Code efficiency, frame error rate and secure key rate

Hossein Mani†, Bernhard Ömer*, Christoph Pacher*, Ulrik Lund Andersen†, Tobias Gehring†

† Center of Macroscopic Quantum States, bigQ, Department of Physics, Fysikvej 307, Technical University of Denmark, 2800 Kgs. Lyngby, Denmark

* Center for Digital Safety & Security, AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria

Summary

A set of highly efficient MET-LDPC codes with asymptotic efficiencies higher than 97 % [1] are introduced.

- The asymptotic efficiency of these codes are calculated with density evolution (DE).
- These codes can be used widely for long distance CV-QKD with lower frame error rate (FER) and higher secret key rate.
- We present the finite length efficiency of some of our codes.
- We plot the secret key rate versus distance by replacing our codes with other existing codes in literature.

Why do we need highly efficient codes?

The secret key rate equation for CV-QKD is

$$K = \frac{n}{N}(1 - \text{FER})\left[\beta\, I_{\text{A,B}} - \mathcal{X}_{\text{E,B}} - \Delta(n)\right]$$

- **N** : Total number of symbols exchanged by Alice and Bob
- **n** : Total number of symbols used for key extraction
- **FER** : Frame error rate of the reconciliation process
- β : Efficiency of the reconciliation process
- $\mathbf{I_{A,B}}$: Classical mutual information between Alice and Bob
- $\mathcal{X}_{\text{E,B}}$: Upper bound on the information that Eve can obtain from Bob
- $\mathbf{\Delta(n)}$: Finite-size correction factor

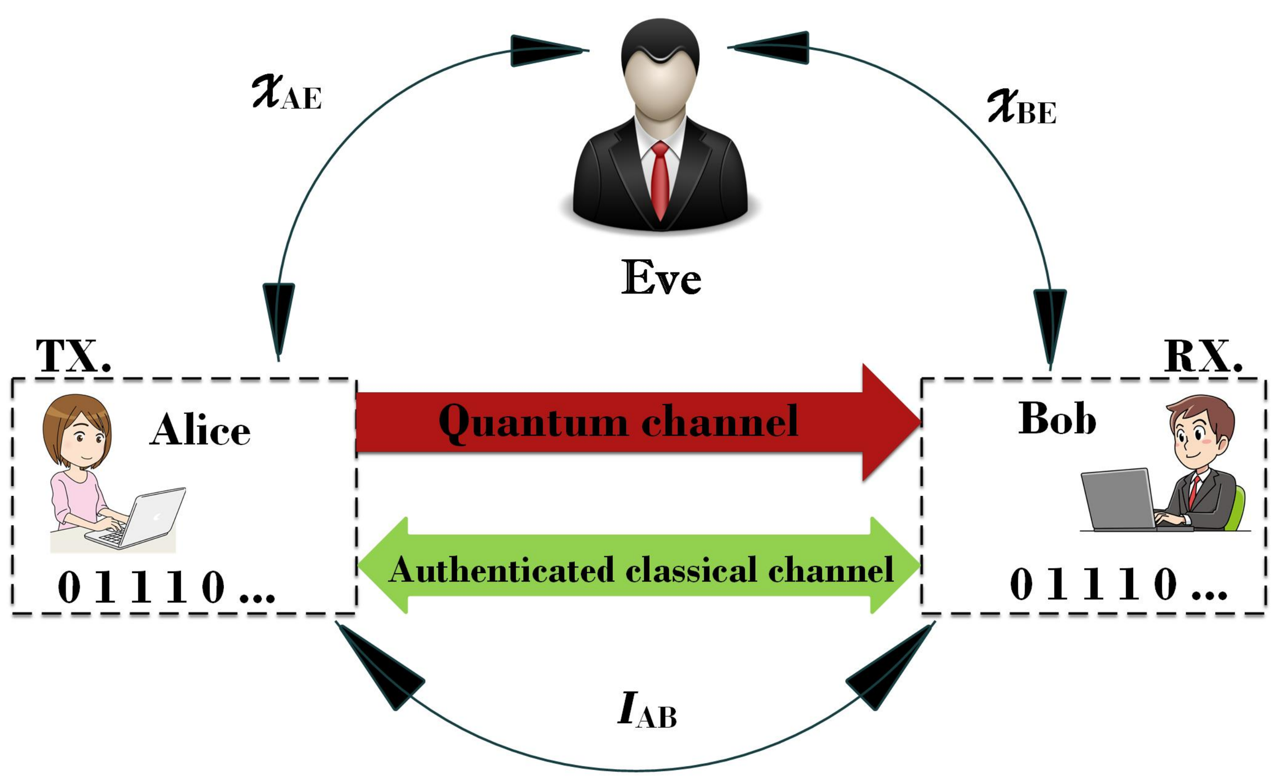

Figure 1. Schematic presentation of QKD system.

References

[1] Phys. Rev. A **103**, 062419.
[2] Phys. Rev. A **77**, 042325.
[3] Phys. Rev. A **84**, 062317 .
[4] Phys. Rev. A **90**, 042329.
[5] Phys. Rev. Lett. **125**, 010502.

Contact info

H. M hosma@fysik.dtu.dk
B. Ö Bernhard.Oemer@ait.ac.at
U. L. A ulrik.andersen@fysik.dtu.dk
C. P Christoph.Pacher@ait.ac.at
T. G † tobias.gehring@fysik.dtu.dk

Reconciliation efficiency (β) and leakage

Parameters	Reconciliation Schemes: Multi-Dimensional [2-3]	Slice (Multi-Level) [4]
β	$\frac{R^{\text{Ch}}}{I_{\text{AWGN}}(s)}$	$\frac{H(\mathcal{Q}(X_B)) - m + \sum_{i=0}^{m-1} R_i^{\text{ch}}}{I(X_B; X_A)}$
$\beta_{\max}$	$\frac{I_{\text{BI-AWGN}}(s)}{I_{\text{AWGN}}(s)}$	$\frac{I(\mathcal{Q}(X_B); \mathcal{Q}(X_A))}{I(X_B; X_A)}$
Leakage	0	$\sum_{i=0}^{m-1} R_i^s \geq H(\mathcal{Q}(X_B) \mid \mathcal{Q}(X_A))$
SNR range	≤ 0 dB	≥ 0 dB

Table 1. Comparison of Multi-Dimensional and Slice reconciliation

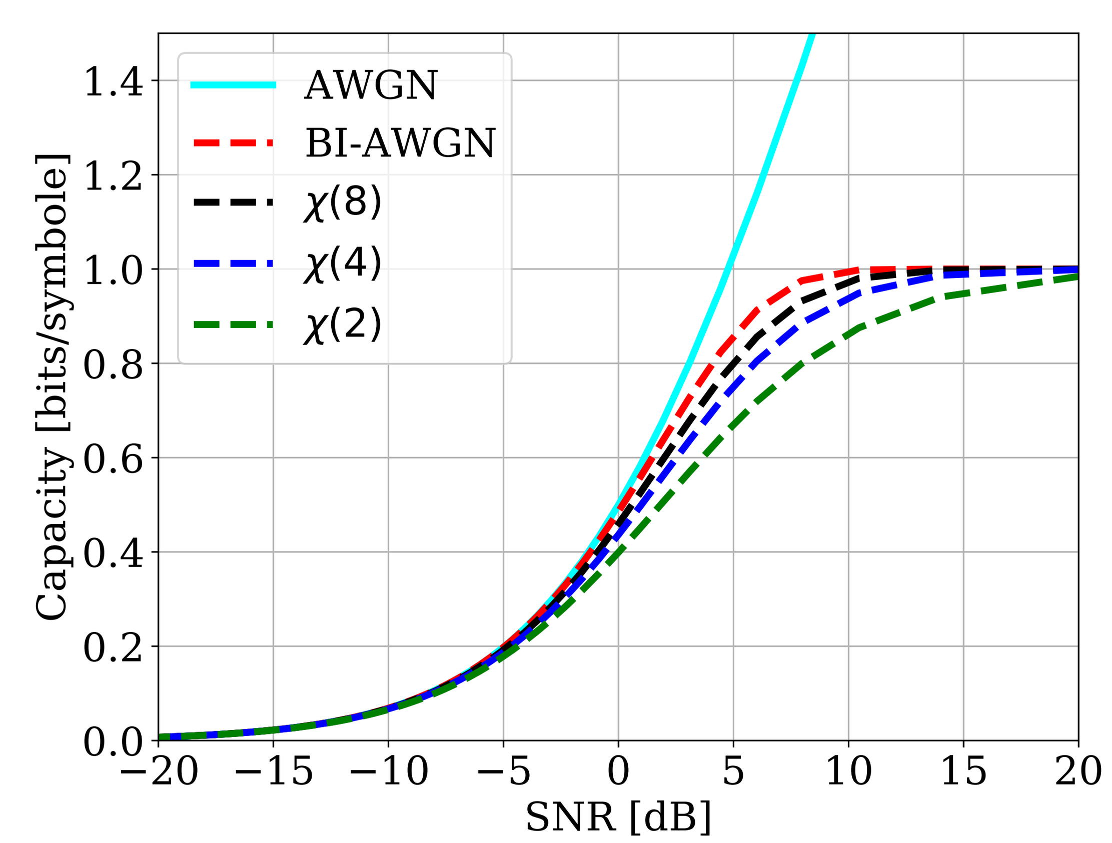

Figure 2. Comparison of capacity for AWGN channel and BI-AWGN channel.

Results: Performance of rate 0.1 MET-LDPC

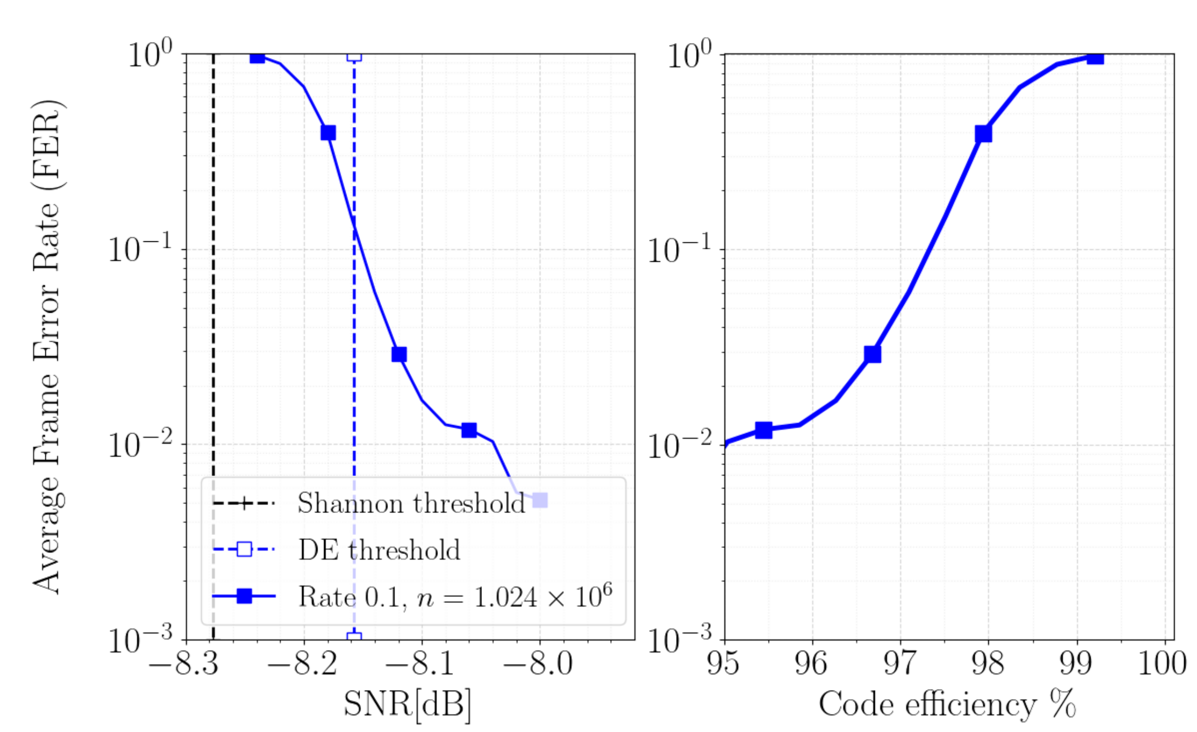

Figure 3. (**Left**) Frame error rate vs SNR for rate **0.10** MET-LDPC code. Dashed blue and black vertical lines show thresholds calculated by density evolution and Shannon threshold. (**Right**) Efficiency vs frame error rate obtained from LDPC decoding.

Results: Performance of rate 0.02 MET-LDPC

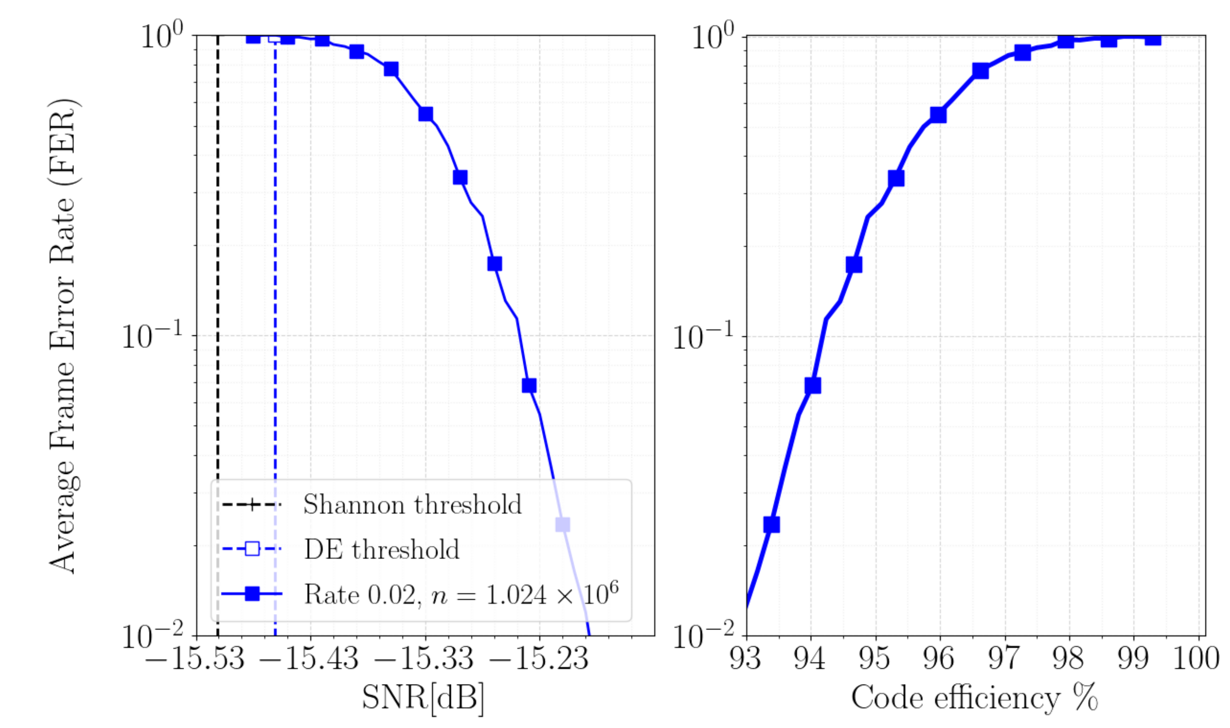

Figure 4. (**Left**) Frame error rate vs SNR for rate **0.02** MET-LDPC code. Dashed blue and black vertical lines show thresholds calculated by density evolution and Shannon threshold. (**Right**) Efficiency vs frame error rate obtained from LDPC decoding.

Results: Secure key rate comparison

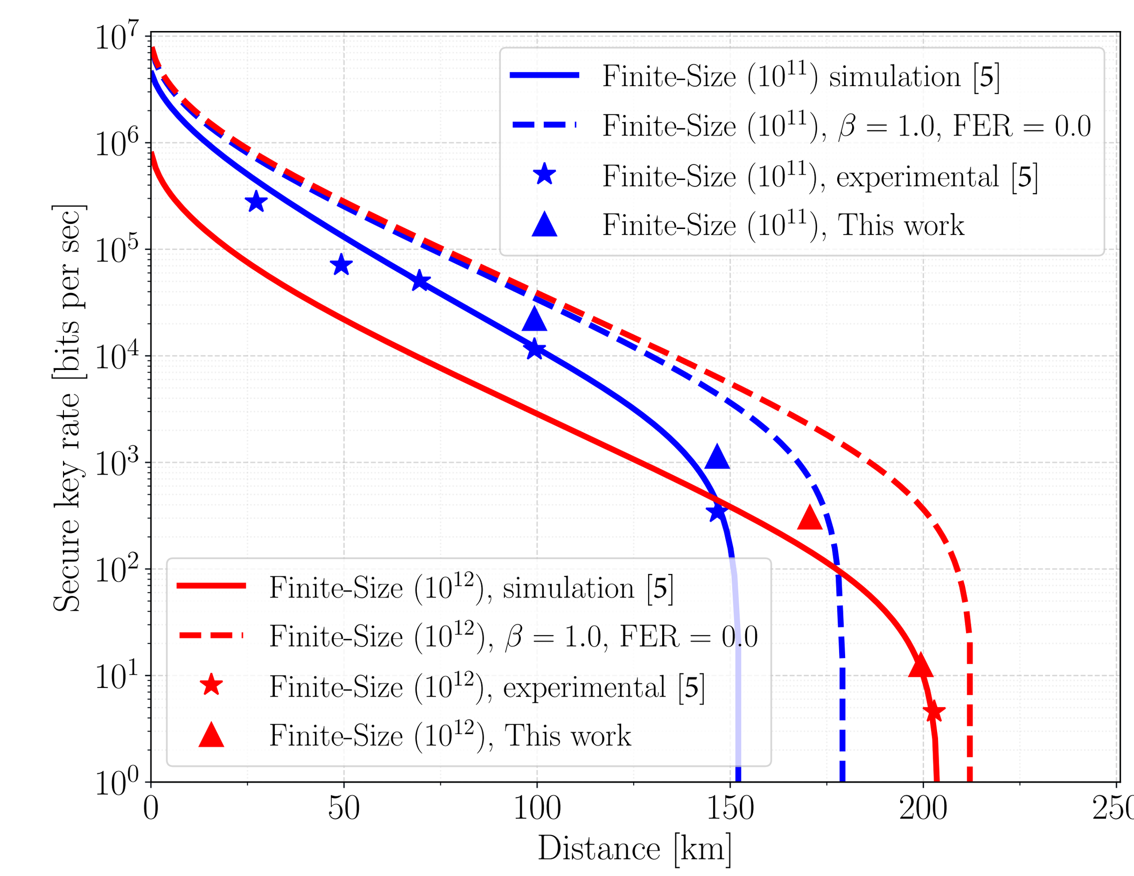

Figure 5. Numerical simulation of secret key rate comparing the performance of our codes with previous codes. The experimental points and the simulation parameters are taken from Table 1 of Ref. [5]: The repetition rate is 5 MHz, the fraction of symbols for parameter estimation is $\nu = 0.1$, the modulation variance V_A has been optimized, and the fiber attenuation is $\alpha = 0.16$ dB/km. The (input related) excess noise is 0.0086 shot-noise units for the blue curves and 0.0081 shot-noise units for the red ones. The electronic noise is 0.2717 and 0.1523 shot-noise units, respectively, and the trusted receiver efficiency is 61.34%.

Acknowledgments

This project has received funding from Innovation Fund Denmark (CryptQ project, grant agreement 0175 – 00018A), the Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNRF142) and innovation program under grant agreement No 820466 (CiViQ) and grant agreement No 820474 (UNIQORN).