Sigma Journal of Engineering and Natural Sciences
Web page info: https://sigma.yildiz.edu.tr
DOI: 10.14744/sigma.2022.00040

Research Article

Secure encryption from cyclic codes

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

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

ARTICLE INFO

Article history
Received: 12 December 2020
Accepted: 27 April 2021

Key words:
Encryption; One Time Pad System; Cyclic Code; Skew Cyclic Code

ABSTRACT

Encryption is the process of scrambling a message and can provide a means of securing information. Information security is becoming more important in data storage and transmission. It is known that most encryption method in the literature. In this paper we propose two new encryption schemes by using cyclic codes. Our method is based on the One Time Pad system. We use the properties of cyclic codes to provide its security.

Cite this article as: Selda Ç, Murat G. Secure encryption from cyclic codes. Sigma J Eng Nat Sci 2022;40(2):380–389.

INTRODUCTION

A cryptosystem is an implementation of cyrptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a cipher system. The various components of a basic cryptosystem are as follows.

Plaintext: It is the data to be protected during transmission.

Encryption Algorithm: It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.

Ciphertext: It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who access to the communication channel.

Decryption Algorithm: It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input and outputs a plaintext. The decrypiton algorithm essentially reverses the encrption algortihm and is thus closely related to it.

Encryption Key: It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.

Decryption Key: It is a value that is known to the receiver. The decryption key is related to the encryption key but it is not always identical to it. The receiver inputs the

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

This paper was recommended for publication in revised form by Regional Editor Vildan Çetkin

decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a key space. An attacker is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. However, he must never know the decryption key.

In 1978, McEliece [21] proposed the first code-based cryptosystem. This system is a general encryption setting for coding theory. McEliece cryptosystem is based on family of Goppa codes (Reed-Solomon codes, Reed-Muller codes) [19, 5]. MDPC cryptosystem [17] of the NTRU cryptosystem [12] was proposed recently. This system is interested the problem by using a hidden code structure which is significantly weaker than that of previously used algebraic codes like Goppa codes. Then a new cryptosystem [9] was proposed.

Alekhnovich introduced an efficient approach based on the random codes [3]. In this system the secret key is a random error vector.

Ajtai-Dwork cryptosystem [2] is based on solving hard lattice problems. This system is also inspired by Regev [24].

The systems based on the Learning Parity with Noise (LPN) has been proposed by exploiting the analogy with LWE [8, 15]. The LPN problem is the problem of decoding random linear codes of fixed dimension and unspecified length over a binary symmetric channel.

Cyclic codes form an important class of linear codes by means of error correcting. They have a very interesting algebraic structure. Furthermore, many important codes, such as binary Hamming codes, Golay codes and BCH codes are equivalent to cyclic codes. Binary cyclic codes were first introduced by Prange [22] in 1957, and have been the topic of hundreds of papers since. However, constacyclic code plays an important role in the error-correcting codes. Boucher et al. [11] explained the cyclic code over a noncommutative ring is called the skew polynomial ring $\mathbb{F}[x;\theta]$, where $\mathbb{F}$ is a finite field and θ is an automorphism over $\mathbb{F}$. Skew cyclic codes were studied by Boucher et al. [11] and Boucher-Ulmer [6]. Abualrub et al. [1] also studied skew cyclic codes over ring also studied skew cyclic codes over ring $\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$. Skew cyclic codes over $\mathbb{F}_p + v\mathbb{F}_p$ were introduced by Gao [10]. Yao et al. [25] presented skew cyclic codes over ring $R = \mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q$, where $u^2 = u$, $v^2 = v$, $uv = vu$, and $q = p^m$. Islam et al. [14] examined skew constacyclic codes over finite non-chain ring $R = \mathbb{F}_p^m + u\mathbb{F}_p^m + v\mathbb{F}_p^m$, where p is an odd prime and $u^2 = u$, $v^2 = v$, $uv = vu = 0$. Dertli et al. [7] studied codes over the ring $R = \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2, u^2 = 0, v^2 = v, uv = vu = 0$.

In [4], it is presented a new efficient encryption from random Quasi-cyclic codes.

In this paper, we propose a secure cryptosystem based on the cyclic codes. It is inspired by the One Time Pad cryptosystem. We examine the security of new system, consider the possible attacks.

The rest of the paper is organized as follows. Section II gives necessary background on coding theory and cryptography. Section III describes the cryptosystem, compares to the other systems. Section IV analyzes its security and explains the possible attacks. Section V collects concluding remarks.

Our Contributions

We propose two new encryption schemes by using cyclic codes. We are inspired by the One Time Pad cryptosystem. The One Time Pad is an encryption technique that cannot be cracked. So we provide an efficient approach for the cryptosystems. Our analysis allows us to work on cyclic codes. Any cyclic shift of a codeword consists of the key and this key has been used only once. However, the ciphertext can be obtained several times. This is an advantage for a cryptosystem. Because it is got many meaningful message and obtained them by different keys. This means it is very difficult to guess the key. Thus, when compared to the other cryptosystem [4, 21], our technique ensures the higher security.

PRELIMINARIES

Cyclic Codes

Among the first codes used practically were the cyclic codes which were generated using shift registers. It was noticed by Prange that the class of cyclic codes has a rich algebraic structure, the first indication that algebra would be a valuable tool in the code design. Moreover, many important codes, such as binary Hamming codes, Golay codes and BCH codes are equivalent to cyclic codes.

Definition 1 [13] Denote a prime number by p, a finite field by $\mathbb{F}_p$. A linear code C of length n over $\mathbb{F}_p$ is a subspace of $\mathbb{F}_p^n$.

Definition 2 [13] A code C is cyclic if

i. C is a linear code and
ii. any cyclic shift of a codeword is also a codeword, whenever $(a_0a_1\ldots a_{n-1})$ is in C, then so is $(a_{n-1}a_0a_1\ldots a_{n-2})$.

Example

i) The binary code {000,101,011,110} is cyclic.
ii) The binary linear code {0000,1001,0110,1111} is not cyclic but it is equivalent to a cyclic code; interchanging the third and fourth coordinates gives the cyclic code {0000, 1001, 0110, 1111}.

Basics It is convenient to think of cyclic codes as consisting of polynomials as well as codewords. With every word $a = (a_0, a_1, \ldots, a_i, \ldots, a_{n-2}, a_{n-1}) \in \mathbb{F}_q^n$ we associate the polynomial of degree less than n $a(x) = a_0 + a_1x + \ldots + a_ix^i + \ldots + a_{n-1}x^{n-1} \in \mathbb{F}_q[x]$.

If c is a codeword of the code C, then we call $c(x)$ the associated code polynomial.

With this convention, the shifted codeword c' has associated code polynomial $c'(x) = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_i x^{i+1} + \ldots + c_{n-2} x^{n-1}$. Thus $c'(x)$ is almost equal to the product polynomial $xc(x)$. More precisely, $c'(x) = xc(x) - c_{n-1}(x^n - 1)$.

Therefore $c'(x)$ has also degree less than n is equal to the remainder when $xc(x)$ is divided by x^n-1. In particular $c'(x) = xc(x) \pmod{x^n - 1}$.

That is $c'(x)$ and $xc(x)$ are equal in the ring of polynomials $\mathbb{F}[x] \pmod{x^n - 1}$, where the arithmetic is done modulo the polynomial x^n-1.

If $c(x)$ is the code polynomial associated with some codeword c of C, then we will allow ourselves to abuse notation by writing $c(x) \in C$.

If $f(x)$ is any polynomial of $\mathbb{F}[x]$ whose remainder, upon division by x^n-1, belongs to C, then we may write $f(x) \in C \pmod{x^n - 1}$.

The cyclic code C has the pleasing polynomial form $c(x) \in C \pmod{x^n - 1}$ if and only if $xc(x) \in C \pmod{x^n - 1}$. Since additional shifts do not take us out of the cyclic code C, we have $x^i c(x) \in C \pmod{x^n - 1}$ and indeed $\sum_{i=0}^{d} a_i x^i c(x) \in C \pmod{x^n - 1}$.

That is for every polynomial $a(x) = \sum_{i=0}^{d} a_i x^i c(x) \in \mathbb{F}[x]$, the product $a(x)c(x)$ still belongs to C.

Definition 3 [17] Let C be a linear code over $\mathbb{F}_p$. The code C is cyclic if $(a_{n-1}, a_0, \ldots, a_{n-2}) \in C$ while $(a_0, \ldots, a_{n-1}) \in C$.

The following statement is used to convert the structure of cyclic codes into an algebraic one.

$\Phi : \mathbb{F}_p^n \rightarrow \mathbb{F}_p[x]/(x^n - 1)$,

$(a_0 a_1 \ldots a_{n-1}) a \rightarrow a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$, where the set of polynomials in x with coefficients in $\mathbb{F}_p$ is denoted by $\mathbb{F}_p[x]$.

It is known that $\mathbb{F}_p[x]/(x^n - 1)$ is a ring for $n \neq 1$.

Theorem 1 Let Φ be the linear map defined as above. The code C of length n over $\mathbb{F}_p$ is a cyclic code if and only if $\Phi(C)$ is an ideal of $\mathbb{F}_p[x]/(x^n - 1)$ [17].

There is one-to-one correspondence between the cyclic codes in $\mathbb{F}_p^n$ and ideals of the ring $\mathbb{F}_p[x]/(x^n - 1)$.

Let $C = < g(x) >$ be a cyclic code of length n over $\mathbb{F}_p$ where $g(x) = g_0 + g_1(x) + \ldots + L + \ldots + g_r x^r$ and $g(x)$ divides x^n-1. In this case, the code C can be expressed as follows.

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

Theorem 2 Let $C \neq \{0\}$ be a cyclic code of length n over $\mathbb{F}_p$.

i) Let $g(x)$ be a monic code polynomial of minimal degree in C. Then $g(x)$ is uniquely determined in C and $C = \{q(x) g(x) \mid q(x) \in \mathbb{F}[x]\}$, where $r = deg(g(x))$. In particular C has dimension $n-r$.

ii) The polynomial $g(x)$ divides x^n-1 in $\mathbb{F}[x]$ [13].

The polynomial $g(x)$ is called the generator polynomial for the code C. The polynomial $h(x) \in \mathbb{F}[x]$ determined by $g(x)h(x) = x^n - 1$ is the check polynomial of C.

Under some circumstances it is convenient to consider x^n-1 to be the generator polynomial of the cyclic code 0 of length n. Then by Theorem 1, there is one-to-one correspondence between cyclic codes of length n and monic divisors of x^n-1 in $\mathbb{F}[x]$.

If we are in possession of a generator polynomial $g(x) = \sum_{j=0}^{r} g_j x^j$ for the cyclic code C, then we can easily construct a generator matrix for C. Consider

$$G = \begin{pmatrix} g_0 & g_1 & \ldots & g_{r-1} & g_r & 0 & 0 & \ldots & 0 \\ 0 & g_0 & g_1 & \ldots & g_{r-1} & g_r & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 0 & g_0 & g_1 & \ldots & g_{r-1} & g_r \end{pmatrix}.$$

The matrix G has n columns and $k = n-r$ rows; so the first row, row g_0, finishes with a string of 0's of length $k-1$. Each successive row is the cyclic shift of the previous row: $g_i = g_i' - 1$, for $i = 1, \ldots, k-1$ As $g(x)h(x) = x^n - 1$, we have $g_0 h_0 = g(0)h(0) = 0^n - 1 \neq 0$.

In particular $g_0 \neq 0$ (and $h_0 \neq 0$). Therefore G is in echelon form. In particular the $k = dim(C)$ rows of G are linearly independent. Clearly the rows of G belong to C, so G is a generator matrix for C.

B. Linear Codes Over $\mathbb{F}_2 + v\mathbb{F}_2$

Consider a commutative ring R as $\mathbb{F}_2 + v\mathbb{F}_2 = \{0, 1, v, 1+v\}$, where $v^2 = v$. R is also the quotient ring $\mathbb{F}_2[v]/(v^2 + v)$. R is a semilocal ring and has two maximal ideals given by $<v>$ and $<1+v>$. A linear code C of length n over R is a $R-$ submodule of R^n. Every element in R can be written as $c = a + bv$, where $a, b \in \mathbb{F}_2$. The Lee weights of $0, 1, v, 1+v \in R$ are as follows.

$W_L(0) = 0, W_L(1) = 1, W_L(v) = 2, W_L(1+v) = 1.$

It is clear that ψ is a bijection.

Definition 4 Let $\mathbb{F}_q$ be a finite field with q elements, where $q = p^m$, p is a prime. Let R denote the commutative ring $\mathbb{F}_2 + v\mathbb{F}_2$, where $v^2 = v$.

i) The Gray map ψ is defined as follows.

$\psi : R \rightarrow \mathbb{F}_2^2, \psi(a + bv) = (b, a + b)$, where $a, b \in \mathbb{F}_2$.

In this case, $\psi(0) = (00), \psi(1) = (01), \psi(v) = (11), \psi(1+v) = (10)$ [23].

ii) The projection map ϕ is defined as follows.

$\phi : R \rightarrow \mathbb{F}_2, \phi(a + bv) = a.$

Theorem 3 The Gray map ψ is $\mathbb{F}_2-$ a linear isometry (or distance preserving) map from R (Lee distance) or $\mathbb{F}_2$ (Hamming distance) [14].

So ψ is a weight-preserving map from (R^n, Lee wight) to ($\mathbb{F}_2^{2n}$ Hamming weight), $W_L(x) = W_H(\psi(x))$.

Definition 5 The cartesian product of vectors $m = (m_1 m_2 \ldots m_n) \in \mathbb{F}_2^n$ and $t = (t_1 t_2 \ldots t_n) \in \mathbb{F}_2^n$ is $m \otimes t = (m_1 m_2 \ldots m_n) \otimes (t_1 t_2 \ldots t_n) = (m_1 m_2 \ldots m_n t_1 t_2 \ldots t_n) \in \mathbb{F}_2^{2n}$.

Definition 6 Let A and B be two codes. In this case $A \otimes B = \{(a, b) \mid a \in A, b \in B\}$ and $A \oplus B = \{a + b \mid a \in A, b \in B\}$.

Let C be a linear code of length n over R. Define the binary linear codes C_1 and C_2 as follows.

$C_1 = \{x \in (\mathbb{F}_2)^n \mid x + vy \in C, \text{ for } \exists y \in \mathbb{F}_2^n\}$ and $C_2 = \{x + y \in \mathbb{F}_2^n \mid x + vy \in C\}$.

Theorem 4 Let C be a linear code of length n over R. Then $\psi(C) = C_1 \otimes C_2$ and $|C| = |C_1||C_2|$. Moreover, $\psi(C)$ is linear [26].

Secret Key Cryptosystem

A cryptosystem is called secret key cryptosystem if some secret piece of information (the key) has to be agreed first between any two parties that want to communicate through the cryptosystem. There are some basic types of secret key cryptosystems:

- **substitution based cryptosystems**
- they substitute the characters of plaintext for another characters;
- **monoalphabetic cryptosystems:**
- they use a fixed substitution, one character is always replaced with the same group of symbols;
- **polyalphabetic cryptosystems:**
- the substitution keeps changing during the encryption;
- **transposition based cryptosystems:**
- they only transpose the characters of plaintext, for example permission/impression.

The cryptosystems can be also divided into block cryptosystems (cryptosystems that are used to encrypt simultaneously blocks of plaintext) and into stream cryptosystems (cryptosystems that encrypt plaintext letter by letter).

Stream cryptosystems are more appropriate in some applications (telecommunication), usually are simpler to implement, faster and have no error propagation. In the stream cryptosystems each block of plaintext is encrypted using a different key.

In the block cryptosystems, the same key is used to encrypt arbitrarily long plaintext block by block.

One Time Pad Cryptosystem: The One Time Pad is a cryptosystem for encoding data using a key of same length as the data. If m is the plaintext, s is key and c is cryptotext, then the encryption algorithm e_s is $c = e_s(m) = m + s$ and the decryption algorithm d_s is $m = d_s(c) = c + s$ [16].

THE NEW ENCRYPTION SCHEMES

In this section, we present two new encryption schemes by using One Time Pad cryptosystem.

First Encryption Scheme

An encryption scheme consists of the following four parameters.

- Setup
- KeyGen
- Encrypt
- Decrypt

So our new encryption scheme can be explained as follows.

Key Generation Procedure:

i. Choose a codeword of a cyclic code of length n with generator matrix $g(x)$ of degree r is called m.
ii. Compute a cyclic shift of the codeword is called s.
iii. Calculate $c = m+s$.
iv. The plaintext is m and the private key is s.

Encryption:

Plaintext : $m_i = a_i(x)g(x)$, where $0 \le i \le p^{n-r}$.

Key : $s_i = x^t a_i(x)g(x)$, where t is the number of shift and $s = s_1 s_2 ... s_n$.

Ciphertext : $c_i = m_i + s_i$.

We assume that $a_i(x)g(x) \neq a_j(x)g(x)$ for $i \neq j, 0 \le i, j \le p^{n-r}$.

Decryption:

Ciphertext : c_i

Plaintext : $m_i = c_i + (p-1)s_i$

Correctness: The correctness of our encryption scheme relies on the structure of a cyclic code. It is known that any cyclic shift of a cyclic code is also a codeword. Every cyclic shift of a codeword consists of key and this key has the same length with the plaintext. Furthermore the key is used only once.

Example 1 Consider length 7 binary cyclic codes. We have the factorization into irreducible polynomials $x^7 - 1 = (x-1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

Since we are looking at binary codes, all the minus signs can be replaced by plus signs:

$x^7 + 1 = (x+1)(x^3 + x + 1)(x^3 + x^2 + 1)$.

As there are 3 irreducible factors, there are 2^3=8 cyclic codes (including 0 and $\mathbb{F}_2^7$). The 8 generator polynomials are

i. 1=1.
ii. $x + 1 = x + 1$
iii. $x^3 + x + 1 = x^3 + x + 1$
iv. $x^3 + x^2 + 1 = x^3 + x^2 + 1$
v. $(x+1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$
vi. $(x+1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$
vii. $(x^3 + x + 1)(x^3 + x^2 + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
viii. $(x+1)(x^3 + x + 1)(x^3 + x^2 + 1) = x^7 + 1$

We try to construct an encryption scheme by using the generator polynomial $g(x) = x^4 + x^3 + x^2 + 1$. So the generator matrix is

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

The codewords generated by the generator matrix are specified as below.

C = {1011100, 0101110, 0010111, 1110010, 0111001, 1001011, 1100101, 0000000}.

If $g(x)=x^4+x^3+x^2+1$, then $a_i(x)\in \mathbb{F}_2[x]/(x^7-1)$, $deg(a_i(x)<7-4=3$. So $a_i(x)=\{1,x,x^2,1+x,x+x^2,1+x^2,1+x+x^2\}$.

Encryption: The encryption scheme constructed based on these codewords is given in the following.

$m_i=a_i(x)g(x), s_i=x^t a_i(x)g(x), (\text{let } t=1)\, c_i=m_i+s_i, 1\le i\le 8.$

$m_1=a_1(x)g(x)=1(1+x^2+x^3+x^4)=1+x^2+x^3+x^4=1011100$

$s_1=xa_1(x)g(x)=x(1+x^2+x^3+x^4)=x+x^3+x^4+x^5=0101110$

$c_1=m_1+s_1=1+x+x^2+x^5=1110010$

$m_2=a_2(x)g(x)=x(1+x^2+x^3+x^4)=x+x^3+x^4+x^5=0101110$

$s_2=xa_2(x)g(x)=x(x+x^3+x^4+x^5)=x^2+x^4+x^5+x^6=0010111$

$c_2=m_2+s_2=x+x^2+x^3+x^6=0111001$

$m_3=a_3(x)g(x)=x^2(1+x^2+x^3+x^4)=x^2+x^4+x^5+x^6=0010111$

$s_3=xa_3(x)g(x)=x(x^2+x^4+x^5+x^6)=1+x^3+x^5+x^6=1001011$

$c_3=m_3+s_3=1+x^2+x^3+x^4=1011100$

$m_4=a_4(x)g(x)=(1+x)(1+x^2+x^3+x^4)=1+x+x^2+x^5=1110010$

$s_4=xa_4(x)g(x)=x(1+x+x^2+x^5)=x+x^2+x^3+x^6=0111001$

$c_4=m_4+s_4=1+x^3+x^5+x^6=1001011$

$m_5=a_5(x)g(x)=(x+x^2)(1+x^2+x^3+x^4)=x+x^2+x^3+x^6=0111001$

$s_5=xa_5(x)g(x)=x(x+x^2+x^3+x^6)=1+x^2+x^3+x^4=1011100$

$c_5=m_5+s_5=1+x+x^4+x^6=1100101$

$m_6=a_6(x)g(x)=(1+x^2)(1+x^2+x^3+x^4)=1+x^3+x^5+x^6=1001011$

$s_6=xa_6(x)g(x)=x(1+x^3+x^5+x^6)=1+x+x^4+x^6=1100101$

$c_6=m_6+s_6=x+x^3+x^4+x^5=0101110$

$m_7=a_7(x)g(x)=(1+x+x^2)(1+x^2+x^3+x^4)=1+x+x^4+x^6=1100101$

$s_7=xa_7(x)g(x)=x(1+x+x^4+x^6)=1+x+x^2+x^5=1110010$

$c_7=m_7+s_7=x^2+x^4+x^5+x^6=0010111$

$m_8=a_8(x)g(x)=0(1+x^2+x^3+x^4)=0=0000000$

Decryption:

$m_i=c_i+(p-1)s_i$

$m_1=c_1+s_1=(1+x+x^2+x^5)+(x+x^3+x^4+x^5)=1+x^2+x^3+x^4=1011100$

$m_2=c_2+s_2=(x+x^2+x^3+x^6)+(x^2+x^4+x^5+x^6)=x+x^3+x^4+x^5=0101110$

$m_3=c_3+s_3=(1+x^2+x^3+x_4)+(x^3+x^5+x^6+x^7)=x^2+x^4+x^5+x^6=0010111$

$m_4=c_4+s_4=(1+x^3+x^5+x^6)+(x+x^2+x^3+x^6)=1+x+x^2+x^5=1110010$

$m_5=c_5+s_5=(1+x+x^4+x^6)+(1+x^2+x^3+x^4)=x+x^2+x^3+x^6=0111001$

$m_6=c_6+s_6=(x+x^3+x^4+x^5)+(1+x+x^4+x^6)=1+x^3+x^5+x^6=1001011$

$m_7=c_7+s_7=(x^2+x^4+x^5+x^6)+(1+x+x^2+x^5)=1+x+x^4+x^6=1100101$

$m_8=c_8+s_8=0+0=0=0000000$

Now we construct another encryption scheme by using the generator polynomial $g(x)=1+x+x^3$ for the same code.

The generator matrix is

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

It is clear that $deg(g(x))=r=3$. So

$a_i(x)\in \mathbb{F}_2[x]/(x^7-1), deg(a_i(x))<n-r=7-3=4.$

$a_i(x)\in\{a_0+a_1(x)+a_2x^2+a_3x^3 : a_0,a_1,a_2,a_3\in\mathbb{F}_2\}.$

$a_i(x)=\{1,x,x^2,x^3,1+x,1+x^2,1+x^3,x+x^2,x+x^3,x^2+x^3,1+x+x^2,1+x+x^3,x+x^2+x^3,1+x^2+x^3,1+x+x^2+x^3,0\}.$

Encryption:

$m_i=a_i(x)g(x), s_i=x^t a_i(x)g(x)(t=1), c_i=m_i+s_i, 1\le i\le 16.$

$m_1=a_1(x)g(x)=1(1+x+x^3)=1+x+x^3=1101000$

$s_1=xa_1(x)g(x)=x(1+x+x^3)=x+x^2+x^4=0110100$

$c_1=m_1+s_1=1+x^2+x^3+x^4=1011100$

$m_2=a_2(x)g(x)=x(1+x+x^3)=x+x^2+x^4=0110100$

$s_2=xa_2(x)g(x)=x(x+x^2+x^4)=x^2+x^3+x^5=0011010$

$c_2=m_2+s_2=x+x^3+x^4+x^5=0101110$

$m_3=a_3(x)g(x)=x^2(1+x+x^3)=x^2+x^3+x^5=0011010$

$s_3=xa_3(x)g(x)=x(x^2+x^3+x^5)=x^3+x^4+x^6=0001101$

$c_3=m_3+s_3=x^2+x^4+x^5+x^6=0010111$

$m_4 = a_4(x)g(x) = x^3(1+x+x^3) = x^3+x^4+x^6 = 0001101$

$s_4 = xa_4(x)g(x) = x(x^3+x^4+x^6) = 1+x^4+x^5 = 1000110$

$c_4 = m_4 + s_4 = 1+x^3+x^5+x^6 = 1001011$

$m_5 = a_5(x)g(x) = (1+x)(1+x+x^3) = 1+x^2+x^3+x^4 = 1011100$

$s_5 = xa_5(x)g(x) = x(1+x^2+x^3+x^4) = x+x^3+x^4+x^5 = 0101110$

$c_5 = m_5 + s_5 = 1+x+x^2+x^5 = 1110010$

$m_6 = a_6(x)g(x) = (1+x^2)(1+x+x^3) = 1+x+x^2+x^5 = 1110010$

$s_6 = xa_6(x)g(x) = x(1+x+x^2+x^5) = x+x^2+x^3+x^6 = 0111001$

$c_6 = m_6 + s_6 = 1+x^3+x^5+x^6 = 1001011$

$m_7 = a_7(x)g(x) = (1+x^3)(1+x+x^3) = 1+x+x^4+x^6 = 1100101$

$s_7 = xa_7(x)g(x) = x(1+x+x^4+x^6) = 1+x+x^2+x^5 = 1110010$

$c_7 = m_7 + s_7 = x^2+x^4+x^5+x^6 = 0010111$

$m_8 = a_8(x)g(x) = (x+x^2)(1+x+x^3) = x+x^3+x^4+x^5 = 0101110$

$s_8 = xa_8(x)g(x) = x(x+x^3+x^4+x^5) = x^2+x^4+x^5+x^6 = 0010111$

$c_8 = m_8 + s_8 = x+x^2+x^3+x^6 = 0111001$

$m_9 = a_9(x)g(x) = (x+x^3)(1+x+x^3) = x+x^2+x^3+x^6 = 0111001$

$s_9 = xa_9(x)g(x) = x(x+x^2+x^3+x^6) = 1+x^2+x^3+x^4 = 1011100$

$c_9 = m_9 + s_9 = 1+x+x^4+x^6 = 1100101$

$m_{10} = a_{10}(x)g(x) = (x^2+x^3)(1+x+x^3) = x^2+x^4+x^5+x^6 = 0010111$

$s_{10} = xa_{10}(x)g(x) = x(x^2+x^4+x^5+x^6) = 1+x^3+x^5+x^6 = 1001011$

$c_{10} = m_{10} + s_{10} = 1+x^2+x^3+x^4 = 1011100$

$m_{11} = a_{11}(x)g(x) = (1+x+x^2)(1+x+x^3) = 1+x^4+x^5 = 1000110$

$s_{11} = xa_{11}(x)g(x) = x(1+x^4+x^5) = x+x^3+x^5+x^6 = 0100011$

$c_{11} = m_{11} + s_{11} = 1+x+x^4+x^6 = 1100101$

$m_{12} = a_{12}(x)g(x) = (1+x+x^3)(1+x+x^3) = 1+x^2+x^6 = 1010001$

$s_{12} = xa_{12}(x)g(x) = x(1+x^2+x^6) = 1+x+x^3 = 1101000$

$c_{12} = m_{12} + s_{12} = x+x^2+x^3+x^6 = 0111001$

$m_{13} = a_{13}(x)g(x) = (x+x^2+x^3)(1+x+x^3) = x+x^5+x^6 = 0100011$

$s_{13} = xa_{13}(x)g(x) = x(x+x^5+x^6) = 1+x^2+x^6 = 1010001$

$c_{13} = m_{13} + s_{13} = 1+x+x^2+x^5 = 1110010$

$m_{14} = a_{14}(x)g(x) = (1+x^2+x^3)(1+x+x^3) = 1+x+x^2+x^3+x^4+x^5+x^6 = 1111111$

$s_{14} = xa_{14}(x)g(x) = x(1+x+x^2+x^3+x^4+x^5+x^6) = 1+x+x^2+x^3x^4+x^5+x^6 = 1111111$

$c_{14} = m_{14} + s_{14} = 0 = 0000000$

$m_{15} = a_{15}(x)g(x) = (1+x+x^2+x^3)(1+x+x^3) = 1+x^3+x^5+x^6 = 1001011$

$s_{15} = xa_{15}(x)g(x) = x(1+x^3+x^5+x^6) = 1+x+x^4+x^6 = 1100101$

$c_{15} = m_{15} + s_{15} = x+x^3+x^4+x^5 = 0101110$

$m_{16} = a_{16}(x)g(x) = 0(1+x+x^3) = 0 = 0000000$

$s_{16} = xa_{16}(x)g(x) = x0 = 0 = 0000000$

$c_{16} = m_{16} + s_{16} = 0 = 0000000$

Decryption:

$m_i = c_i + (p-1)s_i$

$m_1 = c_1 + s_1 = (1+x^2+x^3+x^4)+(x+x^2+x^4) = 1+x+x^3 = 1101000$

$m_2 = c_2 + s_2 = (x+x^3+x^4+x^5)+(x^2+x^3+x^5) = x+x^2+x^4 = 0110100$

$m_3 = c_3 + s_3 = (x^2+x^4+x^5+x^6)+(x^3+x^4+x^6) = x^2+x^3+x^5 = 0011010$

$m_4 = c_4 + s_4 = (1+x^3+x^5+x^6)+(1+x^4+x^5) = x^3+x^4+x^6) = 0001101$

$m_5 = c_5 + s_5 = (1+x+x^2+x^5)+(x+x^3+x^4+x^5) = 1+x^2+x^3+x^4 = 1011100$

$m_6 = c_6 + s_6 = (1+x^3+x^5+x^6)+(x+x^2+x^3+x^6) = 1+x+x^2+x^5 = 1110010$

$m_7 = c_7 + s_7 = (x^2+x^4+x^5+x^6)+(1+x+x^2+x^5) = 1+x+x^4+x^6 = 1100101$

$m_8 = c_8 + s_8 = (x+x^2+x^3+x^6)+(x^2+x^4+x^5+x^6) = x+x^3+x^4+x^5 = 0101110$

$m_9 = c_9 + s_9 = (1+x+x^4+x^6)+(1+x^2+x^3+x^4) = x+x^2+x^3+x^6) = 0111001$

$m_{10} = c_{10} + s_{10} = (1+x^2+x^3+x^4)+(1+x^3+x^5+x^6) = x^2+x^4+x^5+x^6) = 0010111$

$m_{11} = c_{11} + s_{11} = (1+x+x^4+x^6)+(x+x^5+x^6) = 1+x^4$

$+x^5) = 1000110$

$m_{12} = c_{12} + s_{12} = (x + x^2 + x^3 + x^6) + (1 + x + x^3) = 1 + x^2 + x^6 = 1010001$

$m_{13} = c_{13} + s_{13} = (1 + x + x^2 + x^5) + (1 + x^2 + x^6) = x + x^5 + x^6 = 0100011$

$m_{14} = c_{14} + s_{14} = 0 + (1 + x + x^2 + x^3 + x^4 + x^5 + x^6) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = 1111111$

$m_{15} = c_{15} + s_{15} = (x + x^3 + x^4 + x^5) + (1 + x + x^4 + x^6) = 1 + x^3 + x^5 + x^6 = 1001011$

$m_{16} = c_{16} + s_{16} = 0 + 0 = 0 = 0000000$

It is seen that the key is used only once for each encryption. However, the ciphertext can be obtained several times. This situation is an advantage for us since at the end of encryption we get many meaningful message and obtain them from different keys. So it is difficult to guess the key.

Proposition 1 Let C be a cyclic code of length n with generator polynomial $g(x)$ If n is large enough, then the encryption scheme constructed based on C will be more reliable.

Proof. The security of an encryption system is directly proportional to the key length. The key length must equal the length of the message to be encrypted in the One Time Pad cryptosystem. In our encrytpion scheme, the key length is n since the plaintext is length of n. So it is needed to generate a long key to encrypt a long message. It is difficult to transmit and store this key. If n is large enough, then the key cannot be recovered. This means the system is reliable.

Proposition 2 If the polynomial $g(x) \in \mathbb{F}_q[x]$, ($q = p^r$, p is a prime number and r is any positive integer) is primitive, then the encryption scheme can be constructed based on C that is generated by $g(x)$.

Proof. The polynomial $g(x) \in \mathbb{F}_q[x]$ generates a cyclic code if and only if it is primitive since a primitive polynomial generates a cyclic code. So it is needed to choose a primitive polynomial to construct a cryptosystem by using the One Time Pad. Because we work on a cyclic code C.

Second Encryption Scheme

In order to present this scheme, we use the binary cyclic codes. So we developed a new encryption scheme by codes over the ring $R = \mathbb{F}_2 + v\mathbb{F}_2, v^2 = v$.

Key Generation Procedure: Consider the linear code $C = (1+v)C_1 \oplus vC_2$, where $C_1 = <g_1(x)>, C_2 = <g_2(x)>$ and $g_1(x) \mid x^n - 1, g_2(x) \mid x^n - 1$. We can explain the encryption and decryption while $u_i \in C_1, s_j \in C_2, 0 \le i < |C_1|, 0 \le j < |C_2|$.

Encryption:

Plaintext: $m_{i+|C_1|j} = u_i \times s_j \in \psi(C), 0 \le i < |C_1|, 0 \le j < |C_2|$.

Key: $s_j \in C_2, 0 \le j < |C_2|$.

Ciphertext: $c_{i+|C_1|j} = \psi((1+v)u_i + vs_j)$.

Decryption:

Ciphertext: $c_{i+|C_1|j} = \psi((1+v)u_i + vs_j)$

Plaintext: $m_{i+|C_1|j} = \phi[\psi^{-1}(c_{i+|C_1|j}) + vs_j] \times s_j$

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

Let the generator polynomials be $g_1(x) = 1 + x, g_2(x) = 1 + x + x^2$. The binary cyclic codes generated by these generator polynomials, respectively, are $C_1 = \{000, 110, 011, 101\}$ and $C_2 = \{000, 111\}$.

Now we consider $u_0 = 000, u_1 = 110, u_2 = 011, u_3 = 101$ and $s_0 = 000, s_1 = 111$ for i = 0,1,2,3 and j = 0,1.

Encryption:

- Let i = 0, j = 0. That is u_0 = 000 and s_0 = 000. In this case $m_0 = u_0 \times s_0 = 000 \times 000 = 000000$ and $c_0 = \psi[(1+v)u_0 + vs_0] = \psi(000) = 000000$
- Let i = 0, j = 1. That is u_0 = 000 and s_1 = 111. In this case $m_4 = u_0 \times s_1 = 000 \times 111 = 000111$ and $c_4 = \psi[(1+v)u_0 + vs_1] = \psi(vvv) = 111111$
- Let i = 1, j = 0. That is u_1 = 110 and s_0 = 000. In this case $m_1 = u_1 \times s_0 = 110 \times 000 = 110000$ and $c_1 = \psi[(1+v)u_1 + vs_0] = \psi(1 + v1 + v0) = 101000$
- Let i = 1, j = 1. That is u_1 = 110 and s_1 = 111. In this case $m_5 = u_1 \times s_1 = 110 \times 111 = 110111$ and $c_5 = \psi[(1+v)u_1 + vs_1] = \psi(11v) = 010111$
- Let i = 2, j = 0. That is u_2 = 011 and s_0 = 000. In this case $m_2 = u_2 \times s_0 = 011 \times 000 = 011000$ and $c_2 = \psi[(1+v)u_2 + vs_0] = \psi(01 + v1 + v) = 001010$
- Let i = 2, j = 1. That is u_2 = 011 and s_0 = 000. In this case $m_6 = u_2 \times s_1 = 011 \times 111 = 011111$ and $c_6 = \psi[(1+v)u_2 + vs_1] = \psi(v11) = 110101$
- Let i = 3, j = 0. That is u_3 = 101 and s_0 = 000. In this case $m_3 = u_2 \times s_0 = 101 \times 000 = 101000$ and $c_3 = \psi[(1+v)u_3 + vs_0] = \psi(1 + v01 + v) = 100010$
- Let i = 3, j = 1. That is u_3 = 101 and s_1 = 111. In this case $m_7 = u_3 \times s_1 = 101 \times 111 = 101111$ and $c_7 = \psi[(1+v)u_3 + vs_1] = \psi(1v1) = 011101$

Decryption:

- c_0 = 000000, s_0 = 000. So i = 0, j = 0 and

$$m_0 = \phi[\psi^{-1}(c_0) + vs_0] \times s_0 = \phi[\psi^{-1}(000000) + v(000)] \times (000) = \phi[(000) + v(000)] \times (000) = (000) \times (000) = (000000)$$

- $c_1 = 101000$, $s_0 = 000$. So $i = 1$, $j = 0$ and
$$m_1 = \phi[\psi^{-1}(c_1) + vs_0] \times s_0 = \phi[\psi^{-1}(101000) + v(000)] \times (000) = \phi[(1 + v1 + v0) + v(000)] \times (000) = \phi(1 + v1 + v0) \times (000) = (110) \times (000) = (110000)$$
- $c_2 = 001010$, $s_0 = 000$. So $i = 2$, $j = 0$ and
$$m_2 = \phi[\psi^{-1}(c_2) + vs_0] \times s_0 = \phi[\psi^{-1}(001010) + v(000)] \times (000) = \phi[(01 + v1 + v) + v(000)] \times (000) = \phi(01 + v1 + v0) \times (000) = (011) \times (000) = (011000)$$
- $c_3 = 100010$, $s_0 = 000$. So $i = 3$, $j = 0$ and
$$m_3 = \phi[\psi^{-1}(c_3) + vs_0] \times s_0 = \phi[\psi^{-1}(100010) + v(000)] \times (000) = \phi[(1 + v01 + v) + v(000)] \times (000) = \phi(1 + v01 + v) \times (000) = (101) \times (000) = (101000)$$
- $c_4 = 111111$, $s_1 = 111$. So $i = 0$, $j = 1$ and
$$m_4 = \phi[\psi^{-1}(c_4) + vs_1] \times s_1 = \phi[\psi^{-1}(111111) + v(111)] \times (111) = \phi[(vvv) + v(111)] \times (111) = \phi(000) \times (111) = (000) \times (111) = (000111)$$
- $c_5 = 010111$, $s_1 = 111$. So $i = 1$, $j = 1$ and
$$m_5 = \phi[\psi^{-1}(c_5) + vs_1] \times s_1 = \phi[\psi^{-1}(010111) + v(111)] \times (111) = \phi[(1 + v1 + vv) + v(111)] \times (111) = \phi(110) \times (111) = (110) \times (111) = (110111)$$
- $c_6 = 110101$, $s_1 = 111$. So $i = 2$, $j = 1$ and
$$m_6 = \phi[\psi^{-1}(c_6) + vs_1] \times s_1 = \phi[\psi^{-1}(110101) + v(111)] \times (111) = \phi[(v11) + v(111)] \times (111) = \phi(01 + v1 + v) \times (111) = (011) \times (111) = (011111)$$
- $c_7 = 011101$, $s_1 = 111$. So $i = 2$, $j = 1$ and
$$m_7 = \phi[\psi^{-1}(c_7) + vs_1] \times s_1 = \phi[\psi^{-1}(011101) + v(111)] \times (111) = \phi[(1v1) + v(111)] \times (111) = \phi(1 + v01 + v) \times (111) = (101) \times (111) = (101111)$$

Comparison with Other Systems

In the Aguilar et al. [4] encryption framework, there are two independent codes, the random double-circulant structure guarantees the security of the scheme, and the public code *C* guarantees correct decryption. This causes some important results. First, it makes it is possible to consider public families of codes which are difficult to hide but very efficient for decoding. Second it requires finding a tradeoff for the code *C,* between decoding efficiency and practical decoding complexity.

Petrenko et al. [21] developed an encryption method based on cyclic BCH codes. They used RSA encryption algorithm and error correcting codes. So their module allows not only to encrypt a message, but also to protect it from distortion when sending a message.

In our framework, a cyclic code is considered. The security depends on the length of the codewords since the plaintext is any codeword of the cyclic code. The plaintext is encrypted with a key of the same length. Somebody recovering the message cannot find the message even if he tries all the possible keys. Because he finds all the *n*– bit words at the end of this process. Since all the words are also the codewords, it is impossible to guess the plaintext.

SECURITY OF THE SCHEMES

In this section, we explain the security of our schemes. Cyclic codes form an important class of linear codes. We use a codeword of a cyclic code and the One Time Pad encryption method to construct our schemes.

- To encrypt plaintext data, the sender uses a key string equal in length to the plaintext.
- The key is used by mixing (XOR-ing) bit by bit, always a bit of the key with a bit of the plaintext to create a bit of ciphertext.
- This ciphertext is then sent to the recipient.
- At the recipient's end, the encoded message is mixed (XOR-ed) with the duplicate copy of the One Time Key and the plaintext is restored.
- Both sender's and recipient's keys are automatically destroyed after use, to ensure re-application of the same key is not possible.
- So our new encryption schemes are very safe.

Possible Attacks

In our encryption schemes, the key used for encoding the message is completely random and is as long as the message itself. That is why one of the possible attacks to such a cipher is a brute force attack.

The "Bruce Force" Attack: Brute force attacks use exhaustive trial and error methods in order to find the key that has been used for encrypting the plaintext. This means that every possible combination of key bits must be used to decrypt the ciphertext. The correct key would be the one that produces a meaningful plaintext.

Algebraic Attacks

These attacks are usually the best ones for small values of *n*. When *n* decreases it will be easy to find the key.

Our new encryption schemes have some important properties in terms of security. These are confusion and diffusion. The relationship between the plaintext and key is too complex. Moreover, there is no statistical connection between the plaintext and ciphertext. These properties have been minimalized the probability of attack.

CONCLUSION

We presented an efficient approach for constructing code-based cryptosystems. This approach is based on the

One Time Pad cryptosystem. The One Time Pad encryption is the only proven unbreakable encryption method. The One Time encryption method is an additive stream cipher, where a stream truly random keys is generated and then combined with the plaintext for encryption or with the ciphertext for decryption by an "exclusive OR" (XOR) addition. So we used the cyclic codes to construct our new encryption schemes. We analyzed its security. However, this method can be applied for the other linear codes in the future work.

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] Abualrub T, Seneviratne P. Skew codes over ring. Hong Kong: Proc Int Multiconference Eng Comput Sci; 2010. Available at: http://www.iaeng.org/publication/IMECS2010/IMECS2010_pp846-847.pdf. Accessed May 26, 2022.

[2] Ajtai M, Dwork C. A public-key cryptosystem with worst-case/average-case equivalence. 1997. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.45.5652&rep=rep1&type=pdf. Accessed May 26, 2022.

[3] Alekhnovich M. More on average case vs approximation complexity. Proc 44th Annuel IEEE Sym Foun Comput Sci 2003. Available at: https://www.cs.toronto.edu/~toni/Courses/PCP/handouts/misha.pdf. Accessed May 26, 2022.

[4] Aguiler-Melchor C, Blazy O, Deneuville JC, Gaborit P, Zemor G. Efficient Encryption from random Quasi-Cyclic codes. IEEE Trans Info Theory 2018;64:3927–3943. [CrossRef]

[5] Berger TP, Cayrel PL, Gaborit P, Otmani A. Reducing key length of the McEliece cryptosystem. Progress in Cryptology-Second International Conference on Cryptology in Africa. Tunisia: Gammarth; 2009. [CrossRef]

[6] Boucher D, Ulmer F. Coding with skew polynomial rings. J Symb Comput 2009;44:1644–1656. [CrossRef]

[7] Dertli A, Çengellenmiş Y. On $(1+u)-$ Cyclic and Cyclic Codes over $\mathbb{F}_2+u\mathbb{F}_2+v\mathbb{F}_2$,. Eur J Pure Appl Math 2016;9:305–313.

[8] Duc A, Vaudenay S. Helen: A public-key cryptosystem based on the Ipn and the decisional minimal distance problems. International Conference on Cryptology in Africa. Africa, Cairo, Egypt: Springer; 2013. [CrossRef]

[9] Gaborit P, Gaetan M, Ruatta O, Zemor G. Low rank parity check codes and their application to cryptography. Proceedings of the Workshop on Coding and Cryptography WCC' 2013. Norway: Bergen: 2013. Available at; www.selmer.uib.no/WCC2013/pdfs/Gaborit.pdf. Accessed May 26, 2022.

[10] Gao J. Skew cyclic codes over $\mathbb{F}_p+v\mathbb{F}_p$,. J Appl Math Inform 2013;31:337–342. [CrossRef]

[11] Geiselmann DW, Ulmer F. Skew cyclic codes. Appl Algebra Eng Commun 2007;18:379–389. [CrossRef]

[12] Haffstein J, Pipher J, Silverman JH. NTRU: A ring-based public key cryptosystem, In Joe Buhler, editor. Algorithmic Number Theory, Third International Symposium, ANTS-III, Portland, Oregon, USA. USA: Springer: 1998. [CrossRef]

[13] Hill R. A first course in coding theory. USA: Oxford University; 1986.

[14] Islam H, Prakash O. Skew constacyclic codes over $\mathbb{F}_q+u\mathbb{F}_q+v\mathbb{F}_q$,. ArXiv 2017. Available at: https://arxiv.org/pdf/1710.07789.pdf. Accessed May 26, 2022.

[15] Klitz E, Masny D, Pietrzak K. Simple chosen-ciphertext security from low-noise LPN. In Hugo Krawezyk, editor. Public-Key Cryptography – PKC 2014. PKC 2014. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer; 2014. [CrossRef]

[16] Kuklova Z. Coding theory, cryptography and cryptographic protocols-exercises with solutions (given in 2006). Bachelor Thesis. Brno: Masaryk University, Faculty of Informatics; 2007.

[17] Ling S, Xing C. Coding theory: A first course. UK: Cambridge University Press; 2004. [CrossRef]

[18] McEliece RJ. A public-key cryptosystem based on algebraic Coding theory. DSN Prog Rep 1978:114–116.

[19] Misoezki R, Barreto PSLM. Compact McEliece keys from goppa codes. In Michael J. Jacobson Jr, Rijmen V, Safavi-Naini R, editors. Selected areas in cryptography. Heidelberg: Springer; 2009:376–392. [CrossRef]

[20] Misoezki R, Tillich JP, Sendries N, Barreto PSLM. MDPC-McEliece: New mceliece variants from moderate density parity-check codes. 2013. Available at: https://eprint.iacr.org/2012/409.pdf. Accessed May 26, 2022. [CrossRef]

[21] Petrenko V, Ryabtsev S, Pavlov A, Apurin A. Development of an encryption method based on cyclic codes. Proceedings of the 21st International Workshop on Computer Science and Information Technologies. Atlantis Press 2019. [CrossRef]

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

[23] Qian J. Quantum codes from cyclic codes over $\mathbb{F}_2 + v\mathbb{F}_2$. J Inf Comput Sci 2013;10:1715–1722. [CrossRef]

[24] Regev O. New lattice based cryptographic contructions. In Proceedings of the 35th ACM Symposium on Theory of Computing. J ACM 2004;51:899–942. [CrossRef]

[25] Yao T, Shi M, Solé P. Skew cyclic codes over $\mathbb{F}_q + u\mathbb{F}_q + v\mathbb{F}_q + uv\mathbb{F}_q^*$,. J Algebra Comb Discrete Struct App 2015;2:163–168. [CrossRef]

[26] Zhu S, Wang Yu, Shi M. Some results on Cyclic Codes Over $\mathbb{F}_2 + v\mathbb{F}_2$,. IEEE Trans Inf Theory 2010;56:1680–1684. [CrossRef]