Two MET-LDPC Codes Designed for Long-Distance CV-QKD

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

y 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, Gie nggasse 4, 1210 Vienna, Austria

Summary

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

- The rst code is a MET-LDPC code of rate 0:02 with code e ciency of 99:2% obtained by Density Evolution
- The second code is a MET-LDPC code of rate 0:01 with code e ciency of 98:7% obtained by Density Evolution.

Why do we need highly e cient codes?

The secret key rate equation for CV-QKD is

$$K = \frac{n}{N}(1 \quad \mathrm{FER})[\quad I_{A,B} \quad X_{E,B} \quad (n)]$$

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
	:	E ciency of the reconciliation process
$I_{A,B}$	:	Classical mutual information between Alice and Bob
$X_{E,B}$	:	Upper bound on the information that Eve can obtain from Bob
(n)	:	Finite-size correction factor

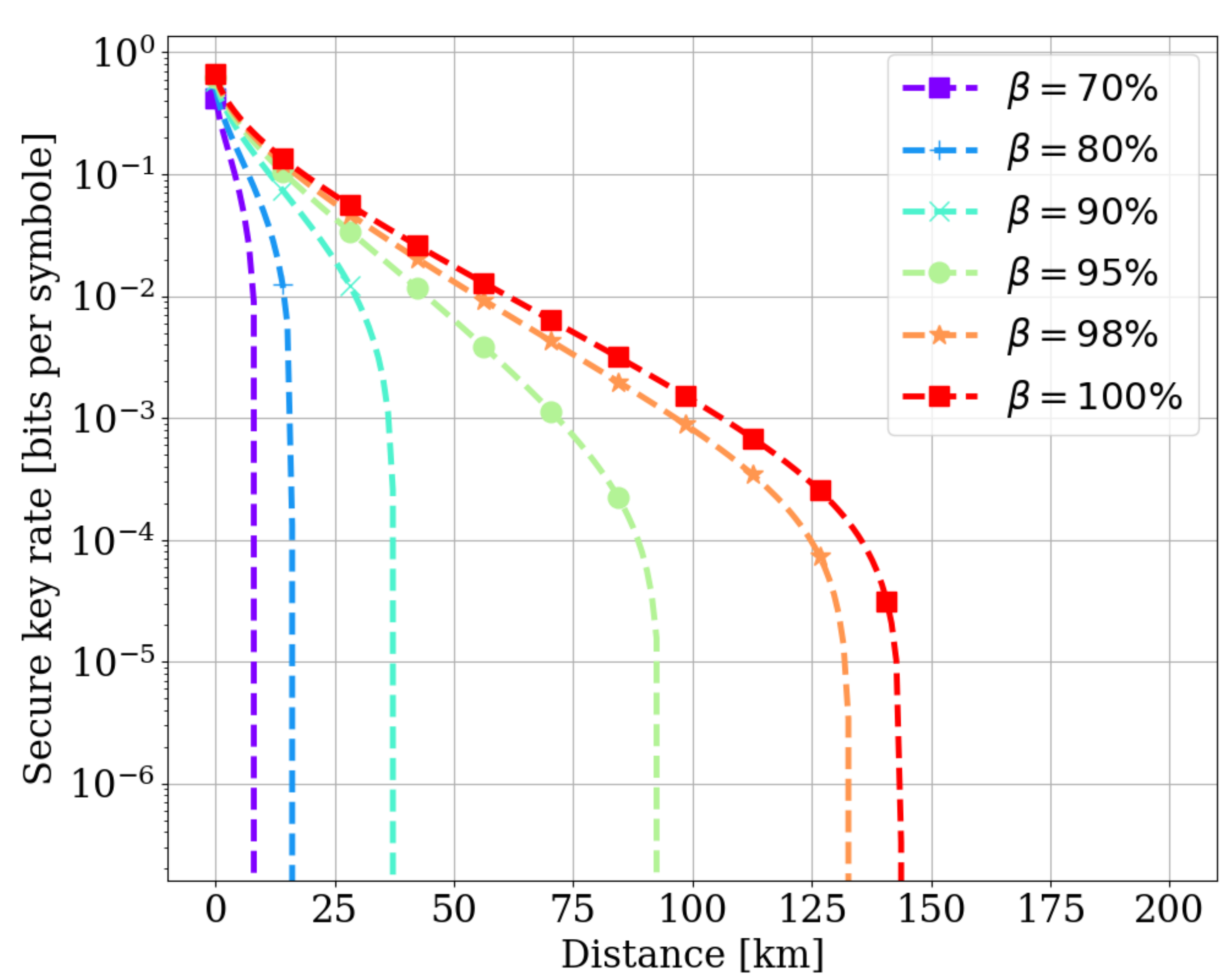

Figure 1 E ective nite secure key rate against collective attack on Gaussian modulated CV-QKD with multidimensional reconciliation. The reconciliation e ciency = $f0{:}7; 0{:}8; 0{:}9; 0{:}95; 1{:}00g$. The parameters used in the calculations are V_{mod} = 8:5 , $_{ch}$ = 0:015 (excess noise), = 0:6 (detector e ciency), v_{el} = 0:041 (trusted electronic noise), N = 2 10^{10}, $n = 10^{10}$, $_{security}$ = 10 ^{10}, and the ber loss is assumed to be 0:2 dB/km.

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

Results: Optimized code structures

bd	b	d	d	d
0:02 0:02 0:96	[0 1]	2 51 0 3 60 0 0 0 1	0:016 0:004 0:30 0:66	4 0 0 9 0 0 0 3 1 0 2 1
$_{Sh}$ = 5:96		$_{DE}$ = 5:94		$_{DE}$ = 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].

bd	b	d	d	d
0:01 0:01 0:98	[0 1]	2 103 0 3 125 0 0 0 1	0:008 0:002 0:32 0:66	4 0 0 9 0 0 0 3 1 0 2 1
$_{Sh}$ = 8:46		$_{DE}$ = 8:41		$_{DE}$ = 98:7%

Table II Structure of optimized MET-LDPC code of rate 0:01 with 3 edge types:

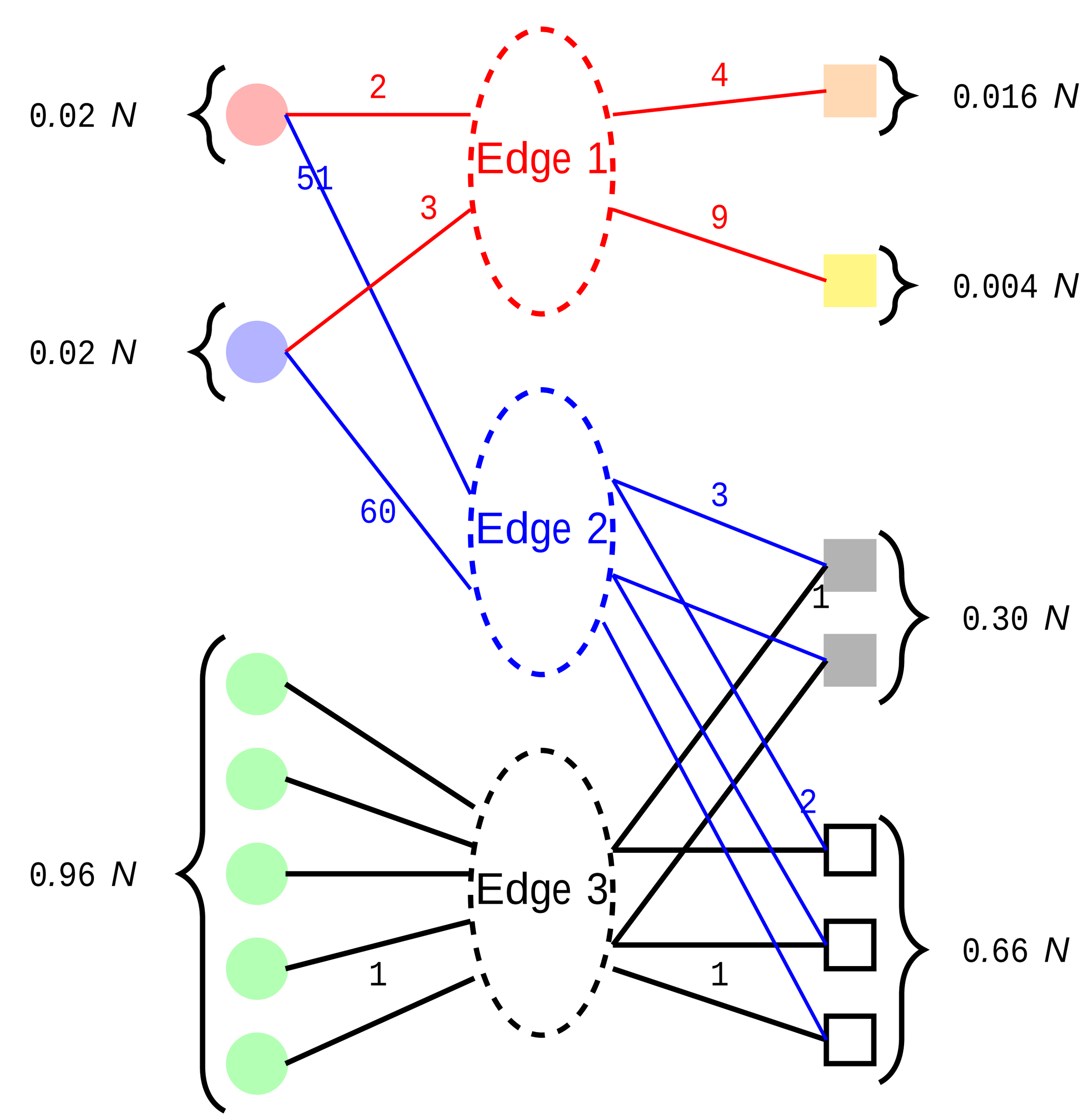

Figure 2 Graphical representation of the MET-LDPC code of rate 0:02. Detailed description can be found in [2].

Contact info

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

Results: Performance comparison

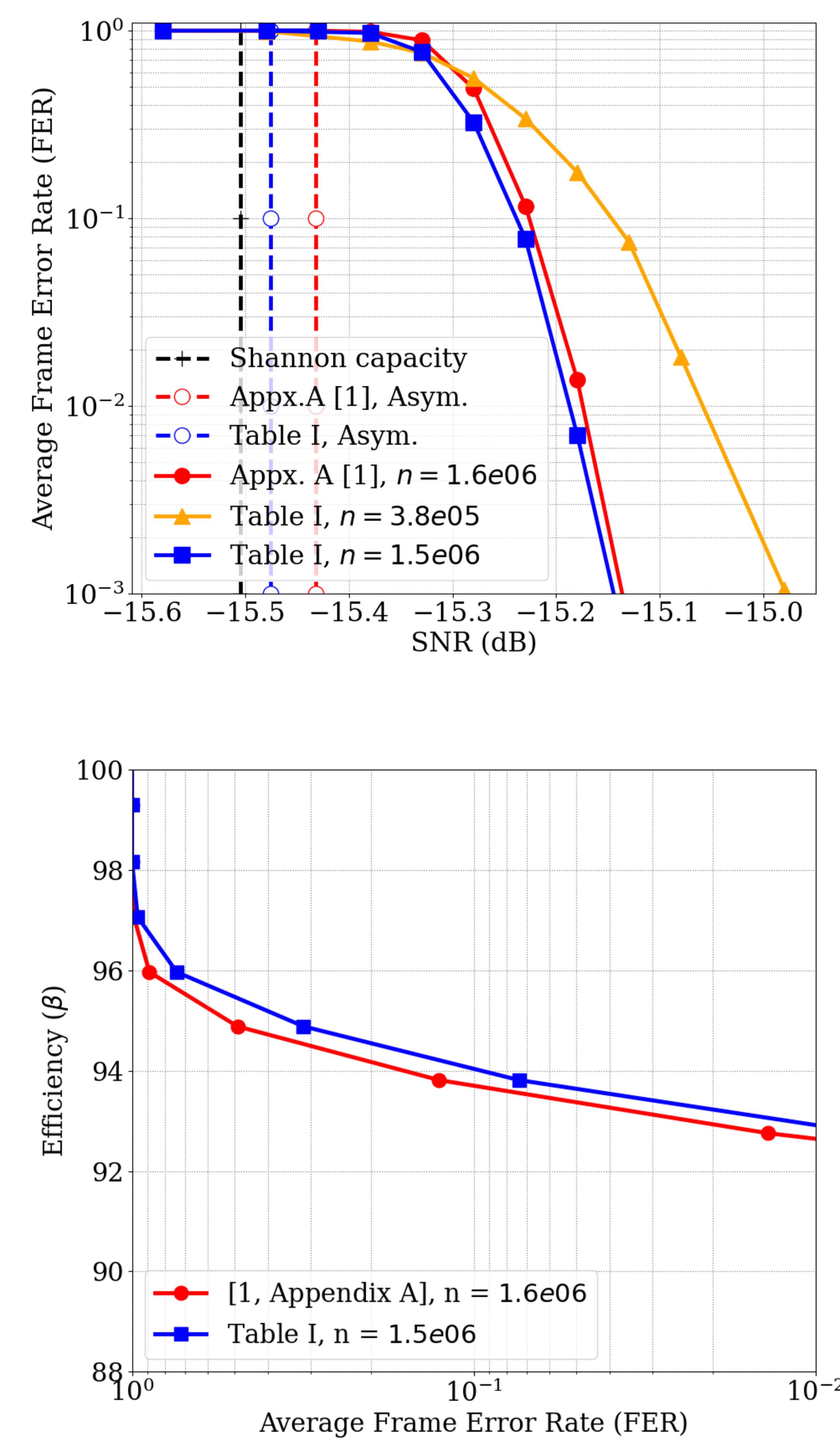

Figure 3 (Upper) Frame error rate vs SNR for rate 0:02 MET-LDPC code. Dashed blue and red vertical lines show thresholds calculated by density evolution. Solid curves show values obtained from LDPC decoding. (Lower) E ciency vs frame error rate obtained from LDPC decoding.

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 (UNIQORN).
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).