Int. J. Nonlinear Anal. Appl. 13 (2022) 1, 707-716
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.5559

A modification of the Cayley-Purser algorithm

Sameerah Faris Khlebus[a,*], Rajaa K. Hasoun[a], Bassam Talib Sabri[a]

[a]College of Business Administration of Informatics, University of Information Technology and Communication, Baghdad, Iraq

(Communicated by Madjid Eshaghi Gordji)

Abstract

Cayley- Purser Algorithm is a public key algorithm invited by Sarah Flannery in 1998. The algorithm of Cayley-Purser is much faster than some public key methods like RSA but the problem of it is that it can be easily broken especially if some of the private key information is known. The solution to this problem is to modify this algorithm to be more secure than before so that it gives its utilizers the confidence of using it in encrypting important and sensitive information. In this paper, a modification to this algorithm based on using general linear groups over Galois field $GF(p^n)$, which is represented by $GL_m(GF(p^n))$ where n and m are positive integers and p is prime, instead of $GL_2(Z_n)$ which is General linear set of inverted matrices 2×2 whose entries are integers modulo n. This $GL_m(GF(p^n))$ ensures that the secret key of this algorithm would be very hard to be obtained. Therefore, this new modification can make the Cayley-Purser Algorithm more immune to any future attacks.

Keywords: Cryptography, Cayley- Purser Algorithm, Galois field $GF(p^n)$, General Linear group over $GF(p^n)(GL_m(GF(p^n))$, Encryption, Decryption

1. Introduction

The fast growth of the internet technology the multimedia data such as text, images, audios and videos will be vulnerable to the coping and the modifying [2]. Numerous technological transformations in the communication system has been presented in last decade include each growing internet and explosive improvements ever rapidly increasing of data transmission [25, 29]. The security of data and information had considered a critical role when the information related to the e-commerce, the e-banking, or the e-payments, or other forms of important data mostly because it required the real data to establish get on illegally. Subsequently, the originality and the security of the data very

*Corresponding author
Email addresses: sameerah.alradhi@uoitc.edu.iq (Sameerah Faris Khlebus), dr.rajaa@uoitc.edu.iq (Rajaa K. Hasoun), Bassam.ali@uoitc.edu.iq (Bassam Talib Sabri)

Received: May 2021 *Accepted:* March 2021

important and critical criteria in the data communication services in modern years [6]. Cryptography techniques need some algorithms for encryption of data. A lot of these available encryption techniques are utilized for the text; few of these encryption methods are utilized in order to encrypt the multimedia data [30, 34]. Cryptography technique is utilized to encrypt the information [27].

The key difference between various forms of technology is key size and strength. For secret communications militaries and governments has been using encryption for a very long period. Nowadays many forms of civilian communications are also using encryption for data security. Conversion of normal text into cipher text is the basic purpose of encryption. Encryption can make sure that data not reaches the wrong person, isn't altered during transmission and can be utilized to ensure the sender identity [33].

Encryption can be defined as the process of changing a message (or plaintext) into an 'unintelligible' form and decryption is the reverse procedure [5]. The ciphertext is transmitted by way of the sender to the meant recipient (Bob) of the plaintext, across an insecure conversation channel (any third celebration can intercept facts that flows through any such channel). The algorithm which is utilized for performing the steps of encryption and the decryption steps is known as the cipher [11, 36]. The cryptosystem can mean any gadget that includes cryptology or simply the algorithms, at the side of units of feasible inputs to them, which are utilized to perform encryption and decryption of messages [3]. There are two kinds of cryptography methods which are [14, 19]:

A) The first kind of the cryptography methods is the secret(private) key encryption or the symmetric key encryption: In the encryption of the SKC, both sides (the sender and receiver) will identify the same secret key. This key will be utilized for the encryption and the decryption. The SKC found in two kinds which are: stream cipher, block cipher. Stream cipher is utilized in order to encode the message bits one by one. Another kind is the block cipher which works on a number of bits and then encrypts them as one unit. Data is encrypted / decrypted if the data shapes is in block. In the encryption of the block cipher, blocks will be produced from dividing the plain text which will be utilized in order to produce cipher text blocks stuffing the plain text into blocks. 64-bit blocks are commonly utilized [7, 10].

B) Public key encryption or asymmetric key encryption(or public key) is utilized in order to avoid the distribution of key problem. In PKC, there are two keys; private and public keys are utilized. For encryption, the public key is utilized, and for encryption that utilizes the private key [10, 8, 4]. Galois Field, which is named as Evariste Galois, also named as finite field, is utilized to refer to the field where many elements are finite.It is especially useful for computer data translation as it is represented in binary forms [4, 38]. This Galois Field (GF) is more utilized in the digital signal processing, the cryptography and the channel coding. There have been different works on planning cost effective encryption hardware utilized in battery-based applications. Most work emphasis on area reduction and propagation delay or critical path [14].That is, computer data consists of a group including two numbers which are 0 and 1, which are the components in a Galois field [31, 17]. In the Galois field the data will be represented as a vector in order to permitthe mathematical operations to effortless and efficiently deflate data [28].

The general linear group over Gailo field $GF(p^n)$: $GL_m(GF(p^n))$ is utilized in the generation of Cayley - Purser Algorithm [10]. The following gives a brief description of general linear group over Galois field $GF(p^n)$ and Cayley - Purser Algorithm [20]

Problem Statement and Preliminaries

The problem of the Cayler-Purser Algorithm is that it can be easily broken especially if some of the private key information known. Also there is little research that deals with studying it and working on modifying it to make it suitable for working in coding systems.

The proposed solution

The solution to this problem is modify this algorithm to be more secure than before so that it gives its utilizers the confidence of using it in encrypting important and sensitive information.

Results achieved

According to the achieved result of the proposed modification (By using Avalanche Effect as measure) and measuring the running time the algorithm be suitable to utilized in order to secure the data (different types text, audio, image, video) in many environments and applications.

2. The General Linear Group Over The Galois Field $GF(p^n), GL_m(GF(p^n))$

Definition 2.1. *Let F be the field. Then the general linear set GLm (F) is a set of inverted matrices $m \times m$ with inputs in F under the matrix multiplier, and if the positive integers are m> 1, then the GLm (F) group is not Abiliangroup [13, 22, 1].*

Definition 2.2. *A finite field (Galois field (GF)) which is named after the French mathematician Evariste Galois. It include a specified number of elements and is a group on which the multiplication, the addition, the subtraction and the division are determined and fulfill some main rules. Also, the Galois field's order is always a prime or a power of the prime.*

The following shows examples of Galois fields [13].

Example 2.3. *A prime field is of order p a Galois field denoted by $GF(p)$ for p is a prime number, and the prime field elements are represented as integers in the range 0,1,2, . . . , (p-1).*

Example 2.4. *The order p^n Finite fields are Galois fields which represented by $GF(p^n)$ for the positive integer n , and the $GF(p^n)$ possible elements may be appear as polynomials of degree strictly minimal than n with coefficients belong to $GF(p)$. Moreover, it is Very traditional to express the elements of the $GF(p^n)$ as binary numbers.That is,theGalois field components in which is utilized in order to represent the computer data include two numbers which are 0 and 1 [39, 18, 21].*

3. Finite Field Arithmetic

In this section, how the operations (addition, subtraction, multiplication, and multiplicative inverse) can be done over the polynomials of $GF(P^n)$ will be showed [13].

3.1. The Addition and the Subtraction

Suppose that $A(x)$ and $B(x)$ are elements in $GF(P^n)$ such that:

$$A(x) = a_{n-1}\ x^{n-1} + a_{n-2}\ x^{n-2} + \ldots + a_1\ x^1 + a_0 \quad \text{and}$$
$$A(x) = b_{n-1}\ x^{n-1} + b_{n-2}\ x^{n-2} + \ldots + b_1\ x^1 + b_0, \quad \text{then}$$
$$C(x) = A(x) + B(x) = \sum_{i=0}^{n-1} c_{\mathrm{i}}\ x^I$$

where the coefficient $c_{\mathrm{i}} = a_{\mathrm{i}} + b_{\mathrm{i}}$ (mod p).
Similarly, if $H(x) = A(x) - B(x)$, then $C_i = a_i - b_i \ \ (mod\ P)$. Note that, $C(x)$ and $H(x)$ are elements in $GF(P^n)$.

3.2. The multiplication and multiplicative Inverse

The multiplication and multiplicative inverse in the Galois Field claims more work. Assume that $A(x), B(x)$ and $K(x)$ are polynomials in $GF(P^n)$, so that $K(x)$ has a degree at least n and is an irreducible polynomial, which cannot be factored. The polynomial $K(x)$ must has degree at least n in order to make the output of the polynomials $A(x)$ and $B(x)$ does not override 11111111 = 255 as the output thatn has to be stored as a byte [13, 40]. Therefore, $T(x) = A(x) \star B(x)\ (modK(x))$ .But, the multiplicative inverse of a polynomial in $GF(P^n)$ is computed utilizing the Extended Euclidean Algorithm as the following:
The multiplicative inverse of $A(x)$ is given by $A^{-1}(x)$ such that $A(x) \star A^{-1}(x) = 1(modK(x))$.

Note that ,computing theoutput of two polynomials and the multiplicativeinverse of a polynomial in the $GF(P^n)$ claims both decreasethe coefficients modulo p and reducing polynomials modulo K(x). The polynomials can decreased with long division. The following example shows the addition, subtraction, multiplication, and multiplicative inverse of polynomials in $GF(P^n)$.

Example 3.1. *Suppose we work in $Gf(23)$ and take the irreducible polynomial coefficient $K(x) = x^3 + x + 1$. Note that, $Gf(2^3) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$, and let $A(x) = x^2 + x + 1$ and $B(x) = x^2 + 1$. Therefore, $A(x) + B(x) = x$, which is equivalent to $(010)_2$ in its binary form. And, $A(x) - B(x) = x$.*
On the other hand, $A(x) \star B(x) = (x^3 + x + 1) \star (x^2 + 1) = [x^4 + x^3 + x + 1](modx^3 + x + 1) = x^2 + x$. Also, by utilizing the extended Euclidean Algorithm, we can get $A^{-1}(x)$ such that $A(x) \star A^{-1}(x) = 1(modK(x))$, which is $A^{-1}(x) = x^2$.

4. Cayley-Purser Algorithm

The Cayley-Purser algorithm is a public-key cryptographic algorithm that was invented in 1998by Sarah Flannery. This algorithm is as secure as the RSA cryptosystem , but it utilizes only modular matrix multiplication instead of modular exponentiation. Also, it is proven that this algorithm is much faster than other asymmetric cryptosystem's algorithms for large. For instance, with 200 digits modulus, this algorithm is about twenty times faster than the algorithms of RSA cryptosystem [40].

Algorithm Setup [23]

The Cayley-Purser Algorithm's utilizers has to do the following:

- Select large prime numbers p and q such that they have the forms $p = 2r_1 + 1; q = 2r_2 + 1$ where r_1 and r_2 are prime numbers.

- Compute, $N = pq$.
- Select A and S which are elements in $GL_2(Z_N)$ so that $SA \neq SC$.
- Choose a positive integer a and calculate $R = S^a$.
- Compute B, such that $B = S^{-1}\ A^{-1}\ S$.
- Announce A, B, R, and N.
- Keep S secret, which is needed for the decryption procedure.

The Encryption Procedure [12]

The sender has to utilize the published receiver's parameters, which are A, B, R, and N. Then she has to do the following:

- Let m be a 2 x 2 matrix with entries in Z_N such that m is representing the plaintext.
- Choose a positive integer $s_1$randomly and compute W= R^{s_1}
- Calculate Q= W^{-1} A W.
- Calculate K= W^{-1} B W
- To encrypt m, calculate E= K m K
- Send the pair (E, Q) to the intended receiver.

The Decryption Procedure [Receiver] [12]

When the intended receiver gets the pair (E, Q), she utilizes her secret key S. Then she has to apply the following decryption algorithm:

- Calculate $L = S^{-1}Q\ S$.
- Calculate $m = LEL$.

The following shows a proof of the decryption procedure [12].
We have to show how the decryption algorithm $LEL = m$ satisfied, and that would be as follows,

$$
\begin{aligned}
&L.H.S \rightarrow LEL = (S^{-1}\ Q\ S)\ E\ (S^{-1}QS)\\
&= \Big(S^{-1}\ (\ W^{-1}\ A\ W)\ S\Big)\ E\Big(S^{-1}\ (W^{-1}\ A\ W)S\Big)\\
&= \Big(W^{-1}\ (\ S^{-1}\ A\ S)\ W\Big)\ E\Big(W^{-1}\ (S^{-1}\ A\ S)\ W\Big) \quad (since\ \ W = R^{s_1} = S^{as_1},\ \text{so } W \text{ commutes with } S)\\
&= \Big(W^{-1}(\ S^{-1}A^{-1}S)^{-1}\ W\Big)\ E\ \Big(W^{-1}(\ S^{-1}A^{-1}S)^{-1}\ W\Big)\\
&= \Big(W^{-1}B^{-1}\ W\Big)\ E\ \Big(W^{-1}B^{-1}\ W\Big) \quad [since\ B = S^{-1}\ A^{-1}\ \ S]\\
&= \Big(\ W^{-1}\ B\ \ W\Big)^{-1}E\Big(\ W^{-1}\ B\ \ W\Big)^{-1}\\
&= K^{-1}EK^{-1} \quad [since\ K = W^{-1}BW]\\
&= K^{-1}(KmK)K^{-1}\\
&= m
\end{aligned}
$$

The Security Of Cayley-Purser Algorithm [12, 9]

It is not easy to find the secret matrix , S. To find the secret matrix S, only A, B, R, and N are known, one might attempt to solve either of the following equations:

$$R = S^a \qquad \text{or} \qquad B = S^{-1}\ A^{-1}\ S$$

For the equation R= S^a **:** only the matrix R is known, and assume that someone knew a, solving this equation shall include the of extracting the a-th root of a matrix modulo the composite integer N=pq. It is proven that if a=2, then extracting the root square of a 2 x 2 matrix requires solving the ordinary quadratic congruence T= S^2 $(mod\ N)$ which is a known problem that equivalent to the factorization problem, factoring N[**15**].

For the equation B = $S^{-1}\ A^{-1}$ S : Only A, N, and B are known, therefore , A^{-1} can be computed easily with modulus N. The secret matrix S can be attacked by solving$S$ B = A^{-1} S. Also, the number of solutions to this equation has proven to be large as long as the group elements have a large arrangement, which can be guaranteed for each component. In other word, the number of possible solutions to this equation is given by the order of centralizer of A in $GL_2(Z_N)$, denoted by $C(A)$. With groups that have a very large order, it is ensured that the order of C(A) would be really large , which makes it computationally impossible to search for S [35].

5. The Proposed Modification of Cayley-Purser Algorithm

This modification focus on the utilization of the $GL_m(GF(p^n))$ in the Cayley-Purser Algorithm instead of $GL_2(Z_N)$, this modification is as the following:
The proposed modification of Cayley-Purser Algorithm's utilizers has to do the following

- Select a Galois field of order $p^n[GF(p^n)]$ where p is a very large prime number of the form $p = 2r_3 + 1$, where r_3 is the large prime number and n is the positive integer.
- Choose an irreducible polynomial , $K(x)$, which has a degree at least n.
- Select A and S which are elements in $GL_m(GF(p^n))$ so that $SA \neq SC$. Note that the entries in the matrices are polynomials or its equivalents in the binary form.
- Choose a positive integer a and calculate $R = S^a$.
- Compute B, such that $B = S^{-1}\ A^{-1}\ S$.
- Announce $A, B, R, K(x)$ and $GF(P^n)$.
- Keep S secret, which is needed for the decryption procedure.

The Encryption Procedure[Sender]:
The sender has to utilize the published receiver's parameters, which are A, B, R, K(x)and $GF(P^n)$. Then she has to do the following:

- Let Y be a m x m matrix with entries in $GF(P^n)$.such that Y is representing the plaintext.
- Choose a positive integer $s_1$randomly and compute W= R^{s_1}
- Calculate Q= W^{-1} A W.

- Calculate K= W^{-1} B W
- To encrypt Y, calculate E= K Y K
- Send the pair (E, Q) to the intended receiver.

The Decryption Procedure[Receiver]:
When the intended receiver gets the pair (E, Q), she utilizes her secret key S. Then she has to apply the following decryption algorithm:

- Calculate L= S^{-1} Q S .
- Calculate Y = L E L.

Note: In order to multiply matrices and find an inverse of a matrix , we need to computing the output of two polynomials and the multiplicative inverse of a polynomial in $GF(p^n)$. Thatclaim both decreasing the coefficients modulo p and decreasing the polynomials modulo K(x).

6. The Proposed CP Modification Avalanche Effect

Avalanche effect is substantial feature for the encryption algorithm. This feature can be seen when the alteration of one bit in plaintext produce the alteration in the outcome of at least half of the bits in the cipher text. The main aim of the avalanche effect is that by alteration only one bit there is large alteration then it is harder to perform an analysis of cipher text, when trying to come up with an attack [9]. Therefore, the avalanche effect can be defined as techniques for ensuring the level of security in any cryptographic method. The small alterations to the plain text or public key, should result in a major alteration in the cipher text [15]. The avalanche effect (AE) can be measured by dividing the number of switched bits by the number of total bits in the ciphertext [24, 32, 16].

$$\frac{\text{Number of Filpped bits in ciphertext}}{\text{Number of total bits in ciphertext}}$$

The original CP algorithm has a good avalanche effect (the AE of key and general AE) since changing in one bit of the keys (public and private) produce another key with high AE, therefore in this work the AE is very high since it is the sum of original CP and GF.

Table 1: Avalanche Effect Test

Plaintext	**Ciphertext**	**Avalanche Effect**
11111111111111111111111111111111	A1 10 83 41 23 24 00 D7 5B 2D E1 C2 F0 F7 AA E3	5978
11111111101111111111111111111111	11 34 14 72 43 51 A0 89 01 C2 D1 10 64 13 6B 0C	
11223366554455447788996644453612	59 80 98 76 76 C1 B5 65 23 44 66 10 85 76 1D 10	6017
22223366554455447788996644453612	76 A2 00 37 14 13 C1 70 22 0C 08 77 45 06 E7 F6	

7. CP Time Analysis

Time-Analysis of the CP algorithm with the RSA shows that the CP algorithm is much faster than the RSA algorithm. Table (1) shows the time analysis of the CP algorithm and RSA algorithm for message length is 1769 characters and Table(2) shows the time analysis of the CP algorithm and RSA algorithm for message length is 21228 characters.

Table 2.

Table 2: CP algorithm running time and RSA running algorithm

Running Time (Seconds) Message=1769 characters				
Trial No.	1	2	3	Average
RSA Encryption	41.94	42.1	41.78	41.94
RSA Decryption	40.99	41.009	41.019	41.009
CP Encryption	1.893	1.872	1.893	1.886
CP Decryption	1.502	1.492	1.492	1.4953

Table 3: CP algorithm running time and RSA running algorithm

Running Time (Seconds) Message=12*1769=21228 characters				
	RSA ENC	RSA DEC	CP ENC	CP DEC
Time Taken	378.078	371.254	17.435	14.371

According to the previous tables result which show the CP algorithm faster, this feature with the proposed modification (using general linear groups over Galois field GF(pn)which is represented by $GL_m(GF(p^n))$ where n and m are positive integers and p is prime, instead of $GL_2(Z_n)$) prove that the modified CP algorithm become suitable to secure the different types of data.

8. Conclusion

Mathematically, the CP algorithm is as safe as the RSA algorithm. The CP algorithm executes faster than the RSA algorithm, and the speed factor increases with the coefficient size.This modification is based on using general linear groups over Galois field $GF(p^n)$, which is represented by $GL_m(GF(p^n))$ where n and m are positive integers and p is prime, instead of $GL_2(Z_n)$ which is the general linear array of 2×2 inverted matrices whose entries are integers modulo n.

References

[1] A. Al Cheikha, *Matrix representation of groups in the finite fields GF(2n)*, Int. J. Soft Comput. Engin. 4 (2014).
[2] B. S. Ali, O.N. Ucan and O. Bayat, *A novel approach for ensuring location privacy using sentiment analysis and analysis for health-care and its effects on humans health*, J. Medical Imag. Health Inf. 10 (2020) 178–184.

[3] B.S. Ali and O.N. Ucan, *Lossy Hyperspectral Image Compression Based on Intraband Prediction and Inter-band Fractal*, 2018 Proc. Fourth Int. Conf. Engin. MIS, Turkey, Istanbul, 2018.
[4] A.M. Ali Argabi and Md. Imran Alam, *A new cryptographic algorithm AEDS (Advanced encryption and decryption standard) for data security*, Int. Adv. Res. J. Sci. Engin. Tech. 6 (2019).
[5] M. Agrawal and P. Mishra, *A Comparative Survey on Symmetric Key Encryption Techniques*, Int. J. Comput. Sci. Engin. 4 (2012).
[6] A. Al Farawn, H. D. Rjeib, N. Ali and B. Al-Sadawi, *Secured e-payment system based on automated authentication data and iterated salted hash algorithm*, TELKOMNIKA Telecommun. Comput. Elect. Cont. 18 (2020) 538–544.
[7] M.A. Al-Shabi, *A survey on symmetric and asymmetric cryptography algorithms in information security*, Int. J. Sci. Res. Pub. 9 (2019).
[8] S. Ahmad, K. Md. Rokibul Alam, H. Rahman and Sh. Tamura, *A Comparison between Symmetric and Asymmetric Key Encryption Algorithm based Decryption Mixnets*, IEEE, 2015.
[9] K. Amish and T. Namita, *Effective Implementation AndAvalanche Effect Of AES*, Int. J. Secur. Privacy Trust Manag. 1 (2012).
[10] A. Gupta, N. Kaur Walia and S. Guru, *Cryptography Algorithms: A Review*, IJEDR, 2 (2014).
[11] S. Bassam, N. Osman and S. Haitham, *New methods for analyzing Spatio-Temporal simulation results of Moran's index*, J. Computer Eng. Inf. Tech. 7 (2018) 9307.
[12] C. Bates, N. Meyer and T. Pulickal, *Cryptographic applications of nonabelian groups*, Math. Arizona, 2008.
[13] Ch. J. Benvenuto, *Galois Field in Cryptography*, 2012.
[14] A. Devi, A. Sharma and A. Rangra, *Performance analysis of Symmetric Key Algorithms: DES, AES*, Int. J. Engin. Comput. Sci. 4 (2015) 12646–12651.
[15] D. Ganga Raju and K. Kiran, *Analysis of Avalanche Effect in Asymmetric Cryptosystem Using NTRU & RSA*, IJDCST, @October Issue- V-1, I-6, SW-10.
[16] K.R. Hasoun, S.F. Khlebus and H.K. Tayyeh, *A new approach of classical hill cipher in public key cryptography*, Int. J. Nonlinear Anal. Appl. 12 (2021) 1071–1082.
[17] Y.Y. Hua, J.-M. Lin, C.W. Chiou, C.-Y. Lee and Y.H. Liu, *Low spacecomplexity digit-serial dual basis systolic multiplier over galois field GF(2m) using hankel matrix and karatsuba algorithm*, IET Inf. Secur. 7 (2013).
[18] J.-S. No, S.W. Golomb, G. Gong, H.-K. Lee and P. Gaal, *Binary pseudorandom sequences for period 2n-1 with ideal autocorrelation*, IEEE Trans. Inf. Theory 44 (1998) 814–817.
[19] M. Kaur, *Survey of various encryption techniques for audio data*, Int. Adv. Res. Comput. Sci. Software Engin. 4 (2014) 1314–1317.
[20] S.S. Kumar, T.J. Wollinger and C. Paar, *Optimum digit serial GF(2m) multipliers for curve-based cryptography*, IEEE Trans. Comput. 55 (2006) 1306–1311.
[21] J.S. Lee and L. E. Miller, *CDMA System Engineering Hand Book*, Artech House. Boston, London, 1998.
[22] C.-Y. Lee, J.-S. Horng, I.-C. Jou and E.-H. Lu, *Low-complexity bitparallel systolic montgomery multipliers for special classes of GF(2m)*, IEEE Trans. Comput. 54 (2005) 1061–1070.
[23] R. Lidl and G. Pilz, *Applied Abstract Algebra*, Springer- Verlage New York, 1984.
[24] A.K. Mandal and A. Tiwari, *Analysis of avalanche effect in plaintext of des usingbinary codes*, International Journal of Emerging Trends and Technology inComputer Science (IJETTCS), 1 (2012) 166–177.
[25] M.S. Naghmash, N.J. Alhyani and A.M. Kadhim, *Optimization of image compression and ciphering based on EZW techniques*, TELKOMNIKA Telecommun. Comput. Elect. Cont. 18 (2020) 511–518.
[26] B.R. Narain and Dr.T. Sasilatha, *Implementation of reconfigurable galois field multipliers over2m using primitive polynomials*, Int. J. Engin. Tech. 7 (2018) 386–389.
[27] S. Neelima and R. Brindha, *512 bit-SHA3 design approach and implementation on field programmable gate arrays*, Int. J. Reconfig. Embedded Syst. 8 (2019) 169–174.
[28] J.-S. Pan, C.-Y. Lee and Y. Li, *Subquadratic space complexity gaussian normal basis multipliers over GF(2m) based on dickson-karatsuba decomposition*, IET Circuits, Devices Syst. 9 (2015) 336–342.
[29] V. Passricha, A. Chopra and P. Sharma, *ShubhanshiSinghal, A secure deduplication scheme for encrypted data*, Int. J. Inf. Commun. Tech. 8 (2019) 77–86.
[30] A. Rabie, Kh. ElShafie, A. Hammuoda and M.Rohiem, *Data ecryption based on multi-order FrFT, and FPGA implementation of DES algorith*, Int. J. Reconfig. Embedded Syst. 9 (2020) 141– 152.
[31] M. Rahma, et al, *Devices for Multiplicative Inverse Calculation in the Binary Galois Fields*, The 9th IEEE International Conference on Dependable Systems, Services and Technologies, 2018, Kyiv, Ukraine, DESSERT, 2018.
[32] S. Ramanujam and M. Karuppiah, *Designing an algorithm with high avalancheeffect*, Int. J. Comput. Sci. Network Secur.11 (2011) 106–111.

[33] S. Ramesh, V. Thanikaiselvan, *A novel efficient multiple encryption algorithm for real time images*, Int. J. Elect. Comput. Engin. 10 (2020) 1327–1336.
[34] R. Suwandi, S. MichrandiNasution and F. Azmi, *Secure E-voting System by Utilizing HomomorphicProperties of the Encryption Algorithm*, TELKOMNIKA, 16 (2018) 862–867.
[35] H.E. Rose,*Elementary Group Properties*, In A Course on Finite Groups, Springer, London, 2009 .
[36] B.T. Sabri, N.A. Yaseen AL-Falahi and I.A. Salman, *Option for optimal extraction to indicate recognition of gestures using the self-improvement of the micro genetic algorithm*, J. Int. Nonlinear Anal. Appl. 12 (2021) 2295–2302.
[37] Sutherland and Scott, *Cayley-Purser Algorithm*, From MathWorld–A Wolfram Web Resource, created by Eric W. Weisstein.
[38] IEEE 1363-2000, *Standard Specifications for Public-Key Cryptography*, Copyright © 2000 IEEE. All rights reserved.
[39] K. Yang, Kg. Kim, *Quasi-orthogonal sequences for code-division multiple access systems*, IEEE Trans. Inf. Theory 46 (2000) 982–993.
[40] S.C. Yang, *CDMA RF System Engineering*, Artech House, Boston-London, 1998.