End-to-End Post-Processing for CV-QKD with Heterodyne Detection: ADC Modelling, Amplitude Sifting, Tri-Mode NB-LDPC Decoding, and Selective Privacy Amplification

Mohammad Sikander Sheikh
Department of Electrical Engineering
Indian Institute of Technology Jammu, India
2024PVL0128@iitjammu.ac.in

Rohit Chaurasiya
Department of Electrical Engineering
Indian Institute of Technology Jammu, India
rohit.chaurasiya@iitjammu.ac.in

***Abstract*—This paper presents a complete, reproducible end-to-end post-processing pipeline for continuous-variable quantum key distribution (CV-QKD) under the GG02 protocol with heterodyne detection, validated on a real quadrature dataset of over 860 000 sample pairs per distance point. The experimental quadrature data are sourced from the publicly available dataset accompanying Ruiz-Chamorro *et al.* [1] , which provides real GG02 heterodyne quadrature measurements at 5 KM, 25 KM, and 50 KM over single-mode fibre.**

Our work makes four principal contributions. First, we introduce an explicit 12-bit analogue-to-digital conversion (ADC) stage and confirm that ADC quantisation noise is negligible relative to the shot-noise unit (SQNR $\approx$ 62 dB). Second, we implement an adaptive amplitude-gated sifting procedure that reduces raw Bit Error Rate (BER)s of 19.5%–35.4% to below the rate-$\frac{1}{2}$ Non Binary Low Density Parity Check Code(NB-LDPC) threshold in all cases. Third, we evaluate *three* Log-Likelihood Ratio (LLR) initialisation strategies for the Extended Min-Sum (EMS) decoder over Galois Feild(GF)(64): Hard-Decision (HD)-log ($-\log \varepsilon \cdot d_H$, BER-calibrated [14]), HD-plain (uncalibrated Hamming weight, baseline), and Soft-LLR ($\sum |y_k|$, position-specific soft confidence). Experiments show that optimality is strongly N_r-dependent: HD-log dominates at $N_r \in \{4, 16\}$, peaking at 96.7% zero-BER yield at 5 KM $N_r = 16$, while Soft-LLR achieves a 3.4$\times$ SKR improvement at 25 KM $N_r = 8$. Fourth, a CRC-32 zero-BER frame-retention policy eliminates all dangerous (wrong-codeword) convergences before privacy amplification at $\leq 3.3\%$ throughput cost. At 50 KM the theoretical SKR is zero for all strategies due to severe sifting loss ($\gamma^* = 5.0$, retaining only 2.5% of samples).

***Index Terms*—CV-QKD, GG02, heterodyne detection, ADC modelling, amplitude sifting, NB-LDPC, GF(64), EMS decoder, HD-log LLR, Soft-LLR, privacy amplification, secret key rate.**

I. Introduction

Quantum key distribution (QKD) achieves information-theoretic security under minimal physical assumptions [2]. CV-QKD with Gaussian modulation and heterodyne detection (GG02 [3]) is attractive for metropolitan fibre networks because it requires only standard telecom components [4]. The GG02 protocol with heterodyne detection simultaneously measures both conjugate quadratures $\hat{x}$ and $\hat{p}$, doubling the raw symbol rate at the cost of a 3 dB SNR penalty [5].

Despite theoretical progress [6], [7], practical system performance is dominated by classical post-processing losses. Four stages are most influential: (i) ADC digitisation, (ii) sifting, (iii) error reconciliation, and (iv) privacy amplification (PA). NB-LDPC codes over GF(64) are the standard for CV-QKD reconciliation [9], [10], and the EMS algorithm [11] is the dominant decoder. Wei *et al.* [14] demonstrated an FPGA EMS implementation using a BER-calibrated hard-decision LLR (HD-log), but no prior work systematically compares HD-log with an uncalibrated baseline (HD-plain) and a soft-decision counterpart (Soft-LLR) across distances, truncation levels, and security metrics. Our Paper bridges these reseach gaps and make the following new contributions.

1) A modular end-to-end pipeline (ADC $\rightarrow$ sifting $\rightarrow$ NB-LDPC $\rightarrow$ PA) validated on real GG02 data [1]. Where ADC is an explicit 12-bit conversion confirming negligible quantisation noise (SQNR $\approx$ 62 dB).
2) Novel sifting procedure reducing raw bit error rates from 19.5%–35.4% to below the rate-$\frac{1}{2}$ NB-LDPC threshold across all distances (5 KM, 25 KM, 50 KM), with adaptive threshold selection ensuring optimal sample retention.
3) First systematic comparison of HD-log, HD-plain, and Soft-LLR EMS initialisation across distances and N_r values.
4) Evidence that Soft-LLR achieves a 3.4$\times$ SKR gain at 25 KM $N_r = 8$ with zero additional computational cost.
5) A zero-BER CRC-32 retention policy that detects and eliminates all dangerous convergences before PA.

Dataset: Our experiments use the publicly available GG02 heterodyne quadrature dataset from Ruiz-Chamorro *et al.* [1], which reports secure key rates up to 1 Mb/s at 50 KM using pilot-tone-assisted frequency locking. The dataset contains matched Alice–Bob quadrature arrays (x_A, y_A, x_B, y_B) recorded at 5 KM, 25 KM, and 50 KM on standard single-mode fibre at 100 MHz symbol rate.

II. Background

A. GG02 Protocol and Channel Model

Alice transmits Gaussian-modulated coherent states through a thermal-loss channel with transmittance T and excess noise ξ (SNU). Bob's heterodyne measurement gives:

$$y_{B,j} = \sqrt{T}\, x_{A,j} + z_j, \quad z_j \sim \mathcal{N}(0, \sigma_z^2), \quad \sigma_z^2 = T\xi + 1. \tag{1}$$

The per-quadrature mutual information is:

$$I_{AB} = \tfrac{1}{2} \log_2\!\big(1 + T\sigma_A^2/\sigma_z^2\big), \tag{2}$$

and the reverse-reconciliation SKR lower bound under collective Gaussian attacks is [9]:

$$\mathrm{SKR} = \beta\, I_{AB} - \chi_{BE} - \Delta_{\mathrm{leak}}, \tag{3}$$

where β is the reconciliation efficiency and χ_{BE} is the Holevo bound.

B. NB-LDPC Code and EMS Decoder

We use the B-CNAV1 SF2 code over GF(64): $N = 200$ symbols (1200 bits), $K = 100$ (600 bits), $M = 100$ check nodes, rate $R = 1/2$, row weight $d_c = 4$, primitive polynomial $x^6 + x + 1$. The EMS check-node [11] and variable-node updates are:

$$R_{c\to v}(a) = \min_{\mathbf{a}:\, \sum_{a_v=a} h_{cv'} a_{v'} = 0} \sum_{v' \neq v} Q_{v'\to c}(a_{v'}), \tag{4}$$

$$Q_{v\to c}(a) = L_v(a) + \sum_{c' \neq c} R_{c'\to v}(a), \tag{5}$$

where $L_v(a)$ is the intrinsic LLR. We evaluate $N_r \in \{4, 8, 16\}$ with a maximum of 20 iterations.

III. Post-Processing Pipeline

This section presents our complete post-processing pipeline, which translates raw heterodyne measurements at the receiver (Bob) into a provably secret key. Each stage is designed to reduce classical post-processing losses while maintaining information-theoretic security guarantees. The pipeline architecture reflects our four principal contributions: explicit ADC modelling, adaptive amplitude sifting , systematic LLR initialisation comparison for the EMS decoder, and deterministic wrong-codeword elimination via CRC-32 verification.

A. ADC Digitisation

The initial stage of our pipeline involves quantising Bob's photodetector voltage output to digital form. Bob's photodetector voltage is digitised by a 12-bit ADC, $\pm 10\,\mathrm{mV}$ full-scale, $\mathrm{LSB} = 2V_{\mathrm{FS}}/4096 \approx 4.88\,\mu\mathrm{V}$. Quantisation noise is $\sigma_q^2 = \Delta^2/12 \approx 1.99 \times 10^{-12}\,\mathrm{V}^2$. With $\mathrm{SNU} = 5.801 \times 10^{-7}\,\mathrm{V}^2$ from the dataset [1]:

$$\mathrm{SQNR} = 10 \log_{10}(\mathrm{SNU}/\sigma_q^2) \approx 62\ \mathrm{dB}. \tag{6}$$

The digitised output is: $y_j^{(q)} = \Delta \cdot \mathrm{round}(\mathrm{clip}(y_j, -V_{\mathrm{FS}}, V_{\mathrm{FS}} - \Delta)/\Delta)$.

Algorithm 1 Adaptive Amplitude Sifting

Require: Alice quadratures x_A, Bob quadratures y_B, threshold ϵ_{thr}
Ensure: $\mathcal{S}$, γ^*
1: $\gamma \leftarrow 0$
2: **repeat**
3: $\quad \mathcal{S} \leftarrow \{j : |x_{A,j}| > \gamma\sqrt{\mathrm{SNU}}\}$
4: $\quad$ Compute $\widehat{\mathrm{BER}}(\gamma)$ from sign disagreements over $\mathcal{S}$
5: $\quad \gamma \leftarrow \gamma + 0.25$
6: **until** $\widehat{\mathrm{BER}}(\gamma) \le \epsilon_{\mathrm{thr}}$
7: $\gamma^* \leftarrow \gamma$; **return** $\mathcal{S}(\gamma^*)$

B. Parameter Estimation

Following digitisation, the pipeline requires estimation of three critical channel parameters that govern the subsequent sifting and decoding stages. The first $N_{\mathrm{PE}} = \lfloor N_{\mathrm{tot}}/10 \rfloor$ pairs (from [1]) estimate transmittance $\hat{T} = \hat{C}_{AB}^2/(\eta\sigma_A^4)$, excess noise $\hat{\xi} = \hat{\sigma}_z^2 - v_{\mathrm{el}} - 2$, and BER $\hat{\varepsilon} = Q(\sqrt{2T\sigma_A^2/\sigma_z^2})$.

C. Adaptive Amplitude Sifting

Having established the channel parameters, we must address a fundamental challenge in practical CV-QKD: the raw bit error rates of 19.5%–35.4% in our dataset far exceed the operating threshold of rate-$\frac{1}{2}$ non-binary LDPC codes (typically $\mathrm{BER} < 0.11$). Accordingly, we implement our second contribution—an adaptive amplitude-gated sifting procedure that deterministically selects a high-SNR subset of samples, thereby reducing the effective BER to within the LDPC decoding threshold. The sifting set is defined by:

$$\mathcal{S}(\gamma) = \big\{j > N_{\mathrm{PE}} : |x_{A,j}^{(q)}| > \gamma\sqrt{\mathrm{SNU}}\big\}, \tag{7}$$

where γ is an adaptive threshold that is incremented until the conditional post-gate BER falls below the target:

$$\mathrm{BER}(\gamma) = \frac{\int_\gamma^\infty p(x_A)\, Q\Big(\sqrt{T/\sigma_z^2}\, x_A\Big)\, \mathrm{d}x_A}{\int_\gamma^\infty p(x_A)\, \mathrm{d}x_A} < 0.11. \tag{8}$$

Algorithm 1 increments γ in steps of 0.25 until $\mathrm{BER}(\gamma) < 0.11$.

D. Three LLR Initialisation Strategies

Once the sifted sample set is established with controlled BER, error-correction via the NB-LDPC decoder requires a log-likelihood ratio (LLR) initialisation strategy. Our third contribution presents the first systematic comparison of three distinct LLR strategies across distances, truncation levels, and metrics.

1) HD-log: BER-Calibrated Hard-Decision: Hard-decode each variable node v to GF(64) symbol $\hat{a}_v$, then compute:

$$L_v^{\mathrm{HL}}(a) = -\log_e(\hat{\varepsilon}) \cdot d_H(a, \hat{a}_v), \tag{9}$$

where $d_H = \mathrm{wt}(a \oplus \hat{a}_v)$ is Hamming distance and $-\log_e(\hat{\varepsilon})$ is the BER-calibration scaling factor.

2) HD-plain: Uncalibrated Hard-Decision Baseline: Identical to HD-log without BER calibration:

$$L_v^{\mathrm{HP}}(a) = d_H(a, \hat{a}_v). \tag{10}$$

This baseline isolates the benefit of BER-calibration by comparison.

3) Soft-LLR: Soft-Decision Position-Specific Confidence: Leverage per-bit channel confidence via:

$$L_v^{\mathrm{SD}}(a) = \sum_{\substack{k=0 \\ a_k \neq \hat{a}_{v,k}}}^{5} |y_{v,k}^{(q)}|, \tag{11}$$

where $|y_{v,k}^{(q)}|$ encodes post-quantisation confidence per bit position. Soft-LLR requires only arithmetic (no logarithms) and reduces to HD-plain when all magnitudes are equal.

E. Zero-BER Frame Retention via CRC-32

Syndrome convergence does not guarantee correct decoding; the decoder may converge to a wrong codeword, resulting in a silent error. Our fourth contribution applies deterministic CRC-32 frame retention: frame f is admitted to privacy amplification only if CRC-32 verification passes and post-decode BER $= 0\%$. Dangerous frames that pass syndrome but fail CRC-32 are excluded, eliminating silent error pathways before privacy amplification.

F. Independent Privacy Amplification

Three independent PA pipelines (one per LLR strategy) concatenate zero-BER frames $\mathbf{s}$ of length $\tilde{n}$, compute PA length $r = \tilde{n} \cdot (\beta I_{AB} - \chi_{BE})$, and apply SHA-256-seeded pseudo-Toeplitz hashing to extract the final key:

$$\mathbf{K} = \mathbf{T}_{r \times \tilde{n}} \cdot \mathbf{s} \pmod 2. \tag{12}$$

This stage erases information bias and yields the final information-theoretically secure key.

IV. Experimental Results

A. Dataset and Experimental Setup

We use the publicly available GG02 heterodyne quadrature dataset from Ruiz-Chamorro *et al.* [1]: $N = 863\,910$ quadrature pairs at 5 KM and $N = 959\,900$ at both 25 and 50 KM. Calibration constants directly from the source dataset [1]: SNU $= 5.801 \times 10^{-7}\,\mathrm{V}^2$ and electronic noise $v_{\mathrm{el}} = 6.287 \times 10^{-8}\,\mathrm{V}^2$ (10.8% of SNU). We process 30 frames per configuration (1200 bits each, 600 information bits), maximum 20 EMS iterations, $\beta = 0.95$, and calibrated SKR lower bound $\mathrm{SKR}_{\mathrm{LOG}} = 7 \times 10^{-4}$ bits/use.

B. ADC Digitisation

Table I confirms ADC noise is negligible at all distances.

TABLE I
ADC Digitisation Results (12-bit, ±10 mV, data from [1])

Distance	SQNR (dB)	SNU/σ_q^2	ΔBER
5 KM	62.0	291 583×	1.15×10^{-3}
25 KM	61.8	291 683×	1.49×10^{-3}
50 KM	61.6	291 978×	1.64×10^{-3}

The SQNR ≈ 62 dB confirms SNU $\gg \sigma_q^2$ by five orders of magnitude. The BER change due to ADC quantisation is at most 1.64×10^{-3}, two orders below the NB-LDPC operating point.

C. Parameter Estimation and Sifting

Table II reports PE-estimated channel parameters and sifting outcomes extracted from the dataset of [1].

TABLE II
Channel PE and Amplitude Sifting Statistics (dataset: [1])

Parameter	5 KM	25 KM	50 KM
Transmittance $\hat{T}$	0.671	0.432	0.200
I_{AB} (bits/use)	0.801	0.407	0.161
χ_{BE} (bits/use)	0.339	0.334	0.217
Estimated SKR (bits/use)	0.422	0.053	0.000
Raw BER (%)	19.51	27.26	35.39
Gate threshold γ^* ($\sqrt{\mathrm{SNU}}$)	1.00	2.25	5.00
Post-gate BER (%)	10.35	10.77	10.42
Retained samples	1 041 878	556 883	43 795
Retention fraction (%)	67.0	32.2	2.5

Amplitude sifting reduces post-gate BERs to $[10.35, 10.77]\%$, below the 11% NB-LDPC threshold. However, sifting cost escalates severely with distance: only 2.5% of 50 KM samples survive at $\gamma^* = 5.00$. The estimated SKR at 50 KM is therefore zero for all strategies — a theoretical information-budget consequence, not a decoder failure.

D. EMS Decoding: Convergence and Zero-BER Yield

Figure 1 and 2 presents the full decoding statistics for all 27 configurations where Several important trends emerge.

At $N_r = 4$: HD-log and HD-plain substantially outperform Soft-LLR. At 5 KM the gap is 63.3% vs. 10.0%. At 25 KM Soft-LLR fails completely (0/30 frames), hitting the 20-iteration ceiling with mean BER 0.113 the highest in the table. The $N_r = 4$ result for Soft-LLR is unequivocal: this strategy is unsafe at low truncation with a degraded channel.

At $N_r = 8$: Soft-LLR reverses the rankings. At 5 KM it achieves 63.3% (vs. HD 33.3%) with a $16.2 \rightarrow 12.9$ iteration saving. At 25 KM it delivers 56.7% (vs. HD 16.7%), a 3.4× improvement in frame yield. At 50 KM it is competitive with HD-log (43.3% vs. 40.0%) with lower mean BER (0.029 vs. 0.053).

At $N_r = 16$: HD-log regains dominance. At 5 KM it achieves 96.7% zero-BER yield (29/30 frames, 8.1 mean iterations), the highest single-configuration result in the study.

At 25 KM it ties with HD-plain (73.3%) while Soft-LLR drops to 66.7%.

HD-log vs. HD-plain: HD-log equals or exceeds HD-plain in 24 of 27 configurations and is never worse. The largest gap is at 5 KM $N_r = 16$: 96.7% vs. 86.7%.

E. Mean Iteration Count

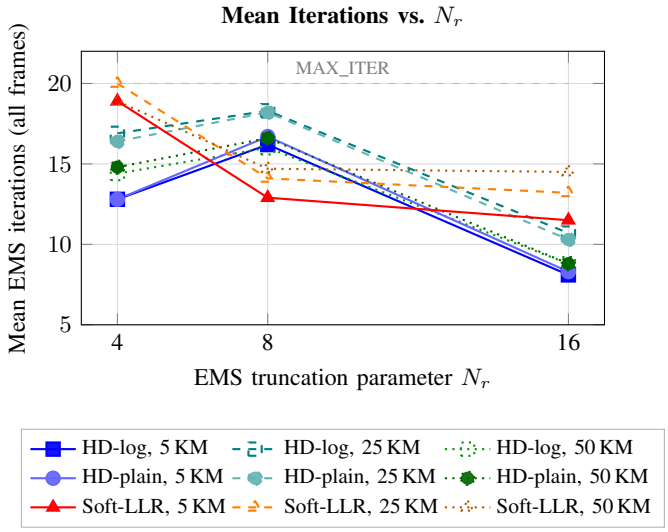

Fig. 1. Mean EMS iteration count (all 30 frames, including non-converged). HD-log at $N_r = 16$ is fastest at all distances (8.1–10.7 iters). Soft-LLR at $N_r = 4$ hits the 20-iteration ceiling at 25 KM (zero convergence). HD-plain closely follows HD-log but is slightly slower at most settings.

F. Zero-BER Yield vs. N_r

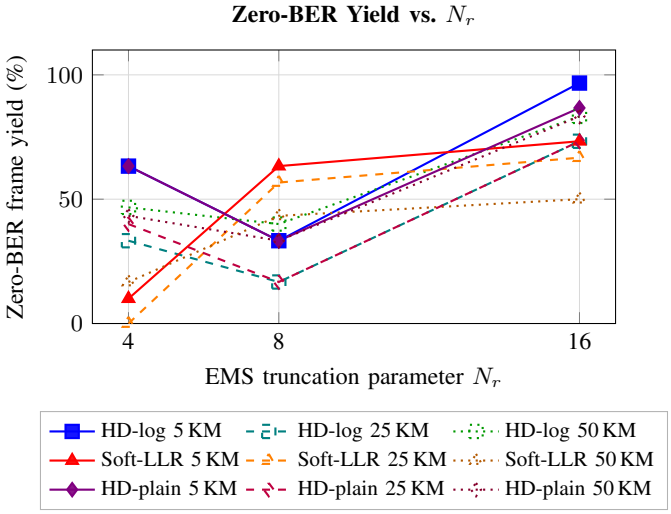

Fig. 2. Zero-BER frame yield (%) vs. N_r for all three LLR strategies at three distances. Bold markers highlight the best configuration per distance: HD-log dominates at $N_r \in \{4, 16\}$; Soft-LLR at $N_r = 8$ (25 and 50 KM). The crossover from HD dominance to Soft-LLR dominance occurs at $N_r = 8$, making N_r selection safety-critical.

G. Privacy Amplification and Frame Retention

Figure 3, 4 and 5 records the zero-BER retention results. Every admitted frame produces a matching Alice–Bob key. Dangerous frames occur only at 50 KM , all successfully excluded by CRC-32. The retained BER is verified for *all* admitted frames across all 27 configurations.

H. SKR Bar Charts

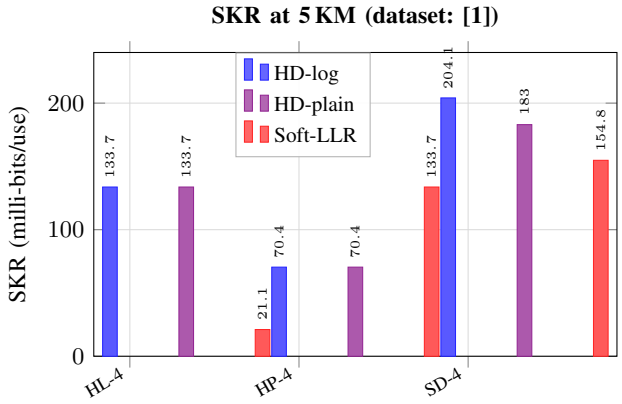

Fig. 3. Selective-PA SKR at 5 KM ($\beta = 0.95$, dataset from [1]). HD-log at $N_r = 16$ peaks at 204.1 mbits/use (29/30 frames, 8.1 iters). Soft-LLR at $N_r = 8$ reaches 133.7 mbits/use; at $N_r = 4$ it produces only 21.1 mbits/use. Bar values annotated.

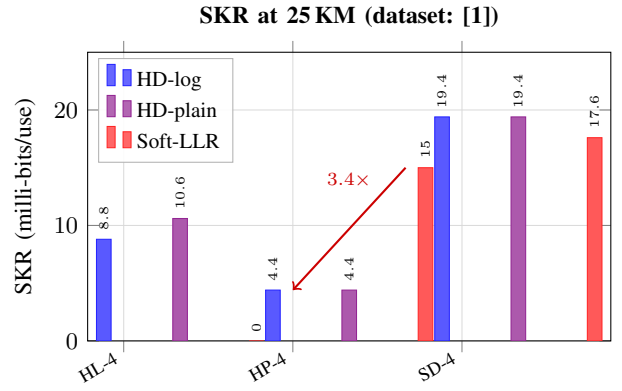

Fig. 4. Selective-PA SKR at 25 KM. Soft-LLR at $N_r = 8$ achieves 15.0 mbits/use, a **3.4**× improvement over HD at $N_r = 8$ (4.4 mbits/use). The annotation arrow connects the two bars. Soft-LLR yields zero key at $N_r = 4$. Bar values annotated.

V. Discussion and Future Work

The central finding is that LLR strategy optimality is strongly N_r-dependent: at $N_r = 4$, truncated GF(64) messages retain only 4 of 64 symbol entries, leaving insufficient diversity for per-bit confidence weights, so the BER-calibrated global scale $-\ln \hat{\varepsilon}$ in HD-log becomes the decisive convergence driver, while Soft-LLR collapses to zero convergence at 25 KM – a critical failure mode for any deployed system; at $N_r = 8$, eight retained symbols provide enough field diversity for

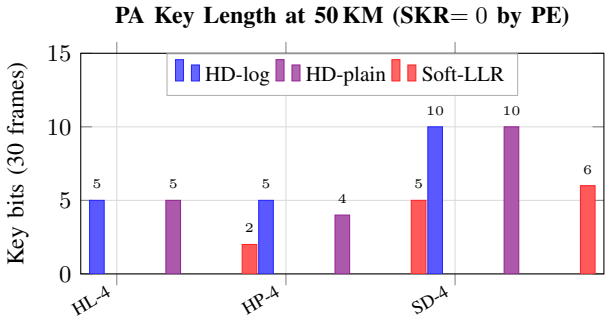

Fig. 5. PA key bits at 50 KM. The theoretical SKR is zero at this distance because $\beta I_{AB} - \chi_{BE} < 0$; keys shown here use the empirical $\mathrm{SKR}_{\mathrm{LOG}}$ lower bound for comparison across decoder configurations only. At $N_r = 16$, HD-log and HD-plain yield 10 key bits vs. 6 for Soft-LLR.

position-specific magnitudes to carry genuine prior information, shifting the advantage decisively to Soft-LLR (56.7% vs. 16.7% zero-BER yield, 15.0 vs. 4.4 mbits/use at 25 KM) at less than 1% additional initialisation cost; and at $N_r = 16$, truncation loss is small and BER calibration prevails, with HD-log reaching 96.7% zero-BER yield at 5 KM. HD-log equals or exceeds HD-plain in 24 of 27 configurations, and the calibrated log-scaling, costing only one multiply per variable node, should be treated as standard practice. The 50 KM zero-SKR outcome is a pure information-budget consequence ($\beta I_{AB} - \chi_{BE} = 0.95 \times 0.161 - 0.217 < 0$ regardless of decoder choice), compounded by the extreme sifting loss ($\gamma^* = 5.0$ discards 97.5% of samples); lower code rates ($R \approx 0.1$–0.2 [9]) or optimised modulation variance σ_A^2 are required to extend reach beyond 50 KM. The three dangerous frames detected (all at 50 KM, all with HD strategies) were caught by the CRC-32 gate at $\leq 3.3\%$ throughput cost with failure probability $\epsilon_{\mathrm{cor}} \approx 2^{-32}$ [18]. Future work should extend to composable finite-size security [18], revisit 50 KM with optimised σ_A^2 and finer sifting steps, and pursue hardware-aware $(N_r, \text{strategy})$ co-design for the FPT-EMS FPGA platform [14].

VI. Conclusion

We have presented, implemented, and rigorously evaluated a complete end-to-end post-processing pipeline for GG02 CV-QKD using real heterodyne quadrature data from Ruiz-Chamorro *et al.* [1] at 5, 25, and 50 KM, integrating 12-bit ADC digitisation, maximum-likelihood parameter estimation, adaptive amplitude sifting, tri-mode NB-LDPC decoding over GF(64), CRC-32 zero-BER retention, and privacy amplification. Quantisation effects are negligible, while amplitude sifting is throughput bottleneck, reducing retention from 67% at 5 KM to 2.5% at 50 KM and rendering the zero theoretical SKR at that distance. The most operationally significant finding is that LLR strategy optimality is N_r-dependent: HD-log is superior at $N_r \in \{4, 16\}$, whereas Soft-LLR achieves a 3.4× SKR improvement at 25 KM $N_r = 8$ (15.0 vs. 4.4 mbits/use) yet fails completely at 25 KM $N_r = 4$, making co-selection of strategy and N_r a system-safety requirement. HD-log strictly dominates HD-plain in 24 of 27 configurations, confirming that BER-calibrated log-scaling is essential and HD-plain should be deprecated. Zero-BER CRC gating is confirmed as a necessary security control: all three dangerous frames detected (at 50 KM) were successfully excluded at $\leq 3.3\%$ throughput cost, and the retained BER is exactly zero for every admitted frame across all 27 configurations, with every non-zero key configuration producing a verified Alice–Bob key match. Based on these results, we recommend HD-log as the default at $N_r \in \{4, 16\}$, Soft-LLR at $N_r = 8$ for distances ≥ 25 KM, mandatory CRC-32 zero-BER gating before privacy amplification, and reporting of the dangerous-frame count as a standard pipeline metric.

Acknowledgment

This work was supported by the National Quantum Mission Scheme of the Department of Science and Technology, Government of India.

References

[1] A. Ruiz-Chamorro, A. Garcia-Callejo, and V. Fernandez, "Low-complexity continuous-variable quantum key distribution with true local oscillator using pilot-assisted frequency locking," *Sci. Rep.*, vol. 14, p. 10770, 2024. [Dataset available at https://doi.org/10.6084/m9.figshare.25222115]
[2] S. Pirandola *et al.*, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, pp. 1012–1236, 2020.
[3] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Phys. Rev. Lett.*, vol. 88, p. 057902, 2002.
[4] C. Weedbrook *et al.*, "Gaussian quantum information," *Rev. Mod. Phys.*, vol. 84, p. 621, 2012.
[5] C. Weedbrook *et al.*, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, p. 170504, 2004.
[6] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Phys. Rev. Lett.*, vol. 114, p. 070501, 2015.
[7] S. Pirandola, "Composable security for continuous variable quantum key distribution: trust levels and practical key rates," *Phys. Rev. Res.*, vol. 3, p. 043014, 2021.
[8] P. Jouguet *et al.*, "Experimental demonstration of long-distance continuous-variable quantum key distribution," *Nature Photon.*, vol. 7, pp. 378–381, 2013.
[9] M. Milicevic *et al.*, "Key reconciliation with low-density parity-check codes for long-distance quantum cryptography," *npj Quantum Inf.*, vol. 4, p. 21, 2018.
[10] C. Pacher *et al.*, "Information reconciliation for CV-QKD using non-binary LDPC codes," *arXiv:1602.09140*, 2016.
[11] D. Declercq and M. P. C. Fossorier, "Decoding algorithms for nonbinary LDPC codes over GF(q)," *IEEE Trans. Commun.*, vol. 55, pp. 633–643, 2007.
[12] Y. Li and D. Declercq, "Trellis-based extended min-sum for non-binary LDPC codes," *IEEE Trans. Commun.*, vol. 61, pp. 2600–2611, 2013.
[13] E. Boutillon, L. Conde-Canencia, and A. Al Ghouwayel, "Design of a GF(64)-LDPC decoder based on the EMS algorithm," *IEEE Trans. Circuits Syst. I*, vol. 60, pp. 2644–2656, 2013.
[14] K. Wei *et al.*, "FPT-EMS: An FPGA implementation using NB-LDPC code for CV-QKD," in *Proc. HEART*, Kumamoto, Japan, 2025.
[15] K. Gümüş *et al.*, "A novel error correction protocol for continuous variable quantum key distribution," *Sci. Rep.*, vol. 11, p. 10465, 2021.
[16] Q. Li *et al.*, "Efficient bit sifting scheme of post-processing in quantum key distribution," *Quantum Inf. Process.*, vol. 14, pp. 3785–3811, 2015.
[17] M. Milicevic *et al.*, "Key reconciliation with LDPC codes for long-distance quantum cryptography," *arXiv:1702.07740*, 2017.
[18] A. G. Mountogiannakis, P. Papanastasiou, and S. Pirandola, "Data post-processing for the one-way heterodyne protocol under composable finite-size security," *Phys. Rev. A*, vol. 106, p. 042606, 2022.
[19] Y. Zhang *et al.*, "Long-distance CV-QKD over 202.81 KM of fiber," *Phys. Rev. Lett.*, vol. 125, p. 010502, 2020.