Available online at http://scik.org
J. Math. Comput. Sci. 10 (2020), No. 6, 2408-2421
https://doi.org/10.28919/jmcs/4882
ISSN: 1927-5307

A PUBLIC KEY CRYPTOSYSTEM BASED ON LATTICE MATRICES

RAJESH GUDEPU*, DPRV SUBBA RAO

Department of Mathematics, ICFAI University, IFHE HYDERABAD-501203, India

Abstract. In this paper, we have developed a public key cryptosystem by using large abelian group of general linear group over bounded distributive lattice. We have defined automorphisms on lattice matrices by the definition lattice automorphisms. We have replaced the exponentiation by conjugation automorphisms, which are mainly used to define the public and private keys and which allows the calculations to be fast and effective. We also talk about different security aspects against known attacks and it is shown that the cryptosystem is highly secure. We have given the proposed scheme with counter example.

Keywords: automorphism; distributive lattice; general linear group; orthogonal matrix and public key cryptosystem.

2010 AMS Subject Classification: 06D99, 15B99, 94A60.

1. INTRODUCTION

Public-key cryptosystem was introduced by Whitfield Diffie and Martin Hellman [3] in 1976. After that many PKC have been proposed and broken. In 1978, Rivest-Shamir-Adleman [10] introduces the first practical Public key cryptosystem (RSA). In 1985, another practical PKC introduced by ElGamal [4]. Later many other PKCs introduced by many authors which can be seen in [7, 8 and 9]. In 2019, Z.Y. Karatas, E. Luy and B.Gonen [12] introduces a PKC based

*Corresponding author
E-mail address: rajeshgudepu9@gmail.com
Received July 26, 2020

on abelian group $\left(H = \left\{ \begin{pmatrix} a_1 & 0 & 0 & \dots & 0 \\ a_2 & a_1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & 0 \\ a_{k-1} & \dots & a_2 & a_1 & 0 \\ a_k & a_{k-1} & \dots & a_2 & a_1 \end{pmatrix} / \, a_i \in Z_n,\, a_1^k \in \mathbb{Z}_n^*,\, 1 \leq i \leq k \right\}\right)$ of general linear group $\mathrm{GL}(k, \mathbb{Z}_n)$) where $\mathbb{Z}_n$ is the residue ring and $\mathbb{Z}_n^*$ is the set of elemnts in $\mathbb{Z}_n$ with a multiplicative inverse. In this cryptosysetems, the author choose randomly two matrices from the abelian group and define encryption and decryption using this matrices but they did not use any exponentiation of matrices.

In present work, we have proposed Public Key Cryptosystem by using abelian subgroup of general linear group over distributive latttice with 0 and 1. We define public and private keys by using commutative automorphisms on lattice matrices.

In Sect. 2, we will discuss some terms used in public key cryptography and some basic definitions of lattice as well as orthogonal matrix which will be used in next sections.

In section 3. As a different approach to Shmatkov V D [11], we have defined automorphisms on matrices over distributive lattices with 0 and 1.

In section 4. we have given the proposed scheme of PKC on lattice matrices.

In section 5. we have given a counter example for our proposed scheme.

In section 6. we have discussed the security analysis of the cryptosystem.

2. PRELIMINARIES

Throughout this paper $\mathbb{N}$ denotes the set of non zero natural numbers.

We recall some basic definitions on cryptography. For details see [2].

Public-key cryptography is a cryptographic system that uses pairs of keys: public keys and private keys.

Public key encryption, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. This is used in an attempt to ensure confidentiality.

A public-key encryption scheme has six components:

(1) **Plaintext**: Which is a message in a form that is easily readable by humans.

(2) **Encryption algorithm**: Which is the process of encoding a message or information (Plaintext) in such a way that only authorized parties can access it.

(3) **Public key**: Which are known to every one.

(4) **Private key**: Which are known only to the owner.

(5) **Cipher text**: Which is the result of encryption performed on plaintext.

(6) **Decryption algorithm**: Which is the process of converting message (Ciphertext) into its original form (Plaintext).

We recall some basic definitions and results on lattice theory, lattice matrices. For details see [1], [5] and [6].

Definition 2.1 (1)**.** A partially ordered set $(L,\leq)$ is a **lattice** if for all $a,b \in L$, the least upper bound of a,b and the greatest lower bound of a,b exist in L. For any $a,b \in L$, the least upper bound and the greatest lower bound are denoted by $a \vee b$ and $a \wedge b$ (or ab), respectively. An element $a \in L$ is called greatest element of L if $\alpha \leq a$, for all $\alpha \in L$. An element $b \in L$ is called least element of L if $b \leq \alpha$, for all $\alpha \in L$. We use 1 and 0 to denote the greatest element and the least element of L, respectively. A lattice L is a distributive lattice, if for any $a,b,c \in L$,

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$$

$$a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$$

Throughout this paper, unless otherwise stated, we assume that L is a distributive lattice with the greatest element 1 and the least element 0.

Let $M_n(L)$ be the set of $n \times n$ ($n \in \mathbb{N}$) matrices over L, the elements of $M_n(L)$ denoted by capital letters and suppose $A \in M_n(L)$, then the $(i,j)^{th}$ entry of A is denoted by a_{ij}. Giveon [5] calls them lattice matrices.

The following are due to Giveon [5] for the lattice matrices $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}] \in M_n(L)$, where $a_{ij}, b_{ij}, c_{ij} \in L$,$1 \leq i,j \leq n$

- $A \leq B$ if and only if $a_{ij} \leq b_{ij}$

- $A+B=C$ if and only if $c_{ij}=a_{ij}\vee b_{ij}$
- $A\wedge B=C$ if and only if $c_{ij}=a_{ij}\wedge b_{ij}=a_{ij}b_{ij}$
- $A\cdot B=AB=C$ if and only if $c_{ij}=\vee_{k=1}^{n}(a_{ik}\wedge b_{kj})$
- $A^T=C$ if and only if $c_{ij}=a_{ji}$
- for $\alpha\in L,\alpha A=\alpha\cdot A=C$, if and only if $c_{ij}=\alpha a_{ij}$
- $A^0=I$, where I is the identity matrix, $A^{K+1}=A^KA$, $O=[0_{ij}],0_{ij}=0$, $E=[e_{ij}],e_{ij}=1$, $1\leq i,j\leq n$,
- $A(BC)=(AB)C,AI=IA=A,AO=OA=O$.
- $A(B+C)=AB+AC,(A+B)C=AC+BC$,if $A\leq B$ and $C\leq D$ then $AC\leq BD$.
- $(A+B)^T=A^T+B^T,(A\wedge B)^T=A^T\wedge B^T,(AB)^T=B^TA^T,((A)^T)^T=A$.
- $M_n(L)$ is a distributive lattice with least element zero as O and greatest element one as E with respect to $\wedge$ and $\vee$.

Definition 2.2 (5)**.** A matrix $A\in M_n(L)$ is orthogonal if and only if each row and each column is orthogonal decomposition of 1 in L.

Theorem 2.3 (5)**.** *$A\in M_n(L)$ is invertible if and only if A is orthogonal.*

Definition 2.4 (5)**.** The set of all invertible order-n square matrices over L is a group under lattice matrix multiplication. This group is called the general linear group of degree n and is denoted GL(n,L), here for our connivent we denote it as G.

Definition 2.5 (5)**.** Let $(L,\leq,\wedge,\vee)$ be a lattice. Then a mapping $\phi:L\to L$ is automorphism if for all $a,b\in L$ it satisfy:

(1) $\phi(0)=0$.

(2) $\phi(1)=1$.

(3) $\phi(a\vee b)=\phi(a)\vee\phi(b)$.

(4) $\phi(a\wedge b)=\phi(a)\wedge\phi(b)$.

(5) if $a\leq b$, then $\phi(a)\leq\phi(b)$.

(6) ϕ is one - one

(7) ϕ is onto

3. AUTOMORPHISMS ON $M_n(L)$

In this section, we construct the general linear group and abelian subgroups of $M_n(L)$ with matrix multiplication operator. As a different approach to V.D.Shmatkov [11], we have proposed an automorphism on $M_n(L)$ and we have discussed about commutative automorphism on $M_n(L)$.

Let us denote the following:

$M_n(L)$ = The set of all $n \times n$ matrices over $L = \left\{ A = [a_{ij}]_{n\times n} / a_{ij} \in L \right\}$.

G = The set of all invertible (orthogonal) matrices over $M_n(L) = \left\{ P \in L \,/\, PP^T = P^T P = I \right\}$

C = The subset of G in which matrix multiplication is commutative.

Theorem 3.1. *If L is a distributive lattice with 0 and 1. Then*

(1) G forms a group (general linear group)

(2) C forms an abelian subgroup of G with the operation matrix multiplication.

Proof. Suppose L is a distributive lattice with 0 and 1 and $M_n(L)$ is the set of all $n \times n$ matrices over L.

(1) Let G be The set of all invertible (orthogonal) matrices over $M_n(L)$.

- If $P, Q \in G$, then $PQ \in G$ (Since the product of orthogonal matrices is again orthogonal.)
- If P, Q and $R \in L$, then $P(QR) = (PQ)R$.
  (Since the matrix multiplication is associative in $M_n(L)$)
- If $P \in G$, then $PI = IP = P$. (Since I is the identity matrix in $M_n(L)$)
- If $P \in G$, then there exist a unique matrix $P^T \in G$ such that $PP^T = P^T P = I$ (where P^T is the inverse of P)

Therefore G forms a group with matrix multiplication.

(2) Let C be the subset of G in which the matrix multiplication is commutative i.e., $P, Q \in C$ such that $PQ = QP$, then we can obtain that $P = Q^T PQ = QPQ^T$ and $Q = P^T QP = PQP^T$

- If $P, Q \in C$, then $PQ \in C$ (Since $(PQ)R = P(RQ) = R(PQ)$, for all $R \in C$)
- If $P \in C$, then $P^T \in C$ (Since $P^T Q = P^T(PQP^T) = QP^T$, for all $Q \in C$)

Therefore C forms an abelian subgroup of G with matrix multiplication.

□

Definition 3.2. A square matrix $A \in M_n(L)$ is said to be **left meet-distributive** if it satisfy $A(X \wedge Y) = AX \wedge AY$, for all $X, Y \in M_n(L)$ and is said to be **right meet-distributive** if it satisfy $(X \wedge Y)A = XA \wedge YA$, for all $X, Y \in M_n(L)$. A matrix is said to be **meet-distributive** if which is both left meet and right meet distributive.

Example 3.3. *Consider the lattice L = {0, a, b, c, d,1 } where the Hasse diagram of L is shown below:*

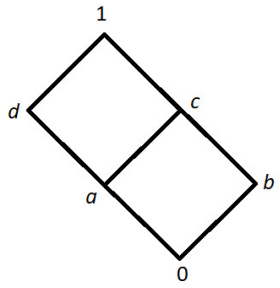

FIGURE 1

$$\text{Let } A = \begin{pmatrix} d & a \\ a & b \end{pmatrix}, X = \begin{pmatrix} a & d \\ c & b \end{pmatrix}, Y = \begin{pmatrix} a & c \\ 1 & d \end{pmatrix}$$

$$\text{So, } A(X \wedge Y) = \begin{pmatrix} d & a \\ a & b \end{pmatrix} \begin{pmatrix} a & b \\ c & b \end{pmatrix} = \begin{pmatrix} a & b \\ c & b \end{pmatrix}$$

$$\text{and } AX \wedge AY = \begin{pmatrix} a & d \\ c & b \end{pmatrix} \wedge \begin{pmatrix} a & b \\ c & c \end{pmatrix} = \begin{pmatrix} a & b \\ c & b \end{pmatrix}$$

Clearly A is left meet-distributive matrix.

$$(X \wedge Y)A = \begin{pmatrix} a & b \\ c & b \end{pmatrix} \begin{pmatrix} d & a \\ a & b \end{pmatrix} = \begin{pmatrix} 0 & c \\ b & c \end{pmatrix}$$

$$\text{and } XA \wedge YA = \begin{pmatrix} 0 & c \\ b & c \end{pmatrix} \wedge \begin{pmatrix} a & c \\ d & c \end{pmatrix} = \begin{pmatrix} o & c \\ b & c \end{pmatrix}$$

Clearly A is right meet-distributive matrix.

Therefore A is meet-distributive matrix.

Theorem 3.4. *A square lattice matrix $P = [p_{ij}]$ over L is left meet-distributive if and only if, for all i, $p_{ij} \wedge p_{ik}$=0, $j \neq k$.*

Theorem 3.5. *A square lattice matrix $P = [p_{ij}]$ over L is right meet-distributive if and only if, for all j, $p_{ij} \wedge p_{kj}$=0, $i \neq k$.*

Since $M_n(L)$ is a distributive lattice. Then we propose an automorphism on $M_n(L)$ by using the definition of lattice automorphism. We will use these automorphism, in section 4, for encryption and decryption in our proposed public key cryptosystem scheme.

Proposition 3.6. *For $P \in G$ and $A \in M_n(L)$, the mapping $\phi : M_n(L) \to M_n(L)$ defined by $\phi(A) = PAP^T$ is an automorphism of $M_n(L)$.*

Proof. Suppose $\phi : M_n(L) \to M_n(L)$ defined by $\phi(A) = PAP^T$, for all $P \in G, A \in M_n(L)$. Then

(1) $\phi(O) = POP^T = O$, O is the zero matrix in $M_n(L)$.

(2) $\phi(E) = PEP^T = E$, E is the one matrix in $M_n(L)$.

(3) $\phi(A \wedge B) = P(A \wedge B)P^T = (PAP^T) \wedge (PBP^T) = \phi(A) \wedge \phi(B)$. (Since P is meet distributive)

(4) $\phi(A \vee B) = P(A \vee B)P^T = (PAP^T) \vee (PBP^T) = \phi(A) \vee \phi(B)$.

(5) $\phi(AB) = P(AB)P^T = (PAP^T PBP^T) = \phi(A)\phi(B)$.

(6) If $A \leq B$, then $\phi(A) \leq \phi(B)$.

Therefore ϕ is homomorphism.

(7) ϕ is one - one:

Let

$$\phi(A) = \phi(B)$$

$$PAP^T = PBP^T$$

$$P^T PAP^T P = P^T PBP^T P$$

$$A = B$$

(8) ϕ is onto: Let $B \in M_n(L)$.

For $P \in G$, So that $P^T BP \in M_n(L)$

Consider,

$$B = PP^T BPP^T$$

$$= PAP^T \, (say P^T BP = A)$$

$$= \phi(A)$$

Therefore ϕ is an automorphism.

□

Remark 3.7. The inverse of an automorphism is an automorphism, and composition of two automorphisms is again an automorphism.

Next we have proposed the case of commutativity for above automorphisms. In section 4, we will use these commutative automorphisms for generating the key in our proposed public key cryptosystem scheme.

Proposition 3.8. *If $P, Q \in C$ and $A \in M_n(L)$, the mapping $\phi, \psi : M_n(L) \to M_n(L)$ defined by $\phi(A) = PAP^T$, $\psi(A) = QAQ^T$, then ϕ and ψ commutative automorphisms of $M_n(L)$.*

Proof. Let $P, Q \in C$ and $A \in M_n(L)$.

Suppose $\phi : A \to PAP^T$, $\psi : A \to QAQ^T$ are two mappings on $M_n(L)$.

From the proposition 3.2, clearly ϕ and ψ are automorphisms on $M_n(L)$.

Now consider,

$\phi\psi(A) = \phi(QAQ^T) = PQAQ^TP^T = PQA(PQ)^T$ and

$\psi\phi(A) = \psi(PAP^T) = QPAP^TQ^T = QPA(QP)^T = PQA(PQ)^T$ (Since $P,Q \in C$)

Therefore, ϕ and ψ commutative automorphisms. □

4. MAIN RESULT

Public key cryptosystem based on lattice matrices

In this section, we have proposed a public key cryptosystem scheme, in which the key generation depends on the commutative automorphism on $M_n(L)$ and encryption depends on the automorphism on $M_n(L)$.

The proposed scheme

Key Generation

(1) Choose two matrices P and Q in the subgroup C with $P \neq Q$.

(2) Define two commutative inner product automorphisms of $M_n(L)$. $\phi : A \to PAP^T$ and $\psi : A \to QAQ^T$ for every $A \in M_n(L)$. Clearly ϕ and ψ commute as P and Q commute (By proposition 3.4).

(3) Compute the following automorphisms of $M_n(L)$: $\rho = \phi^2\psi$ and $\sigma = \phi\psi^2$ which are given by

$\rho : A \to (P^2Q)A(P^2Q)^T$, $\sigma : A \to (PQ^2)A(PQ^2)^T$.

Note that ρ and σ commute (By remark 3.3), and $\rho = \phi\psi^{-1}\sigma$, $\sigma = \phi^{-1}\psi\rho$.

(4) Select a random invertible matrix $N \in G$ which does not belong to group C.

(5) Compute the matrices $N^T, \rho(N)$ and $\sigma(N^T)$.

(6) The public key is $(\rho(N), \sigma(N^T))$ and the private key is (P,Q).

Encryption

(1) Represent the plaintext M as a matrix over L, that is, $M \in M_n(L)$.

(2) Choose a random matrix $X \in C$. (Similarly, we choose a new random matrix for every plaintext.)

(3) Define the automorphism $\upsilon : A \to XAX^T$, where $A \in M_n(L)$.

(4) Compute the matrices $\upsilon(\rho(N)), \upsilon(\sigma(N^T))$.

(5) Send the ciphertext: $C = (C_1, C_2) = (\upsilon(\sigma(N^T)), M\upsilon(\rho(N)))$.

Decryption

(1) Compute $d = \phi\psi^{-1}(C_1) = \phi\psi^{-1}(\upsilon(\sigma(N^T))) = \upsilon(\rho(N^T))$.

(2) Compute $C_2 d = M\upsilon(\rho(N))\phi\psi^{-1}(\upsilon(\sigma(N^T))) = M$.

5. EXAMPLE

In this section, we have constructed an example in 3×3 case, to our mentioned public key cryptosystem .

Consider the lattice $L = \{0, a, b, c, d, e, f, g, h, i, j, k, l, m, n, o, p, q, r, s, t, u, v, 1\}$ where the Hasse diagram of L is shown below:

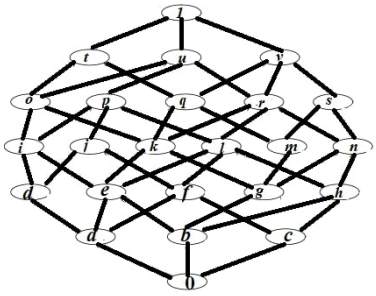

FIGURE 2

Key Generation

(1) Choose two matrices $P = \begin{pmatrix} j & 0 & m \\ m & j & 0 \\ 0 & m & j \end{pmatrix}$ and $Q = \begin{pmatrix} c & t & 0 \\ 0 & c & t \\ t & 0 & c \end{pmatrix}$ in the subgroup C with $P \neq Q$

.

(2) Define two commutative inner product automorphisms of $M_3(L)$

$\phi : A \to PAP^T$ and $\psi : A \to QAQ^T$ for every $A \in M_3(L)$.

(3) Compute the following automorphisms of $M_n(L)$:

$\rho = \phi^2\psi$ and $\sigma = \phi\psi^2$ which are given by

$$\rho : A \to (P^2Q)A(P^2Q)^T,\ \sigma : A \to (PQ^2)A(PQ^2)^T.$$

Note that ρ and σ commute (By remark 3.3), and $\rho = \phi\psi^{-1}\sigma$, $\sigma = \phi^{-1}\psi\rho$.

(4) Select a random matrix $N = \begin{pmatrix} d & c & m \\ m & 0 & j \\ c & t & 0 \end{pmatrix} \in G$ which does not belong to group C.

(5) Compute the matrices $N^T = \begin{pmatrix} d & m & c \\ c & 0 & t \\ m & j & 0 \end{pmatrix}, \rho(N) = \begin{pmatrix} 0 & j & m \\ t & 0 & c \\ c & m & d \end{pmatrix}$ and $\sigma(N^T) = \begin{pmatrix} 0 & m & j \\ c & d & m \\ t & c & 0 \end{pmatrix}$.

(6) The public key is $(\rho(N), \sigma(N^T))$ and the private key is (P, Q).

Encryption

(1) Represent the plaintext $M = \begin{pmatrix} e & i & k \\ h & l & f \\ p & n & u \end{pmatrix}$ as a matrix over L, that is, $M \in M_n(L)$.

(2) Choose a random matrix $X = \begin{pmatrix} s & d & 0 \\ 0 & s & d \\ d & 0 & s \end{pmatrix} \in C$. (Similarly, we choose a new random matrix for every plaintext.)

(3) Define the automorphism $\upsilon : A \to XAX^T$, where $A \in M_n(L)$.

(4) Compute the matrices $\upsilon(\rho(N)) = \begin{pmatrix} 0 & c & t \\ m & d & c \\ j & m & 0 \end{pmatrix}, \upsilon(\sigma(N^T)) = \begin{pmatrix} d & m & c \\ c & 0 & t \\ m & j & 0 \end{pmatrix}$.

(5) Send the ciphertext: $C = (C_1, C_2)$

$$\text{where } C_1 = \upsilon(\sigma(N^T)) = \begin{pmatrix} d & m & c \\ c & 0 & t \\ m & j & 0 \end{pmatrix},$$

$$C_2 = M\upsilon(\rho(N))) = \begin{pmatrix} e & o & e \\ l & f & h \\ u & n & p \end{pmatrix}.$$

Decryption

(1) Compute $d = \phi\psi^{-1}(C_1) = \phi\psi^{-1}(\upsilon(\sigma(N^T))) = \upsilon(\rho(N^T)) = \begin{pmatrix} 0 & m & j \\ c & d & m \\ t & c & 0 \end{pmatrix}$.

(2) Compute $C_2 d = M\upsilon(\rho(N))\phi\psi^{-1}(\upsilon(\sigma(N^T))) = \begin{pmatrix} e & i & k \\ h & l & f \\ p & n & u \end{pmatrix}$.

6. Security Analysis

6.1. A Chiphertext Only Attack. Assume that (C_1, C_2) is the ciphertext of the plaintext M. So, the attacker needs to solve the system

$$C_1 = X\sigma(N^T)X^T$$

$$C_2 = MX\rho(N)X^T.$$

The attacker can compute $C_2C_1 = MX\rho(N)\sigma(N^T)X^T$, and more conveniently, try to solve this system for X and M.

Thus, if L is large bounded distributive lattice not having long sub chain and $n \in \mathbb{N}$ is chosen large enough, then it is infeasible to compute X, and hence M.

Here, the security in the proposed scheme increases significantly as any size of matrices can be chosen which will increase the dimension of the system.

6.2. A Known-Plaintext Attack. Note that for each plaintext M, a specific matrix X is used in the scheme. Hence, it does not matter how many pairs of plaintexts and ciphertexts someone knows, it is infeasible to obtain a plaintext from a corresponding ciphertext. Thus, this attack will not be efficient as well.

6.3. A Chosen Chiphertext Attack. By using this attack, someone can obtain an unknown plaintext. Assume that $C = (C_1, C_2)$ is the corresponding ciphertext of the desired plaintext M. The attacker can choose a random invertible matrix M^* and be given access to the plaintext of the ciphertext (C_1, M^*C_2) which is M^*M. Then the attacker obtains$(M^*)^T M^*M = M$.

However, an elementary modification on the proposed system can be used in order to prevent this type of attack. It is the same idea given in [12]. This problem can be solved by the change $C_2 = X\rho(N)X^T MX\rho(N)X^T$. In decryption, the plaintext can be obtained by $M = dC_2d$ with $d = \phi\psi^{-1}(C_1)$. This change will prevent the proposed system from this type of attack since the matrices M and X do not commute in general.

Conclusion. In this paper, We have defined automorphisms on lattice matrices by the definition lattice automorphism. we have developed a public key cryptosystem by using large abelian group of general linear group over distributive lattice with 0 and 1. We have defined commutative automorphisms to obtain the public key and private key. One can choose the best size for the security and computation time depending on the needs. Also, since exponentiation is not used, the encryption and decryption will be more simple and faster. A counter example has given in section 5.

ACKNOWLEDGMENTS

The authors thank the management of FST, IFHE, Hyderabad for providing the necessary facilities.

CONFLICT OF INTERESTS

The author(s) declare that there is no conflict of interests.

REFERENCES

[1] G. Birkhoff, Lattice Theory, American Mathematical Society, Providence, RI, USA, 3rd edition, 1967.

[2] C. Paar, J. Pelzl, B. Preneel, Understanding cryptography: a textbook for students and practitioners, 2nd corrected printing, Springer, Berlin, 2010.

[3] W. Diffie, M. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory. 22 (1976), 644-654.

[4] T. Elgamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE Trans. Inform. Theory. 31 (1985), 469-472.

[5] Y. Giveon, Lattice matrices, Inform. Control, 7 (1964), 477-84.

[6] G. Gratzer, General lattice theory, Academic Press, New York, 1978.

[7] M. Khan, T. Shah, A Novel Cryptosystem Based on General Linear Group, 3D Res. 6 (2015), 2.

[8] K. Koyama, U.M. Maurer, T. Okamoto, S.A. Vanstone, New Public-Key Schemes Based on Elliptic Curves over the Ring Zn, in: J. Feigenbaum (Ed.), Advances in Cryptology - CRYPTO '91, Springer Berlin Heidelberg, Berlin, Heidelberg, 1992: pp. 252-266.

[9] P. Paillier, Public-Key Cryptosystems Based on Composite Degree Residuosity Classes, in: J. Stern (Ed.), Advances in Cryptology - EUROCRYPT '99, Springer Berlin Heidelberg, Berlin, Heidelberg, 1999: pp. 223-238.

[10] R.L. Rivest, A. Shamir, L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM. 21 (1978), 120-126.

[11] V.D. Shmatkov, Isomorphisms and Automorphisms of Matrix Algebras Over Lattices, J. Math. Sci. 211 (2015), 434-440.

[12] Z.Y. Karatas, E. Luy, B. Gonen, A public key cryptosystem based on matrices, Int. J. Computer Appl. 182 (2019), 47-50.