The McEliece Based Public-Key Cryptosystem Approach

Selda Çalkavur

August 17, 2021

The McEliece based public-key cryptosystem approach

Selda Çalkavur

Math Dept, Kocaeli University, Kocaeli, Turkey,
Email: selda.calkavur@kocaeli.edu.tr

Abstract—**In this paper, we introduce a new public-key cryptosystem based on linear codes. McEliece studied the first code-based public-key cryptosystem. We are inspired by McEliece system in the construction of the new system. We examine its security using linear algebra and compare it with the other code-based cryptosystems. Our new cryptosystem is too reliable in terms of security.**

Index Terms: Linear codes, public-key cryptosystem, linear system

2010 AMS Mathematics Subject Classifications: 94B05, 11T71, 94A60, 14C20.

I. Introduction

Public-key cryptosystem is one of the most important topic in cryptography. Diffie and Hellman [7] were first introduced the public-key cryptography. Then Rivest, Shamir and Adleman [26] invented the first practical public-key cryptosystem. Their system is based on the hardness of factoring integers. Shor [28] wrote a quantum algorithm to solve the abelian hidden subgroup problem. Some quantum-safe public-key cryptosystems have been proposed recently [25], [13], [8].

Code-based cryptography was first suggested by McEliece [19] using binary Goppa codes in 1978. This system has the efficient encryption and decryption algorithms. The security of the McEliece cryptosystem is related to decoding a random linear code in some metric. Many new cryptosystems have been presented using different codes replacing Goppa codes [2], [3], [5], [14], [18], [21], [22], [23], [29], but most of them are broken by using the algebraic structures of the codes [1], [4], [6], [9], [17], [20], [27], [30], [31].

Gabidulin et al. [10] proposed a kind of McEliece based on Gabidulin codes. They are a family of rank metric-codes. Overbeck [24] broke the Gabudulin's cryptosystem. Next, Gaborit et al. [11] developed a new family of rank-metric codes is called Low Rank Parity Check (LRPC) codes. LRPC code-based cryptosystem is a reliable system.

In this work, we introduce a new public-key cryptosystem based on linear codes by combining McEliece cryptosystem. We give the encryption and decryption algorithms by using coding theory and linear algebra. We analyse its effectiveness by means of security. We result by the comparison between our cryptosystem and the three other code-based public-key cryptosystems in the literature: McEliece's system [19], Krouk et al. [16] and Kim et al. [15] system.

The paper is organized as follows. Section II reminds some necessary informations on coding theory and cryptography. Section III describes the new cryptosystem and explains its security. Section IV considers the comparison with the other systems. Section V concludes the paper.

II. Preliminaries

We begin by defining the linear codes.

Definition 1. ([12]) Let q be a prime power. $\mathbb{F}_q$ being denote the finite field of order q, an $[n,k]$- linear code C over $\mathbb{F}_q$ is a subspace of $\mathbb{F}_{q^n}$, where n is length of the code C and k is dimension of C.

Definition 2. ([12]) The dual code of C is the set of those vectors $\mathbb{F}_{q^n}$ which are orthogonal to every codeword of C. It is denoted by $C^{\perp}$. $C^{\perp}$ is an $[n, n-k]$- linear code.

Definition 3. ([12]) A $k \times n$ matrix G is the generator matrix for a linear code C. The rows of G consist of a basis of C. Note that an $[n,k]$- code C over $\mathbb{F}_q$ has q^k codewords.

A. Public-Key Cryptosystems

Public-key cryptography or asymmetric cryptography is a cryptographic system which contains the public-key and private key. The public-key is known to everyone, but the private key should only be known to the sender. Encryption is done with the public-key and decryption with the private key. These keys are not completely independent of each other. There must be a mathematical relationship between them. So public-key cryptosystems are built on mathematical functions.

With public-key cryptography, robust authentication is also possible. A sender can combine a message with a private key to create a short digital signature on the message. Anyone with the sender's corresponding public-key can combine that message with a claimed digital signature; if the signature matches the message, the origin of the message is verified.

Public-key algorithms are main security principles in modern cryptosystems. Asymmetric encryption is slower than good symmetric encryption. Both symmetric and asymmetric encryption systems are used today.

III. The System

In this section, we present a new public-key cryptosystem based on linear codes by a different approach. Consider the following steps to construct the public and private key.

A. Key-Generation Procedure

The user named Alice does the following.

1) Selects an $[n, k]$- linear code C over $\mathbb{F}_q$ with $k \times n$ generator matrix G.
2) Selects random a non-singular $n \times n$ matrix M over $\mathbb{F}_q$.
3) Calculates the $k \times n$ matrix $G^{'} = GM$ and the invers matrix M^{-1}.
4) The public-key is $G^{'}$ and private key is (G, M, M^{-1}).

B. Encryption Algorithm

If the other user named Bob wants to send the message m of length k, then he should do the following, where m is non-zero element of $\mathbb{F}_{q^k}$.
I-) Gets the Alice's public-key $G^{'}$.
II-) Considers the message $m \in \mathbb{F}_{q^k}$.
III-) Calculates the ciphertext $c \in \mathbb{F}_{q^n}$ as $c = mG^{'}$.
IV-) Sends the ciphertext c to Alice.

C. Decryption Algorithm

Alice gets the ciphertext c and follows the below steps to decrypt the message.
i) Uses the private key (G, M, M^{-1}).
ii) Calculates $c^{'} = cM^{-1}$.
iii) Obtains m from $c^{'}$ by solving the linear system $c^{'} = cM^{-1}$ of rank k.

Decryption is correct since $c^{'} = cM^{-1} = mG^{'}M^{-1} = mGMM^{-1} = mG$.

Proposition 1. *Let C be an $[n, k]$- linear code over $\mathbb{F}_q$ with generator matrix G. The size of plaintext is $q^k - 1$ in the new system.*

Proof. The plaintext is any non-zero element of $\mathbb{F}_{q^k}$ and $\mathbb{F}_{q^k}$ has $q^k - 1$ non-zero elements. □

Proposition 2. *The number of ciphertext is q^n.*

Proof. The ciphertext is any element of $\mathbb{F}_{q^n}$. So the size of ciphertext is q^n. □

Example 1. Consider the $[4, 2]$- linear code over $\mathbb{F}_3$. The generator matrix G of C is

$$G = \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}.$$

Select any random non-singular matrix is

$$M = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 2 & 2 & 0 & 1 \end{pmatrix}$$

over $\mathbb{F}_3$. The invers matrix is

$$M^{-1} = \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}.$$

In this case, the matrix $G^{'} = GM$ will be

$$G^{'} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}$$

over $\mathbb{F}_3$. So Alice's public-key is

$$G^{'} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix}$$

and private key is $(G, M, M^{-1}) =$

$$(\begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 2 \\ 1 & 1 & 0 & 1 \\ 2 & 2 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix}).$$

Encryption: Bob gets Alice's public-key to encrypt the plaintext $m = (12) \in \mathbb{F}_{3^2}$ and calculates the ciphertext $c \in \mathbb{F}_{3^4}$ as

$$c = mG^{'} = (12) \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 1 & 2 \end{pmatrix} = (0202).$$

Then he sends the ciphertext $c = (0202)$ to Alice.
Decryption: Alice calculates the plaintext $m \in \mathbb{F}_{3^2}$ by her own private key as follows.

$$c^{'} = cM^{-1} = mG$$

$$(0202) \begin{pmatrix} 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 0 & 2 & 0 \\ 0 & 0 & 2 & 2 \end{pmatrix} = (m_1 m_2) \begin{pmatrix} 1 & 0 & 2 & 2 \\ 0 & 1 & 2 & 1 \end{pmatrix}$$

$$(1201) = (m_1, m_2, 2m_1 + 2m_2, 2m_1 + m_2).$$

It is obtained $m_1 = 1, m_2 = 2$ by solving the above linear system. So the plaintext will be $m = (m_1 m_2) = (12)$.

D. Security of the System

The security of the new system is based on the difficulty of solving the factorization problem of matrices in linear algebra. The mathematical relationship between the public-key and private key is very strong. This relationship is the factorization problem of matrices, the size of matrix being too big. That is the problem of finding matrices G and M. There is no easy way to solve this problem in mathematics. Thus it is benefical having the large q, n and k. More clearly, even if an attacker knows the public-key, it is not possible to find the private key, and knows the public-key and ciphertext, it is impossible practically. So our new code-based public-key cryptosystem is robust against attacks since the solution of the algebra problem on which it is based is unknown. The only way to crack the cipher is by trial and error, but is not possible practically.

Theorem 1. *Let C be an $[n, k]$- linear code over $\mathbb{F}_q$ with generator matrix G. If the code parameters are large enough, the system will be too reliable by means of security.*

Proof. If k and q are large enough, then the system can generate a large number of plaintext. In this case, it will be difficult to reach the plaintext for the attacker. Moreover, if k, q and n are large enough, it will be impossible to obtain the private key for the attacker. Because the solution of factorization problem of matrices is very hard. So the code parameters must be large enough to ensure the security of the system. □

IV. Comparison with the other Systems

McEliece [19] introduced the public-key cryptosystem based on error-correcting codes. McEliece used binary Goppa codes, providing efficient encryption and decryption algorithms. The security of the McEliece cryptosystem depends on the difficulty of decoding a random linear code in some metric. Krouk and Ovchinnikov [16] developed the public-key cryptosystem based on bursts-correcting codes. They inspired by McEliece cryptosystem. The security of their system is also based on the hardness of decoding in the linear code. However, Krouk and Ovchinnikov's cryptosystem is safer than McEliece's. Kim et al. [15] suggested a new code-based public-key encryption scheme which is called McNie. They also inspired by McEliece and Niederreiter cryptosystems, but they showed that is not more difficult to crack McEliece than McNie. The security of McNie is based on the (Rank) Syndrome Decoding Problem.

In our study, we propose another code-based public-key cryptosystem. This system is based on any linear code. Its security relies on the hardness of solving the factorization problem of matrices using the linear algebra. Our system is faster than the other code-based public-key cryptosystem by means of implementation. So it is safer than cryptosystems of this class.

V. Conclusion

In this work, we propose a new code-based public-key cryptosystem using linear codes. This system is inspired by McEliece cryptosystem. The security is based on linear algebra. More clearly, it depends on the difficulty of solving the factorization problem of matrices. The size of parameters of the linear code is considered in terms of security. It is compared with the other code-based public-key cryptosystems. The new cryptosystem stands well.

References

[1] M. Baldi and F. Chiaraluce, Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes, In Information Theory, 2007, ISIT 2007, IEEE International Symposium, pp. 2591-2595, 2007.

[2] M. Baldi, F. Chiaraluce, R. Garello, and F. Mininni, Quasi-cyclic low-density parity-check codes in the McEliece cryptosystem, In Communications, ICC'07, IEEE International Conference, pp. 951-956, June, 2007.

[3] T. Berger and P. Loidreau, How to mask the structure of codes for a cryptographic use, Designs, Codes and Cryptography, vol. 35, no. 1, pp. 63-79, 2005.

[4] I. V. Chizhov and M. A. Borodin, The failure of McEliece PKC based on Reed-Muller codes, IACR Cryptology ePrint Archive, p. 287, 2013.

[5] A. Conteaut and F. Chabaud, A new algorithm for finding minimum-weight words in a linear code: application to McEliece's cryptosystem and to narrow-sense BCH codes of length 511, IEEE Transactions on Information Theory, vol. 44, no. 1, pp. 367-378, 1998.

[6] A. Couvreur, I. Márquez-Corbella, and R. Pellikaan, A polynomial time attack against algebraic geometry code based public key cryptosystems, In Information Theory (ISIT), IEEE International Symposium, pp. 1446-1450, 2014.

[7] W. Diffie and M. Hellman, New directions in cryptography, IEEE Transactions on Information Theory, 22(6), pp. 644-654, 1976.

[8] L. Eldar and P. W. Shor, An efficientquantum algorithm for a variant of the closest lattice-vector problem, arXiv preprint, arXiv: 1611.06999, 2016.

[9] C. Faure and L. Minder, Cryptanalysis of the McEliece cryptosystem over hyperelliptic codes, In Proceedings of the 11th international workshop on Algebraic and Combinatorial Coding Theory, ACCT, vol. 2008, pp. 99-107, June 2008.

[10] E. M. Gabidulin, A. V. Paramonov, and O. V. Tretjakov, Ideals over a non-commutative ring and their application in cryptology, Workshop on the Theory and Application of Cryptographic Techniques, pp. 482-489, Springer, Berlin, Heidelberg, 1991.

[11] P. Gaborit, G. Murat, O. Ruatta, and G. Zémor, Low rank parity check codes and their application to cryptography, The Proceedings of Workshop on Coding and Cryptography (WCC), pp. 168-180, Borgen, Norway, 2013.

[12] R. Hill, A First Course in Coding Theory, Oxford University, Oxford, 1986.

[13] J. Hoffstein, J. Pipher, and J. Silverman, NTRU: A ring-based public-key cryptosystem, Algorithmic number theory, pp. 267-288, 1998.

[14] H. Janwa and O. Moreno, McEliece public key cryptosystems using algebraic-geometric codes, Designs, Codes and Cryptography, 8(3), pp. 293-307, 1996.

[15] J. L. Kim, Y. -S. Kim, L. Galvez, M. J. Kim, N.Lee, McNie: A new code-based public-key cryptosystem, arXiv: 1812.05008v2 [cs.CR], 27 Jan. 2019.

[16] E. Krouk, A. Ovchinnikov, Code Based Public-Key Cryptosystem Based on Bursts-Correcting Codes, AICT 2017: The Thirteenth Advanced International Conference on Telecommunications, IARIA, 2017.

[17] G. Landais and J. P. Tillich, An efficient attack of a McEliece cryptosystem variant based on convolutional codes, In International Workshop on Post-Quantum Cryptography, pp. 102-117, Springer, Berlin, Heidelberg, 2013.

[18] C. Löndhal and T. Johansson, A New Version of McEliece Based on Convolutional Codes, In ICICS, vol. 7618, pp. 461-470, 2012.

[19] R. J. McEliece, A Public-Key Cryptosystem Based on Algebraic Coding Theory, DSN progress report 42(44), pp. 114-116, 1978.

[20] L. Minder and A. Shokrollahi, Cryptanalysis of the Sidelnikov cryptosystem, Advances in Cryptology-EUROCRYPT 2007, pp. 347-360, 2007.

[21] R. Misoczki, J. P. Tillich, N. Sendrier, and P. Barreto, MDPC-McEliece: New McEliece variants from moderate density parity-check codes, IEEE International Symposium on Information Theory-ISIT 2013, pp. 2069-2073, 2013.

[22] C. Monico, J. Rosenthal, and A. Shokrollahi, Using low density parity check codes in the McEliece cryptosystem, In Information Theory, Proceedings, IEEE International Symposium, p. 215, 2000.

[23] H. Niedderreiter, Knapsack-type cryptosystems and algebraic coding theory, Problems of Control and Information Theory, vol. 15, no. 1934, 1986.

[24] R. Overbeck, A new structural attack for GPT and variants, Mycrypt 2005: Progress in Cryptology, LNCS, vol. 3715, pp. 50-63, 2005.

[25] O. Regev, On lattices, learning with errors, random linear codes and cryptography, Journal of the ACM, vol. 56, no.6, Art. 34, 40, 2009.

[26] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[27] N. Sendrier, On the concatenated structure of a linear code, Applicable Algebra in Engineering, Communication and Computing, vol. 9, no. 3, pp. 221-242, 1998.

[28] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM journal on computing, vol. 26, no. 5, pp. 1484-1509, 1997.

[29] V. M. Sidelnikov, A public-key cryptosystem based on binary Reed-Muller codes, Discrete Mathematics and Applications, vol. 4, no. 3, pp. 191-208, 1994.

[30] V. M. Sidelnikov and S. O. Shestakov, On insecurity of cryptosystems based on generalized Reed-Solomon codes, Discrete Mathematics and Applications, vol. 2, no. 4, pp. 439-444, 1992.

[31] C. Wieschebrink, Cryptanalysis of the Niederreiter public key scheme based on GRS subcodes, In International Workshop on Post-Quantum Cryptography, pp. 61-72, Springer, Berlin, Heidelberg, May 2010.