Chapter

A Public Key Cryptosystem Using Cyclotomic Matrices

Md. Helal Ahmed, Jagmohan Tanti and Sumant Pushp

Abstract

Confidentiality and Integrity are two paramount objectives in the evaluation of information and communication technology. In this chapter, we propose an arithmetic approach for designing asymmetric key cryptography. Our method is based on the formulation of cyclotomic matrices correspond to a diophantine system. The strategy uses in cyclotomic matrices to design a one-way function. The result of a one-way function that is efficient to compute, however, is hard to process its inverse except if privileged information about the hidden entry is known. Also, we demonstrate that encryption and decryption can be efficiently performed with the asymptotic complexity of $\mathcal{O}(e^{2.373})$. Finally, we study the computational complexity of the cryptosystem.

Keywords: finite fields, discrete logarithm problem, cyclotomic numbers, cyclotomic matrix, public key, secret key

1. Introduction

Apart from a rich history of Message encryption, the cryptosystem became more popular in the twentieth century upon the evolution of information technology. Until the last part of the 1970s, all cryptographic message was sent by the symmetric key. This implies somebody who has sufficient data to encode messages likewise has enough data to decode messages. Consequently, the clients of the framework must have to impart the secret key furtively. As a result of an issue stealthily key sharing, Diffie and Hellman [1] developed a totally new sort of cryptosystem called public key cryptosystem.

In a Public key cryptosystem, both parties (in a two-party system) have a pair of public enciphering and secret deciphering keys [2, 3]. Any party can send encrypted messages to an assigned party using a public enciphering key. However, only the assigned party can decrypt the message utilizing their corresponding secret deciphering key [4]. After that various public key cryptosystems were introduced based on tricky mathematical problems. Among these, RSA is the longest reasonable use of cryptography. Since its design, in spite of all effort, it has not been broken yet. The security of the RSA is acknowledged to be established on the issue of the factorization of an enormous composite number. Be that as it may, there are some practical issues in RSA execution. The fundamental issue is the key arrangement time that is absurdly long for computationally restricted processors used in certain applications. Another issue is the size of the key. It was demonstrated that the time required to factor an n-bit integer by *index calculus factorization* technique is of order $2^{n^{1/2+\delta}}, \delta > 0$ [5]. In 1990's, J. Pollard [6] demonstrated that it was possible in time bounded by $2^{n^{1/3+\delta}}, \delta > 0$. The reduction of the exponent of n has significant outcomes over the long run. It should likewise be expanded each year as a result of upgrades in the factorization calculations and computational power. Until 2015, it was prescribed the base size of the RSA key should be 1024 bits and subsequently increases to 4096 & 8192 bits by 2015 & 2025 respectively [7]. While trying to remedy these issues, Discrete logarithm problem (DLP) has been utilized (to reduce key setup time and size of the key).

Discrete logarithm problem (DLP) is a mathematical problem that occurs in many settings and it is hard to compute exponent in a known multiplicative group [8]. Diffie-Hellman [1], ElGamal [9], Digital Signature Algorithm [10], Elliptic curve cryptosystems [11, 12] are the schemes evolved under the Discrete logarithm algorithm. The security of Diffie-Hellman relied upon the complexity of solving the discrete logarithm problem. However, the scheme has some disadvantages. It has not been demonstrated that breaking the Diffie-Hellman key exchange has relied upon DLP and also the scheme is vulnerable to a man-in-the-middle attack. For the security aspect, cryptosystem [9] was proposed, to introduce a digital signature algorithm (DSA) that's primarily based on Diffie-Hellman DLP and key distribution scheme. It was demonstrated that DSA is around multiple times littler than the RSA signature and later DSA has been supplanted by the elliptic curves digital signature algorithm (ECDSA). Nonetheless, it has some practical implementation problems [13–15]. The length of the smallest signature is of 320 bits, which is still being too long for computationally restricted processors. Another issue emerged is as a correlation with RSA in a field with prime characteristics, which is forty times slower than RSA [16].

There are some other designs for public-key cryptosystems based on some extensive features of matrices. However, there were some practical implementation problems. Thus it had never achieved wide popularity in the cryptographic community. McElice [17] come up with a public key cryptosystem rooted on the Goppa codes Hamming metric. The scheme has the advantage that it has two to three orders of magnitude faster than RSA. Despite its advantage, it has some drawbacks. It was demonstrated that the length of the public key is 2^{19} bits and the data expansion is too large. Some other extensions of the scheme can also be found in [18–20]. Unfortunately, the scheme & its variants has been broken in [21–23]. Later, Gabidulin [24] come up with the rank metric & the Gabidulin codes over a finite field with q elements, where $q = p^r$ i.e. $\mathbf{F}_q$, as an alternative for the Hamming metric. The efficiency of the scheme relied on same set of parameters and the complexity of the decoding algorithm for random codes in rank metric is tons higher than the Hamming metric [17, 25–27]. Numerous fruitful attacks were utilized on the structure of the public code [28–30]. To prevent these attacks, numerous alterations of the cryptosystems were made, consequently drastically increases the size of the key [31–33]. Lau and Tan [34] proposed new encryption with a public key matrix by considering the addition of a random distortion matrix over $\mathbf{F}_q$ of full column rank n. There are also many other design on matrices, which are not cited here, but none of them gain wide popularity in the cryptographic community due to lack of efficient implementation problems in one and another way.

Thinking about these inadequacies, it would be desirable to have a cryptosystem dependent on other than the presumptions as of now being used. Thus, we propose a cyclotomy asymmetric cryptosystem (CAC) based on strong assumptions of DLP that have to reduce the key size and faster the computational process.

1.1 Outline of our scheme

In this chapter, we consider two significant problems in the theory of cyclotomic numbers over $\mathbf{F}_p$. The first one deals with an efficient algorithm for fast computation of all the cyclotomic numbers of order $2l^2$, where l is prime. The subsequent one deals with designing public key cryptosystem based on cyclotomic matrices of order $2l^2$. The strategy employs for designing public-key cryptosystem utilizing cyclotomic matrices of order $2l^2$, whose entries are cyclotomic numbers of order $2l^2$, l be prime, where cyclotomic numbers are certain pairs of solutions $(a, b)_{2l^2}$ of order $2l^2$ over a finite field $\mathbf{F}_p$ with p elements.

In our approach, to designing cyclotomy asymmetric cryptosystem (CAC) based on trapdoor one-way function (OWF). The public key is obtained by choosing a non-trivial generator $\gamma \in \mathbf{F}_p^*$. The chosen value of the generator constructs a cyclotomic matrix of order $2l^2$. It is believed that cyclotomic matrices of order $2l^2$ is always non-singular if the value of $k > 1$. Since there are efficient algorithms for the construction of cyclotomic matrices. Consequently, the key setup time in our proposed cryptosystem is much shorter than previously designed cryptosystems.

In the scheme, the secret key is given by choosing a different non-trivial generator, which is accomplished by discrete logarithm problem (DLP) over a finite field $\mathbf{F}_p^*$. A key-expansion algorithm is employed to expand the secret keys, which form a non-singular matrix of order $2l^2$. Here it is important to note that, if one can change the generators of $\mathbf{F}_p^*$, then entries of cyclotomic matrices get interchanged among themselves, however, the nature of the cyclotomic matrices remain as same. The decryption algorithm involves efficient algebraic operations of matrices. Hence the decryption in our proposed CAC is very efficient. In view of the perspective on the efficient encryption and decryption features, the polynomial time algorithm ensures that the proposed CAC makes it attractive in computationally restricted processors.

The chapter is organized as follows: Section 2 presents the definition and notations, including some well-known properties of cyclotomic numbers of order $2l^2$. Section 3 presents the construction of cyclotomic matrices of order $2l^2$. Section 4 contains encryption and decryption algorithms of CAC along with a numerical example. In addition, the computational complexity of the proposed CAC is discussed and in Section 5 presents the encryption & decryption can be efficiently perform with asymptotic complexity of $\mathcal{O}(e^{2.373})$. Finally, a brief conclusion is reflected in Section 6.

2. Cyclotomic numbers

Cyclotomic numbers are one of the most vital objects in Number Theory. These numbers had been substantially utilized in Cryptography, Coding Theory and other branches of Information Theory. Thus, calculation of cyclotomic numbers, so called to as cyclotomic number problems, of various orders is one of the primary problems in Number Theory. Complete answers for cyclotomic number problem for $e = 2 - 6$, 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 20, 22, l, $2l$, l^2, $2l^2$ with l an odd prime had been investigated by many authors see ([35–40] and the references there in). The section contains the generalized definition of cyclotomic numbers of order e, useful notations followed by properties of cyclotomic numbers of order $2l^2$. These properties play a vital role in determining which cyclotomic numbers of order $2l^2$ are sufficient for the determination of all $4l^4$ cyclotomic numbers of order $2l^2$. The section also examines the cyclotomic matrices of order $2l^2$.

2.1 Definition and notations

Let $e \geq 2$ be an integer, and $p \equiv 1(\text{mod} e)$ an odd prime. One writes $p = ek + 1$ for some positive integer k. Let $\mathbf{F}_p$ be the finite field of p elements and let γ be a generator of the cyclic group $\mathbf{F}_p^*$. For $0 \leq a, b \leq e - 1$, the cyclotomic number $(a, b)_e$ of order e is defined as the number of solutions (s, t) of the following:

$$\gamma^{es+a} + \gamma^{et+b} + 1 \equiv 0 \ (\text{mod}\, p); \qquad 0 \leq s, t \leq k - 1. \tag{1}$$

2.2 Properties of cyclotomic numbers of order $2l^2$

In this subsection, we recalled some elementary properties of cyclotomic numbers of order $2l^2$ [38]. Let $p \equiv 1 \ (\text{mod} 2l^2)$ be a prime for an odd prime l and we write $p = 2l^2k + 1$ for some positive integer k. It is clear that $(a, b)_{2l^2} = (a', b')_{2l^2}$ whenever $a \equiv a' \ (\text{mod} 2l^2)$ and $b \equiv b' \ (\text{mod} 2l^2)$ as well as $(a, b)_{2l^2} = (2l^2 - a, b - a)_{2l^2}$. These imply the following:

$$(a, b)_{2l^2} = \begin{cases} (b, a)_{2l^2} & \text{if } k \text{ is even,} \\ (b + l^2, a + l^2)_{2l^2} & \text{if } k \text{ is odd.} \end{cases} \tag{2}$$

Applying these facts, one can check that

$$\sum_{a=0}^{2l^2-1} \sum_{b=0}^{2l^2-1} (a, b)_{2l^2} = q - 2 \tag{3}$$

and

$$\sum_{b=0}^{2l^2-1} (a, b)_{2l^2} = k - n_a, \tag{4}$$

where n_a is given by

$$n_a = \begin{cases} 1 & \text{if } a = 0, \ 2 \mid k \text{ or if } a = l^2, \ 2 \nmid k, \\ 0 & \text{otherwise.} \end{cases}$$

3. Cyclotomic matrices

This section presents the procedure to determine cyclotomic matrices of order $2l^2$ for prime l. We determine the equality relation of cyclotomic numbers and discuss how few of the cyclotomic numbers are enough for the construction of whole cyclotomic matrix. Further generators for a chosen value of p will be determined followed by the generation of a cyclotomic matrix. At every step, we have included a numerical example for the convenience to understand the procedure easily.

Definition:- Cyclotomic matrix of order $2l^2$, l be a prime, is a square matrix of order $2l^2$, whose entries are pair of solutions $(a,b)_{2l^2}$; $0 \leq a, b \leq 2l^2 - 1$, of the Eq. (1).

For instance **Table 1** depicts a typical cyclotomic matrix of order 8 (assuming $l = 2$). Whose construction steps have been given in the next subsection.

3.1 Construction of cyclotomic matrix

Typically construction of a cyclotomic matrix has been subdivided into four subsequent steps. Below are those ordered steps for the construction of a cyclotomic matrix;

1. For given l, choose a prime p such that p satisfies $p = 2l^2k + 1$, $k \in \mathbf{Z}^+$. The initial entries of the cyclotomic matrix are the arrangement of pair of numbers $(a,b)_{2l^2}$ where a and b usually vary from 0 to $2l^2 - 1$.

2. Determine the equality relation of pair of $(a,b)_{2l^2}$, which reduces the complexity of pair of solution $(a,b)_{2l^2}$ of Eq. (1), that is discuss in next subsection.

3. Determine the generators of chosen p (i.e. generators of $\mathbf{F}_p^*$). Let $\gamma_1, \gamma_2, \gamma_3, \ldots, \gamma_n$ be generators of $\mathbf{F}_p^*$.

4. Choose a generator (say γ_1) of $\mathbf{F}_p^*$ and put in Eq. (1). This will give cyclotomic matrix of order $2l^2$ w.r.t. chosen generator γ_1.

The first step initializes the entries of cyclotomic matrix of order $2l^2$. Value of p will be determined for given l. Assuming $l = 2$, an example of such initialization of matrix of order 8 has been shown in **Table 1**.

For the construction of cyclotomic matrix, it does not require to determine all the cyclotomic numbers of a cyclotomic matrix which is shown in **Table 1** [36]. By well-known properties of cyclotomic numbers of order $2l^2$, cyclotomic numbers are divided into various classes, therefore there are a pair of the relation between the entries of initial table (**Table 1**) of a cyclotomic matrix. Thus to avoid calculating the same solutions in multiple times, we determine the equality relation of

(a,b)				**b**				
a	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,6)	(0,7)
1	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,7)
2	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,6)	(2,7)
3	(3,0)	(3,1)	(3,2)	(3,3)	(3,4)	(3,5)	(3,6)	(3,7)
4	(4,0)	(4,1)	(4,2)	(4,3)	(4,4)	(4,5)	(4,6)	(4,7)
5	(5,0)	(5,1)	(5,2)	(5,3)	(5,4)	(5,5)	(5,6)	(5,7)
6	(6,0)	(6,1)	(6,2)	(6,3)	(6,4)	(6,5)	(6,6)	(6,7)
7	(7,0)	(7,1)	(7,2)	(7,3)	(7,4)	(7,5)	(7,6)	(7,7)

Table 1.
Cyclotomic matrix of order 8.

cyclotomic numbers (i.e. equality of solutions of $(a,b)_{2l^2}$). In the next subsection, we will discuss which cyclotomic numbers are enough for the construction of the cyclotomic matrix. Thus it helps us to the faster computation of cyclotomic matrix.

3.2 Determination of equality relation of cyclotomic numbers

This subsection presents the procedure to determine the equality relation of cyclotomic numbers (i.e. the relation of pair of $(a,b)_{2l^2}$), which reduces the complexity of solutions of pair of $(a,b)_{2l^2}$ (see also [36]). For the determination of cyclotomic matrices, it is not necessary to obtain all $4l^4$ cyclotomic numbers of order $2l^2$. The minimum number of cyclotomic numbers required to determine all the cyclotomic numbers (i.e. required for construction of cyclotomic matrix) depends on the value of positive integer k on expressing prime $p = 2l^2k + 1$. By (2), if k is even, then

$$(a,b)_{2l^2} = (b,a)_{2l^2} = (a-b,-b)_{2l^2} = (b-a,-a)_{2l^2} = (-a,b-a)_{2l^2} = (-b,a-b)_{2l^2} \tag{5}$$

otherwise

$$\begin{aligned}(a,b)_{2l^2} &= \left(b+l^2, a+l^2\right)_{2l^2} = \left(l^2+a-b,-b\right)_{2l^2} = \left(l^2+b-a, l^2-a\right)_{2l^2} \\ &= (-a,b-a)_{2l^2} = \left(l^2-b,a-b\right)_{2l^2}.\end{aligned} \tag{6}$$

Thus by (5) and (6), cyclotomic numbers $(a,b)_{2l^2}$ of order $2l^2$ can be divided into various classes.

- $2|k$ and $l \neq 3$: In this case, (5) gives classes of singleton, three and six elements. $(0,0)_{2l^2}$ form singleton class, $(-a,0)_{2l^2}$, $(a,a)_{2l^2}$, $(0,-a)_{2l^2}$ form classes of three elements where $1 \le a \le 2l^2 - 1 \pmod{2l^2}$ and rest $4l^4 - 3 \times 2l^2 + 2$ of the cyclotomic numbers form classes of six elements.

- $2|k$ and $l = 3$: In this case, (5) divide cyclotomic numbers $(a,b)_{18}$ of order 18 into classes of singleton, second, three and six elements. $(0,0)_{18}$ form singleton class, $(-a,0)_{18}$, $(a,a)_{18}$, $(0,-a)_{18}$ form classes of three elements, where $1 \le a \le 17 \pmod{18}$, $(6,12)_{18} = (12,6)_{18}$ which is grouped into classes of two elements and rest $4l^4 - 3 \times 2l^2$ of the cyclotomic numbers form classes of six elements.

- $2\nmid k$ and $l \neq 3$: Using (6), once again we get classes of singleton, three and six elements. $\left(0,l^2\right)_{2l^2}$ forms singleton class, $(0,a)_{2l^2}$, $\left(a+l^2,l^2\right)_{2l^2}$, $\left(l^2-a,-a\right)_{2l^2}$ form classes of three elements, where $0 \le a \neq l^2 \le 2l^2 - 1\left(\bmod 2l^2\right)$ and rest $4l^4 - 3 \times 2l^2 + 2$ of the cyclotomic numbers form classes of six elements.

- $2\nmid k$ and $l = 3$: In this situation, (6) partitions cyclotomic numbers $(a,b)_{18}$ of order 18 into classes of singleton, two, three and six elements. Here $(0,9)_{18}$ form singleton class, $(0,a)_{18}$, $(a+9,9)_{18}$, $(9-a,-a)_{18}$ form classes of three elements, where $0 \le a \neq 9 \le 17 \pmod{18}$, $(6,3)_{18} = (12,15)_{18}$ which is grouped into classes of two elements and rest $4l^4 - 3 \times 2l^2$ of the cyclotomic numbers form classes of six elements.

DOI: http://dx.doi.org/10.5772/intechopen.101105

Algorithm 1 Equality relation of cyclotomic numbers.

START
Declare integer variable $e, l, p, k, flag$.
INPUT l, an odd prime and $e = 2l^2$
Declare an array of size $e \times e$, where each element of array is 2 tuple structure (i.e. ordered pair of $(a, b)_{2l^2}$, where a and b are integers).
INPUT p, prime number greater than 2
if $(p-1)\%e == 0$ **then**
    $k = (p-1)/e$
    if k even **then**
        Update table (E)
    else
        Update table (O)
    end if
end if

Here **Update table (E)** means each entry $(a, b)_{2l^2}$ of the table will be updated by applying the relations $(a, b)_{2l^2} = (b, a)_{2l^2} = (a-b, -b)_{2l^2} = (b-a, -a)_{2l^2} = (-a, b-a)_{2l^2} = (-b, a-b)_{2l^2}$, and **Update table (O)** means each entry $(a, b)_{2l^2}$ of the table will be updated by applying the relations $(a, b)_{2l^2} = \left(b + l^2, a + l^2\right)_{2l^2} = \left(l^2 + a - b, -b\right)_{2l^2} = \left(l^2 + b - a, l^2 - a_{2l^2}\right) = (-a, b-a)_{2l^2} = \left(l^2 - b, a - b\right)_{2l^2}$.

Further, if entries of the updated table are non-negative, then each entry should be replace by $\left(\text{mod} 2l^2\right)$, otherwise add $2l^2$. It is clear from above exploration, cyclotomic numbers of order $2l^2$ are divided into different classes depending on the values of k and l. For $l = 2$ and let k be even, then $(0, 0)_8$ give unique solution, cyclotomic numbers of the form $(-a, 0)_8$, $(a, a)_8$, $(0, -a)_8$ where $1 \leq a \leq 7 \pmod 8$ gives the same solutions and rest of cyclotomic numbers (i.e. 42) which forms classes of six elements has maximum 7 distinct numbers of solutions. Therefore the initial table (i.e. **Table 1**) of cyclotomic matrix reduces to **Table 2**. Similarly, for $l = 2$ and let k be odd, then $(0, 4)_8$ give unique solution, cyclotomic numbers of the form $(0, a)_8$, $(a + 4, 4)_8$, $(4 - a, -a)_8$ where $0 \leq a \neq 4 \leq 7 (\text{mod} 8)$ gives the same solutions and rest of cyclotomic numbers (i.e. 42) which forms classes of six elements has maximum 7 distinct numbers of solutions. Therefore the initial table

(a,b)				**b**				
a	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,6)	(0,7)
1	(0,1)	(0,7)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,2)
2	(0,2)	(1,2)	(0,6)	(1,6)	(2,4)	(2,5)	(2,4)	(1,3)
3	(0,3)	(1,3)	(1,6)	(0,5)	(1,5)	(2,5)	(2,5)	(1,4)
4	(0,4)	(1,4)	(2,4)	(1,5)	(0,4)	(1,4)	(2,4)	(1,5)
5	(0,5)	(1,5)	(2,5)	(2,5)	(1,4)	(0,3)	(1,3)	(1,6)
6	(0,6)	(1,6)	(2,4)	(2,5)	(2,4)	(1,3)	(0,2)	(1,2)
7	(0,7)	(1,2)	(1,3)	(1,4)	(1,5)	(1,6)	(1,2)	(0,1)

Table 2.
Cyclotomic matrix of order 8 for even k.

(a,b)	**b**							
a	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,6)	(0,7)
1	(1,0)	(1,1)	(1,2)	(1,3)	(0,5)	(0,3)	(1,3)	(1,7)
2	(2,0)	(2,1)	(2,0)	(1,7)	(0,6)	(1,3)	(0,2)	(1,2)
3	(1,1)	(2,1)	(2,1)	(1,0)	(0,7)	(1,7)	(1,2)	(0,1)
4	(0,0)	(1,0)	(2,0)	(1,1)	(0,0)	(1,0)	(2,0)	(1,1)
5	(1,0)	(0,7)	(1,7)	(1,2)	(0,1)	(1,1)	(2,1)	(2,1)
6	(2,0)	(1,7)	(0,6)	(1,3)	(0,2)	(1,2)	(2,0)	(2,1)
7	(1,1)	(1,2)	(1,3)	(0,5)	(0,3)	(1,3)	(1,7)	(1,0)

Table 3.
Cyclotomic matrix of order 8 for odd k.

(i.e. **Table 1**) of cyclotomic matrix reduces to **Table 3**. One can observe that 64 pairs of two parameter numbers $(a, b)_8$ reduced to 15 distinct pairs (see **Tables 2** and **3**).

Remark 3.0 By Algorithm 1, to compute $2l^2$ cyclotomic numbers, it is enough to compute $2l^2 + \lceil (2l^2 - 1)(2l^2 - 2)/6 \rceil$, if $(2l^2 - 1)(2l^2 - 2)|6$, otherwise $2l^2 + \lceil (2l^2 - 1)(2l^2 - 2)/6 \rceil + 1$. Further, when l is the least odd prime i.e. $l = 3$, then $(2l^2 - 1)(2l^2 - 2) \nmid 6$. Therefore $l = 3$, it is enough to calculate 64 distinct cyclotomic numbers of order $2l^2$ and for $l \neq 3$, it is sufficient to calculate $2l^2 + (2l^2 - 1)(2l^2 - 2)/6$ distinct cyclotomic numbers of order $2l^2$.

3.3 Determination of generators of $\mathbf{F}_p^*$

To determine the solutions of (1), we need the generator of the cyclic group $\mathbf{F}_p^*$. Let us choose finite field of order p that satisfy $p = 2l^2k + 1; k \in \mathbf{Z}^+$. Let $\gamma_1, \gamma_2, \gamma_3, \dots, \gamma_n$ be generators of $\mathbf{F}_p^*$. We consider finite field of order 17 (i.e. $\mathbf{F}_{17}$), since the chosen value of $p = 17$ with respect to the value of l take previously. Now to determine the generators of cyclic group $\mathbf{F}_{17}^*$. The detail procedure to obtain the generator of $\mathbf{F}_{17}^*$ has been depicted in Algorithm 2. If G_{17} is a set that contain all the generator of $\mathbf{F}_{17}^*$, we could get elements of G_{17} as $\{3, 5, 6, 7, 10, 11, 12, 14\}$.

Algorithm 2 Determination of generators of $\mathbf{F}_p^*$.

Declare integer variable p, count
Declare integer array $arr\mathbf{F}_p[p]$, $arr\mathbf{F}_p flag[p]$
for $i = 1$ to $p - 1$ **do**
    $arr\mathbf{F}_p[i] = i$, $arr\mathbf{F}_p flag[i] = 0$
end for
Declare integer array $arr\mathbf{G}_p[max]$
Declare integer variable $flag = 0$, r, γ
for $i = 1$ to $p - 1$ **do**
    count = 0
    for $f = 1$ to $p - 1$ **do**
        $arr\mathbf{F}_p flag[f] = 0$
    end for
    $\gamma = arr\mathbf{F}_p[i]$

    for $a = 1$ to $p - 1$ **do**
        $r = power(\gamma, a) \pmod{p}$
        for $j = 1$ to $p - 1$ **do**
            if r is equal to $arr\mathbf{F}_p[j]$ **then**
                $arr\mathbf{F}_p flag[j] = 1$
            end if
        end for
    end for
    for $k = 1$ to $p - 1$ **do**
        if $arr\mathbf{F}_p flag[k]$ is equal to 1 **then**
            count++
        end if
    end for
    if count is equal to $p - 1$ **then**
        γ is generator
    end if
end for

3.4 Generation of cyclotomic matrices

This subsection, present an algorithm for the generation of cyclotomic matrices of order $2l^2$. Note that entries of cyclotomic matrices are solutions of (1). Thus we need the generator of the cyclic group $\mathbf{F}_p^*$, which is discussed in the previous subsection. On substituting the generators of $\mathbf{F}_p^*$ in Algorithm 3, we obtain the cyclotomic matrices of order $2l^2$ corresponding to different generators of $\mathbf{F}_p^*$. The chosen value of $p = 17$ implies $k = 2$ w.r.t. assume value of $l = 2$. Therefore the cyclotomic matrix will be obtain from **Table 2**. Let us choose a generator (say $\gamma_1 = 3$) from set G_{17}. On substituting $\gamma_1 = 3$ in Algorithm 3, it will generate cyclotomic matrix of order 8 over $\mathbf{F}_{17}$ w.r.t. chosen generator $\gamma_1 = 3$. Matrix B_0 show the corresponding cyclotomic matrix of order 8 w.r.t. chosen generator $3 \in \mathbf{F}_{17}^*$.

$$\mathbf{B}_0 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}.$$

Algorithm 3 Generation of cyclotomic matrix.

INPUT: The value of p, l, γ
Declare an array $arr[ROW][COL]$ (where elements are two tuple structure)
Declare integer variable $p,\ l,\ k,\ \gamma,\ x,\ y,\ A,\ s,\ t,\ a,\ b,\ count = 0,\ p_1,\ p_2$
for a equal to 0 to number of rows **do**
    for b equal to 0 to number of columns **do**
        for x is equal to 0 to k **do**

for y is equal to 0 to k **do**
$p_1 = 2l^2 * s + arr[a][b].l$
$p_2 = 2l^2 * t + arr[a][b].m$
$A = power(\gamma, p_1) + power(\gamma, p_2) + 1$
if $A \pmod{p}$ is equal to 0 **then**
$count++$
end if
end for
end for
$arr[a][b].n = count$
$count = 0$
end for
end for

Remark 3.1 It is noted that if we change the generator of $\mathbf{F}_p^*$, then entries of cyclotomic matrices get interchanged among themselves but their nature remains the same.

Remark 3.2 It is obvious that (by (4)) cyclotomic matrices of order $2l^2$ is always singular if the value of $k = 1$.

4. The public-key cryptosystem

In this section, we present the approach for designing a public key cryptosystem using cyclotomic matrices discussed in Section 3. The scheme employ matrices of order $2l^2$, whose entries are cyclotomic numbers of order $2l^2$. The public key is a non-trivial generator, say γ' of a set of generator in $\mathbf{F}_p^*$ along with p and l. The set of generator is obtain by Algorithm 2. The chosen public keys generate a cyclotomic matrix as of required order (i.e. order of $2l^2$) make use of Algorithm 3. Here, we define a trapdoor one-way function $\phi : \mathbf{F}_p^* \to \mathbf{F}_p^*$ as $\phi(r_0) = log_{\gamma'}(\gamma'')$; $r_0 \in \vec{N}$, γ', γ'' are non-trivial generators of $\mathbf{F}_p^*$. Thus, the secret key are the values of p, l, γ'' & r_0. To encrypt a message, define composition of matrix as $M_{2l^2}(A * B) \to M_{2l^2}(C)$, where A is a message block matrix, B is a cyclotomic matrix w.r.t. $\gamma' \in \mathbf{F}_p^*$ and C is the ciphertext matrix. Other way one can define $M_{2l^2}(B * A) \to M_{2l^2}(C)$. Therefore, the length of the ciphertext in CAC is equal to $2l^2$.

To decrypt a message, an algorithm is required to expand the secret keys provided by the secret values. Therefore, the Algorithm 4 is utilized for this purpose.

Algorithm 4 Secrete key expansion.

SECRET INPUT: The values of p, l, r_0 and γ''
Algorithm 1
Algorithm 2

The main purpose, to utilize the above algorithm is to construct a non-singular cyclotomic matrix of order $2l^2$ w.r.t. non-trivial generator γ'' ($\gamma'' \neq \gamma'$) in $\mathbf{F}_p^*$. Now to decrypt the message, we define inverse composition relation of matrices, which is $M_{2l^2}(C * Z) \to M_{2l^2}(A)$, where matrix Z is obtain by some efficient algebraic computation of matrix. Other way one can define $M_{2l^2}(Z * C) \rightarrow M_{2l^2}(A)$ respectively.

4.1 Determination of matrix Z

The following steps have been taken for the determination of matrix Z.

1. Determine the equality of cyclotomic matrix of order $2l^2$ corresponding to the secret values of p & l, which is perform by Algorithm 1.

2. Each entry of equality of cyclotomic matrix is multiplied by r_0.

3. Compute the inverse of equality of cyclotomic matrix generated in step 2.

4. Finally, on substitution the values of the generated cyclotomic matrix corresponding to γ'' to an inverse matrix in step 3.

The following two algorithms (i.e. Algorithm 5 & 6) are utilized to encrypt and decrypt a message in the proposed CAC, respectively.

Algorithm 5 Encryption.

1: Transfer the plain text (message) into its numerical value and store in matrix of order $2l^2$
2: PUBLIC INPUT: The values of p, l and γ'
3: Execute Algorithm 3
4: Check: Generated cyclotomic matrix in step 3 is non-singular
5: Cipher matrix: Multiply cyclotomic matrix and the matrix generated in step 1
6: Ciphertext: The corresponding text values of matrix generated in step 5

Algorithm 6 Decryption.

1: Input: The cipher matrix/ciphertext
2: Execute Algorithm 4
3: Each entries of equality of cyclotomic matrix (i.e. output matrix of Algorithm 1) is multiply by r_0. The entries of the generated matrix are pair of cyclotomic number
4: Compute the inverse of generated matrix in step 3 and substitute the value of each pair of cyclotomic number from generated matrix in step 2
5: Now multiply the cipher text matrix to generated matrix in step 4, we get back to the original plain text message.

4.2 Computational complexity of the CAC

In this section, we would validate the computational complexity of the proposed CAC. The computational complexity measures the amount of computational effort required, by the best as of now known techniques, to break a system [2]. However, it is exceptionally hard to demonstrate the computational complexity of public-key cryptosystems [2, 3]. For instance, if the public modulus of RSA is factored into its prime components, at that point the RSA is broken. Be that as it may, it is not demonstrated that breaking RSA is identical to factoring its modulus [41]. Here, we study the computational complexity of the CAC by providing arguments related to the inversion of the one-way function in CAC to a best known computational algorithm. The complexity of anonymous decryption could be understood as; if we assume that an attacker wants to recover the secret key by using all the information's available to them. Then they need to solve the discrete logarithm problem (DLP) to find the secret key followed by a number of steps described in Algorithm 6. Since, the one-way function is define analogous to discrete logarithm problem (DLP). However, although most mathematicians and computer scientists believe that the DLP is unsolvable [42]. The complexity of the DLP depends on the cyclic group. It is believed to be a hard problem for the multiplicative group of a finite field of large cardinality. Therefore even determining the very first step is nearly unsolvable.

If it is the case that somehow attacker manages to solve the DLP, then they have to determine Eq. (1) and calculate all the solutions corresponding to different pairs $(a, b)_{2l^2}$. Further, it is required to determine the relation matrix based on equality relation among the solutions of Eq. (1). Where entries of the relation matrix are the two-tuple structure of $(a, b)_{2l^2}$. Finally, entries of inverse of the relation matrix are required to replace through the implication of DLP.

Here we could observe the computational complexity as it increases with the value of p and $2l^2$. Therefore it is nearly impossible to determine the secret key for a large value of p and $2l^2$; hence uphold the secure formulation claim of the proposed work.

4.3 An example of the CAC

In this section, we provide an example for the proposed CAC. The example is designed according to guidelines described in Section 4. The main purpose of this example is to show the reliability of our cryptosystem. It is important to note that this example is non-viable for the proposed CAC, since the values of the parameters are too small.

Example 1 Let us consider $2l^2 = 8$ (i.e. $l = 2$) and $p = 17$. Suppose we want to send a message X whose numerical value store in matrix $\mathbf{A}$ of order 8.

$$\mathbf{A} = \begin{bmatrix} 2 & 3 & 5 & 9 & 8 & 0 & 2 & 1 \\ 1 & 5 & 9 & 2 & 9 & 3 & 0 & 5 \\ 2 & 1 & 3 & 2 & 5 & 6 & 8 & 7 \\ 5 & 3 & 0 & 7 & 8 & 7 & 3 & 1 \\ 4 & 2 & 3 & 1 & 9 & 8 & 7 & 3 \\ 0 & 9 & 2 & 3 & 5 & 6 & 8 & 9 \\ 1 & 0 & 2 & 9 & 6 & 7 & 9 & 8 \\ 9 & 1 & 3 & 2 & 4 & 4 & 5 & 6 \end{bmatrix}$$

We choose two distinct non-trivial generators of a set of generator in $\mathbf{F}_{17}^*$ (the set of generator is obtain by employing Algorithm 2), say $\gamma' = 11$ and $\gamma'' = 3$. Now, we evaluate the complex relation between these chosen generators, which can perform by DLP. One can write $3^7 = 11 \pmod{17}$. Consider that $r_0 = 7$. The public key is the public values $l = 2$, $p = 17$ & $\gamma' = 11$ and the private key is the secret values $l = 2$, $p = 17$, $r_0 = 7$ & $\gamma'' = 3$. The public values generated cyclotomic matrix of order 8 as required, which is

$$\mathbf{B}_3 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \end{bmatrix}$$

Determinant of $\mathbf{B}_3$ is equal to 1, implies non-singular. Now we encrypt the message $\mathbf{A}$ by multiplying matrix $\mathbf{B}_3$ and $\mathbf{A}$, which is as follows:

$$\mathbf{C} = \mathbf{B}_3 \times \mathbf{A} = \begin{bmatrix} 2 & 1 & 3 & 2 & 5 & 6 & 8 & 7 \\ 5 & 12 & 2 & 10 & 13 & 13 & 11 & 10 \\ 11 & 4 & 8 & 11 & 12 & 4 & 7 & 7 \\ 5 & 7 & 12 & 3 & 18 & 11 & 7 & 8 \\ 14 & 4 & 3 & 9 & 12 & 11 & 8 & 7 \\ 2 & 5 & 11 & 11 & 15 & 10 & 9 & 13 \\ 1 & 9 & 4 & 12 & 11 & 13 & 17 & 17 \\ 6 & 3 & 6 & 3 & 14 & 14 & 15 & 10 \end{bmatrix}$$

The matrix $\mathbf{C}$ is a ciphertext matrix. To transmit the message, entries of the matrix converted into text. To decrypt the message, first, we expand the secret keys which are performed by Algorithm 4. It generates a non-singular cyclotomic matrix of order 8, which is shown by matrix $\mathbf{B}_0$. Now each entry of equality of cyclotomic matrix (i.e. output matrix of Algorithm 1) is multiplied by $r_0 = 7$. We get matrix D whose entries are pair of cyclotomic numbers.

$$\mathbf{D} = \begin{bmatrix} (0,0) & (0,7) & (0,6) & (0,5) & (0,4) & (0,3) & (0,2) & (0,1) \\ (0,7) & (0,1) & (1,2) & (1,6) & (1,5) & (1,4) & (1,3) & (1,2) \\ (0,6) & (1,2) & (0,2) & (1,3) & (2,4) & (2,5) & (2,4) & (1,6) \\ (0,5) & (1,6) & (1,3) & (0,3) & (1,4) & (2,5) & (2,5) & (1,5) \\ (0,4) & (1,5) & (2,4) & (1,4) & (0,4) & (1,5) & (2,4) & (1,4) \\ (0,3) & (1,4) & (2,5) & (2,5) & (1,5) & (0,5) & (1,6) & (1,3) \\ (0,2) & (1,3) & (2,4) & (2,5) & (2,4) & (1,6) & (0,6) & (1,2) \\ (0,1) & (1,2) & (1,6) & (1,5) & (1,4) & (1,3) & (1,2) & (0,7) \end{bmatrix}$$

Now compute the inverse of $\mathbf{D}$ and substitute the value from $\mathbf{B}_0$ to each pair of cyclotomic numbers. The matrix becomes

$$\mathbf{D}^* = \begin{bmatrix} -1 & 1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & -1 & 0 & 1 & -1 & 1 \\ -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & -1 & 1 & -1 \\ -1 & 0 & 0 & -1 & 0 & 1 & 0 & 1 \\ 1 & -1 & 0 & 1 & 1 & -1 & 1 & -1 \end{bmatrix}$$

Finally, we obtain $\mathbf{D}^* \times \mathbf{C} = \mathbf{A}$.

5. The complexity of CAC

Time and space are usually prominent factors to establish the effectiveness of security solutions. In the before seen sections, we have established the computational difficulty to break the proposed work. Further, we would demonstrate the complexity of the solution in terms of worst-case running time.

The time complexity of Algorithm 1 in worst case is $\mathcal{O}(e^2)$. Since formation of matrix of order e and Update_Table() individually will take $\mathcal{O}(e^2)$. In algorithm 2, **for** loop in line number 9, 15, and 17 contributes $\mathcal{O}(e^3)$ in worst case. Since,

$$e = \frac{p-1}{k}$$
$$\Rightarrow e^3 = \left(\frac{p-1}{k}\right)^3 \equiv \left(\frac{p^3}{k^3}\right)$$

Since k is a positive integer, therefore when k attains its minimum value i.e. 1,

$$\frac{p^3}{k^3} \equiv p^3 \equiv e^3.$$

For any higher value of k, there is guarantee that

$$\frac{p^3}{k^3} < e^3.$$

Hence, we conclude that Algorithm 2 can take $\mathcal{O}(e^3)$ in worst case.

Similarly, in Algorithm 3, **for** loop in line number 4, 5, 6, 7 contributes $e.\ e.\ k.\ k$ or say $\mathcal{O}(e^2k^2)$ running time in worst case. Using similar analogy as in case of Algorithm 2, worst case complexity will be $\mathcal{O}(e^2)$.

5.1 Encryption

Encryption as expressed in Algorithm 5 constitutes of three logical divisions and the complexity of encryption would be the sum of the complexity of its part. The state divisions within are as follows;

1. Generating cyclotomic matrix

2. Checking the singularity of the cyclotomic matrix.

3. Multiplication of generated cyclotomic matrix and matrix corresponds to plain text.

Starting from the generation of the cyclotomic matrix, comprises the total complexity $\mathcal{O}(e^2)$ as stated earlier. Further, checking singularity involves the computation of determinants of the matrix of order e. In worst case computing determinant of a matrix of order n by fast algorithm [43] takes $\mathcal{O}(n^{2.373})$. Hence, singularity of the cyclotomic matrix of order e could be computed in $\mathcal{O}(e^{2.373})$ time. Finally, multiplication of cyclotomic matrix of order e and matrix corresponds to plain text of order e will take $\mathcal{O}\left(e^{2.3728639}\right)$ time. Therefore, Complexity of Encryption would become $\mathcal{O}(e^2) + \mathcal{O}(e^{2.373}) + \mathcal{O}\left(e^{2.3728639}\right) \equiv \mathcal{O}(e^{2.373})$. Thus a polynomial time complexity seems to be quite worthwhile.

5.2 Decryption

Decryption as expressed in Algorithm 6 that include Algorithm 4 which sums the complexity of Algorithm 1 and 3, therefore takes $\mathcal{O}(e^2) + \mathcal{O}(e^2) \equiv \mathcal{O}(e^2)$ time. Further, multiplication of cyclotomic matrix of order e by a constant value r_0, therefore yield $\mathcal{O}(e^2)$ complexity. Likewise, inverse of a matrix of order n can be computed by a fast algorithm [43] in $\mathcal{O}(n^{2.373})$, therefore, inverse of generated matrix of order e could be computed in $\mathcal{O}(e^{2.373})$ time. Finally multiplication of two matrix of order e could be computed in $\mathcal{O}\left(e^{2.3728639}\right)$ by best known algorithm [44] till date. Therefore, Complexity of decryption would be $\mathcal{O}(e^2) + \mathcal{O}(e^2) + \mathcal{O}(e^{2.373}) + \mathcal{O}\left(e^{2.3728639}\right)$, which becomes $\mathcal{O}(e^{2.373})$.

6. Conclusion

In this chapter, we have introduced a secured asymmetric key cryptography model applying the principle of cyclotomic numbers over a finite field. Procedure to generate cyclotomic matrix along with public & private key have been presented, where the relation between the public & private key has acquired by discrete logarithm problem (DLP). Finally, a convincing argument to strengthen the claim has been presented followed by the method of encryption, decryption & a numerical example.

Acknowledgements

The authors are thankful and acknowledge the Central University of Jharkhand, Ranchi, Jharkhand for providing the necessary facilities to carry out this research.

Mathematics Subject Classification (2010)

11T22; 11T71; 94A60; 11T24

Author details

Md. Helal Ahmed[1], Jagmohan Tanti[1*] and Sumant Pushp[2]

1 Department of Mathematics, Central University of Jharkhand, Ranchi, India

2 Department of Computer Science and Technology, Tezpur University, Assam, India

*Address all correspondence to: jagmohan.t@gmail.com

References

[1] Diffie, W., Hellman, M.: New directions in cryptography. IEEE transactions on Information Theory **22** (6), 644–654 (1976)

[2] Miller, V.S.: Use of elliptic curves in cryptography. In: Conference on the theory and application of cryptographic techniques, pp. 417–426. Springer (1985)

[3] Wiener, M.J., Zuccherato, R.J.: Faster attacks on elliptic curve cryptosystems. In: International workshop on selected areas in cryptography, pp. 190–200. Springer (1998)

[4] Ahmad, J.I., Din, R., Ahmad, M. Analysis review on public key cryptography algorithms. International Journal of Electrical and Computer Engineering (IJECE) **12**(2), 447–454 (2018)

[5] Korzhik, V.I., Turkin, A.I.: Cryptanalysis of mcelieces public-key cryptosystem. In: Workshop on the Theory and Application of of Cryptographic Techniques, pp. 68–70. Springer (1991)

[6] Razborov, A.A., Rudich, S.: Natural proofs. Journal of Computer and System Sciences **55**(1), 24–35 (1997)

[7] Shirolkar, D., Katre, S.: Jacobi sums and cyclotomic numbers of order l2. Acta Arithmetica **1**(147), 33–49 (2011)

[8] Menezes, A.J., Katz, J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryptography. CRC press (1996)

[9] ElGamal, T.: A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory **31** (4), 469–472 (1985)

[10] Bruce, S. Applied cryptography. 2nd John Wiley and Sons, Inc (1996)

[11] Koblitz, N., Menezes, A.J.: A survey of public-key cryptosystems. SIAM review **46**(4), 599–634 (2004)

[12] Ourivski, A.V., Johansson, T.: New technique for decoding codes in the rank metric and its cryptography applications. Problems of Information Transmission **38**(3), 237–246 (2002)

[13] Johnson, D., Menezes, A.: The elliptic curve digital signature algorithm (ecdsa) (1999) 21. Johnson, D., Menezes, A., Vanstone, S.: The elliptic curve digital signature algorithm (ecdsa). International journal of information security **1**(1), 36–63 (2001)

[14] Katre, S., Rajwade, A.: Complete solution of the cyclotomic problem in $\mathbf{F}q$ for any prime modulus $l, q = p^a$, $\mathrm{p} \equiv 1(\mathrm{mod}\, 1)$. Acta Arithmetica **45**(3), 183–199 (1985)

[15] Zuccherato, R.: Using a pki based upon elliptic curve cryptography: Examining the benefits and difficulties. Entrust-Securing Digital Identities and Information (2003).

[16] De Win, E., Mister, S., Preneel, B., Wiener, M.: On the performance of signature schemes based on elliptic curves. In: International Algorithmic Number Theory Symposium, pp. 252–266. Springer (1998)

[17] Meier, A.V.: The elgamal cryptosystem (2005)

[18] Davida, G.I., Walter, G.G.: A public key analog gyptosystem. In: Advances in CryptologyEUROCRYPT87

[19] Loidreau, P.: Designing a rank metric based mceliece cryptosystem. In: International Workshop on Post-

Quantum Cryptography, pp. 142–152. Springer (2010)

[20] Pollard, J.M.: Factoring with cubic integers. In: The development of the number field sieve, pp. 4–10. Springer (1993)

[21] Lau, T.S.C., Tan, C.H.: A new technique in rank metric code-based encryption. Cryptography **2**(4), 32 (2018)

[22] Sidelnikov, V.M., Shestakov, S.O.: On insecurity of cryptosystems based on generalized reed-solomon codes. Discrete Mathematics and Applications **2**(4), 439–444 (1992)

[23] Stinson, D.R., Paterson, M.: Cryptography: theory and practice. CRC press (2018)

[24] Gabidulin, E.M.: Theory of codes with maximum rank distance. Problemy Peredachi Informatsii **21**(1), 3–16 (1985)

[25] Canteaut, A., Chabaud, F.: A new algorithm for finding minimum-weight words in a linear code: application to mceliece's cryptosystem and to narrow-sense bch codes of length 511. IEEE Transactions on Information Theory **44** (1), 367–378 (1998)

[26] Chabaud, F., Stern, J.: The cryptographic security of the syndrome decoding problem for rank distance codes. In: International Conference on the Theory and Application of Cryptology and Information Security, pp. 368–381. Springer (1996)

[27] Overbeck, R.: Structural attacks for public key cryptosystems based on gabidulin codes. Journal of Cryptology **21**(2), 280–301 (2008)

[28] Gibson, J.K.: Severely denting the gabidulin version of the mceliece public key cryptosystem. Designs, Codes and Cryptography **6**(1), 37–45 (1995)

[29] Gibson, K.: The security of the gabidulin public key cryptosystem. In: International Conference on the Theory and Applications of Cryptographic Techniques, pp. 212–223. Springer (1996)

[30] Park, C.S.: Improving code rate of mceliece's public-key cryptosystem. Electronics Letters **25**(21), 1466–1467 (1989)

[31] Gabidulin, E., Ourivski, A.: Modified gpt pkc with right scrambler. In: International workshop on coding and cryptography (Paris, 8-12 January 2001), pp. 233–242 (2001)

[32] Gabidulin, E.M., Ourivski, A.V., Honary, B., Ammar, B.: Reducible rank codes and their applications to cryptography. IEEE Transactions on Information Theory **49**(12), 3289–3293 (2003)

[33] McEliece, R.J.: A public-key cryptosystem based on algebraic coding theory. Coding Thv **4244**, 114–116 (1978)

[34] Le Gall, F.: Powers of tensors and fast matrix multiplication. In: Proceedings of the 39th international symposium on symbolic and algebraic computation, pp. 296–303 (2014)

[35] Acharya, V.V., Katre, S. Cyclotomic numbers of order 2l, l an odd prime. Acta Arithmetica **69**(1), 51–74 (1995)

[36] Ahmed, M.H., Tanti, J. Computation of jacobi sums and cyclotomic numbers with reduced complexity. Bulletin of Pure & Applied Sciences-Mathematics and Statistics **38** (1), 466–470 (2019)

[37] Ahmed, M.H., Tanti, J. Cyclotomic numbers and jacobi sums: A survey. In: Class Groups of Number Fields and Related Topics, pp. 119–140. Springer (2020)

[38] Ahmed, M.H., Tanti, J., Hoque, A. Complete solution to cyclotomy of order $2l^2$ with prime l. The Ramanujan Journal **53**(3), 529–550 (2020)

[39] Koblitz, N.: Elliptic curve cryptosystems. Mathematics of computation **48**(177), 203 209 (1987)

[40] Sidelnikov, V.M., Shestakov, S.O.: On encryption based on generalized reedsolomon codes. Diskretnaya Math **4**, 57–63 (1992)

[41] Goldwasser, S., Bellare, M.: Lecture notes on cryptography. Available: http://www.cs.ucsd.edu/users/mihir/papers/gb.html (2008)

[42] Schneier, B.: Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons (2007)

[43] Aho, A.V., Hopcroft, J.E. The design and analysis of computer algorithms. Pearson Education India (1974).

[44] Lin, M.C., Chang, T.C., Fu, H.L.: Information rate of mceliece's public-key cryptosystem. Electronics Letters **26** (1), 16–18 (1990)