Tight Error Correction Performance for CV-QKD in Constrained Storage Devices

Panagiotis Papanastasiou

School of Physics, Engineering and Technology

University of York

Copenhagen – 13 May 2025

Talk in QSI Workshop: Securing the Future Quantum Internet

Structure of the Talk

- Motivation & Constraints

Structure of the Talk

- Motivation & Constraints
- Composable Rate and Reconciliation Efficiency

Structure of the Talk

- Motivation & Constraints
- Composable Rate and Reconciliation Efficiency
- Leakage and Storage Modeling

Structure of the Talk

- Motivation & Constraints
- Composable Rate and Reconciliation Efficiency
- Leakage and Storage Modeling
- Simulation Results and Trade-offs

Structure of the Talk

- Motivation & Constraints
- Composable Rate and Reconciliation Efficiency
- Leakage and Storage Modeling
- Simulation Results and Trade-offs
- Summary & Outlook

Motivation & Constraints

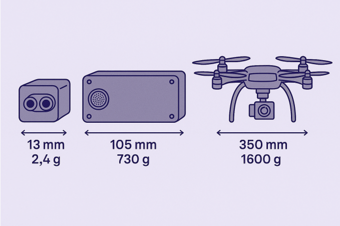
- QKD security proofs often assume ideal classical **post-processing** — unrealistic in in-field deployments.

Motivation & Constraints

- QKD security proofs often assume ideal classical **post-processing** — unrealistic in in-field deployments.
- Devices like **drones**, **sensors**, and **IoT nodes** face strict limits on memory, power, computation, space and weight.

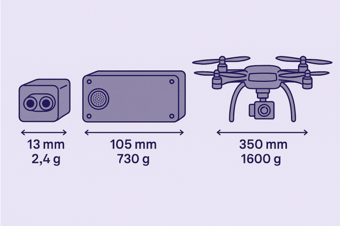
Motivation & Constraints

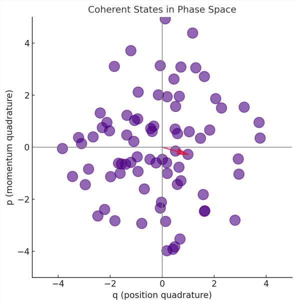
- Devices like **drones**, **sensors**, and **IoT nodes** face strict limits on memory, power, computation, space and weight.
- **CV-QKD** offers a compact, telecom-ready alternative to DV-QKD, ideal for such **constrained platforms**.



Motivation & Constraints

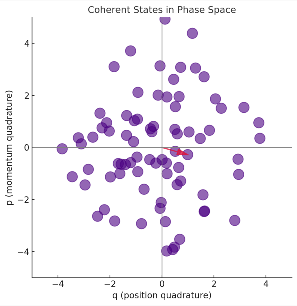
- Devices like **drones**, **sensors**, and **IoT nodes** face strict limits on memory, power, computation, space and weight.
- **CV-QKD** offers a compact, telecom-ready alternative to DV-QKD, ideal for such **constrained platforms**.

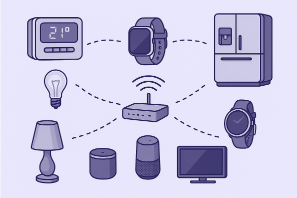




Motivation & Constraints

- Devices like **drones**, **sensors**, and **IoT nodes** face strict limits on memory, power, computation, space and weight.
- **CV-QKD** offers a compact, telecom-ready alternative to DV-QKD, ideal for such **constrained platforms**.
- These networks are short-range and latency-sensitive — **long-distance communication is not the main goal**.





Motivation & Constraints

- Devices like **drones**, **sensors**, and **IoT nodes** face strict limits on memory, power, computation, space and weight.
- **CV-QKD** offers a compact, telecom-ready alternative to DV-QKD, ideal for such **constrained platforms**.
- These networks are short-range and latency-sensitive — **long-distance communication is not the main goal**.
- **CV-QKD** performs well at short distances, offering high mutual information — but this requires **fine digitization** and **non-binary LDPC codes**, increasing resource demands.
- **Accurate models** linking leakage, runtime, and memory are key to **performance analysis** and **system design**.

Rate with Finite-Size Reconciliation Efficiency and Composable Terms

$$R := p_{\mathrm{ec}} \left(\frac{n}{N}\right) \left[\zeta\, I(x:y) - \chi^{\epsilon_{\mathrm{ec}}}(x:E) - \frac{\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}}{\sqrt{n}} + \frac{\theta}{n}\right]$$

$$\epsilon = \epsilon_{\mathrm{s}} + \epsilon_{\mathrm{h}} + 2p_{\mathrm{ec}}\epsilon_{\mathrm{pe}} + \epsilon_{\mathrm{ec}} + \epsilon_{\mathrm{cor}}, \quad \text{and } \epsilon_{\mathrm{ec}} := 1 - p_{\mathrm{ec}}(1 - \epsilon_{\mathrm{cor}}).$$

S. Pirandola and P. Papanastasiou, Phys. Rev. Research 6, 023321 (2024)

Rate with Finite-Size Reconciliation Efficiency and Composable Terms

$$R := p_{\mathrm{ec}} \left(\frac{n}{N}\right) \left[\zeta\, I(x:y) - \chi^{\epsilon_{\mathrm{ec}}}(x:E) - \frac{\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}}{\sqrt{n}} + \frac{\theta}{n}\right]$$

- p_{ec}: probability of successful error correction.
- $\frac{n}{N}$: fraction of signals retained after parameter estimation.

S. Pirandola and P. Papanastasiou, Phys. Rev. Research 6, 023321 (2024)

Rate with Finite-Size Reconciliation Efficiency and Composable Terms

$$R := p_{\mathrm{ec}}\left(\frac{n}{N}\right)\left[\zeta\, I(x:y) - \chi^{\epsilon_{\mathrm{ec}}}(x:E) - \frac{\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}}{\sqrt{n}} + \frac{\theta}{n}\right]$$

- p_{ec}: probability of successful error correction.
- $\frac{n}{N}$: fraction of signals retained after parameter estimation.
- $I(x:y)$: mutual information between the parties (CV domain).

S. Pirandola and P. Papanastasiou, Phys. Rev. Research 6, 023321 (2024)

Rate with Finite-Size Reconciliation Efficiency and Composable Terms

$$R := p_{\mathrm{ec}} \left(\frac{n}{N}\right) \left[\zeta\, I(x:y) - \chi^{\epsilon_{\mathrm{ec}}}(x:E) - \frac{\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}}{\sqrt{n}} + \frac{\theta}{n}\right]$$

- p_{ec}: probability of successful error correction.
- $\frac{n}{N}$: fraction of signals retained after parameter estimation.
- $I(x:y)$: mutual information between the parties (CV domain).
- $\chi(x:E)$: Holevo bound — quantifies Eve's information.

S. Pirandola and P. Papanastasiou, Phys. Rev. Research 6, 023321 (2024)

Rate with Finite-Size Reconciliation Efficiency and Composable Terms

$$R := p_{\mathrm{ec}} \left(\frac{n}{N}\right) \left[\zeta\, I(x:y) - \chi^{\epsilon_{\mathrm{ec}}}(x:E) - \frac{\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}}{\sqrt{n}} + \frac{\theta}{n}\right]$$

- p_{ec}: probability of successful error correction.
- $\frac{n}{N}$: fraction of signals retained after parameter estimation.
- $I(x:y)$: mutual information between the parties (CV domain).
- $\chi(x:E)$: Holevo bound — quantifies Eve's information.
- $\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}$: penalty from the Asymptotic Equipartition Property (AEP).

S. Pirandola and P. Papanastasiou, Phys. Rev. Research 6, 023321 (2024)

Rate with Finite-Size Reconciliation Efficiency and Composable Terms

$$R := p_{\mathrm{ec}}\left(\frac{n}{N}\right)\left[\zeta\, I(x:y) - \chi^{\epsilon_{\mathrm{ec}}}(x:E) - \frac{\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}}{\sqrt{n}} + \frac{\theta}{n}\right]$$

- p_{ec}: probability of successful error correction.
- $\frac{n}{N}$: fraction of signals retained after parameter estimation.
- $I(x:y)$: mutual information between the parties (CV domain).
- $\chi(x:E)$: Holevo bound — quantifies Eve's information.
- $\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}$: penalty from the Asymptotic Equipartition Property (AEP).
- θ: correction from *non-ideal* amplification and verification.

S. Pirandola and P. Papanastasiou, Phys. Rev. Research 6, 023321 (2024)

Rate with Finite-Size Reconciliation Efficiency and Composable Terms

$$R := p_{\mathrm{ec}} \left(\frac{n}{N}\right) \left[\zeta\, I(x:y) - \chi^{\epsilon_{\mathrm{ec}}}(x:E) - \frac{\Delta_{\mathrm{aep}}^{\epsilon_{\mathrm{s}}}}{\sqrt{n}} + \frac{\theta}{n}\right]$$

- $\zeta = \zeta_{\mathrm{digit}} \cdot \zeta_{\mathrm{leak}}$: reconciliation efficiency.
  - $\zeta_{\mathrm{digit}} := \frac{I(k:y)}{I(x:y)}$ — reduction due to digitization.
  - $\zeta_{\mathrm{leak}} := 1 - \frac{\Delta_{\mathrm{leak}}^{\epsilon_{\mathrm{ec}}}}{I(k:y)\sqrt{n}}$ — reduction due to finite-size leakage.

S. Pirandola and P. Papanastasiou, Phys. Rev. Research 6, 023321 (2024)
M. Tomamichel et al., Quantum Inf. Process. 16, 280 (2017)

Leakage Bounds and Storage Requirements for Non-Binary LDPC Codes

Tight Finite-Size Leakage Bound

$$\Delta_{\text{leak}}^{\epsilon_{\text{ec}}} := \sqrt{V(k|y)} \cdot \Phi^{-1}(1 - \epsilon_{\text{ec}})$$

$$\log_2 |\mathcal{M}| \leq nH(k|y) + \Delta_{\text{leak}}^{\epsilon_{\text{ec}}} \sqrt{n} + \mathcal{O}(\log_2 n)$$

M. Tomamichel et al., Quantum Inf. Process. 16, 280 (2017)

Leakage Bounds and Storage Requirements for Non-Binary LDPC Codes

Tight Finite-Size Leakage Bound

$$\Delta_{\text{leak}}^{\epsilon_{\text{ec}}} := \sqrt{V(k|y)} \cdot \Phi^{-1}(1-\epsilon_{\text{ec}})$$

$$\log_2 |\mathcal{M}| \leq nH(k|y) + \Delta_{\text{leak}}^{\epsilon_{\text{ec}}}\sqrt{n} + \mathcal{O}(\log_2 n)$$

- $H(k|y)$: conditional Shannon entropy of the digitized key given the other party's variable.

M. Tomamichel et al., Quantum Inf. Process. 16, 280 (2017)

Leakage Bounds and Storage Requirements for Non-Binary LDPC Codes

Tight Finite-Size Leakage Bound

$$\Delta_{\text{leak}}^{\epsilon_{\text{ec}}} := \sqrt{V(k|y)} \cdot \Phi^{-1}(1 - \epsilon_{\text{ec}})$$

$$\log_2 |\mathcal{M}| \leq nH(k|y) + \Delta_{\text{leak}}^{\epsilon_{\text{ec}}} \sqrt{n} + \mathcal{O}(\log_2 n)$$

- $V(k|y)$: the conditional entropy variance — quantifies fluctuations in the information content conditioned on the other party's variable, and governs second-order deviation from the Shannon limit.

M. Tomamichel et al., Quantum Inf. Process. 16, 280 (2017)

Leakage Bounds and Storage Requirements for Non-Binary LDPC Codes

Tight Finite-Size Leakage Bound

$$\log_2 |\mathcal{M}| \leq nH(k|y) + \Delta_{\text{leak}}^{\epsilon_{\text{ec}}}\sqrt{n} + \mathcal{O}(\log_2 n)$$

- $\Phi^{-1}(1-\epsilon_{\text{ec}})$: quantile of the Gaussian tail — set by the error correction success probability.

M. Tomamichel et al., Quantum Inf. Process. 16, 280 (2017)

Leakage Bounds and Storage Requirements for Non-Binary LDPC Codes

Tight Finite-Size Leakage Bound

$$\log_2 |\mathcal{M}| \leq nH(k|y) + \Delta_{\text{leak}}^{\epsilon_{\text{ec}}} \sqrt{n} + \mathcal{O}(\log_2 n)$$

- $\mathcal{O}(\log_2 n)$: logarithmic correction term due to finite sample size.

M. Tomamichel et al., Quantum Inf. Process. 16, 280 (2017)

Leakage Bounds and Storage Requirements for Non-Binary LDPC Codes

Tight Finite-Size Leakage Bound

$$\log_2 |\mathcal{M}| \leq nH(k|y) + \Delta_{\text{leak}}^{\epsilon_{\text{ec}}} \sqrt{n} + \mathcal{O}(\log_2 n)$$

- d: number of bits per symbol — defines the alphabet size used in non-binary LDPC codes.
- Leakage is quantified via the syndrome alphabet size: $\log_2 |\mathcal{M}| = ndR_{\text{synd}}$
- R_{synd}: the syndrome rate of the LDPC code — determined by code structure.

Leakage Bounds and Storage Requirements for Non-Binary LDPC Codes

Tight Finite-Size Leakage Bound

$$\log_2 |\mathcal{M}| \leq nH(k|y) + \Delta_{\text{leak}}^{\epsilon_{\text{ec}}} \sqrt{n} + \mathcal{O}(\log_2 n)$$

- d: number of bits per symbol — defines the alphabet size used in non-binary LDPC codes.
- Leakage is quantified via the syndrome alphabet size: $\log_2 |\mathcal{M}| = ndR_{\text{synd}}$
- R_{synd}: the syndrome rate of the LDPC code — determined by code structure.
- Dense matrix estimate: $M_{\text{code}} := n^2 dR_{\text{synd}}$

P. Papanastasiou et al., arXiv:2504.06384v1

Leakage Bounds and Storage Requirements for Non-Binary LDPC Codes

Tight Finite-Size Leakage Bound

$$\log_2 |\mathcal{M}| \leq nH(k|y) + \Delta_{\text{leak}}^{\epsilon_{\text{ec}}}\sqrt{n} + \mathcal{O}(\log_2 n)$$

- d: number of bits per symbol — defines the alphabet size used in non-binary LDPC codes.
- Leakage is quantified via the syndrome alphabet size: $\log_2 |\mathcal{M}| = ndR_{\text{synd}}$
- R_{synd}: the syndrome rate of the LDPC code — determined by code structure.
- Dense matrix estimate: $M_{\text{code}} := n^2 dR_{\text{synd}}$
- Sparse CRS format (with $\bar{d}_v = 2$):

$$M_{\text{sparse}} = 2nd + 2n\lceil\log_2(n)\rceil + (nR_{\text{synd}} + 1)\lceil\log_2(2n)\rceil$$

Leakage, Storage, and Rate Trade-offs

- At fixed **low loss**, DR with homodyne yields high rates at small block sizes.
- As **loss increases**, ζ improves linearly, but leakage also increases.

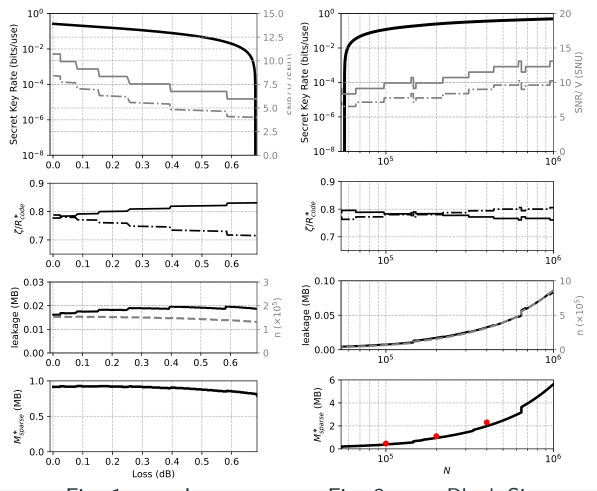


Fig. 1 – vs. Loss   Fig. 3 – vs. Block Size

Leakage, Storage, and Rate Trade-offs

- **Block size** is a key driver: larger n boosts rate, but also memory and leakage.
- **Trade-off:** Higher p_{ec} improves the final rate but comes at the cost of increased leakage and memory footprint.

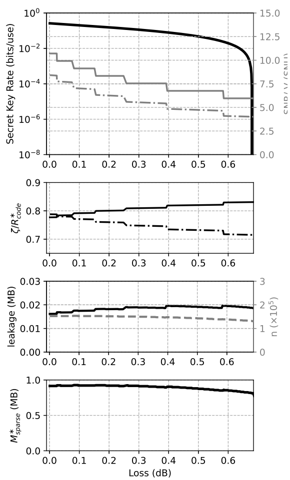


Fig. 1 – vs. Loss

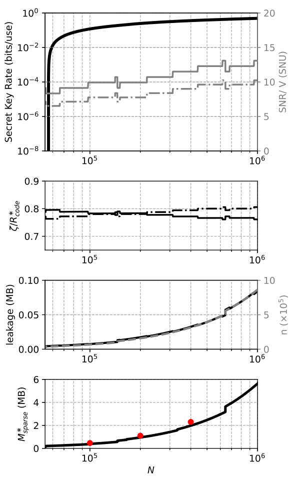


Fig. 3 – vs. Block Size

Leakage, Storage, and Rate Trade-offs

- **Encoding is lightweight:** memory requirements remain within a few MB — suitable for constrained transmitters.
- **Storage growth remains near-linear**, even in sparse format; simulated points match theory.

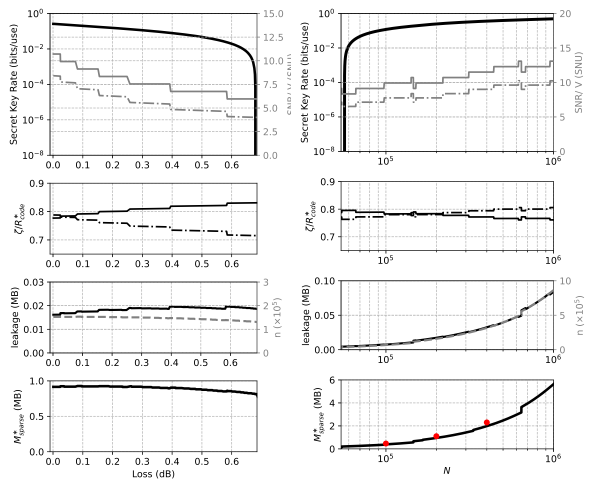


Fig. 1 – vs. Loss   Fig. 3 – vs. Block Size

Summary and Outlook

- CV-QKD is ideally suited for **constrained**, **short-range platforms** — but demands adapted post-processing.

Summary and Outlook

- CV-QKD is ideally suited for **constrained**, **short-range platforms** — but demands adapted post-processing.
- We developed a **composable key rate** with **finite-size leakage bounds** and explicit memory modeling.

Summary and Outlook

- CV-QKD is ideally suited for **constrained**, **short-range platforms** — but demands adapted post-processing.
- We developed a **composable key rate** with **finite-size leakage bounds** and explicit memory modeling.
- **Non-binary LDPC codes** in sparse format, optimized for resolution and SNR, enable **near-optimal efficiency** with MB-scale memory — supporting lightweight encoding on constrained devices.

Summary and Outlook

- CV-QKD is ideally suited for **constrained**, **short-range platforms** — but demands adapted post-processing.
- We developed a **composable key rate** with **finite-size leakage bounds** and explicit memory modeling.
- **Non-binary LDPC codes** in sparse format, optimized for resolution and SNR, enable **near-optimal efficiency** with MB-scale memory — supporting lightweight encoding on constrained devices.
- Our results show that rate, leakage, and memory are tightly coupled — enabling **trade-off-aware** design for **real CV-QKD deployments**.

Summary and Outlook

- CV-QKD is ideally suited for **constrained**, **short-range platforms** — but demands adapted post-processing.
- We developed a **composable key rate** with **finite-size leakage bounds** and explicit memory modeling.
- **Non-binary LDPC codes** in sparse format, optimized for resolution and SNR, enable **near-optimal efficiency** with MB-scale memory — supporting lightweight encoding on constrained devices.
- Our results show that rate, leakage, and memory are tightly coupled — enabling **trade-off-aware** design for **real CV-QKD deployments**.
- Beyond security, the rate also benchmarks **runtime** — guiding simulations of error correction in constrained quantum platforms.

Summary and Outlook

- CV-QKD is ideally suited for **constrained**, **short-range platforms** — but demands adapted post-processing.
- We developed a **composable key rate** with **finite-size leakage bounds** and explicit memory modeling.
- **Non-binary LDPC codes** in sparse format, optimized for resolution and SNR, enable **near-optimal efficiency** with MB-scale memory — supporting lightweight encoding on constrained devices.
- Our results show that rate, leakage, and memory are tightly coupled — enabling **trade-off-aware** design for **real CV-QKD deployments**.
- Beyond security, the rate also benchmarks **runtime** — guiding simulations of error correction in constrained quantum platforms.

Thank you!