

## Summary

We propose two new highly efficient MET-LDPC codes for the post processing of CV-QKD

- The first code is a MET-LDPC code of rate **0.02** with code efficiency of 99.2% obtained by Density Evolution
- The second code is a MET-LDPC code of rate **0.01** with code efficiency of 98.7% obtained by Density Evolution.

## Why do we need highly efficient codes?

The secret key rate equation for CV-QKD is

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

- 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
- $\beta$**  : Efficiency of the reconciliation process
- $I_{A,B}$**  : Classical mutual information between Alice and Bob
- $\mathcal{X}_{E,B}$**  : Upper bound on the information that Eve can obtain from Bob
- $\Delta(n)$**  : Finite-size correction factor

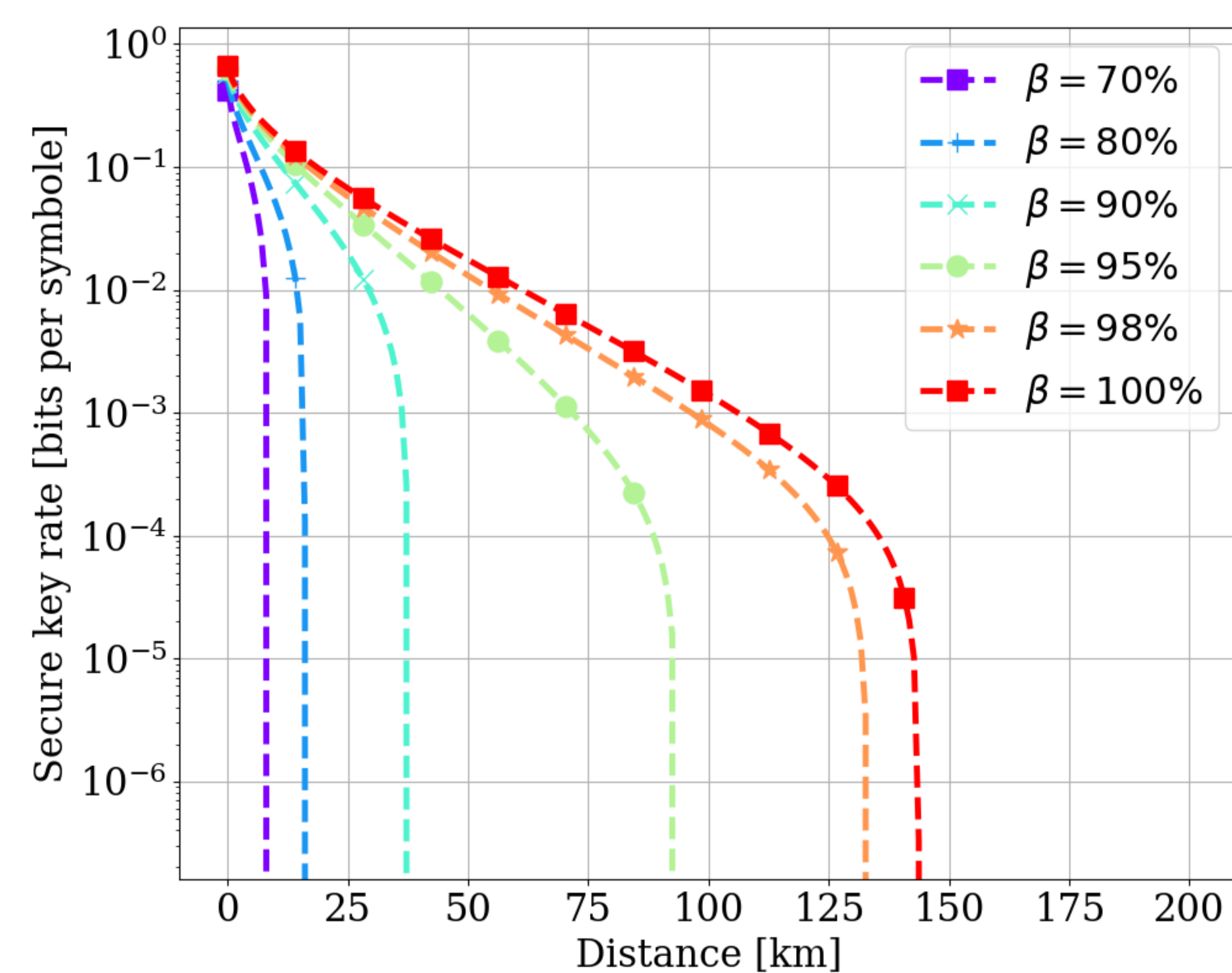


Figure 1 Effective finite secure key rate against collective attack on Gaussian modulated CV-QKD with multidimensional reconciliation. The reconciliation efficiency  $\beta = \{0.7, 0.8, 0.9, 0.95, 1.00\}$ . The parameters used in the calculations are  $V_{\text{mod}} = 8.5$ ,  $\xi_{\text{ch}} = 0.015$  (excess noise),  $\eta = 0.6$  (detector efficiency),  $v_{\text{el}} = 0.041$  (trusted electronic noise),  $N = 2 * 10^{10}$ ,  $n = 10^{10}$ ,  $\epsilon_{\text{security}} = 10^{-10}$ , and the fiber loss is assumed to be 0.2 dB/km.

## Results: Optimized code structures

$\nu_{bd}$	<b>b</b>	<b>d</b>	$\mu_d$	<b>d</b>
0.02		2 51 0	0.016	4 0 0
0.02	[0 1]	3 60 0	0.004	9 0 0
0.96		0 0 1	0.30	0 3 1
			0.66	0 2 1

$\sigma_{\text{Sh}}^* = 5.96$   $\sigma_{\text{DE}}^* = 5.94$   $\beta_{\text{DE}} = 99.2\%$

Table I Structure of optimized MET-LDPC code of rate **0.02** with 3 edge types. Detailed description can be found in [2].

$\nu_{bd}$	<b>b</b>	<b>d</b>	$\mu_d$	<b>d</b>
0.01		2 103 0	0.008	4 0 0
0.01	[0 1]	3 125 0	0.002	9 0 0
0.98		0 0 1	0.32	0 3 1
			0.66	0 2 1

$\sigma_{\text{Sh}}^* = 8.46$   $\sigma_{\text{DE}}^* = 8.41$   $\beta_{\text{DE}} = 98.7\%$

Table II Structure of optimized MET-LDPC code of rate **0.01** with 3 edge types:

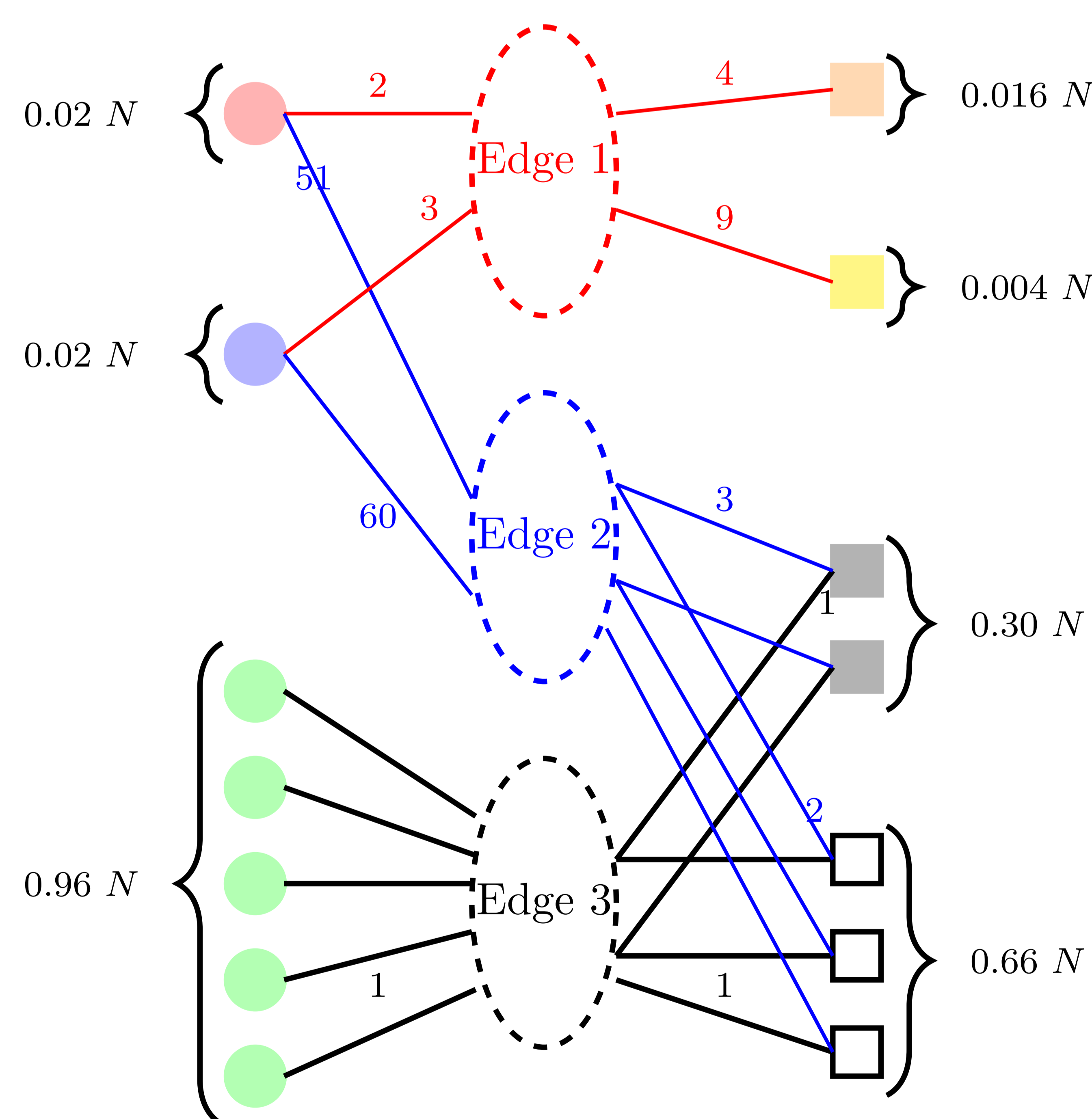


Figure 2 Graphical representation of the MET-LDPC code of rate 0.02. Detailed description can be found in [2].

## Results: Performance comparison

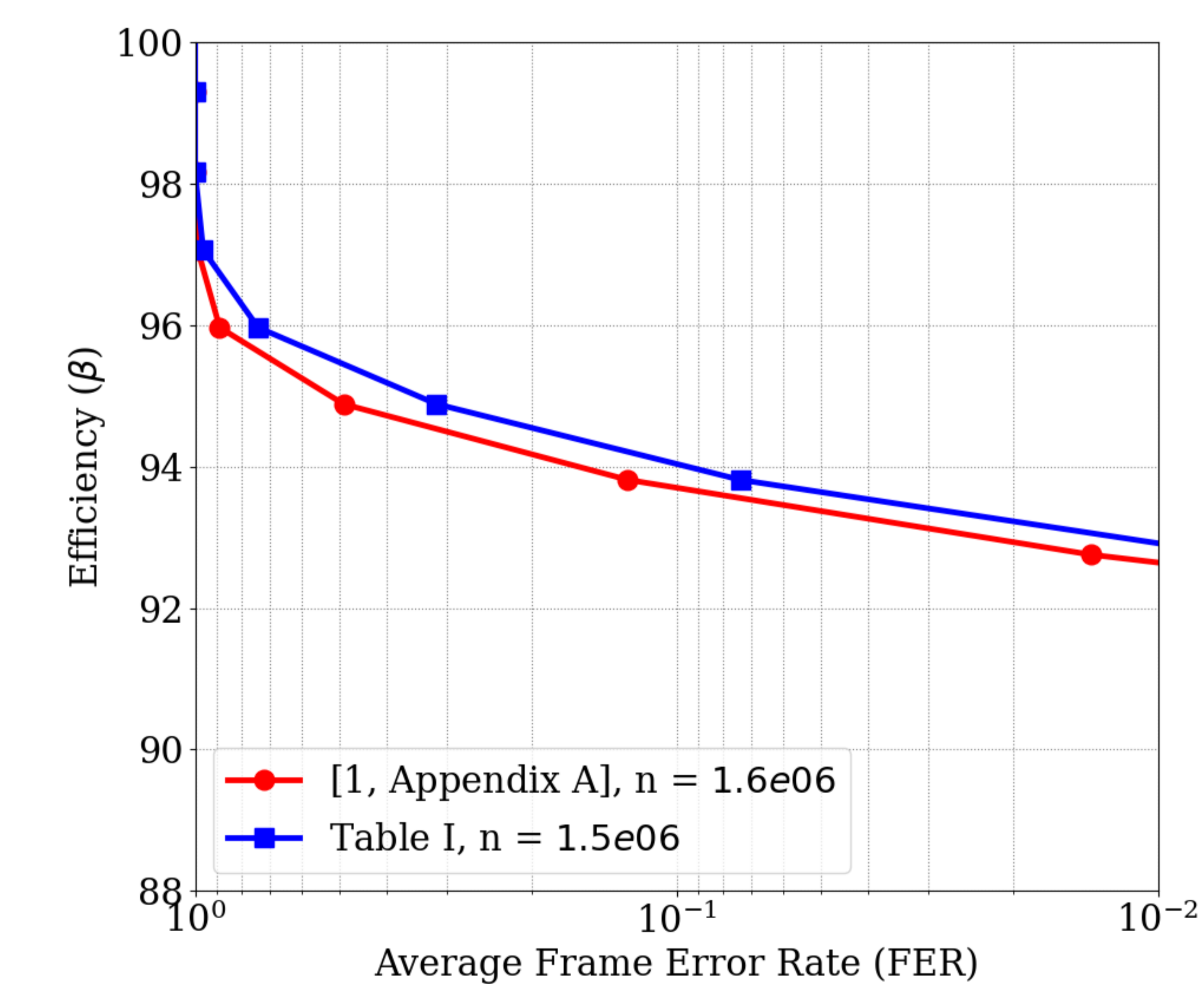
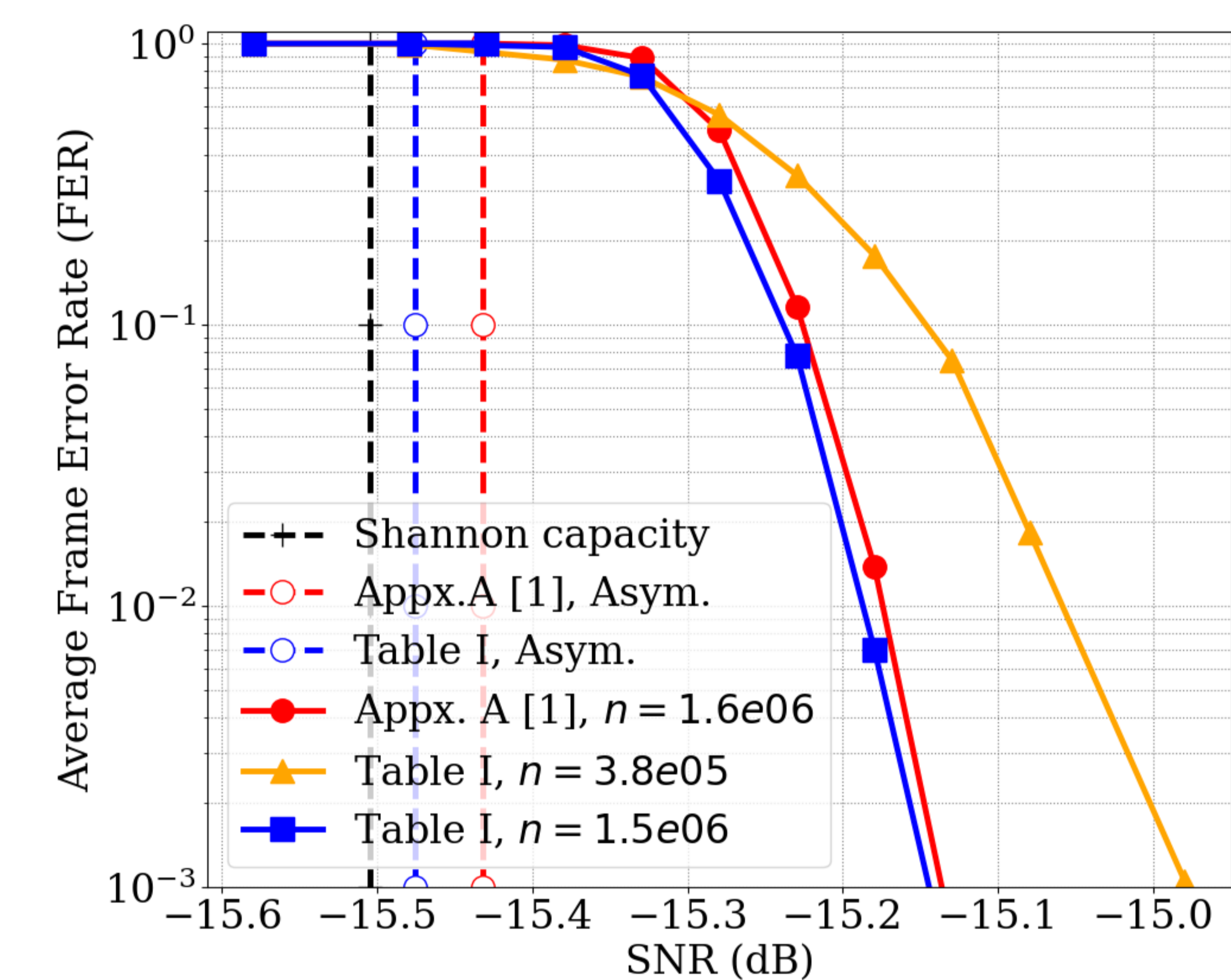


Figure 3 (Upper) Frame error rate vs SNR for rate **0.02** MET-LDPC code. Dashed blue and red vertical lines show thresholds calculated by density evolution. Solid curves show values obtained from LDPC decoding. (Lower) Efficiency vs frame error rate obtained from LDPC decoding.

## References

- [1] Paul Jouguet, et al. "Long-distance continuous-variable quantum key distribution with a Gaussian modulation," *Phys. Rev. A*, vol. 84, p. 062317, Dec 2011. [Online]. Available: <https://link.aps.org/doi/10.1103/PhysRevA.84.062317>
- [2] Hossein Mani, et al. "Reconciliation of Weakly Correlated Information Sources Utilizing Generalized EXIT Chart." arXiv preprint arXiv:1812.05867 (2018). [Online]. Available: <https://arxiv.org/abs/1812.05867>

## Contact info

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

## Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 820466 (CiViQ) and grant agreement No 820474 (UNIQUORN).  
 The authors thank the Quantum Innovation Center Qubiz funded by the Innovation Fund Denmark for support. H.M., T.G., and U.L.A. acknowledge support from the Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNRF142).