The first National Conference on Applied Mathematics, Statistics and Applications
NCAMSA 2024 Conference
November 18-19, 2024, Batna - Algeria

Une nouvelle version du cryptosystème McEliece basée sur les codes de Lucas.

Rachid Chergui
Laboratoire d'Algèbre et Théorie des Nombres
Faculté de Mathématiques USTHB, Po. Box 32, El Alia,16111, Algiers, Algeria
e-mail: rchergui@usthb.dz

Abstract

McEliece [1] inventa le premier système de chiffrement basé sur la théorie algébrique des codes. Dans ces cryptosystèmes, la clé publique est constituée par la matrice génératrice d'un codes linéaire. Quoique McEliece a utilisé la famille des codes de Goppa binaires irréductibles.Le schéma que nous proposons repose sur les codes de Lucas. Notre système présente le bénéfice de résister aux attaques fondées sur les matrices creuses. En outre, la dimension des clés est diminuée.

Keywords : Cryptosystème McEliece , Nombre de Lucas , Algorithme, Complexité.

1 Introduction

McEliece [1] a créé le premier système de cryptographie basé sur la théorie algébrique des codes peu après la publication de l'article fondateur de la cryptographie à clé publique par Diffie et Hellman [4]. Dans ces systèmes de cryptographie la clé publique est constituée par la matrice génératrice d'un codes linéaire.Des efforts ont été entrepris pour diminuer la dimension de cette clé en employant diverses méthodes. À l'heure actuelle, diverses stratégies ont été suggérées en ajustant la structure du code de Goppa, comme les codes Reed Muller [5, 6], les codes LDPC [8, 9], les codes convolutionnels [7] etc.....

References:

[1] R. J .McEliece. *A public-key cryptosystem based on algebraic coding theory.* DSN Progress Report, 42-44, pp. 114–116, 1978.

[2] R. Chergui. Zeckendorf Arithmetic For Lucas Numbers, Palestine Journal of Mathematics, Vol 9(1), 337–342, 2020.

[3] A. Apostolico and A. Fraenkel, Robust transmission of unbounded strings using Fibonacci representations. IEEE Trans. on Information Theory, Vol 33, (1987), pp 238-245.

[4] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Inform. Theory, 22(6), pp 644-654, 1976.

[5] G.A. Karpunin, On the key space of the McEliece cryptosystem based on binary Reed-Muller codes, Disc. Math. Applic., vol. 14, no. 3, pp. 257–262, Jul. 2004.

[6] V. M. Sidelnikov, A public-key cryptosytem based on Reed-Muller codes, Discr. Math. Applic., vol. 4, no. 3, pp. 191–207, Jan. 1994.

[7] Londahl, C. and T. Johansson. A new version of McEliece PKC based on convolutional codes, Information and Communications Security - ICICS , Lecture Notes in Computer Science, Springer, 461-470. 2012.

[8] M. Baldi, F. Chiaraluce, R. Garello, and F. Mininni, Quasi-cyclic low-density paritycheck codes in the McEliece cryptosystem, in Proc. IEEE Int. Conf. on Commun., Glasgow, UK, pp. 951–956.Jun. 2007

[9] Baldi, M. , M. Bodrato, and G. F. Chiaraluce. A1new analysis of the McEliece cryptosystem based on QC-LDPC codes. Security and Cryptography for Networks (SCN), Lecture Notes in Computer Science, Springer, 5229 : 246-262.2008