Sigma J Eng Nat Sci, Vol. 42, No. 2, pp. 529−533, April, 2024

Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2024.00041

Research Article

Secure encryption over the ring $F_2 + uF_2 + vF_2 + uvF_2$

Neriman ŞOLT[1], Selda ÇALKAVUR[2,*], Murat GÜZELTEPE[2]

[1]*Department of Mathematics, Sakarya University, Sakarya, 54050, Türkiye*
[2]*Department of Mathematics, Kocaeli University, Kocaeli, 41380, Türkiye*

ARTICLE INFO

Article history
Received: 01 June 2022
Revised: 13 August 2022
Accepted: 12 November 2022

Keywords:
One Time Pad Method; Cyclic Code; Ring

ABSTRACT

Cryptology is a part of mathematics as encryption and decryption. The purpose of encryption is to make information incomprehensible when it is in the hands of unauthorized people. The receiver can decrypt the message that encrypted by the sender with helping of the key. The important point is that the key cannot be decrypted by other people. One Time Pad method solves this problem. The key is used only once each encryption in this method. So, the key becomes harder to guess. If the key is solved by unauthorized people, the message cannot be solved. Because of with each decryption, many meaningful messages are obtained. Every cyclic shift in a cyclic code constructs a new key and in each encryption is used the new key. Many keys are generated thanks to cyclic codes. In this paper, we improve the new encryption scheme by using the cyclic codes with One Time Pad method.

Cite this article as: Şolt N, Çalkavur S, Güzeltepe M. Secure encryption over the ring $F_2 + uF_2 + vF_2 + uvF_2$. Sigma J Eng Nat Sci 2024;42(2):529−533.

INTRODUCTION

Cryptology has been the field of study of scientists for centuries. Especially, it has been frequently used in the military field where information security and privacy are important. Gilbert Vernam developed an encryption method that could not be deciphered [1]. This system is referred to the Vernam password or One Time Pad (OTP) method. In 1940, the security of the OTP method was proved by Shannon [16]. Shannon showed that using one time keys makes the Vernam system unbreakable. The security of the system is ensured with random disposables keys. The key must be unbreakable so that the ciphertext cannot be decrypted by anyone other than the receiver. When someone wants to decode the message, he/she tries all possible keys and always gets meaningful messages. It is difficult to guess which one is the message to be forwarded. One time pad is a cryptosystem for encoding binary data using a binary key of the same length as the data. If w is a binary plaintext, k is a binary key and c is a binary cryptotext, then the encryption algorithm is $c = w + k$ and the decryption algorithm is $w = c + k$ [2]. Many authors have used the OTP method in their papers [12-14]. Their papers include a new key generation technique. Çalkavur and Güzeltepe [3] applied this encryption scheme based on cyclic codes over the ring $F_2 + vF_2$ and they developed secure encryption method.

The minimum distance of a code is related to the error correcting capacity of the code. The more minimum

***Corresponding author.**
*E-mail address: selda.calkavur@kocaeli.edu.tr

This paper was recommended for publication in revised form by Editor in Chief Ahmet Selim Dalkilic

Published by Yıldız Technical University Press, İstanbul, Turkey

distance, the code can be corrected the more errors. Cyclic, negacyclic, constacyclic, quasi-cyclic codes and their skew codes are used to obtain a large minimum distance code. By using these codes, the existence of codes on the rings is detected and codes with high minimum distance can be obtained. Cyclic codes have been the focus of studies for hundreds of years since they are an important class of linear codes. In 1957, Prange introduced binary cyclic codes [10]. Abualrup et al. studied skew cyclic codes over ring in [11]. Yildiz and Karadeniz [4] studied the codes over the ring $F_2 + uF_2 + vF_2 + uvF_2$, where $u^2 = v^2 = 0$, $uv = vu$, and Dertli [5] studied codes over the ring $F_2 + uF_2 + vF_2 + uvF_2$ where $u^2 = u$, $v^2 = v, uv = vu$. In [15], given some upper bounds on repetition codes studied over the ring $F_2 + uF_2 + vF_2 + uvF_2$ where $u^2 = u$, $v^2 = v, uv = vu$.

In this study, we propose the secure encryption scheme by cyclic codes over the ring $F_2 + uF_2 + vF_2 + uvF_2$ where $u^2 = u$, $v^2 = v, uv = vu$. This scheme is based on One Time Pad method. We analyze the security of the new system and consider the possible attacks.

The paper is organized as follows. Basics definitions and theorems that we need in the sequel are given in Section 2. In Section 3, presents a new encryption system. In Section 4, analyzes security of system and explains the possible attacks.

Our Contributions

We present a new encryption scheme by cyclic codes based on One Time Pad method. Any cyclic shift of a codeword consists of the key. This key has been used only once each encryption. At the end of each encryption, we obtain many meaningful messages from different keys. We use the ring $F_2 + uF_2 + vF_2 + uvF_2$, where $u^2 = u$, $v^2 = v, uv = vu$. The encryption scheme is more complex structure due to the structure of this ring. Keys that are more difficult to crack can be produced on this ring. So, it is difficult to guess the key.

PRELIMINARIES

The definitions and theorems given in this section are preliminary for a better understanding of the subject. From now on, R is defined the ring $F_2 + uF_2 + vF_2 + uvF_2$, where $u^2 = u$, $v^2 = v, uv = vu$.

Basic Definitions and Theorems

Definition 1 [6] Let F_q is a finite field of order q. A linear code C of length n over F_q is a subspace of F_q^n.

Definition 2 [7] A code C is *cyclic* if C is a linear code and any cyclic shift of a codeword is also a codeword, whenever $(a_0, a_1, \ldots, a_{n-1})$ is in C, then so is $(a_{n-1}, a_0, a_1, \ldots, a_{n-2})$.

[3] Let F_q be the set of polynomials in x whose coefficients are from the field F_q. It is convenient to think of cyclic codes as consisting of polynomials as well as codewords. With every word $a = a_0, a_1, \ldots, a_i, \ldots, a_{n-2}, a_{n-1}) \in F_q^n$ we can write the polynomial of degree less than n, $a(x) = a_0 + a_1x + \ldots + a_i x_i + \ldots + a_{n-1}x^{n-1} \in F_q[x]$.

We know that every codeword can be written as a polynomial. Thus, each cyclic shift of a codeword is also expressed as a polynomial. Let $c(x)$ is a code polynomial and c' is the shifted codeword $c'(x) = c_{n-1} + c_0 x + c_1x^2 + \ldots + c_i x^{i+1} + \ldots + c_{n-2}x^{n-1}$. Thus $c'(x)$ is equal to the product polynomial $xc(x)$. More precisely, $c'(x) = xc(x) - c_{n-1}(x^n - 1)$. This means $c'(x)$ and $xc(x)$ are equal to polynomials in the ring $F[x](\text{mod } x^n - 1)$. If $f(x)$ is any polynomial of $F[x]$ whose remainder upon division by $x^n - 1$, belongs to C, then we may write $f(x) \in C$ (mod $x^n - 1$). Since each cyclic shift belongs to the cyclic code C, we can write $x^i c(x) \in C$ (mod $x^n - 1$) and indeed $\sum_{i=0}^{d} a_i x^i c(x) \in C \left(\text{mod}\, x^n - 1\right)$.

The below statement is used to convert the structure of cyclic code into an algebraic one.

$$\theta : F_q^n \to F_q[x]/(x^n - 1)$$
$$(a_0 a_1 \ldots a_{n-1}) \to a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$$

where the set of polynomials in x with coefficient in F_q is denoted by $F_q[x]$.

Theorem 1 [3,6] Let θ be the linear map defined as above. Then any nonempty subset C of F_q^n is a *cyclic code* if and only if $\theta(C)$ is an ideal of $F_q[x]/(x^n - 1)$.

There is a relationship between the cyclic codes in F_q^n and ideals of the ring $F_q[x]/(x^n - 1)$. Let $C = \langle g(x) \rangle$ be a cyclic code of length n, where $g(x) = g_0 + g_1x + \ldots + g_r x^r$ and $x^n - 1$ is divisible by $g(x)$. The code C can be expressed as follows:

$C = \{a_i(x) g(x) : a_i \in F_q[x]/(x^n - 1), \deg(a_i(x)) < n - r\}$, where $i = p^{n-r}$.

Definition 3 [6] Let u be a word in F_q^n as $u = (u_1, u_2, \ldots, u_n)$. The number of nonzero coordinates of u is called the *Hamming weight* of u and is defined as follows:

$$w_H(u) = \begin{cases} 1 & \text{if } u \neq 0 \\ 0 & \text{if } u = 0. \end{cases}$$

Codes over the ring $F_2 + uF_2 + vF_2 + uvF_2$

The ring R is defined as a characteristic 2 ring with 16 elements, where $u^2 = u$, $v^2 = v$ and $uv = vu$. There exists an isomorphism,

$$F_2 + uF_2 + vF_2 + uvF_2 \cong F_2[u,v]/\langle u^2 - u, v^2 - v, uv - vu\rangle$$
$$= \{a + ub + vc + uvd \mid a,b,c,d \in F_2\}$$
$$= \begin{Bmatrix} 0,1,u,v,u+v,u+v+uv,1+u+v,1+u+v+uv, \\ 1+u,1+v,v+uv,uv,1+uv,u+uv,1+u+uv,1+v+uv \end{Bmatrix}.$$

R has four maximal ideals such that

$$I_{1+uv} = \{0, 1+uv, u+uv, v+uv, 1+u, 1+v, u+v, 1+u+v+uv\}$$
$$I_{1+u+uv} = \{0, v, 1+u, v+uv, uv, 1+u+v, 1+u+uv, 1+u+v+uv\}$$
$$I_{1+v+uv} = \{0, u, 1+v, u+uv, uv, 1+u+v, 1+v+uv, 1+u+v+uv\}$$
$$I_{u+v+uv} = \{0, u, v, uv, u+v+uv, v+uv, u+uv, u+v\}.$$

For information about the ring see [5].

Definition 4 [5] A linear code C of length n over the ring R is an R −*submodule* of R^n

Definition 5 [5] For $a + ub + vc + uvd \in R$

$$\phi : R \to F_2^4$$
$$\phi(a+ub+vc+uvd) = (a, a+b, a+c, a+b+c+d)$$

is defined a *Gray map*. The Gray map of the elements is defined as,

$$\begin{array}{llll} \phi(0)=(0000) & \phi(uv)=(0001) & \phi(u+v)=(0110) & \phi(u+v+uv)=(0111) \\ \phi(1)=(1111) & \phi(1+u)=(1010) & \phi(1+uv)=(1110) & \phi(1+v+uv)=(1101) \\ \phi(u)=(0101) & \phi(1+v)=(1100) & \phi(u+uv)=(0100) & \phi(1+u+v)=(1001) \\ \phi(v)=(0011) & \phi(v+uv)=(0010) & \phi(1+u+uv)=(1011) & \phi(1+u+v+uv)=(1000). \end{array}$$

The *projection map* ψ is defined as follows

$$\psi : R \to F_2$$
$$\psi(a+ub+vc+uvd) = a.$$

In Definition 3, the Hamming weight is defined. In the next definition, Lee weights will be constructed using the Gray map.

Definition 6 [5] Let

$$\phi : R^n \to F_2^{4n}$$
$$\phi(a+ub+vc+uvd) = (a, a+b, a+c, a+b+c+d)$$

By using this map, we can define the *Lee weight*. For any element $a + ub + vc + uvd \in R$, we define w_L $(a + ub + vc + uvd) = w_H$ $(a, a + b, a + c, a + b + c + d)$, where w_H denotes the ordinary Hamming weight for binary codes. Lee weights are as follows.

$$w_L(0)=0,\ w_L(1)=4,$$
$$w_L(uv)=w_L(u+uv)=w_L(v+uv)=w_L(1+u+v+uv)=1,$$
$$w_L(u)=w_L(v)=w_L(1+u)=w_L(1+v)=w_L(v+u)=w_L(1+u+v)=2,$$
$$w_L(1+uv)=w_L(1+u+uv)=w_L(1+v+uv)=w_L(u+v+uv)=3.$$

Definition 7 [5] The *cartesian product* of vectors $v=(v_1,v_2,...,v_n)\in F_2^n, s=(s_1,s_2,...,s_n)\in F_2^n, w=(w_1,w_2,...,w_n)\in F_2^n$ and $t=(t_1,t_2,...,t_n)\in F_2^n$ is

$$v\otimes s\otimes w\otimes t=(v_1,v_2,...,v_n)\otimes(s_1,s_2,...,s_n)\otimes(w_1,w_2,...,w_n)\otimes(t_1,t_2,...,t_n)$$
$$=(v_1,v_2,...,v_n,s_1,s_2,...,s_n,w_1,w_2,...,w_n,t_1,t_2,...,t_n)\in F_2^{2n}.$$

Definition 8 [5] Let $A1$, $A2$, $A3$ and $A4$ be any four codes. Then,

$$A_1\oplus A_2\oplus A_3\oplus A_4=\{a_1+a_2+a_3+a_4 : a_1\in A_1, a_2\in A_2, a_3\in A_3, a_4\in A_4\}$$
$$A_1\otimes A_2\otimes A_3\otimes A_4=\{(a_1,a_2,a_3,a_4) : a_1\in A_1, a_2\in A_2, a_3\in A_3, a_4\in A_4\}$$

Let C be a linear code of length n over R. We can define the binary linear codes $C1$, $C2$, $C3$ and $C4$ as follows.

$$C_1=\{a\in F_2^n : \exists a,b,c\in {F_2}^n, a+ub+vc+uvd\in C\}$$
$$C_2=\{a+b\in F_2^n : \exists a,b\in {F_2}^n, a+ub+vc+uvd\in C\}$$
$$C_3=\{a+c\in F_2^n : \exists a,c\in {F_2}^n, a+ub+vc+uvd\in C\}$$
$$C_4=\{a+b+c+d\in F_2^n : a+ub+vc+uvd\in C\}.$$

Then ϕ (C) = $C1 \otimes C2 \otimes C3 \otimes C4$ and $|C| = |C1||C2||C3||C4|$.

Theorem 2 [5] Let C be a cyclic code over R of length n. Then C is an ideal in R that is generated by $\langle (1+u+v+uv)C_1\oplus(u+uv)C_2\oplus(v+uv)C_3\oplus(uv)C_4\rangle$ where $C_1=\langle f_1(x)\rangle$, $C_2=\langle f_2(x)\rangle$, $C_3=\langle f_3(x)\rangle$, $C_4=\langle f_4(x)\rangle$ and $f_1(x)\,|\,x^n-1$, $f_2(x)\,|\,x^n-1$, $f_3(x)\,|\,x^n-1$, $f_4(x)\,|\,x^n-1$.

The New Encryption Scheme

In this section, we apply to R, where $u^2 = u$, $v^2 = v$, $uv = vu$ the encryption scheme which introduced in the previous section. The purpose of this section is to show that the one time pad method works perfectly over the ring R.

Key Generation Procedure:

The linear code is $C=(1+u+v+uv)C_1\oplus(u+uv)C_2\oplus(v+uv)C_3\oplus(uv)C_4$, where $C_1=\langle f_1(x)\rangle$, $C_2=\langle f_2(x)\rangle$, $C_3=\langle f_3(x)\rangle$, $C_4=\langle f_4(x)\rangle$ and $f_1(x)\,|\,x^n-1$, $f_2(x)\,|\,x^n-1$, $f_3(x)\,|\,x^n-1$, $f_4(x)\,|\,x^n-1$. We choose the codewords such that $u_i\in C_1$, $s_j\in C_2$, $m_k\in C_3$, $n_l\in C_4$, while $0 \le k < C3$, $0 \le l < C4$.

Encryption:

Plaintext: $p_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l}=u_i\times s_j\times m_k\times n_l\in\phi(C)$, $0\le i<|C_1|, 0\le j<|C_2|, 0\le k<|C_3|, 0\le l<|C_4|$.

Key: $nl \in C_4$, $0 \le l < |C_4|$.

Ciphertext: $C_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l}=$
$\phi((1+u+v+uv)u_i+(u+uv)s_j+(v+uv)m_k+(uv)n_l)$.

Decryption:

Ciphertext: $C_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l}=$
$\phi((1+u+v+uv)u_i+(u+uv)s_j+(v+uv)m_k+(uv)n_l)$.

Plaintext: $p_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l}=$
$\psi\left[\phi^{-1}\left(C_{i+|C_1|j+|C_1||C_2|k+|C_1||C_2||C_3|l}\right)+(uv)n_l\right]\times s_j\times m_k\times n_l$.

Example 1 Let us take the length of 3 binary cyclic codes. We have the factorization into irreducible polynomials $x^3 - 1 = (x+1)(x^2+x+1)$.

Let us take as the generator polynomials $f_1(x) = x+1$, $f_2(x) = x^2+x+1$. These generator polynomials generate the binary cyclic codes are, respectively, $C_1 = C_2 = \{000,110,011,101\}$, $C_3 = C_4 = \{000,111\}$. We choose $u_0 = s_0 = 000$, $u_1 = s_1 = 110$, $u_2 = s_2 = 011$, $u_3 = s_3 = 101$ and $m_0 = n_0 = 000$, $m_1 = n_1 = 111$ for $i = 0,1,2,3$ and $j = 0,1$.

Encryption:

Let $i=0, j=0, k=0, l=0$. Then $u_0 = 000$, $s_0 = 000$, $m_0 = 000$, $n_0 = 000$. We get

$p_0 = u_0 \times s_0 \times m_0 \times n_0 = 000 \times 000 \times 000 \times 000 = 000000000000$

$c_0 = \phi((1+u+v+uv)u_0 + (u+uv)s_0 + (v+uv)m_0 + (uv)n_0) = \phi(000) = 000000000000$

Let $i=0, j=0, k=0, l=1$. Then $u_0 = 000$, $s_0 = 000$, $m_0 = 000$, $n_1 = 111$. We get

$p_{32} = u_0 \times s_0 \times m_0 \times n_1 = 000 \times 000 \times 000 \times 111 = 000000000111$

$c_{32} = \phi((1+u+v+uv)u_0 + (u+uv)s_0 + (v+uv)m_0 + (uv)n_1) = \phi(uv) = 000100010001$

Let $i=0, j=0, k=1, l=0$. Then $u_0 = 000$, $s_0 = 000$, $m_1 = 111$, $n_0 = 000$. We get

$p_{16} = u_0 \times s_0 \times m_1 \times n_0 = 000 \times 000 \times 111 \times 000 = 000000111000$

$c_{16} = \phi((1+u+v+uv)u_0 + (u+uv)s_0 + (v+uv)m_1 + (uv)n_0) = \phi(v+uv) = 001000100010$

Let $i=0, j=1, k=0, l=0$. Then $u_0 = 000$, $s_1 = 110$, $m_0 = 000$, $n_0 = 000$. We get

$p_4 = u_0 \times s_1 \times m_0 \times n_0 = 000 \times 110 \times 000 \times 000 = 000110000000$

$c_4 = \phi((1+u+v+uv)u_0 + (u+uv)s_1 + (v+uv)m_0 + (uv)n_0) = \phi(u+uv) = 010001000100$

Let $i=1, j=0, k=0, l=0$. Then $u_1 = 110$, $s_0 = 000$, $m_0 = 000$, $n_0 = 000$. We get

$p_1 = u_1 \times s_0 \times m_0 \times n_0 = 110 \times 000 \times 000 \times 000 = 110000000000$

$c_1 = \phi((1+u+v+uv)u_1 + (u+uv)s_0 + (v+uv)m_0 + (uv)n_0) = \phi(1+u+v+uv+0) = 100010000000$

Decryption:

$c_0 = 000000000000$, $n_0 = 000$. So, $i=j=k=l=0$,

$p_0 = \psi[\phi^{-1}(000000000000) + (uv)n_0] \times s_0 \times m_0 \times n_0$
$= \psi[(000)+(000)] \times (000) \times (000) \times (000) = 000000000000$

$c_1 = 100010000000$, $n_0 = 000$. So, $i=1, j=k=l=0$,

$p_1 = \psi[\phi^{-1}(100010000000) + (uv)n_0] \times s_0 \times m_0 \times n_0$
$= \psi[(1+u+v+uv+0) + (000)] \times (000) \times (000) \times (000)$
$= 110000000000$

$c_4 = 010001000100$, $n_0 = 000$. So, $j=1, i=k=l=0$,

$p_4 = \psi[\phi^{-1}(010001000100) + (uv)n_0] \times s_1 \times m_0 \times n_0$
$= (000) \times (110) \times (000) \times (000) = 000110000000$

$c_{16} = 001000100010$, $n_0 = 000$. So, $k=1, j=i=l=0$,

$p_{16} = \psi[\phi^{-1}(001000100010) + (uv)n_0] \times s_0 \times m_1 \times n_0$
$= (000) \times (000) \times (111) \times (000) = 000000111000$

$c_{32} = 000100010001$, $n_1 = 111$. So, $i=j=k=0, l=1$,

$p_{32} = \psi[\phi^{-1}(000100010001) + (uv)n_1] \times s_0 \times m_0 \times n_1$
$= (000) \times (000) \times (000) \times (111) = 000000000111$

In this scheme, we use a key of the same length with the data. Even if message is found by somebody, the message is unpredictable. When someone wants to solve the message, he/she finds all n-bit words. He/she cannot guess which one is the plaintext.

In this example we give some of the ciphertexts. The other ciphertexts can be encrypted by the same way.

Security of Scheme

The security of our scheme depends on the length of the codewords. The sender uses a key equal in length to the plaintext. Plaintext is encrypted with the key. The key is used by mixing (XOR) bit by bit. This means that a bit of the key is combined with a bit of the plaintext to build a bit of ciphertext. The message is received by the recipient. The recipient solves the message with the One Time Ped and restores the plaintext. After the sender and recipient have used the keys, the keys automatically destroyed. As a result, it is impossible to re-use the same key.

Comparison with the Other Cryptosystems

Petrenko et al. [8] developed the software encryption module with a cyclic BCH code. They used the RSA algorithm as well as error correcting code. Their module not only encrypts a message but also protects it from damage while sending a message.

Aguilar et al. [9] have proposed a general approach for building code-based cryptosystem that is both effective and efficient. They introduced two new cryptosystems, the Hamming Quasi-Cyclic cryptosystem based on the Hamming metric, and the Rank Quasi-Cyclic cryptosystem based on the rank metric. They analyzed the error term yielding an easy-to-verify decryption for the Hamming metric.

In our system, a cyclic code is used with the OTP method. In this method, the security of the system is ensured with random disposables keys. The key length must be equal to the length of the message to be encrypted. This is provided by our system. So, if the key length is large enough, then the key cannot be decrypted by anyone other than the receiver. At the end of each encryption, we obtain many meaningful messages from different keys. When an unauthorized person tries all the possible keys, he finds all the n-bit words and all the words are also codewords. Our system is very safe for the brute force attacks. Because brute force attacks use exhaustive trial and error methods in order to find the key that is used for encrypting the plaintext. As a result, guessing the plaintext is impossible.

CONCLUSION

In this article, we presented a new encryption scheme over the ring R. This scheme is based on the one time pad cryptosystem. In this method, it is used random key that the same length with data. The key is used only once every scheme providing an unbreakable password. At the end of each encryption, we obtain many meaningful messages from different keys. If someone tries all the possible keys, he finds all the codewords. This means, he gets all meaningful messages every time. It is very hard to predict which message is key. So, it is difficult to find the key. We analyzed its security. Thus, our schemes are very reliable by means of security. This article shows that the system can be used in areas where security is important.

AUTHORSHIP CONTRIBUTIONS

Authors equally contributed to this work.

DATA AVAILABILITY STATEMENT

The authors confirm that the data that supports the findings of this study are available within the article. Raw data that support the finding of this study are available from the corresponding author, upon reasonable request.

CONFLICT OF INTEREST

The author declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

ETHICS

There are no ethical issues with the publication of this manuscript.

REFERENCES

[1] Vernam G. S. Cipher printing telegraph systems for secret wire and radio telegraphic communications. Trans J Am Inst Electr Eng 1926;45:295–301. [CrossRef]

[2] Kuklová Z. Coding theory, cryptography and cryptographic protocols-exercises with solutions. Bachelor Thesis, Masaryk University, Brno, Faculty of Informatics; 2007.

[3] Çalkavur S. Güzeltepe M. Secure encryption from cyclic codes. Sigma J Eng Nat Sci 2022;40:380–389. [CrossRef]

[4] Yildiz B. Karadeniz S. Cyclic codes over $F_2 + uF_2 + vF_2 + uvF_2$. Des Codes Cryptogr 2011;58:221–234. [CrossRef]

[5] Dertli A. Halkalar Üzerinde Tanımlı Kodlar Hakkında Bazı Araştırmalar [master thesis]. Samsun: Ondokuz Mayıs University; 2016.

[6] Ling S. Xing C. Coding Theory: A First Course. Cambridge University Press. 2004. [CrossRef]

[7] Hill R. A First Course in Coding Theory. Oxford: Oxford University; 1990.

[8] Petrenko V. Ryabtsev S. Pavlov A. Apurin A. Development of an Encryption Method Based on Cyclic Codes, 21st International Workshop on Computer Science and Information Technologies. pp.196-201, Atlantis Press. 2019. [CrossRef]

[9] Aguilar-Melchor C. Blazy O. Deneuville J. C. Gaborit P. Zémor G. Efficient encryption from random quasi-cyclic codes. IEEE Trans Inform Theor 2018;64:3927–3943. [CrossRef]

[10] Prange E. The use of information sets in decoding cyclic codes. IRE Trans Inform Theor 1962;8:5–9. [CrossRef]

[11] Abualrub T. Seneviratne P. Skew codes over ring. Proceedings of the International MultiConference of Engineers and Computers Sciences 2010 Vol. II, IMECS, , Hong Kong, March 17-19, 2010

[12] Srikantaswamy SG, Phaneendra HD. Enhanced onetime pad cipher with morearithmetic and logical operations with flexible key generation algorithm. Int J Netw Secur Appl 2011;6:3. [CrossRef]

[13] Hussein MN, Megahed MH, Abdel Azeem MH. Design and simulation of authenticated encryption AENOTP stream cipher algorithm, 13th International Computer Engineering Conference. 2017. p. 393–398. [CrossRef]

[14] Patil S. Devare M. Kumar A. Modified one time pad data security scheme :Random key generation approach. Int J Comput Sci Secur 2014;3:139–145.

[15] Ma F. Gao J. Bounds on Covering Radius of Some Codes Over $F_2 + uF_2 + vF_2 + uvF_2$. IEEE 2021;9:47668–47676, 2021. [CrossRef]

[16] Shannon C. Communication theory of secrecy systems. Bell Syst Tech J 1949;28:656–715. [CrossRef]