Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 28, S. 320-324, Kasım 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 28, pp. 320-324, November 2021

Research Article

A New Public-Key Cryptosystem Based on LCD Codes

Selda Çalkavur[1*]

[1*] Kocaeli University, Faculty of Science and Arts, Departmant of Mathematics, Kocaeli, Turkey, (ORCID: 0000-0002-1502-123X), selda.calkavur@kocaeli.edu.tr

(1st International Conference on Applied Engineering and Natural Sciences ICAENS 2021, November 1-3, 2021)

(**DOI:** 10.31590/ejosat.999112)

ATIF/REFERENCE: Çalkavur, S. (2021). A New Public-Key Cryptosystem Based on LCD Codes. *Avrupa Bilim ve Teknoloji Dergisi*, (28), 320-324.

Abstract

A cryptosystem is a structure or scheme consisting of a set of algorithms that converts plaintext to ciphertext to encode or decode messages securely. The cryptosystem points at a computer system that employs cryptography. Cryptosystems are classified by the method they use to encrypt data. One of them is symmetric key encryption. While the symmetric key algorithm uses the same key for encryption and decryption, asymmetric key encryption or public-key encryption uses the different keys. So it is more reliable than symmetric cipher algorithm. In this paper, we propose a new public-key cryptosystem by using LCD codes and explain the signature protocol based on this system which is reliable.

Keywords: Public-key cryptosystem, Digital signature, LCD code.

[*] Corresponding Author: selda.calkavur@kocaeli.edu.tr

1. Introduction

Public-key encryption is a method of encrypting data with two different keys. One of the keys is the public-key which is available for anyone to use. The other is the private key.. The data encrypted with the public-key can only be decrypted with the private key, and the data encrypted with the private key can only be decrypted with the public-key. Public- key encryption is also known as asymmetric encryption.

The first public-key cryptosystem was introduced by Diffie and Hellman in 1976. Diffie and Hellman's [8] key agreement is the first solution for the key distribution problem. They developed some public-key cryptography techniques. Then Rivest et al. [26] worked on an important public-key cryptosystem which is entitled RSA algorithm in 1978. This system can be used to provide both privacy and digital signature. The security of RSA lies in the difficulty of the integer factorization problem. McEliece [21] proposed a public-key cryptosystem based on error-correcting codes, binary Goppa codes, in 1978. McEliece cryptosystem has no practical usage because of its large key size.

Several alternative systems have been proposed after McEliece's scheme. It was used for generalized Reed-Solomon codes of McEliece's method by Niederreiter [25]. Berger et al. [3] introduced the use of subcodes of generalized Reed-Solomon codes. Berlekamp et al. [5] completed the decoding task of arbitrary linear code. Besides it was shown that the attacks revealing of the structure are also possible in [28], [14]. Krouk [13] presented a different class of public-key cryptosystems. It is based on the task of complete decoding. This means the decoding of coset leaders is done in the standard array [18]. The attacks occuring during encryption were examined in [16]. Some examples of the systems were considered in [16], [12]. Janwa and Moreno [11] suggested the use of algebraic geometry codes. Sidelnikov [29] presented the use of Reed-Muller codes. The use of MDPC codes was introduced by Misoczki et al. [22], the use of convolotional codes was introduced by Löndahl and Johansson [17]. Berger et al. [4] and Misoczki-Barreto [23] presented quasi-cyclic and quasi-dyadic constitution by using McEliece encryption schemes. Most of them have been broken the code based McEliece cryptosystem, but the original binary Goppa code based McEliece encryption scheme is still used safely.

LCD codes consist of an important class of linear codes. Massey studied LCD codes in 1992 [19]. Moreover, some LCD cyclic codes were constructed by Massey [20]. In [31] Massey and Yang obtained a necessary and sufficient condition for a cyclic code of lenth n over finite fields to be an LCD code. Sendrier examined LCD codes correspond the asymptotic Gilbert-Varshamov bound [27]. Esmaeili and Yari [9] introduced complementary-dual-quai-cyclic codes. Carlet and Guilley examined an implementation of LCD codes against side-channel attacks in [6]. Alahmadi et al. [1] constructed a multisecret-sharing scheme based on LCD codes.

In this study, we propose a new public-key cryptosystem based on LCD codes and examine the signature protocol. We explain that it is a secure system, discuss some possible attacks on the system.

The rest of the paper is organized as follows. The next section gives some necessary background on cryptography and coding theory. Section III introduces the new public-key cryptosystem, the signature protocol. Section IV analyzes its security and considers some possible attacks. Section V compares to the other systems. Section VI concludes the paper.

2. Preliminaries

In this section, we remind some important topics that are necessary for the paper.

2.1. Public-Key Cryptosystems

A cryptosystem is an application of cryptographic methods and ensures the information security services. It can be examined under two titles as symmetric and asymmetric systems. Symmetric cryptosystems based on a natural concept. However, asymmetric or public-key cryptosystems are very difficult to comprehend. There are two keys in the public-key cryptosystems. One of them is public-key and the other is private key. In a public-key cryptosystem, any person can encrypt a message using the intended receiver's public-key, but the encrypted message can only be decrypted with the receiver's private key. There must be a mathematical relationship between the public-key and private key. This relation must be built on an equation that cannot be easily solved. Otherwise, when this equation solved, the private key can be obtained. This situation threatens the security of the system. The public-key can be known by everyone since the public-key cannot decryption, only encryption can. However, the private key must be known only by user.

Diffie-Hellman cryptosystem [8] and RSA cryptosystem [26] are pioneers of public-key cryptosystem.

2.2. Signatures

An electronic signature depends on both message and signer. The public-key cryptosystem must be used to implement the signatures. Otherwise the recipient could change the message before showing the signed message. In a public-key cryptosystem, person A encrypts the document she/he wants to sign with her/his private key. Person B opens the document with A's public-key. If B does not, the signature is not valid or the signature has been broken by someone. Thus it has been authenticated.

2.3. Linear Codes

A linear code C of length n and dimension k is a subspace of $(F_q)^n$, where F_q is the finite fields with q elements. Such a code is denoted by $[n, k]$. All vectors in $(F_q)^n$ that are orthogonal to every codeword of C consist of the dual code $C^{\perp}$. $C^{\perp}$ is an $[n, n-k]$ $-$code. The codewords of C are generated by the rows of generator matrix G. G is a $k \times n$ matrix the rows of which form a basis of C. The parity-check matrix H is a generator matrix for the dual code $C^{\perp}$. H is an $(n-k) \times n$ matrix.

2.4. LCD Codes

Linear Complementary Dual (LCD) code is a linear code C satisfying $C \cap C^{\perp} = 0$ [19]. Any code over a field is equivalent to a code generated by a matrix of the form $(I_k|A)$, where I_k is the $k \times k$ identity matrix [7]. C is LCD if $\binom{G}{H}$ is invertible [24].

3. Code-Based Cryptosystem Using LCD Codes

In this part, we propose a new public-key cryptosystem by using LCD codes. An user, for example Alice, constructs her own the public-key and private key as follows.

1) Select an $[n,k]$ −LCD code C over F_q with generator matrix G and parity-check matrix H.

2) Construct $n \times n$ matrix $T = \binom{G}{H}$.

3) Calculate $n \times n$ inverse matrix $T^{-1} = \binom{G}{H}^{-1}$.

4) Public-key is (G,H), private key is $T^{-1} = \binom{G}{H}^{-1}$.

3.1. Encryption Algorithm

Suppose that Bob wants to send Alice a message m. Bob should do the following.

I- Take the Alice's public-key $(\boldsymbol{G},\boldsymbol{H})$.
II- Consider the message $m \in (F_q)^n$, m is non-zero.
III- Calculate $c_1 = G.m^T$ and $c_2 = H.m^T$.
IV- Obtain the ciphertext c as c_1c_2.
V- Send Alice the ciphertext c.

3.2. Decryption Algorithm

Alice should do the following to find the plaintext m from the ciphertext c.

i) Use the private key $\boldsymbol{T^{-1}} = \binom{\boldsymbol{G}}{\boldsymbol{H}}^{-1}$.
ii) Calculate $m = \binom{G}{H}^{-1}.c^T$, where ^{T} denotes transposition.

Proposition 1. Let C be an $[n,k]$ −LCD code over F_q with generator matrix G. In the new public-key cryptosystem based on C, the size of plaintext is $q^n - 1$.

Proof. The plaintext is any non-zero elements of $(F_q)^n$ and $(F_q)^n$ consists of $q^n - 1$ non-zero elements.

Corollary 1. The number of ciphertext is $q^n - 1$.

Proof. It is easily seen from Proposition 1.

Example 1. Alice considers an LCD [3, 2]-code over F_2. The generator matrix and parity-check matrix are

$$G = \begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\end{pmatrix},\ H = (1 \quad 1 \quad 1)$$

for this code. Since C is LCD, the matrix $\boldsymbol{T} = \binom{\boldsymbol{G}}{\boldsymbol{H}}$ is invertible. Alice calculates the matrix

$$\boldsymbol{T^{-1}} = \binom{\boldsymbol{G}}{\boldsymbol{H}}^{-1}.$$

Alice's public-key is

$$\left(G = \begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\end{pmatrix},\ H = (1 \quad 1 \quad 1) \right)$$

and private key is

$$\boldsymbol{T^{-1}} = \binom{\boldsymbol{G}}{\boldsymbol{H}}^{-1} = \begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\\ 1 & 1 & 1\end{pmatrix}^{-1} = \begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}.$$

Encryption: Bob takes Alice's public-key to encrypt the message $m = (001) \in (F_2)^3$ and calculates c as follows.

$$c_1 = G.m^T = \begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\end{pmatrix}.\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$$

and

$$c_2 = H.m^T = (1 \quad 1 \quad 1).\begin{pmatrix}0\\0\\1\end{pmatrix} = (1).$$

So $c = c_1c_2 = (011)$. Then he sends Alice $c = (011)$.

Decryption: Alice calculates m from c by her own private key.

$$m = \binom{G}{H}^{-1}.c^T = \begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\\ 1 & 1 & 1\end{pmatrix}^{-1}.\begin{pmatrix}0\\1\\1\end{pmatrix} = \begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}.\begin{pmatrix}0\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\end{pmatrix}.$$

3.3. Signatures

Our new public-key cryptosystem can also be used for the digital signatures.

3.3.1. Sign

If Alice wants to send Bob the signed message m, then she applies to the message her own private key. That is

$$\sigma^T = \binom{G}{H}^{-1}.m^T.$$

Then she sends Bob the signed message (m,σ).

3.3.2. Verify Signature

Bob calculates ${m_1}^T = G.\sigma^T$ and ${m_2}^T = H.\sigma^T$ to verify the signature. Therefore obtains $m = m_1m_2$. So the signature is verified.

Example 2. (continued)

Sign: Alice calculates

$$\sigma^T = \binom{G}{H}^{-1}.m^T$$

to sign the message $m = (001) \in (F_2)^3$.

$$\sigma^T = \begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\\ 1 & 1 & 1\end{pmatrix}^{-1}.\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 1 & 0 & 1\end{pmatrix}.\begin{pmatrix}0\\0\\1\end{pmatrix} = \begin{pmatrix}1\\1\\1\end{pmatrix}$$

and she sends Bob $(m,\sigma) = ((001),(111))$.

Verify Signature: Bob should do the following to verify the signature.

$${m_1}^T = G.\sigma^T = \begin{pmatrix}1 & 1 & 0\\ 1 & 0 & 1\end{pmatrix}.\begin{pmatrix}1\\1\\1\end{pmatrix} = \begin{pmatrix}0\\0\end{pmatrix}$$

and

$$m_2{}^T = H.\sigma^T = (1 \quad 1 \quad 1).\begin{pmatrix}1\\1\\1\end{pmatrix} = (1).$$

Therefore $m = m_1 m_2 = (001)$ is obtained. So the signature is verified.

4. Security of the System

It is seen that the encryption and decryption algorithms can be applied simply. So we should examine some possible attacks. The security of the system based on an $[n,k]$ −LCD code over F_q depends on the size of parameters q, n and k. If n and k are large enough, the first attack seems ineffective. In this case, there are a lot of chances for G and H.

When n is big enough, it will be difficult to find the inverse of the matrix $T = \binom{G}{H}$. So an enemy cryptanalyst cannot break the private key. Moreover, it is also benefical having a large q. Because the number of plaintext will increase. This means an attacker cannot guess the plaintext. However, when n and q are large it might be costly in term of arithmetic application.

4.1. Robustness of LCD Codes Against Existing Attacks

Theorem 1. Let G be an $k \times n$ generator matrix and H be an $(n-k) \times n$ parity-check matrix of an $[n,k]$ −LCD code C over $\boldsymbol{F_q}$. With the above conditions, the new cryptosystem based on C is robust against attacks.

Proof. We construct a public-key cryptosystem based on an LCD code. If $\binom{G}{H}$ is invertible, C is LCD [24]. So that the square matrix $\binom{G}{H}$ is of full rank n. That is if $\binom{G}{H}$ generates the full n dimensional space, then each element of $(F_q)^n$ could have any random matrix as its LCD public-key. This also means it has an efficient decryption algorithm for random $[n,k]$ −LCD codes with sufficiently large n. Because it is a difficult problem finding the inverse of matrices with large size.

5. Comparison with the Other Systems

In [30], Wang proposed the linear code based encryption scheme RLCE which shares many characteristic with random linear codes. In the key setup process, it is used the parameters n, k, d, t of an $[n,k,d]$ −code with generator matrix G. There is an efficient algorithm to correct at least t errors for this linear code given by G. RLCE scheme guarantees correct decryption and is secure. This system is a public-key cryptosystem.

McEliece's [21] public-key cryptosystem is based on Goppa codes. McEliece presented a secure system by using linear codes.

Krouk and Ovchinikov [15] developed a cryptosystem based on bursts-correcting codes and used a linear $[n,k]$ −code with generator matrix G to construct their system. They inspired by McEliece cryptosystem, however, proved that their system is more reliable than McEliece cryptosystem.

In our framework, LCD codes were considered. We used an important property for the generator matrix G and parity-check matrix H of an LCD code. The security relies on the difficulty of finding the inverse of the matrix $\binom{G}{H}$ and depends on the length n and size q.

6. Conclusion

In this paper, we proposed a new public-key cryptosystem based on LCD codes and presented the signature protocol. We analyzed its security, explain some possible attacks. The security of the system depends on the size of parameters q and n. We compared it with the other public-key cryptosystems based on linear codes. This method should be applied for the LCD codes that have large n and q. Our system is an effective method for a public-key cryptosystem.

7. Acknowledge

I would like to thank to Dr. Patrick Solé for helpful discussions.

References

[1] Alahmadi, A., Altassan, A., AlKenani, A., Çalkavur, S., Shoaib, H., Solé, P., (2020), A Multisecret-Sharing Scheme Based on LCD Codes, Mathematics, vol. 8, no. 272.

[2] Baldi, M., Bodrato, M., and Chiaraluce, F., (2008), A new analysis of the mceliece cryptosystem based on qc-ldpc codes, In Security and Cryptography for Networks, pp. 246-262, Springer.

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

[4] Berger, T. P., Cayrel, P. -L., Gaborit, P. , and Otmani, A., (2009), Reducing key length of the mceliece cryptosystem. In Progress in Cryptology-AFRICACRYPT 2009, pp. 77-97, Springer.

[5] Berlekamp, E., McEliece, R., and Tilborg, H. van, (1978), On the inherent intractability of certain coding problems (corresp.), IEEE Transactions on Information Theory, vol. 24, no. 3, pp. 384-386, May.

[6] Carlet, C. , Guilley, S., (2014), Complementary dual codes for counter measures to side-channel attacks, In Proceedings of the 4th ICMCTA Meeting, Palmela, Portugal, 15-18 September 2014.

[7] Dougherty, S. T. , Kim, J. -L., Özkaya, B., Solé, P., (2017), The combinatorics of LCD codes: Linear programming bound and orthogonal matrices, IJICOT 2017, vol. 4, pp. 116-128.

[8] Diffie, W., and Hellman, (1976), M. E., New Directions in Cryptography, IEEE Transactions on Information Theory, IT-22, no. 6, pp.644-654, November 1976.

[9] Esmaeili, M., Yari, S., (2009), On complementary-dual quasi-cyclic codes, Finite Fields Appl., vol. 15, pp. 357-386.

[10] Güneri, C., Özkaya, B., Solé, P., (2016), Quasi-cyclic complementary dual codes, Finite Fields Appl., vol. 42, pp. 67-80.

[11] Janwa, H., and Moreno, O., (1996), McEliece public key cryptosystems using algebraic-geometric codes, Designs, Codes and Cryptography, vol. 8, no. 3, pp. 293-307.

[12] Kabatiansky, G. , Semenov, S. and Krouk, E., (2005), Error-Correcting Coding and Security for Data Networks: Analysis of the Superchannel Concept, John Wiley, Sons, p. 278.

[13] Krouk, E., (1983), A New Public-Key Cryptosystem, in Sixth Joint Swedish-Russian International Workshop on Information Theory, Moelle, Sweden, pp. 285-286.

[14] Krouk, E., Ovchinnikov, A., and Vostokova, E., (2016), About one modification of McEliece cryptosystem based on Plotkin construction, in 2016 XV International Symposium Problems of Redundancy in Information and Control Systems (REDUNDANCY), pp. 75-78, September 2016.

[15] Krouk, E., Ovchinnikov, A., (2017), Code-Based Public-Key Cryptosystem Based on Bursts-Correcting Codes, AICT 2017, The Thirteenth Advanced International Conference on Telecommunications, pp. 93-95, IARIA.

[16] Krouk, E., and Serger, U., (1998), A Public Key Cryptosystem Based on Total Decoding of Linear Codes, in VI International Workshop "Algebraic and combinatorial coding theory", Pskov, pp. 116-118.

[17] Löndahl, C., and Johansson, T., (2012), A new version of mceliece pkc based on convolutional codes, In Information and Communications Security, pp. 461-470, Springer.

[18] MacWilliams, F., and Sloane, N., (1983), The Theory of Error-Correcting Codes, North-Holland publishing company, p. 782.

[19] Massey, J. L., (1992), Linear codes with complementary duals, Discrete Math. 106/107, pp. 337-342.

[20] Massey, J. L., (1994), Reversible codes, Inf. Control, vol. 7, pp. 369-380.

[21] McEliece, R. J., (1978), A Public-Key Cryptosystem Based on Algebraic Coding Theory, 1978 DSN progress report, pp. 42-44, Jet Propulsion Labaratory, Pasadena, California.

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

[23] Misoczki, R., and Barreto, P., (2009), Compact mceliece keys from goppa codes, In Selected Areas in Cryptography, pp. 376-392, Springer.

[24] Ngo, X. T., Bhasin, S., Danger, J. L., Guilley, S. , Najm, S., (2015), Linear Complementary Dual Code Improvement to Strengthen Encoded Circuit Against Hardware Trojan Horses, In Proceedings of the 2015 IEEE International Symposium on Hardware Oriented Security and Trust (HOST), Washington, DC, USA, 5-7 May 2015.

[25] Niederreiter, H., (1986), Knapsack-type cryptosystems and algebraic coding theory, Prob. Control and Information Theory, vol. 15, no. 2, pp. 159-166.

[26] Rivest, R. L. , Shamir, A., Adleman, L., (1978), A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, https://doi.org/10.1145/359340.359342.

[27] Sendrier, N., (2004), Linear codes with complementary duals meet the Gilbert-Varshamov bound, Discrete Math., vol. 285, pp. 345-347.

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

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

[30] Wang, Y., (2016), Quantum Resistant Random Linear Code Based Public Key Encryption Scheme RLCE, 2016 IEEE International Symposium on Information Theory (ISIT), DOI:10.1109/ISIT.2016.7541753, Barcelona, Spain.

[31] Yang, X., Massey, J. L., (1994), The condition for a cyclic code to have a complementary duals meet the Gilbert-Varshamov bound, Discrete Math., vol. 126, pp. 391-393.