List of Publications and Preprints

Sven Puchinger, Technical University of Munich (TUM)

August 2019

Journal Articles

[preprint] **S. Puchinger**, J. Renner, A. Wachter-Zeh. Decoding High-Order Interleaved Rank-Metric Codes. *submitted to: IEEE Transactions on Information Theory*, 2019.

[J5] **S. Puchinger**, J. Rosenkilde né Nielsen, I. Bouw. Improved Power Decoding of Interleaved One-Point Hermitian Codes. *Designs, Codes and Cryptography*, DOI:10.1007/s10623-018-0577-z, 2018.

[J4] **S. Puchinger** and A. Wachter-Zeh. Fast Operations on Linearized Polynomials and their Applications in Coding Theory. *Journal of Symbolic Computation*, vol. 89, pp. 194–215, 2018

[J3] **S. Puchinger**, J. Rosenkilde né Nielsen, W. Li, and V. Sidorenko. Row Reduction Applied to Decoding of Rank-Metric and Subspace Codes. *Designs, Codes and Cryptography*, vol. 82(1-2), pp. 389–409, 2017.

[J2] **S. Puchinger**, S. Müelich, David Mödinger, J. Rosenkilde né Nielsen, and M. Bossert. Decoding interleaved Gabidulin codes using Alekhnovich's algorithm. *Electronic Notes in Discrete Mathematics*, 57:175–180, 2017.

[J1] S. Müelich, **S. Puchinger**, and M. Bossert. Low-Rank Matrix Recovery using Gabidulin Codes in Characteristic Zero. *Electronic Notes in Discrete Mathematics*, 57:161–166, 2017.

Peer-Reviewed Conference Papers

[preprint] J. Renner, **S. Puchinger**, A. Wachter-Zeh. Interleaving Loidreau's Rank-Metric Cryptosystem. submitted to *International Symposium on Problems of Redundancy in Information and Control Systems*, 2019.

[C30] L. Holzbaur, **S. Puchinger**, A. Wachter-Zeh. On Error Decoding of Locally Repairable and Partial MDS Codes. accepted at *IEEE Information Theory Workshop (ITW)*, 2019.

[C29] H. Bartz, T. Jerkovits, **S. Puchinger**, J. Rosenkilde. Fast Root Finding for Interpolation-Based Decoding of Interleaved Gabidulin Codes. accepted at *IEEE Information Theory Workshop (ITW)*, 2019.

[C28] A. Neri, **S. Puchinger**, A. Horlemann-Trautmann. Invariants and Inequivalence of Linear Rank-Metric Codes. accepted at *IEEE International Symposium on Information Theory (ISIT)*, 2019.

[C27] C. Sippel, C. Ott, **S. Puchinger**, M. Bossert. Reed–Solomon Codes over Fields of Characteristic Zero. accepted at *IEEE International Symposium on Information Theory (ISIT)*, 2019.

[C26] L. Holzbaur, H. Liu, **S. Puchinger**, A. Wachter-Zeh. On Decoding and Applications of Interleaved Goppa Codes. accepted at *IEEE International Symposium on Information Theory (ISIT)*, 2019.

[C25] S. Müelich, **S. Puchinger**, V. Stukalov, and M. Bossert. A Channel Model and Soft-Decision Helper Data Algorithms for ROPUFs. accepted at *International ITG Conference on Systems, Communications and Coding*, 2019.

[C24] **S. Puchinger**, J. Renner, and A. Wachter-Zeh. Twisted Gabidulin Codes in the GPT Cryptosystem. In *International Workshop on Algebraic and Combinatorical Coding Theory*, 2018.

[C23] S. Müelich, **S. Puchinger**, and M. Bossert. Constructing an LDPC Code Containing a Given Vector. In *International Workshop on Algebraic and Combinatorical Coding Theory*, 2018.

[C22] A. Wachter-Zeh, **S. Puchinger**, and J. Renner. Repairing the Faure–Loidreau Public-Key Cryptosystem. In *IEEE International Symposium on Information Theory (ISIT)*, 2018.

[C21] P. Beelen, M. Bossert, **S. Puchinger**, and J. Rosenkilde né Nielsen. Structural Properties of Twisted Reed–Solomon Codes with Applications to Code-Based Cryptography. In *IEEE International Symposium on Information Theory (ISIT)*, 2018.

[C20] S. Müelich, **S. Puchinger**, and M. Bossert. Using Convolutional Codes for Key Extraction in SRAM Physical Unclonable Functions. In *Trustworthy Manufacturing and Utilization of Secure Devices (TRUDEVICE) Workshop*, 2018.

[C19] **S. Puchinger**, J. Rosenkilde né Nielsen, and J. Sheekey. Further Generalisations of Twisted Gabidulin Codes. In *International Workshop on Coding and Cryptography*, 2017.

[C18] **S. Puchinger**, I. Bouw, and J. Rosenkilde né Nielsen. Improved Power Decoding of One-Point Hermitian Codes. In *International Workshop on Coding and Cryptography*, 2017.

[C17] **S. Puchinger**, S. Müelich, and M. Bossert. On the Success Probability of Decoding (Partial) Unit Memory Codes. In *International Workshop on Optimal Codes and Related Topics*, 2017.

[C16] **S. Puchinger** and J. Rosenkilde né Nielsen. Decoding of Interleaved Reed–Solomon Codes Using Improved Power Decoding. In *IEEE International Symposium on Information Theory (ISIT)*, 2017.

[C15] P. Beelen, **S. Puchinger**, and J. Rosenkilde né Nielsen. Twisted Reed–Solomon Codes. In *IEEE International Symposium on Information Theory (ISIT)*, 2017.

[C14] U. Speidel, **S. Puchinger**, and M. Bossert. Constraints for Coded Tunnels Across Long Latency Bottlenecks with ARQ-based Congestion Control. In *IEEE International Symposium on Information Theory (ISIT)*, 2017.

[C13] Y. Cassuto, E. Hemo, **S. Puchinger**, and M. Bossert. Multi-Block Interleaved Codes for Local and Global Read Access. In *IEEE International Symposium on Information Theory (ISIT)*, 2017.

[C12] **S. Puchinger**, S. Müelich, K. Ishak, and M. Bossert. Code-Based Cryptosystems Using Generalized Concatenated Codes. In Ilias S. Kotsireas and Edgar Martínez-Moro, editors, *Springer Proceedings in Mathematics & Statistics: Applications of Computer Algebra: Kalamata, Greece, July 20–23 2015*, volume 198, pages 397–423. Springer International Publishing, 2017.

[C11] **S. Puchinger**, S. Müelich, A. Wachter-Zeh, and M. Bossert. Timing Attack Resilient Decoding Algorithms for Physical Unclonable Functions. In *International ITG Conference on Systems, Communications and Coding (SCC)*, 2017.

[C10] M. H. Mohamed, **S. Puchinger**, and M. Bossert. Guruswami–Sudan List Decoding for Complex Reed–Solomon Codes. In *International ITG Conference on Systems, Communications and Coding (SCC)*, 2017.

[C9] **S. Puchinger**, S. Stern, M. Bossert, and R. F. H. Fischer. Space-Time Codes Based on Rank-Metric Codes and Their Decoding. In *IEEE International Symposium on Wireless Communication Systems (ISWCS)*, pages 125–130, 2016.

[C8] **S. Puchinger** and A. Wachter-Zeh. Sub-Quadratic Decoding of Gabidulin Codes. In *IEEE International Symposium on Information Theory (ISIT)*, pages 2554–2558, 2016.

[C7] S. Müelich, **S. Puchinger**, David Mödinger, and M. Bossert. An Alternative Decoding Method for Gabidulin Codes in Characteristic Zero. In *IEEE International Symposium on Information Theory (ISIT)*, pages 2549–2553, 2016.

[C6] M. Hiller, L. Kürzinger, G. Sigl, S. Müelich, **S. Puchinger**, and M. Bossert. Low-Area Reed Decoding in a Generalized Concatenated Code Construction for PUFs. In *IEEE Computer Society Annual Symposium on VLSI*, 2015.

[C5] W. Li, J. S.R. Nielsen, **S. Puchinger**, and V. Sidorenko. Solving Shift Register Problems over Skew Polynomial Rings using Module Minimisation. In *International Workshop on Coding and Cryptography*, 2015.

[C4] **S. Puchinger**, S. Müelich, M. Bossert, Matthias Hiller, and Georg Sigl. On Error Correction for Physical Unclonable Functions. In *International ITG Conference on Systems, Communications and Coding*, 2015.

[C3] **S. Puchinger**, M. Cyran, R. F. H. Fischer, M. Bossert, and Johannes B. Huber. Error Correction for Differential Linear Network Coding in Slowly Varying Networks. In *International ITG Conference on Systems, Communications and Coding*, 2015.

[C2] S. Müelich, **S. Puchinger**, M. Bossert, M. Hiller, and G. Sigl. Error Correction for Physical Unclonable Functions Using Generalized Concatenated Codes. In *International Workshop on Algebraic and Combinatorical Coding Theory*, 2014.

[C1] **S. Puchinger**, A. Wachter-Zeh, and M. Bossert. Improved Decoding of Partial Unit Memory Codes Using List Decoding of Reed–Solomon Codes. In *International Zurich Seminar on Communications*, 2014.