ROMANIAN JOURNAL OF INFORMATION SCIENCE AND TECHNOLOGY
Volume 21, Number 3, 2018, 210–218

A Homomorphic Property of the Cryptosystems Based on Word Problem

P. Jeyanthi ABISHA[1] and D. Jayaseelan SAMUEL[1]

[1]Department of Mathematics, Madras Christian College,
Chennai - 600059, INDIA
E-mail: abishajeyanthi@mcc.edu.in, jayaseelansamuel@mcc.edu.in

Abstract. There are many cryptosystems in the literature based on formal language theory. Some of them are public key cryptosystems and others are symmetric key cryptosystems. Homomorphic encryption is a form of encryption that allows computations to be carried out on ciphertext, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. In this paper, we discuss a homomorphic property of public key cryptosystems based on word problem. An encryption scheme is probabilistic if when the same message is encrypted several times, different ciphertexts are obtained. A homomorphic property of public key encryption schemes based on word problems along with probabilistic property are used in this paper for constructing an electronic voting scheme.

Key-words: E-voting; Finitely Presented Partially Commutative Groups; Homomorphic Encryption; Public Key Cryptosystems; Word Problem.

1. Introduction

Cryptography is the science of keeping secrets secret. It is the study of sending messages in disguised form so that the intended recipient can remove the disguise and read the message. Diffie and Hellman introduced the concept of Public Key Cryptosystem (PKC) [7]. In public key cryptography, the encryption key is available to everyone and the decryption key is kept secret by the owner. In public key cryptosystems, we are looking for family of functions such that each function f is computable by an efficient algorithm but it is infeasible to compute the pre-images. Such functions are called one-way functions. For each function in that family there is some secret information which enables an efficient computation of the inverse of f. This secret information is called trapdoor information. One-way functions with this property are called trapdoor functions.

In 1984, Wagner and Magyarik [22] proposed a public key cryptosystem based on the word problem. Salomaa has very elegantly formulated [18] the general technique to construct public key cryptosystems based on formal language theory: Choose a difficult (undecidable or intractable) problem Q and a sub problem P, which is solvable in linear time. Shuffle P to obtain P_1, which looks like Q. The manner of shuffling is the trapdoor, which is secret. Use P_1 to encrypt and P to decrypt. There are many cryptosystems in the literature based on formal language theory [2–4, 13–15, 18–20, 22]. In [2], a PKC based on the finitely presented partially commutative group is described and this cryptosystem is used to send picture messages in [1]. In this paper, we discuss a homomorphic property of the cryptosystems based on the word problem and also show how a system of this type can be used for e-voting.

2. Homomorphic Encryption

The homomorphic encryption is a kind of encryption scheme which allows a third party (e.g., cloud, service provider) to perform certain computations on the ciphertext while preserving the features of the function and format of the plaintext. An encryption scheme is said to have the additive homomorphic property if one can obtain $E(m_1 + m_2)$ from $E(m_1)$ and $E(m_2)$ without the knowledge of messages m_1 and m_2.
There are three types of homomorphic encryption schemes: partially homomorphic schemes, fully homomorphic schemes and somewhat homomorphic schemes.

- Partial homomorphic schemes are those in which computations on ciphertexts can be carried out over one operation.
- Fully homomorphic schemes are those in which computations can be carried out on ciphertexts over more than one operation.
- Somewhat homomorphic schemes are fully homomorphic schemes in which the operations can be carried out only a certain finite number of times.

The famous RSA encryption scheme [17] and ElGamal encryption scheme [8] are examples of partial homomorphic schemes which are homomorphic over multiplication. The Goldwasser-Micali scheme [10] which is the first probabilistic public key encryption scheme is homomorphic over addition of binary numbers. In 2009, Gentry [9] constructed a first plausible fully homomorphic encryption based on ideal lattices which is homomorphic with respect to both addition and multiplication. The systems described in [5, 21] are somewhat homomorphic encryption schemes.

The aim of this paper is to examine the homomorphic property in the cryptosystems based on the word problem [1, 2, 19] over the word operation of catenation.

The homomorphic property over catenation is as follows:

$$m_1 \cdot m_2 = D(E(m_1) \cdot E(m_2))$$

where E denotes the encryption algorithm, D denotes the decryption algorithm and $\cdot$ denotes the operation of catenation.

We modify the system described in [2] and check the variant for homomorphic property over catenation and its application for e-voting. Similar results hold good for the systems in [1, 19].

3. PKC on Free Partially Commutative Groups

First, some necessary definitions [2, 19] are recalled and then a variant of the public key cryptosystem [2] on free partially commutative groups is given.

3.1. Basic Definitions

An alphabet Σ is a finite and nonempty set of symbols. By the free monoid Σ^* generated by Σ, we mean the set of all words (over Σ) having catenation as multiplication. This set includes the empty word λ. We set $\Sigma^+ = \Sigma^* \setminus \lambda$, where the subsemigroup Σ^+ of Σ^* is said to be the free semigroup generated by Σ. The length of a word w is denoted by $|w|$. For basic definitions in formal languages theory, we refer to [18].

Definition 3..1. *Given an alphabet Σ, we consider $\Sigma^{-1} = \{a^{-1} \mid a \in \Sigma\}$ and $\Sigma^{\pm 1} = \Sigma \cup \Sigma^{-1}$. A word x in $\Sigma^{\pm 1}$ is called reduced if it does not contain any subword of the form $a^\sigma a^{-\sigma}, a \in \Sigma, \sigma = \pm 1$.*

Definition 3..2. *Let Σ be an alphabet and $\theta = \{(a, b) \mid$ for some $a, b \in \Sigma\}$ be a concurrency relation on Σ. It means that a and b can be commuted. In other words, an occurrence of ab can be replaced by ba and ba by ab. If a word $u \in \Sigma^*$ is obtained from a word $v \in \Sigma^*$ by such a sequence of replacements then we say that u and v are equivalent with respect to the relation θ and it is denoted by $u \equiv_\theta v$ or $u \equiv v$ mod θ .*

Definition 3..3. *A group G, or more precisely, a presentation of the group G, denoted by $G = \langle \Sigma, R\rangle$, is given by an alphabet Σ and a set R of pairs in $(\Sigma^{\pm 1})^* \times \{\lambda\}$ called defining relators of G. If Σ and R are finite, we say that G is a finitely presented group. If $R = \emptyset$, G is called the free group generated by Σ, denoted by $F(\Sigma)$.*

Given a group $G = \langle \Sigma, R\rangle$, we consider the binary relation on $(\Sigma^{\pm 1})^*$ denoted by $\underset{G}{\Longleftrightarrow}$ or simply $\Longleftrightarrow$ and defined as follows: For any $x, y \in (\Sigma^{\pm 1})^*, x \underset{G}{\Longleftrightarrow} y$ if and only if one of the following cases hold.

1. $x = urv, y = uv$ with $(r, \lambda) \in R$ and $u, v \in (\Sigma^{\pm 1})^*$.
2. $x = uv, y = urv$ with $(r, \lambda) \in R$ and $u, v \in (\Sigma^{\pm 1})^*$.
3. $x = ua^\sigma a^{-\sigma} v, y = uv$ with $a \in \Sigma, \sigma = \pm 1, u, v \in (\Sigma^{\pm 1})^*$.
4. $x = uv, y = ua^\sigma a^{-\sigma} v$ with $a \in \Sigma, \sigma = \pm 1, u, v \in (\Sigma^{\pm 1})^*$.

Then we define $\overset{*}{\underset{G}{\Longleftrightarrow}}$ to be the reflexive, transitive closure of $\underset{G}{\Longleftrightarrow}$. It is easy to see that $\overset{*}{\underset{G}{\Longleftrightarrow}}$ is a congruence relation and the quotient $(\Sigma^{\pm 1})^* / \overset{*}{\underset{G}{\Longleftrightarrow}}$ is a group also denoted by G. The congruence class of a word x is denoted by $[x]_G$ or simply $[x]$. Evidently, $x \overset{*}{\underset{G}{\Longleftrightarrow}} y$ if and only if $[x]_G = [y]_G$. We usually write $x =_G y$ instead of $[x]_G = [y]_G$ and say that the words x and y are equal in G. The word problem for a group G consists in deciding for any two words x, y in $(\Sigma^{\pm 1})^*$, whether $x =_G y$ or equivalently in deciding, for any given word x, whether $x =_G \lambda$.

Definition 3..4. *A Thue system T on Σ is a finite subset of $\Sigma^* \times \Sigma^*$. Each member of T is called a rule. The Thue congruence $\overset{*}{\underset{T}{\longleftrightarrow}}$ generated by T is the reflexive, transitive closure of the symmetric relation $\underset{T}{\longleftrightarrow}$, defined as follows: For any u, v such that $(u, v) \in T$ or $(v, u) \in T$ and any $x, y \in \Sigma^*, xuy \longleftrightarrow xvy$. Two strings $w, z \in \Sigma^*$ are congruent with respect to T if and only if $w \overset{*}{\underset{T}{\longleftrightarrow}} z$ where $\overset{*}{\underset{T}{\longleftrightarrow}}$ is the reflexive, transitive closure of $\underset{T}{\longleftrightarrow}$.*

The word problem for the Thue system on Σ is as follows: given any two words x and y in Σ^*, is $x \overset{*}{\underset{T}{\longleftrightarrow}} y$? In general, the word problem is undecidable for Thue systems.

Definition 3..5. *Let Σ be an alphabet and θ_0 be a partially commutative (concurrency) relation on Σ. Let $\theta \subseteq \Sigma^{\pm 1} \times \Sigma^{\pm 1}$ be the extension of θ_0 to $\Sigma^{\pm 1}$:*

$$\theta = \{(a, b), (a^{-1}, b), (a, b^{-1}), (a^{-1}, b^{-1}) \mid (a, b) \in \theta_0\}.$$

This develops the following Thue system T on $\Sigma^{\pm 1}$, where

$$T = \{(aa^{-1}, \lambda), (a^{-1}a, \lambda) \mid a \in \Sigma\} \cup \{(cd, dc) \mid c, d \in \theta\}.$$

T presents the free partially commutative group $G(\theta_0)$. This $G(\theta_0)$ is the finitely generated group $\langle \Sigma, R \rangle$ where the set of defining relators $R = \{(cdc^{-1}d^{-1}, \lambda) : (c, d) \in \theta\}$. If θ_0 is empty, then $G(\theta_0)$ is just the free group on Σ and if θ_0 contains every pair of distinct letters, then $G(\theta_0)$ is the free abelian group on Σ.

A well known result, due to Novikov [16], says that the word problem for finitely presented group is undecidable. But the algorithm solving the word problem for free group is quite simple because for any free group $F(\Sigma)$ and any $x, y \in (\Sigma^{\pm 1})^*, x =_F y$ if and only if x and y can be reduced to the same word. Wrathall [23] proved that the word problem for finitely presented free partially commutative group is decidable in linear time.

Definition 3..6. *Let Σ be an alphabet and $X \subseteq \Sigma^*$. Then, X is said to be a code if whenever $x_1x_2 \ldots x_n = y_1y_2 \ldots y_m$ where $x_i, y_i \in X,\ i = 1, 2, 3, \ldots, n,\ j = 1, 2, \ldots, m$, then m = n and $x_i = y_i$ for all i.*

3.2. Construction of PKC

Let Σ be an alphabet and θ_0 be a partially commutative relation on Σ such that $G(\theta_0)$ is the finitely presented free partially commutative group.

Fix n different reduced words $x_1, x_2, \ldots, x_n$ in $(\Sigma^{\pm 1})^*$ such that

1. $\{x_1, x_2, \ldots, x_n\}$ is a code.
2. The word x_ix_j is reduced without cancellation where $i, j \in \{1, 2, \ldots, n\}$. That is, the last letter of x_i and the first letter of x_j are not inverses of each other.

Let Δ be an alphabet of cardinality much greater than that of Σ. Let g be a morphism from $\Delta^{\pm 1}$ to $\Sigma^{\pm 1} \cup \{\lambda\}$ such that

1. $g(c^{\sigma_1}) = a^{\sigma_2}$ implies $g(c^{-\sigma_1}) = a^{-\sigma_2},\ c \in \Delta,\ \sigma_1, \sigma_2 = \pm 1,\ a \in \Sigma$.

2. If $g(c^{\sigma}) = \lambda$ implies $g(c^{-\sigma}) = \lambda,\ c \in \Delta,\ \sigma = \pm 1$.

3. If $g(c) = a, g(d) = b$ and $(a, b) \in \theta$, then c and d commute where $c, d \in \Delta$.

Select n words $w_1, w_2, \dots, w_n$ from $(\Delta^{\pm 1})^*$ such that $g(w_i) \in [x_i]_G$ where $i \in \{1, 2, \dots, n\}$. Fix a finite subset $\bar{R}$ of $(\Delta^{\pm 1})^* \times \{\lambda\}$ such that if $(uv^{-1}, \lambda) \in \bar{R}$ then one of the following is true:

1. $(g(u)(g(v)^{-1}), \lambda) \in R$.

2. $g(u) =_{G(\theta_0)} \lambda$ and $g(v) =_{G(\theta_0)} \lambda$.

Then, $\bar{G} = \langle \Delta, \bar{R} \rangle$ is a finitely presented partially commutative group. The public encryption key is $(\bar{G}, \{w_1, w_2, \dots, w_n\})$ and the secret decryption key is $(G, \{x_1, x_2, \dots, x_n\}, g)$. To encrypt a message over $\{1, 2, \dots, n\}$, first replace each occurrence of $1, 2, \dots, n$ by $x_1, x_2, \dots, x_n$ respectively, then insert an arbitrary number of relators from $\bar{R}$ and reduce it to obtain a ciphertext c. To decrypt the ciphertext c, first find $g(w)$ and reduce it to obtain a word z. Now, factorize z over $x_1, x_2, \dots, x_n$. If $z = x_{i_1} x_{i_2} \dots x_{i_m}$, then $i_1 i_2 \dots i_m$ is the corresponding message.

This cryptosystem has the homomorphic property over catenation.

3.3. Example

Let us consider the alphabet $\{a, b, c, a^{-1}, b^{-1}, c^{-1}\}$ as $\Sigma^{\pm 1}$ where $\Sigma = \{a, b, c\}$ and $\Sigma^{-1} = \{a^{-1}, b^{-1}, c^{-1}\}$.

Let $\theta_0 = \{(a, c)\}$ and $\theta = \{(a, c), (a^{-1}, c), (a, c^{-1}), (a^{-1}, c^{-1})\}$.

$$R = \{(aca^{-1}c^{-1}, \lambda), (a^{-1}cac^{-1}, \lambda), (ac^{-1}a^{-1}c, \lambda), (a^{-1}b^{-1}ab, \lambda)\}.$$

Choose $x_1 = bcc,\ x_2 = abc,\ x_3 = bbc$ and $x_4 = b^{-1}ac,\ x_5 = aab,\ x_6 = bc^{-1}a$.
Let $\Delta = \{c_1, c_2, c_3, c_4, c_5, c_6\}$.
Define $g : (\Delta^{\pm 1})^* \to (\Sigma^{\pm 1})^*$ by

$$g(c_1) = g(c_2^{-1}) = a, \quad g(c_1^{-1}) = g(c_2) = a^{-1},$$

$$g(c_4^{-1}) = b, \qquad g(c_4) = b^{-1},$$

$$g(c_6^{-1}) = c^{-1}, \qquad g(c_6) = c,$$

$$g(c_3) = g(c_3^{-1}) = g(c_5) = g(c_5^{-1}) = \lambda,$$

and choose $w_1 = c_3^{-1}c_4^{-1}c_6c_6,\ w_2 = c_2^{-1}c_4^{-1}c_6,\ w_3 = c_4^{-1}c_5c_4^{-1}c_6, w_4 = c_4c_3c_1c_6,$
$w_5 = c_1c_2^{-1}c_4^{-1}c_5^{-1},\ w_6 = c_4^{-1}c_6^{-1}c_1$.

$$\bar{R} = \{(c_2^{-1}c_6c_3c_1^{-1}c_6^{-1}, \lambda), (c_1^{-1}c_5c_2^{-1}c_3^{-1}, \lambda), (c_3c_5, \lambda), (c_4c_5c_4^{-1}c_5c_3^{-1}, \lambda),$$
$$(c_2c_3c_2^{-1}c_5, \lambda)\}.$$

$\bar{G} = \langle \Delta, \bar{R} \rangle$

Consider the messages $m_1 = 23$ and $m_2 = 1$.

To encrypt m_1, replace each occurrence of $1, 2, \ldots, 6$ in m_1 by $w_1, w_2, \ldots, w_6$ respectively, insert relators and then reduce

$$\begin{array}{rcl} w_2w_3 & = & c_2^{-1}c_4^{-1}c_6c_4^{-1}c_5c_4^{-1}c_6 \\ & =_{\bar{G}} & c_2^{-1}c_6c_3c_1^{-1}c_6^{-1}c_2^{-1}c_4^{-1}c_4c_5c_4^{-1}c_5c_3^{-1}c_6c_4^{-1}c_5c_3c_5c_4^{-1}c_6c_3c_5 \\ & =_{\bar{G}} & c_2^{-1}c_6c_3c_1^{-1}c_6^{-1}c_2^{-1}c_5c_4^{-1}c_5c_3^{-1}c_6c_4^{-1}c_5c_3c_5c_4^{-1}c_6c_3c_5. \end{array}$$

Thus, one possible encryption of m_1 is

$$E(m_1) = c_2^{-1}c_6c_3c_1^{-1}c_6^{-1}c_2^{-1}c_5c_4^{-1}c_5c_3^{-1}c_6c_4^{-1}c_5c_3c_5c_4^{-1}c_6c_3c_5.$$

Similarly, to encrypt m_2, replace each occurrence of $1, 2, \ldots, 6$ in m_2 by $w_1, w_2, \ldots, w_6$ respectively, insert relators and then reduce

$$\begin{array}{rcl} w_1 & = & c_3^{-1}c_4^{-1}c_6c_6 \\ & =_{\bar{G}} & c_3^{-1}c_3c_5c_4^{-1}c_4c_5c_4^{-1}c_5c_3^{-1}c_6c_2^{-1}c_6c_3c_1^{-1}c_6^{-1}c_6 \\ & =_{\bar{G}} & c_5c_5c_4^{-1}c_5c_3^{-1}c_6c_2^{-1}c_6c_3c_1^{-1}. \end{array}$$

Thus, one possible encryption of m_2 is $E(m_2) = c_5c_5c_4^{-1}c_5c_3^{-1}c_6c_2^{-1}c_6c_3c_1^{-1}$.
Now, $E(m_1) \cdot E(m_2) =$
$c_2^{-1}c_6c_3c_1^{-1}c_6^{-1}c_2^{-1}c_5c_4^{-1}c_5c_3^{-1}c_6c_4^{-1}c_5c_3c_5c_4^{-1}c_6c_3c_5c_5c_5c_4^{-1}c_5c_3^{-1}c_6c_2^{-1}c_6c_3c_1^{-1}$.
To decrypt, apply g on $E(m_1) \cdot E(m_2)$ and then reduce

$$\begin{array}{rcl} g(E(m_1) \cdot E(m_2)) & = & ac\lambda a^{-1}c^{-1}a\lambda b\lambda\lambda cb\lambda\lambda\lambda bc\lambda\lambda\lambda\lambda b\lambda\lambda cac\lambda a^{-1} \\ & =_G & aca^{-1}c^{-1}abcbbcbcaca^{-1} \\ & =_G & caa^{-1}c^{-1}abcbbcbccaa^{-1} \\ & =_G & cc^{-1}abcbbcbcc \\ & =_G & abcbbcbcc \\ & =_G & x_2x_3x_1 \\ & = & m_1 \cdot m_2. \end{array}$$

Hence, clearly $m_1 \cdot m_2 = D(E(m_1) \cdot E(m_2))$.

4. Application to E-voting

In electronic voting schemes [6], the homomorphic property provides a tool to obtain the tally of the encrypted votes. In this section, we present a method for implementing word problem based cryptosystems for e-voting. To illustrate, we use the cryptosystem based on free partially commutative groups which is described in the previous section.

4.1. Set up

We consider the situation of voting in which there is a trusted center, which is executing the tally of individual votes, n candidates who are standing in the election and any number of voters.

The center can check the validity of votes from each user before tallying them so that invalid votes may be discarded. The center may issue a certificate to the voter stating that the vote is accepted if its vote is valid or stating that the vote is not accepted if the vote is invalid. The center also has to check whether the voter has voted for only one candidate and if it is not so then, the vote will be treated as invalid. It is also the duty of the center to check that a valid voter will vote only once in the voting process.

First, the center runs the setup of the cryptosystem described above and send the encryption key $(\bar{G}, \{w_1, w_2, \dots, w_n\})$ to the legal voters, where $\{w_1, w_2, \dots, w_n\}$ corresponds to the vote space.

4.2. Voting

The public encryption key is $(\bar{G}, \{w_1, w_2, \dots, w_n\})$.

1. To vote for the candidate $j \in \{1, 2, \dots, n\}$, choose the word w_j in $\{w_1, w_2, \dots, w_n\}$.
2. Insert relators from $\bar{R}$ and reduce to obtain arbitrary cryptotext v.
3. Send the vote v to the center.

The insertion and reduction in (2) guarantee the probabilistic nature of encryption. Hence the ciphertext v from different voters for the same candidates will be different. As the word problem for the partially commutative group is unsolvable, we cannot distinguish two votes as to whether they are for the same candidate or for different candidates.

4.3. Tallying

The secret decryption key is $(G, \{x_1, x_2, \dots, x_n, \}, g)$.
The mix-nets [11] are multiparty computation and communication protocol where the encrypted ballots are shuffled so that they cannot be traced to their respective voters. To tally the votes the trusted center will do the following steps.

1. Catenate all the votes using mix-nets and reduce to obtain a word c.
2. Calculate $g(c)$.
3. Reduce $g(c)$ to obtain a reduced word z.
4. Factorize z over elements $x_1, x_2, \dots, x_n$, say $z = x_{i_1} x_{i_2} \dots x_{i_k}$ (This factorization is unique as $\{x_1, x_2, \dots, x_n\}$ is a code).
5. Count the number of occurrences of each $x_1, x_2, \dots, x_n$ in z.

The number of occurrences of x_j in z is equal to the number of votes for the candidate j.

Clearly, each of these steps can be done in linear time. As PKC has homomorphic property over catenation, we obtain the correct number in spite of the arbitrary mixing and catenation which occurs in (1).

5. Conclusion

In this paper, a homomorphic property of the cryptosystems based on word problems are explored and an application of such a system to electronic voting scheme is presented. A polynomial time chosen ciphertext attack for PKC described in [2] is given in [12]. The attack uses the property of the morphism g used: g maps a letter to a letter or λ. The modified system described in this paper is also vulnerable under the same attack. This issue should be taken care in future by suitably modifying the system.

Acknowledgment. The authors gratefully acknowledge the continuous support of Dr. Rani Siromoney and Dr. K.G. Subramanian for more than three decades in leading and guiding us to do research in the field of cryptography based on formal languages theory.

References

[1] P. J. ABISHA, D. G. THOMAS, D. Jayaseelan SAMUEL, *Public Key Cryptosystems and Line Pictures*, The Journal of Combinatorial Mathematics and Combinatorial Computing, **63**, pp. 5–14, 2009.

[2] P. J. ABISHA, D. G. THOMAS, K. G. SUBRAMANIAN, *Public Key Cryptosystems Based on Free Partially Commutative Monoids*, Proceeding of INDOCRYPT 2003, Lecture Notes in Computer Science, **2904**, pp. 218–227, 2003.

[3] M. ANDRAŞIU, A. ATANASIU, Gh. PĂUN, A. SALOMAA, *A New Cryptosystem Based on Formal Language Theory*, Bull. Math. Soc. Sci. Math Roumanie, **36**(1), pp. 3–16, 1992.

[4] M.ANDRAŞIU, J. DASSOW, Gh. PĂUN, A. SALOMAA, *Language-theoretic problems arising from Richelieu cryptosystems*, Theor. Comput. Sci., **116**(2), pp. 339–357, 1993.

[5] D. BONEH, EJ. GOH, K. NISSIM, *Evaluating 2-DNF Formulas on Ciphertexts*, TCC 2005, Lecture Notes in Computer Science, **3378**, pp. 325–341, 2005.

[6] H. DELFS, H. KNEBL, *Introduction to Cryptography - Principles and Applications*, Third Edition, Springer, 2015.

[7] W. DIFFIE, M. HELLMAN, *New Direction in Cryptography*, IEEE Transactions and Information Theory, **IT-22**(6), pp. 644–654, November 1976.

[8] T. ELGAMAL, *A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE Transactions on Information Theory, **31**, pages 469–472, 1985.

[9] G. GENTRY, *Fully Homomorphic Encryption using Ideal Lattices*, Proceedings of STOC'09, pp. 169–178, 2009.

[10] S. GOLDWASSER, S. MICALI, *Probabilistic Encryption*, Journal of Computer and System Sciences, **28**, pp. 270–299, 1984.

[11] P. GOLLE, S. ZHONG, D. BONEH, M. JAKOBSSON, A. JUELS, *Optimistic mixing for exit-polls*, Advances in cryptography - ASIACRYPT 02, Lecture Notes in Computer Science, **2501**, pp. 451–465, 2002

[12] M. I. GONZÁLEZ VASCO, R. STEINWANDT, *Pitfalls in Public Key Cryptosystems Based on Free Partially Commutative Monoids and Groups*, Applied Mathematics Letters, **19**, pp. 1037–1041, 2006.

[13] D. Jayaseelan Samuel, P.J. Abisha, *A Block Cipher Based on Shuffle and θ-Deletion on Trajectories*, International Journal of Pure and Applied Mathematics, Vol. 113, No. 10, pp. 226–234, 2017.

[14] D. Jayaseelan SAMUEL, P. J. ABISHA, *A Novel Cryptosystem Based on Cooperating Distributed Grammar Systems*, International Journal of Artificial Intelligence and Soft Computing (IJAISC), **6**(30), pp. 174–186, 2017.

[15] K. G. SUBRAMANIAN, P. J. ABISHA, R. SIROMONEY, *A DOL/TOL Public Key Cryptosystem*, Information Processing Letters, **26**, pp. 95–97, 1987.

[16] P. S. NOVIKOV, *On the Algorithmic Unsolvability of the Word Problem in Group Theory*. Trudy Mat. Inst. Steklov, **44**, pp. 1–143, 1955.

[17] R. L. RIVEST, A. SHAMIR, L. ADLEMAN, *A Method for Obtaining Digital Signatures and Public Key Cryptosystems*. Commun. of the ACM, **21**, pp. 120–126, 1978.

[18] A. SALOMAA, *Computation and Automata*, Cambridge University Press, 1986.

[19] G. SIROMONEY, R. SIROMONEY, K. G. SUBRAMANIAN, V. R. DARE, P. J. ABISHA, *Generalized Parikh Vector and Public Key Cryptosystems*, A perspective in Theoretical Computer Science - Commemorative Volume for Gift Siromoney, Ed. R. Narasimhan, World Scientific, pp. 301–323, 1689.

[20] R. TAO, *Finite Automata and Applications to Cryptography*, TSINGHUA University Press, Springer, 2008.

[21] M. VAN DIJK, C. GENTRY, S. HALEVI, V. VAIKUNTANATHAN, *Fully Homomorphic Encryption over the Integers*, EUROCRYPT 2010, Lecture Notes in Computer Science, **6110**, pp. 24–43, 2010.

[22] N. R. WAGNER, M. R. MAGYARIK, *A Public Key Cryptosystem Based on Word Problem*, Crypto'84, Lecture Notes in Computer Science, **209**, pp. 19–36, 1984.

[23] C. WRATHALL, *The Word Problem for Free Partially Commutative Groups*, Journal of Symbolic Computations, **6**, pp. 99–104, 1988.