Departamento de Matemática
Universidade de Aveiro

CIDMA CENTRO DE I&D EM MATEMÁTICA E APLICAÇÕES
CENTER FOR R&D IN MATHEMATICS AND APPLICATIONS

Seminário do Grupo de Álgebra e Geometria

A McEliece Cryptosystem with a Convolutional Mask

Miguel Beltrá Vidal
Universidade de Alicante, Espanha

Resumo

Decoding a linear code is in general a difficult task. With the Hamming metric the decoding problem is known to be an NP-hard problem [1], so generic decoding algorithms have a running time which is exponential in the code parameters. In 1978, McEliece designed the first public-key cryptosystem based on coding theory [2]. The public-key is the generator matrix of a code having an efficient decoding algorithm that has being masked to remove any visible structure and the ciphertext is a codeword with some errors added intentionally to hide the message. An attacker only has generic decoding algorithms to recover the message while the legitimate recipient can use the efficient decoding algorithm to recover it. The original proposal uses binary Goppa codes [3] which have an efficient decoding algorithm [4] but a low error-correction capability, which translates into big public-keys, so the cryptosystem has never been used in practice for this reason.

The recent improvements on quantum computing have stress out the necessity of having alternatives to the classical public-key schemes based on integer factorization [5] and discrete logarithms [6], for which attacks based on Shor's algorithm [7] can be performed in a large quantum computer. The McEliece cryptosystem is suitable for this context since there are no known feasible attack based on quantum algorithms, so there is a high interest to find alternatives to the original McEliece cryptosystem with smaller keys. Changing Goppa codes by codes with better error-correction capability such as GRS codes [8] or using a convolutional approach [9] are some of the proposals we can find in the literature. However, they are susceptible to strong structural attacks [10, 11].

By combining both approaches and constructing the cryptosystem adequately to avoid these attacks, we can get public keys which are up to a seventh of the size for the current NIST proposal [12] as it is shown in a recent work [13].

References

[1] Elwyn R. Berlekamp, Robert J. McEliece, and Henk C. A. Van Tilborg. On the inherent intractability of certain coding problems. IEEE Transactions on Information Theory, 24(3):384–386, 1978.

[2] R. J. McEliece. A public-key cryptosystem based on algebraic coding theory. Deep Space Network Progress Report, 44:114–116, 1978.

[3] Valerii Denisovich Goppa. A new class of linear correcting codes. Problemy Peredachi Informatsii, 6(3):24–30, 1970.

[4] N. Patterson. The algebraic decoding of Goppa codes. IEEE Transactions on Information Theory, 21(2):203–207, 1975.

[5] R. L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Commun. ACM, 21(2):120–126, feb 1978.

[6] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 31(4):469–472, 1985.

[7] P. W. Shor. Polynomial Time Algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 26(5):1481–1509, 1997.

[8] I. S. Reed and G. Solomon. Polynomial Codes Over Certain Finite Fields. Journal of the Society for Industrial and Applied Mathematics, 8(2):300–304, 1960.

[9] Carl Löndahl and Thomas Johansson. A New Version of McEliece PKC Based on Convolutional Codes. In Information

and Communications Security: 14th International Conference, ICICS 2012, Hong Kong, China, October 29-31, 2012. Proceedings, page 461–470, Berlin, Heidelberg, 2012. Springer-Verlag.

[10] V. M. Sidelnikov and S. O. Shestakov. On insecurity of cryptosystems based on generalized Reed-Solomon codes. Discrete Mathematics and Applications, 2(4):439–444, 1992.

[11] Grégory Landais and Jean-Pierre Tillich. An Efficient Attack of a McEliece Cryptosystem Variant Based on Convolutional Codes. In Philippe Gaborit, editor, Post-Quantum Cryptography, pages 102–117, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg.

[12] Daniel J. Bernstein, Tung Chou, Tanja Lange, Ingo von Maurich, Rafael Mizoczki, Ruben Niederhagen, Edoardo Persichetti, Christiane Peters, Peter Schwabe, Nicolas Sendrier, Jakub Szefer, and Wang Wen. Classic McEliece: conservative code-based cryptography. Round 4 submission to the NIST post-quantum cryptography call, October 2022.

[13] P. Almeida, M. Beltrá, D. Napp, and C. Sebastião. Smaller Keys for the McEliece Cryptosystem: A Convolutional Variant with GRS Codes. Submitted to IEEE Transactions on Information Theory, 2023.

Sala Sousa Pinto, 6 de novembro de 2023, 14:00

This seminar is partly supported by the Portuguese Foundation for Science and Technology (FCT - Fundação para a Ciência e a Tecnologia), through CIDMA - Center for Research and Development in Mathematics and Applications, within project UIDB/04106/2020.

fct Fundação para a Ciência e a Tecnologia

REPÚBLICA PORTUGUESA