Proceedings of the Jangjeon Mathematical Society
23 (2020), No. 1. pp. 99 – 107

www.jangjeon.or.kr
http://dx.doi.org/10.17777/pjms2020.23.1.99

SYMMETRIC KEY END TO END CRYPTOSYSTEM USING PLATEAUED FUNCTIONS AND HADAMARD MATRIX

PRASANNA POOJARY, KRISHNA PRAKASHA, HARIKRISHNAN P. K.,
VADIRAJA BHATTA G. R.*, DEEPMALA, AND ABHISHEK MITRA

Abstract. Hadamard matrices are a special type of matrices having various applications in cryptography. Here we present a method for the construction of Hadamard matrices using plateaued Boolean functions. The key generated using Hadamard matrices is used for end to end encryption of the messages using symmetric key cryptography. The performance of the proposed system is compared with the Advanced Encryption Standard (AES), and RSA cryptosystems. The results prove that the proposed system outperforms existing systems.

2000 Mathematics Subject Classification. 06E30, 94C10, 11T71.

Keywords and phrases. End-to-End cryptosystem, Security, Boolean functions, Hadamard matrix, Trace.

1. Introduction

E-commerce and M-commerce are very much accessible and widely used services over the internet. E-commerce is any transaction over the internet. E-commerce through mobile devices is termed as M-commerce. The users and resources located at different places and the sensitive information is to be protected and transferred using the suitable, reliable mechanism in online transactions. The most secure method to communicate privately online is possible by incorporating End-to-End encryption between communicating links. In End-to-End encrypted communication paradigm, except sender or the receiver of the message, others cannot decrypt the communication or able to access the data or modify it secretly. End-to-End encryption paradigm ensures the privacy of data, where sensitive information is exchanged over a communication channel. The data is free from active or passive attack. The primary objective is to encrypt data at the web level and to decrypt it at the server or database level. The success of End-to-End security is based on the protocols and mechanisms incorporated at the endpoint of communication. The endpoint could be a client or server, and security starts either at client/server or both sides as shown in Fig. 1.

Using End-to-End encryption, the protection of confidentiality and integrity of transmitted data by encoding it on sender and decoding at the receiver is achieved. The cryptographic keys used are available at two endpoints of the communication network, and it is made possible with the help of symmetric or asymmetric key cryptographic techniques [8]. The man in the middle attack can be addressed by secure user authentication before the usage of the key. The ciphertext generated is transmitted unaltered (except

error cases) across the network to the destination terminal or host with the inclusion of strong cryptographic algorithm for encryption. There are many cryptographic algorithms and techniques available to provide various network security services [9]. This paper explains an efficient symmetric key cryptosystem to provide End-to-End security using the plateaued Boolean function for the generation of the key matrix.

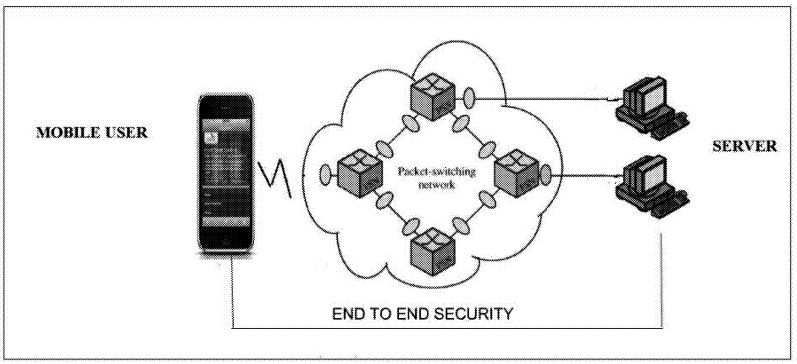

FIGURE 1. End-to-End security

J. L. Walsh introduced Walsh orthogonal function set in 1923 [14]. Later Siemns and Kitai in [12] found the Fourier transform of these functions. The Hadamard transform (also known as the Walsh-Hadamard transform, Hadamard-Rademacher-Walsh transform, Walsh transform, or Walsh-Fourier transform) is an example of a generalized class of Fourier transforms. It performs an orthogonal, symmetric, involutive, linear operation on real numbers (or complex numbers, although the Hadamard matrices themselves are purely real).

A finite field with 2^n elements denoted as $\mathbb{F}_{2^n}$, is basically an extended field of a two element field $\mathbb{F}_2 = \{0, 1\}$ using an irreducible polynomial of degree n over $\mathbb{F}_2$. Moreover $\mathbb{F}_{2^n}$ is isomorphic to n dimensional vector space over $\mathbb{F}_2$. A Boolean function in n variables is an arbitrary function from $\mathbb{F}_{2^n} \to \mathbb{F}_2$, where $\mathbb{F}_2 = \{0, 1\}$ is a Boolean domain and n is a non-negative integer. Zheng and Zhang introduced Plateaued Boolean function in 1999 [15]. Walsh Hadamard transform plays a very important role to design and define plateaued functions. If squared Walsh-Hadamard transform of a Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ takes at most one nonzero value then the function is known as plateaued [2]. Moreover, if the values of its Walsh-Hadamard transform belong to the set $\{0, \pm 2^{\frac{n+r}{2}}\}$ for some fixed r, $0 \leq r \leq n$, then the n-variable Boolean function is said to be r-plateaued. The cases $r = 0, 1$ and 2 have attracted much attention due to their cryptographic, algebraic and combinatorial properties [6]. There are mainly three important classes of plateaued functions, i.e., 0-Plateaued functions which are also called as bent functions. 1-Plateaued functions and 2-Plateaued functions are called as near bent and semi bent function. Bent and semi bent functions occur in even dimensions whereas near bent functions occur in odd dimension.

Moosavi et al., [7] explained an End-to-End secure systems in mobility enabled healthcare networks. The author's proposed certificate-based secure and efficient user authentication and authorization architecture. The authors proposed a three-tier architecture and incorporated certificate based Datagram Transport Layer Security (DTLS) handshake and session resumption technique.

Raza et al., [10] discussed End-to-End secure communication architecture for the cloud-connected Internet of Things (SecureSense) with the implementation of the Constrained Application Protocol (CoAP). The proposed scheme addresses the issues of communication protocols for a cloud platform and IoT security. The authors used off the shelf sensor nodes with integrated hardware cryptographic capabilities to reduce the overheads involved in asymmetric key cryptography for the resource-constrained devices.

Mohammed Riyadh Abdmeziem et al., [1] proposed a lightweight End-to-End key management protocol for electronic health applications. The protocol establishes a secure end to the channel between a remote entity and resource-constrained devices to deliver captured information to ensure authentication and confidentiality. The system developed to obtain assistance from powerful entities, and resource consuming cryptographic primitives are offloaded to powerful entities. The authors formally validated security properties using AVISPA.

Neetesh Saxena et al., in [11] discussed an efficient symmetric key transfer mechanism for mobile users. The authors proposed a novel scheme for secure End-to-End transmission of SMS in contrast to the services provided by traditional SMS systems to prevent replay, the man in the middle attack, and impersonation attacks. The protocol succeeded to achieve less message exchange ratio for authentication and high throughput by better bandwidth consumption.

2. Preliminaries

Definition 2.1. [13] A Hadamard matrix of order n is an $n \times n$ matrix H in which every entry ± 1 such that $HH^T = nI_n$.

Definition 2.2. [3, 4] The Walsh function is defined as

$$W_a(b) = (-1)^{\sum_{i=1}^{n} a_i b_i},$$

where n-tuples $a = a_1 a_2 \dots a_n$ of binary digits $a_i = 0, 1$ and for two such n-tuples a and b, $c_i = a_i + b_i \mod 2$.

Definition 2.3. [2] The Walsh-Hadamard transform of a function f in n variables is the integer-valued function on $\mathbb{F}_{2^n}$, whose value at $a \in \mathbb{F}_{2^n}$ is defined as

$$W_f(a) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{f(x)+\langle a \cdot x \rangle},$$

where $\langle a \cdot x \rangle = \sum_{i=1}^{n} a_i x_i$ is usual dot product.

Definition 2.4. [6] A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called a near bent if its Walsh-Hadamard transform satisfies:

$$W_f(a) \in \{0, \pm 2^{\frac{n+1}{2}}\}, \text{ for all } a \in \mathbb{F}_{2^n}.$$

Near bent functions on $\mathbb{F}_{2^n}$ exist only when n is odd.

Definition 2.5. [6] A Boolean function $f : \mathbb{F}_{2^n} \to \mathbb{F}_2$ is called a semi bent if its Walsh-Hadamard transform satisfies:

$$W_f(a) \in \{0, \pm 2^{\frac{n+2}{2}}\}, \text{ for all } a \in \mathbb{F}_{2^n}.$$

semi bent functions on $\mathbb{F}_{2^n}$ exist only when n is even.

Definition 2.6. [5] If c is an element of $K = GF(q^n)$, its trace relative to the subfield $F = GF(q)$ is defined as follows:

$$Tr_F^K(c) = c + c^q + c^{q^2} + \ldots + c^{q^{n-1}}.$$

3. Construction of Hadamard matrices using Plateaued Boolean functions and its applications

Definition 3.1. Hadamard matrix using Plateaued Boolean function is defined as

(1)

$$H_M = \begin{bmatrix} (-1)^{f(x_1)+\langle a_1 \cdot x_1 \rangle} & (-1)^{f(x_2)+\langle a_1 \cdot x_2 \rangle} & \ldots & (-1)^{f(x_n)+\langle a_1 \cdot x_n \rangle} \\ (-1)^{f(x_1)+\langle a_2 \cdot x_1 \rangle} & (-1)^{f(x_2)+\langle a_2 \cdot x_2 \rangle} & \ldots & (-1)^{f(x_n)+\langle a_2 \cdot x_n \rangle} \\ \ldots & \ldots & \ldots & \ldots \\ (-1)^{f(x_1)+\langle a_n \cdot x_1 \rangle} & (-1)^{f(x_2)+\langle a_n \cdot x_2 \rangle} & \ldots & (-1)^{f(x_n)+\langle a_n \cdot x_n \rangle} \end{bmatrix}, \forall a_i, x_i \in \mathbb{F}_{2^n}.$$

Example 3.2. Construction of Hadamard matrix using Plateaued Boolean function $f(x) = x_0x_1 + x_0 + x_1 + x_2$ over the finite field of order 8.
$\mathbb{F}_{2^3} = \{000, 001, 010, 011, 100, 101, 110, 111\}$
$f(000) = 0,\ f(001) = 1,\ f(010) = 1,\ f(011) = 0,\ f(100) = 1,\ f(101) = 0,$
$f(110) = 1,\ f(111) = 0.$

$$H_M = \begin{bmatrix} (-1)^{f(x_1)+\langle a_1 \cdot x_1 \rangle} & (-1)^{f(x_2)+\langle a_1 \cdot x_2 \rangle} & \ldots & (-1)^{f(x_8)+\langle a_1 \cdot x_8 \rangle} \\ (-1)^{f(x_1)+\langle a_2 \cdot x_1 \rangle} & (-1)^{f(x_2)+\langle a_2 \cdot x_2 \rangle} & \ldots & (-1)^{f(x_8)+\langle a_2 \cdot x_8 \rangle} \\ \ldots & \ldots & \ldots & \ldots \\ (-1)^{f(x_1)+\langle a_8 \cdot x_1 \rangle} & (-1)^{f(x_2)+\langle a_8 \cdot x_2 \rangle} & \ldots & (-1)^{f(x_8)+\langle a_8 \cdot x_8 \rangle} \end{bmatrix} \forall a_i, x_i \in \mathbb{F}_{2^3}.$$

$$H_M = \begin{bmatrix} (-1)^{0+0} & (-1)^{1+0} & (-1)^{1+0} & (-1)^{0+0} & (-1)^{1+0} & (-1)^{0+0} & (-1)^{0+0} & (-1)^{1+0} \\ (-1)^{0+0} & (-1)^{1+1} & (-1)^{1+0} & (-1)^{0+1} & (-1)^{1+0} & (-1)^{0+1} & (-1)^{0+0} & (-1)^{1+1} \\ (-1)^{0+0} & (-1)^{1+0} & (-1)^{1+1} & (-1)^{0+1} & (-1)^{1+0} & (-1)^{0+0} & (-1)^{0+1} & (-1)^{1+1} \\ (-1)^{0+0} & (-1)^{1+1} & (-1)^{1+1} & (-1)^{0+0} & (-1)^{1+0} & (-1)^{0+1} & (-1)^{0+1} & (-1)^{1+0} \\ (-1)^{0+0} & (-1)^{1+0} & (-1)^{1+0} & (-1)^{0+0} & (-1)^{1+1} & (-1)^{0+1} & (-1)^{0+1} & (-1)^{1+1} \\ (-1)^{0+0} & (-1)^{1+1} & (-1)^{1+0} & (-1)^{0+1} & (-1)^{1+1} & (-1)^{0+0} & (-1)^{0+1} & (-1)^{1+0} \\ (-1)^{0+0} & (-1)^{1+0} & (-1)^{1+1} & (-1)^{0+1} & (-1)^{1+1} & (-1)^{0+1} & (-1)^{0+0} & (-1)^{1+0} \\ (-1)^{0+0} & (-1)^{1+1} & (-1)^{1+1} & (-1)^{0+0} & (-1)^{1+1} & (-1)^{0+0} & (-1)^{0+0} & (-1)^{1+1} \end{bmatrix}$$

$$H_M = \begin{bmatrix} (-1)^0 & (-1)^1 & (-1)^1 & (-1)^0 & (-1)^1 & (-1)^0 & (-1)^0 & (-1)^1 \\ (-1)^0 & (-1)^0 & (-1)^1 & (-1)^1 & (-1)^1 & (-1)^1 & (-1)^0 & (-1)^0 \\ (-1)^0 & (-1)^1 & (-1)^0 & (-1)^1 & (-1)^1 & (-1)^0 & (-1)^1 & (-1)^0 \\ (-1)^0 & (-1)^0 & (-1)^0 & (-1)^0 & (-1)^1 & (-1)^1 & (-1)^1 & (-1)^1 \\ (-1)^0 & (-1)^1 & (-1)^1 & (-1)^0 & (-1)^0 & (-1)^1 & (-1)^1 & (-1)^0 \\ (-1)^0 & (-1)^0 & (-1)^1 & (-1)^1 & (-1)^0 & (-1)^0 & (-1)^1 & (-1)^1 \\ (-1)^0 & (-1)^1 & (-1)^0 & (-1)^1 & (-1)^0 & (-1)^1 & (-1)^0 & (-1)^1 \\ (-1)^0 & (-1)^0 & (-1)^0 & (-1)^0 & (-1)^0 & (-1)^0 & (-1)^0 & (-1)^0 \end{bmatrix}$$

$$H_M = \begin{bmatrix} 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

One can even observe that $H_M \cdot H_M^T$ is $8I_8$.

With this, we are giving the algorithm for key generation constructed using the plateaued Boolean functions as defined in the definition 3.1.

Algorithm 1 Key generation Algorithm

```
1: procedure KEY GENERATION
2:     Input n;
3:     F:=FiniteField (2^n);
4:     B <x> :=PolynomialRing(F);
5:     P:=PrimitiveElement(F);
6:     f:= Plateaued function
7:     M := IdentityMatrix(IntegerRing(), 2^n);
8:     k := 0;
9:     for each 'i' in 'F' do
10:        k := k + 1;
11:        l := 0;
12:        for each 'j' in 'F' do
13:            l := l + 1;
14:            R:=Trace(Evaluate(f,j)+i·j);
15:            if (R==1) then
16:                R:=1;
17:            else
18:                R:=0;
19:            end if
20:            M[k, l] := (−1)^R;
21:        end for
22:    end for
23: end procedure
```

Algorithm 2 End-to-End encryption

procedure End-to-End encryption
Initialization: Let 'msg' be plaintext message, 'mLength' be length of 'msg', 'cleartextMatrix' be a 2 dimensional array with size = $2^n \times 2^n$, 'asciiCleartextMatrix' contains the ASCII value of cleartextMatrix
Select an 'n',where mLength $\leq 2^n \times 2^n$
cleartextMatrix= row major format(msg)
Key matrix 'K' is generated as given in the above Algorithm 1
asciiCiphertextMatrix = (asciiCleartextMatrix · K)
end procedure

Algorithm 3 End-to-End decryption

procedure End-to-End decryption
Find the inverse of key matrix 'K'
asciiCleartextMatrix=(asciiCiphertextMatrix · inverseKey)
cleartextMatrix=convert ASCII values to characters from asciiCleartextMatrix
end procedure

4. Testing of the Proposed method

The Test environment details are given in Table 1. A network is created and the proposed system is used to provide End-to-End secure communication between the source and the receiver.

Table 1. Test environment

Device	HP Probook 440 G4 (Laptops)
OS	Windows 8.1 Enterprise and Ubuntu 16.04
RAM	4 GB
Processor	Intel R(Core), TMi5-52000 cpu @2.2 GHz
Software	OpenSSL, JDK, Python

5. Results and discussion

In this case we considered a near bent function defined on $\mathbb{F}_{2^n}$ by $f(x) = \mathrm{Tr}(x)^{2^i+1}$, with $\gcd(i, n) = 1$ for the implementation of the proposed algorithm 1 for key generation. Algorithm 2 and algorithm 3 are implemented for encryption and for decryption of the proposed work respectively and we have found the following results as shown in table 2.

TABLE 2. Time taken by different crypto systems (in seconds) for the message "I am the plain text"

Execution	AES	RSA	Proposed method
1	37.6	44	16
2	37.3	50	17
3	37.7	45	18
4	37.5	45	18
5	40.9	45	18
Average	38.2	45.8	17.4

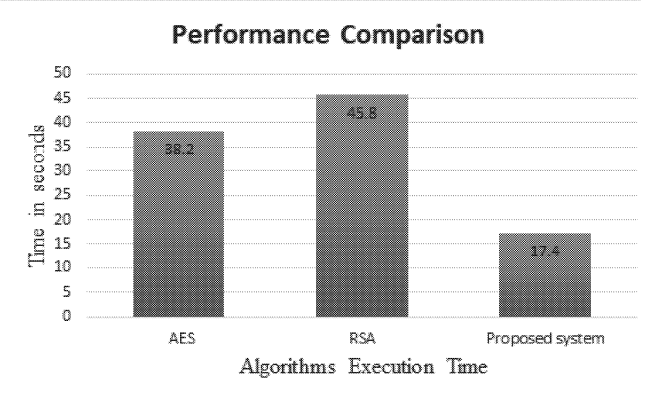

FIGURE 2. Performance of different algorithms

The performance of the proposed system is compared with popular symmetric and asymmetric cryptosystems. The execution time of the compared algorithms is shown in Fig 2. The compared algorithms are executed for five trials with an input text *I am the plain text.* The average execution time of the compared algorithms are plotted, and the proposed method consumed minimum time compared to RSA and AES cryptosystems to prove its superiority among other methods.

6. SECURITY OF THE PROPOSED RESEARCH WORK

The Hadamard matrices constructed using plateaued Boolean functions can be used as a secret key for secure transmission in symmetric key cryptography. It seems to be in some regular pattern when we observe the columns and rows of the matrix. Even though $+1$ and -1 are arranged through columns and rows in some trivial pattern, it is highly difficult to identify the plateaued Boolean functions which are used to form Hadamard matrices. Moreover, for encryption and decryption, one can use these matrices easily which are of size $2^n \times 2^n$ with the help of plateaued Boolean functions over $\mathbb{F}_{2^n}$.

Generally, it is highly expected that the key used in symmetric key cryptography must be large enough for security and small enough for the sake of smooth and secured exchange of key through some advanced key exchange

protocol. In our case, as we are using plateaued Boolean functions with the help of trace terms, it may be up to the level of the easy transaction of key exchange between the end users and by its properties, it is highly safe.

Even in case of hacking by adversary through the brute force method, the system may not be crippled as there exists plenty of plateaued Boolean functions over the finite field of any order. The proposed method of formation of the Hadamard matrix using plateaued Boolean functions deserves expectations as it is a one-way process.

7. Conclusion

In symmetric key cryptosystem, the key plays a significant role. The key generation and transmission are required to be secured from either passive or active attacks. In the present work, authors discuss a novel method for the key generation in symmetric key cryptosystem using Hadamard matrices with the help of plateaued Boolean functions over a finite field. The Hadamard matrix formed is used as the key for encryption. Moreover, these matrices will not easily reveal the information about the plateaued Boolean functions which are generators of the matrices. The performance comparison of the proposed system with AES and RSA encryption is made. The proposed system brings remarkable facts which may lead to more efficient cryptosystems.

Acknowledgements

The authors would like to thank the editor and referees for their valuable comments and suggestions, which improved the quality of this article. The corresponding author, second author and third author acknowledges Manipal Institute of Technology (MIT), Manipal Academy of Higher Education, India for their kind encouragement. The first author is grateful to Manipal Academy of Higher Education for their support through the Dr. T. M. A. Pai Ph. D. scholarship program.

References

[1] M. R. Abdmeziem and D. Tandjaoui, *An end-to-end secure key management protocol for e-health applications*, Computers & Electrical Engineering, 44 (2015), pp. 184–197.

[2] C. Carlet, *Boolean and vectorial plateaued functions and apn functions*, IEEE Transactions on Information Theory, 61 (2015), pp. 6272–6289.

[3] N. J. Fine, *On the walsh functions*, Transactions of the American Mathematical Society, 65 (1949), pp. 372–414.

[4] P.-E. Hagmark and P. Lounesto, *Walsh functions, clifford algebras and cayley-dickson process*, in Clifford Algebras and Their Applications in Mathematical Physics, Springer, 1986, pp. 531–540.

[5] R. J. McEliece, *Finite fields for computer scientists and engineers*, vol. 23, Springer Science & Business Media, 2012.

[6] S. Mesnager, *Bent functions*, Springer, 2016.

[7] S. R. Moosavi, T. N. Gia, E. Nigussie, A. M. Rahmani, S. Virtanen, H. Tenhunen, and J. Isoaho, *End-to-end security scheme for mobility enabled healthcare internet of things*, Future Generation Computer Systems, 64 (2016), pp. 108–124.

[8] K. Prakasha, B. Muniyal, and V. Acharya, *Automated user authentication in wireless public key infrastructure for mobile devices using aadhar card*, IEEE Access, 7 (2019), pp. 17981–18007.

[9] K. Prakasha, B. Muniyal, V. Acharya, S. Krishna, and S. Prakash, *Efficient digital certificate verification in wireless public key infrastructure using enhanced certificate revocation list*, Information Security Journal: A Global Perspective, 27 (2018), pp. 214–229.
[10] S. Raza, T. Helgason, P. Papadimitratos, and T. Voigt, *Securesense: End-to-end secure communication architecture for the cloud-connected internet of things*, Future Generation Computer Systems, 77 (2017), pp. 40–51.
[11] N. Saxena and N. S. Chaudhari, *Easysms: A protocol for end-to-end secure transmission of sms*, IEEE Transactions on information forensics and security, 9 (2014), pp. 1157–1168.
[12] K. H. Siemens and R. Kitai, *A nonrecursive equation for the fourier transform of a walsh function*, IEEE Transactions on Electromagnetic Compatibility, (1973), pp. 81–83.
[13] D. R. Stinson, *Combinatorial designs: constructions and analysis*, Springer Science & Business Media, 2007.
[14] J. L. Walsh, *A closed set of normal orthogonal functions*, American Journal of Mathematics, 45 (1923), pp. 5–24.
[15] Y. Zheng and X.-M. Zhang, *Plateaued Functions*, Springer Berlin Heidelberg, 1999, pp. 284–300.

Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India.
E-mail address: poojaryprasanna34@gmail.com

Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India.
E-mail address: kkp.prakash@manipal.edu

Department of Mathematics, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India.
E-mail address: pk.harikrishnan@manipal.edu

Department of Mathematics, Center for cryptography, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India.
E-mail address: vadiraja.bhatta@manipal.edu

Mathematics Discipline, PDPM Indian Institute of Information Technology, Design and Manufacturing, Jabalpur, Madhya Pradesh, India.
E-mail address: dmrai23@gmail.com

Department of Information and Communication Technology, Manipal Institute of Technology, Manipal Academy of Higher Education, Manipal, Karnataka, India.
E-mail address: abhishek.mitra.a1@gmail.com