Structured Matrix Days 2019
May 23–24, 2019 – Limoges, France

Generalized Sparse Matrices and Applications to Decoding and Cryptography

Maxime BROS[1],

In contexts which involve structured matrices, one often wants to exploit this structure to accelerate computations with these matrices. In code-based cryptography, one wants also this structure to be easily hidden. More precisely, the structure of the matrix, depending on the code chosen by the cryptographer, has to be masked so that an adversary could not recover the private key or the plaintext. First of all, I will show that sparsity for two different metrics can be use to create codes that are decodable in polynomial time ; the first one is the standard sparsity with a small number of nonzero entries (Moderate Density Parity Check codes [2]) whereas the second one uses matrices whose entries belong to a vector space of small dimension (Low Rank Parity Check codes [3]). I will use these two examples to describe how their structure is hidden for cryptographic purposes (both code-based and rank-based cryptography). I will also mention algebraic attacks on rank-based cryptosystems using Gröbner basis.

Keywords: MDPC, LRPC, code and rank-based cryptography, hidding matrices structure, McEliece cryptosystem, NIST post-quantum cryptography

References

[1] MCELIECE, ROBERT J A public-key cryptosystem based on algebraic *Coding Thv*, 4244, 114-116, (1978).

[2] MISOCZKI, RAFAEL AND TILLICH, JEAN-PIERRE AND SENDRIER, NICOLAS AND BARRETO, PAULO SLM MDPC-McEliece: New McEliece variants from moderate density parity-check codes *2013 IEEE international symposium on information theory*, 2069-2073, (2013).

[3] GABORIT, PHILIPPE AND MURAT, GAÉTAN AND RUATTA, OLIVIER AND ZEMOR, GILLES Low Rank Parity Check codes and their application to cryptography *The International Workshop on Coding and Cryptography (WCC 13)*, 2013, (2013).

[4] ARAGON, N. AND BARRETO, P. AND BETTAIEB, S. AND BIDOUX, LOIC AND BLAZY, O. AND DENEUVILLE, J.-C. AND GABORIT, P. AND GUERON, S. AND GÜNEYSU, T. AND AGUILAR MELCHOR, C. AND MISOCZKI, R. AND PERSICHETTI, E. AND SENDRIER, N. AND TILLICH, J.-P. AND ZÉMOR, G. BIKE *NIST submission for Post-Quantum Cryptography*, (November 2017).

[1]Université de Limoges, CNRS, XLIM, UMR 7252, Limoges, France
maxime.bros@etu.unilim.fr