) causing 2 table lookups for each CN update. In contrast, our proposed ID-MS algorithm requires only one lookup. Hence the decoding complexity of the proposed algorithm is less than the current approaches that can achieve near-SPA performance.

5. Conclusion

The ID-MSA proposed in this paper exhibits more than 5 dB performance improvement over the MSA, achieving near-SPA decoding performance with reduced computational complexity. Simulation results validate the efficacy of our approach and demonstrate its effectiveness across a wide range of low rates. This makes it a promising solution for efficient low-rate decoding, particularly suitable for CV-QKD systems and other related applications.

Acknowledgement

This work was funded by the German Federal Ministry of Education and Research (BMBF) under grant agreement 16KISQ056 (DE-QOR).

References

1. I. B. Djordjevic, *Physical-layer security and quantum key distribution* (Springer Nature, 2019), 1st ed.
2. Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Phys. Rev. Lett. **125**, 010502 (2020).
3. K. Gümüş and L. Schmalen, "Low rate protograph-based LDPC codes for continuous variable quantum key distribution," in *Proc. International Symposium on Wireless Communication Systems (ISWCS),* (2021).
4. P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," Phys. Rev. A **84**, 062317 (2011).
5. H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, and U. L. Andersen, "Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution," Phys. Rev. A **103** (2021).
6. W. E. Ryan and S. Lin, *Channel Codes - Classical and Modern* (Cambridge University Press, 2009).
7. M. Magaña and P. Poocharoen, "Different perspective and approach to implement adaptive normalised belief propagation-based decoding for low-density parity check codes," IET Commun. **6**, 2314–2325 (2012).
8. Z. Zhou, K. Peng, J. Song, and Z. He, "DE-aided ANMSA with edge classification and its application for 5G-NR LDPC codes," in *IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB),* (2021).
9. G. Liva and M. Chiani, "Protograph LDPC codes design based on EXIT analysis," in *Proc. IEEE GLOBECOM,* (2007).
10. E. Boutillon, F. Guillou, and J.-L. Danger, "Lambda-Min decoding algorithm of regular and irregular LDPC codes," in *Proc. International Symposium on Turbo Codes & Related Topics (ISTC) ,* (2003).