Key Generation Technique based on Triangular Coordinate Extraction for Hybrid Cubes

Muhammad Faheem Mushtaq, Sapiee Jamel, Kamaruddin Malik Mohamad, Shamsul Kamal Ahmad Khalid, and Mustafa Mat Deris
Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, 86400 Parit Raja, Batu Pahat, Johor, Malaysia.
faheem.mushtaq88@gmail.com

***Abstract*—Cryptographic algorithms play an important role in information security where it ensures the security of data across the network or storage. The generation of Hybrid Cubes (HC) based on permutation and combination of integer numbers are utilized in the construction of encryption and decryption key in the non-binary block cipher. In this study, we extend the hybrid cube encryption algorithm (HiSea) and our earlier Triangular Coordinate Extraction (TCE) technique for HC by increasing the complexity in the mathematical approaches. We proposed a new key generation technique based on TCE for the security of data. In this regard, the Hybrid Cube surface (HCs) is divided into four quarters by the intersection of primary and secondary diagonal and each quarter is rotated by using the rotation points. The overall security of HC is improved by the rotation of HCs and enhanced the complexity in the design of key schedule algorithm. The brute force and entropy test are applied in experimental results which proved that the proposed technique is suitable for implementing a key generation technique and free from any predicted keys pattern.**

***Index Terms*—Cryptographic Algorithms; Hybrid Cubes; Key Generation Technique; Non-Binary Block Cipher.**

I. INTRODUCTION

Security is the major aspects of storing information and sending it across the network from one location to other with secure manner. Cryptography ensures the secure communication and provides a way to protect sensitive information by transforming it into an unreadable format (encryption) and only the authorized recipient able to convert it into original text (decryption). It compromising different mathematical processes involving in encryption algorithms was designed to secure from unauthorized access [1, 2, 3]. Unfortunately, the developments of fully secure cryptographic algorithms are quite difficult due to the presence of challenges from the cryptanalysts whose tries to access any available cryptosystems. As the rapid growth of the internet and other forms of network communication become more dominant, a vast range of applications are made to secure cryptographic algorithms. To achieve the high-security requirements, right selection of algorithms brings a high protection from cryptographic components to cryptanalysis [4]. Furthermore, every cryptographic algorithm needed to fulfill the execution time's test and validation considered as approval with Advanced Encryption Standard (AES) [5]. There are three main types of methods that are utilized in the construction of secure encryption and decryption algorithms that contain permutation, substitution, and their combination form. Moreover, the key schedule of AES is used to modify the last round key that can be available fast using the look-ahead technique as well as obtaining the all intermediate round key simultaneously and become more beneficial when fast decryption is needed [6]. The substitution-based key derivation function is proposed that receives a short key length as an input, generate blocks of the key and transform these key through Quasigroup string transformation like a substitution mechanism to give randomization [7]. The key derivation function is used to generate random and unpredictable secret keys.

The generation of the magic cube from a magic square and two orthogonal latin square is adopted to propose encryption and decryption algorithms [8]. Magic cube consists of six surfaces or sub-cubes having 3-Demensional (3D) coordinate. Moreover, the permutations using image encryption algorithm show that every state of the cube is actually a permuted mentioned in [9]. They rotate the cubes which are similar to Rubik's Cube and use these cubes to reverse a new scrambled image. An image permutation algorithm based on geometrical projection and shuffling in the design of key schedule algorithm which increases the security of original image is proposed in [10]. A magic cube transformation and natural chaotic sequence in an image encryption algorithm utilized the concept of confusion and diffusion is considered in [10, 11]. These scientific mathematical properties are used to enhance the complexity of the overall algorithm. Furthermore, the 3D magic cube based technique is proposed to be used as information hiding scheme [13]. The secret information is placed in the cover pixel LSBs of the image by using the spatial coordinates.

The combination of Latin squares, magic squares, orthogonal Latin square and magic cubes are utilized in the generation of the Hybrid Cubes (HC) which include good diffusive characteristics [14]. They find a new way for further development of transformation that is based on permutation and combination of integer numbers and develops non-binary block cipher. The effectiveness of non-binary block cipher is based on different component mainly encryption and decryption algorithms, key generation and its parameters. Furthermore, the generation of two-dimensional (2D) hybrid cube encryption algorithm (HiSea) is a non-binary block cipher based on integer numbers [15]. The hybridization and rotation of HC are generated encryption algorithm and key as a cubical form by randomly shuffled cube [16]. The limitation of HiSea encryption algorithm and Rajavel's cubical encryption algorithm was performed hybridization which needs high computation cost. Moreover, the 2D encryption algorithm using the concept of cartesian coordinate geometry and circle generation is proposed in [17]. The circle generation process considers the translation and rotation of

axis which is individually performed on a different circle. The computing information about complex geometric primitives is often costly, while computational geometry determines many asymptotically effective algorithms for such problems are indicated [18].

In this regard, this paper extends our earlier proposed technique [19] to increase their mathematical approaches by designing new key generation technique for HC of order 4. HC is divided into six faces and each face of HC is divided into four quarters like triangular form by the intersection of diagonals. Four key matrices are used to generate one triangular key matrix based on Triangular Coordinate Extraction (TCE) steps. Modulo-16 is employed on the key matrix that is used to calculate the value of triangular key matrix during the rotation of HCs. The process of key generation is evaluated which produce the invertible matrix that is used in the generation of encryption and decryption key. The rotation of HCs creates complexity in the message and increases the difficulty to predicting original message from cryptanalyst. The experimental results show that the proposed method for generating key matrices from HCs rotation is suitable for evaluating the key generation technique. Furthermore, brute force attack on large key space will make challenging and time-consuming.

The remaining paper is organized as follows: Section II discusses some preliminaries which include the overview of the hybrid cube, rotation and translation of coordinates and the key schedule algorithm that is used in our proposed technique. Section III outlines the proposed a key generation technique based on TCE for HC. Section IV explains the experimental results and discussion. Section V presents the conclusion and future work of this research.

II. PRELIMINARIES

We use the following preliminaries which are used in the construction of the Key generation technique for hybrid cube.

A. Hybrid cubes

Hybrid cubes are generated by the combination of two magic cubes using inner matrix multiplication of layers proposed in [14]. HC of order 4 is defined by $H_{i,j}$, $i \in \{1, 2, \ldots, 879\}$ and $j \in \{1,2,3,4\}$ defined as

$$H_{i,j} = MC_{i,j} \times MC_{i+1,j} \quad (1)$$

where the $MC_{i,j}$ is j^{th} layer of i^{th} magic cubes.

Let us consider the HC 1 is formed by inner matrix multiplication of magic cube 1 layer having coordinates {x=1,2,3,4} and magic cube 2 layer {x=1,2,3,4}. Similarly, HC 2 is formed on inner matrix multiplication of magic cube 2 and 3, and so on. A new cube structure HC of order 4 is developed using the layers of magic cubes where the layer entries belong to the set of integers 1 to 4096. The new cube layer ensures invertible matrix which is used in the design of encryption and decryption keys. HiSea consist of key schedule algorithm, encryption and decryption algorithm are main components in the development of non-binary block cipher explained in [15]. All possible combination of HC layers as the basis for the construction of encryption and decryption keys utilized in the non-binary block cipher. Furthermore, an improved key generation and the encryption algorithm are introduced which is based on HC rotation and construction of HC by randomly shuffle cube [16]. The rotation of HC creates the shuffling of data which try to protect the data from cryptanalyst.

B. Translation and rotation of coordinates

The translation of an object is applied by shifting the position along the straight path from one coordinate to another coordinate location [20]. To translate a 2D point by the addition of translation distance t_x and t_y, to move point of coordinate position (x, y) to a new position (x', y'), so $x' = x + t_x$ and $y' = y + t_y$. Translation is a rigid body transformation that is every point on the object is translated with the same amount. The changing in the position of a circle needs to translate the center coordinates and reconstruct the circle in the new location.

The rotation of the object is applied by shifting the position along a circular path in *xy* plane. During rotation, we specify the rotation position (x_1, y_1) and angle θ of the pivot point (rotation point) where the object is to be rotated. Counter clockwise rotations explain the positive values for the rotation angle and negative values define the rotation angle in the clockwise direction. The rotation about rotation axis is also described that is passing through the rotation point and perpendicular to *xy* plane [20]. The rotation of point from (x, y) to (x', y') position using angle θ is relative to the origin of coordinate. The transformation equation at position (x, y) is $x' = x\cos\theta - y\sin\theta$ and $y' = x\sin\theta + y\cos\theta$. The rotation of a circle about the non-central axis by the movement of central position using arc, it subtends the specified angle rotation.

C. Key schedule Algorithm

Key schedule algorithm is generating secret keys and act as a vital role in the development of encryption and decryption key. The poor key generation produces weak keys which are utilized for the encryption process, it can be easily attack using brute force technique. The cryptanalyst is continuously trying all possible combination to get plaintext from ciphertext using this attack. AES considered that all cryptographic algorithms must support the key lengths include 128-bit, 192-bit and 256-bit key with number of rounds 10, 12 and 14 respectively [5, 21]. The round keys are taken from the cipher key or expanded key by using key schedule and employed in the construction of block cipher. It ensures high diffusion over the multiple no. of rounds and used invertible transformation. Furthermore, a new AES key schedule algorithm is presented which includes every round sub-key that is effectively and efficiently independent from each other, this is the reason there is no bit leakage among round sub-keys. It analyzed a strengthened key schedule by using Shannon's bit confusion and diffusion properties that are the basis of secure communication [22].

III. PROPOSED TECHNIQUE

This section explains the methodology of our proposed key generation technique based on TCE for HC. The purpose of the construction of this proposed technique is to increase the complexity in the design of key schedule algorithm of HC. It also computationally secures the process of encryption and decryption of existing HC encryption algorithm. Key

generation technique consists of three main steps. The first step includes the design of rotation and key generation which is used to identify the rotation pattern of HCs. The rotation of HCs around the four quarters is generated by the intersection of primary and secondary diagonal. The second step calculates the value of coordinate during the rotation of HCs. The final step explains the process of key generation technique. The resultant matrix of the proposed technique is invertible, which is used in the construction of encryption and decryption keys. More details of these steps are demonstrated in the following sub-sections.

A. Design of rotation and key generation technique

The design of HCs is divided into six faces and each face is further divided into four quarters (Q1, Q2, Q3, Q4) by intersection of two diagonal lines pass through the center of a circle. The primary diagonal lies on the x-axis and the y-axis utilize as the secondary diagonal. At the first stage, the rotation of HCs of the first face is considered and after that, we apply the proposed technique on the rest of five faces of HCs. The rotation of triangular HCs is counter clockwise that is the main component in the generation of key schedule as shown in Figure 1.

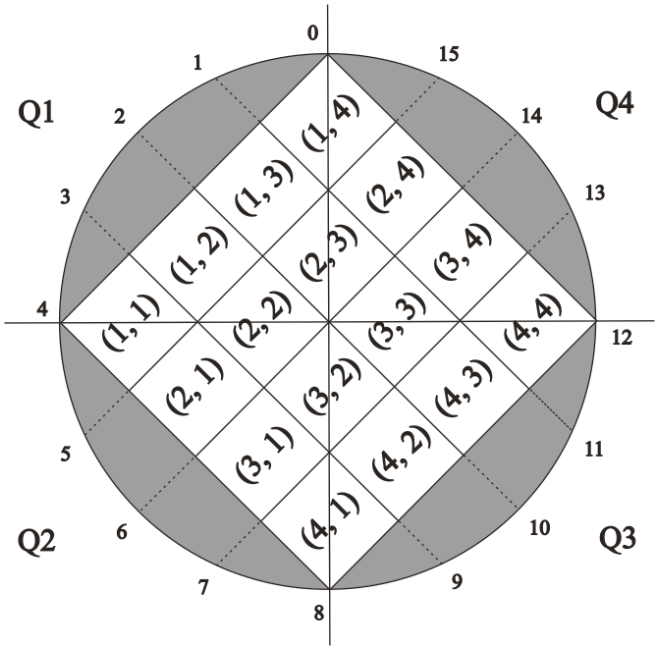

Figure1: Rotation and key generation technique for HC

The position of coordinates in HCs is represented as rotation points 0 to 15 from quarters Q1 to Q4. The HCs is rotated in the counter-clockwise from rotation points 0 to 4 in Q1, 4 to 8 in Q2, 8 to 12 in Q3 and 12 to 0 in Q4.

The range of rotation points is presented in Q1 and Q2 quarters as shown in Figure 2. It helps to extract coordinate values during the rotation of HCs.

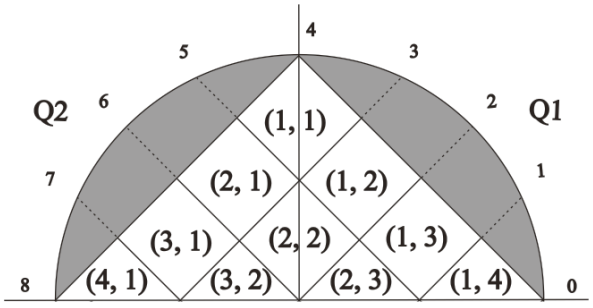

Figure 2: Range of Rotation points in Q1 and Q2

The value of coordinates in quarter Q1 and Q2 is represented in Table 1. The rotation points are used to calculate the value of triangular key matrix which is based on the unique matrix that is taken by using the modulo operation. The calculation of key matrix value using rotation points increases the complexity of the design of key generation and increase the difficulty for the cryptanalysis to address the keys with minimum number of possibilities.

Table 1
Value of coordinates in Q1 and Q2

Rotation points	Quarter	Value
0 – 1	Q1	$\frac{1}{2}(1,4)$
1 – 2	Q1	$1(1,3)+\frac{1}{2}(2,3)$
2 – 3	Q1	$1(1,2)+\frac{1}{2}(2,2)$
3 – 4	Q1	$\frac{1}{2}(1,1)$
4 – 5	Q2	$\frac{1}{2}(1,1)$
5 – 6	Q2	$1(2,1)+\frac{1}{2}(2,2)$
6 – 7	Q2	$1(3,1)+\frac{1}{2}(3,2)$
7 – 8	Q2	$\frac{1}{2}(4,1)$

The range of rotation points lies in Q3 and Q4 coordinates as shown in Figure 3. During the rotation of HCs, rotation points are utilized in the extraction of coordinate values.

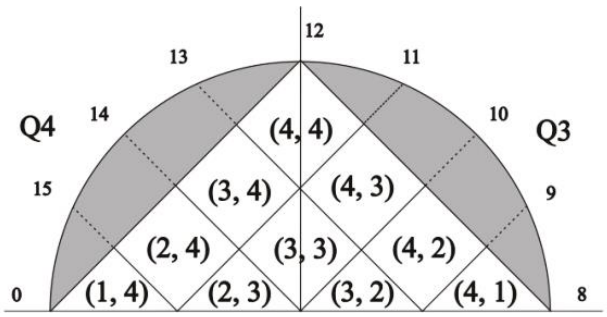

Figure 3: Range of Rotation points in Q3 and Q4

The value of coordinates in quarter Q3 and Q4 is mentioned in Table 2.

Table 2
Value of coordinates in Q3 and Q4

Rotation points	Quarters	Values
8 – 9	Q3	$\frac{1}{2}(4,1)$
9 – 10	Q3	$1(4,2)+\frac{1}{2}(3,2)$
10 – 11	Q3	$1(4,3)+\frac{1}{2}(3,3)$
11 – 12	Q3	$\frac{1}{2}(4,4)$
12 – 13	Q4	$\frac{1}{2}(4,4)$
13 – 14	Q4	$1(3,4)+\frac{1}{2}(3,3)$
14 – 15	Q4	$1(2,4)+\frac{1}{2}(2,3)$
15 - 0	Q4	$\frac{1}{2}(1,4)$

Definition 1. Let the HCs be a 4 x 4 matrix, then we define the properties of diagonal coordinates of HCs as mentioned in [19]. The intersection of diagonals can be possible if the coordinates satisfy the reflexive and symmetric properties. The properties of diagonal are:

i. Primary diagonal for the HCs square matrix is defined as the collection of entries *HCs(i, j)*, where *i = j*. The coordinates include in the primary diagonal are as follows,
{(1, 1), (2, 2), (3, 3), (4, 4)}
ii. Secondary diagonal for the HCs square matrix is defined as a collection of entries *HCs(i, j)*, where $i + j = 5$ can be calculated by the mean of symmetric coordinates *(i, j)* and *(j, i)* of HCs matrix. The coordinates include in the secondary diagonal are as follows,
{(1, 4), (2, 3), (3, 2), (4, 1)}

When the value of diagonal *HCs(i, j)* satisfy the properties of primary and secondary diagonal then the value of coordinates of a particular cell is $\frac{1}{2}$*HCs(i,j)*.

B. Coordinate Extraction

Next step is to extract the coordinates during the rotation of HCs based on the properties discussed in Definition 1. The triangular quarters Q1 of HCs is the passage from rotation points 0 – 4, Q2 is the passage from rotation points 4 – 8, Q3 is the passage from rotation points 8 – 12 and Q4 are the passage from rotation points 12 – 0 respectively. The value of coordinates is extracted using the formulas discuss in table 3.

Table 3
Extract the value of HCs coordinates

Quarters	Extraction of coordinate value
Q1	$\sum_{i=0}^{1}\sum_{j=1+i}^{4-i}(i+1,\ j)$
Q2	$\sum_{j=0}^{1}\sum_{i=1+j}^{4-j}(i,4-j)$
Q3	$\sum_{i=0}^{1}\sum_{j=1+i}^{4-i}(4-i,j)$
Q4	$\sum_{j=0}^{1}\sum_{i=1+j}^{4-j}(i,j+1)$

C. Process of Key Generation Technique

HCs are ordered based on rows and columns of order 4. The four key matrices are generated from HiSea encryption algorithm [23]. The key generation technique is implemented based on TCE which tends to increase the complexity of HC. The process of key generation is presented in the following steps:

i. Firstly, the steps of TCE are demonstrated according to the quarters on four key matrices, it will generate one Triangular Key Matrix (TKM).
ii. Apply modulo-16 on each coordinate of TKM generated using TCE steps. Each run will give 1 value in the new matrix. The new Modulo Matrix (MM) contains the coordinate value that is in the range of 0 to 15.

Definition 2. Let the HCs be a 4 x 4 matrix, if any repeated value was found in the MM coordinates, then we will replace it using the following rules:

$$a = a - 1 \text{ for } 1^{st} \text{ repetition}$$
$$a = a - 2 \text{ for } 2^{nd} \text{ repetition}$$
$$a = a - 3 \text{ for } 3^{rd} \text{ repetition}$$

It will continue until we get zero value. After reaching on the zero value, if repetition still exist then we will replace by using the following rules:

$$a = a + 1 \text{ for } 1^{st} \text{ repetition}$$
$$a = a + 2 \text{ for } 2^{nd} \text{ repetition}$$

This process will continue until we get the non-repeated matrix value.

i. If the new MM is consisting of repeated value in each coordinate of rows and columns, then we apply the properties of Definition 2 on newly generated matrix in order to get the Unique Matrix (UM) value.
ii. Calculate the value of TKM by using rotation points which are based on UM matrix generated from modulo operation. A New Key Matrix (NKM) is generated through the calculation of coordinate values based on the rotation points.
iii. Rotate the quarters of NKM in the counter-clockwise to generate the Rotation Cube Matrix (RCM).
iv. Test the randomness of RCM using the random matrix technique in HiSea encryption algorithm.
v. Brute force attack on key generation technique can be estimated using key space.

IV. Experimental Results and Discussion

In this section, the steps of key generation technique are demonstrated using four key matrices taken from HC encryption algorithm. The resultant rotation cube matrix produces a matrix of order 4 which is invertible. This invertible matrix is used in the generation of encryption and decryption key in the non-binary block cipher. Moreover, some experimental results include the entropy and brute force attack that are evaluated to prove the validity of the proposed key generation technique. The step by step processes of key generation technique is described below.

A. Step 1

The selection of four key matrices (A, B, C, D) from HiSea encryption algorithm is required to generate one TKM matrix. Each key matrix is used to develop one row for TKM matrix based on TCE steps. These key matrices are shown as:

$$A = \begin{bmatrix} 140 & 1634 & 3150 & 437 \\ 420 & 3249 & 2304 & 20 \\ 1980 & 64 & 289 & 3660 \\ 2805 & 594 & 30 & 1932 \end{bmatrix}$$

$$B = \begin{bmatrix} 812 & 3136 & 1089 & 156 \\ 21 & 1634 & 3150 & 780 \\ 3596 & 594 & 30 & 1365 \\ 1332 & 81 & 1024 & 2756 \end{bmatrix}$$

$$C = \begin{bmatrix} 1365 & 66 & 558 & 3596 \\ 3660 & 576 & 1 & 1980 \\ 20 & 1681 & 4096 & 420 \\ 780 & 3186 & 1598 & 21 \end{bmatrix}$$

$$D = \begin{bmatrix} 2756 & 625 & 256 & 1332 \\ 1932 & 66 & 558 & 2805 \\ 437 & 3186 & 1598 & 140 \\ 156 & 1600 & 2401 & 812 \end{bmatrix}$$

The first row of TKM matrix is generated using key matrix A and second row of TKM is generated by key matrix B by utilizing the steps of TCE. Similarly, the key matrix C and D are used to generate third and fourth rows of TKM matrix. The TKM matrix of order 4 is presented as:

$$TKM = \begin{bmatrix} 7849 & 5529 & 3169 & 6161 \\ 7101 & 5803 & 3461 & 5191 \\ 3393 & 5881 & 8073 & 6257 \\ 3237 & 5451 & 6877 & 5095 \end{bmatrix}$$

B. Step 2

In this step, we apply modulo 16 on the TKM matrix generated from the four key matrices. The MM matrix is as follows:

$$MM = \begin{bmatrix} 9 & 9 & 1 & 1 \\ 13 & 11 & 5 & 7 \\ 1 & 9 & 9 & 1 \\ 5 & 11 & 13 & 7 \end{bmatrix}$$

C. Step 3

The MM matrix is generated that contains the repeated values. So, in order to remove repetition, we apply the properties of Definition 2 on MM matrix that generate UM matrix. The UM matrix is given as follows:

$$UM = \begin{bmatrix} 9 & 8 & 1 & 0 \\ 13 & 11 & 5 & 7 \\ 2 & 6 & 4 & 3 \\ 10 & 12 & 14 & 15 \end{bmatrix}$$

D. Step 4

In this step, we calculate the value of TKM by using the rotation point defined in UM. Considering the UM matrix with the respective value of coordinate in each quarter shown in Table 1 and Table 2, we put the value of TKM according to that coordinate and then do the calculation. The resultant matrix of NKM is given as follows:

$$NKM = \begin{bmatrix} 8391 & 1618 & 4899 & 3080 \\ 10293 & 2547 & 10002 & 1618 \\ 8430 & 6333 & 3924 & 3924 \\ 10913 & 2547 & 6921 & 3080 \end{bmatrix}$$

E. Step 5

This step contains the rotation of NKM matrix based on TCE steps. The RCM matrix is shown as follows:

$$RCM = \begin{bmatrix} 10913 & 8430 & 10293 & 8391 \\ 2547 & 6333 & 2547 & 1618 \\ 6921 & 3924 & 10002 & 4899 \\ 3080 & 3924 & 1618 & 3080 \end{bmatrix}$$

Hence, the RCM matrix after rotation is tested which is invertible. The complexity in the key generation provides more security and efficiency in the ciphertext.

F. Step 6

The strength of overall implementation of key generation technique is estimated by using random matrix technique (entropy test). The entropy for the RCM matrix is calculated by using MATLAB function CalculateEnt(). The normalized Shannon entropy test for RCM matrix is 0.9415 which is closer to 1 rather than 0. Hence, this matrix represents the HC blocks consist of 16 decimal numbers is 94.15% random, which can be considered as almost random.

G. Step 7

The encryption keys used in this technique is 4 x 4 matrix of integer numbers. Each entry of encryption key lies between the range of {1, 2, ..., 4096} or within 212 bits. The key space for encryption and decryption keys are 2^{12} x 2^{12} x …. x 2^{12} =212)^{16} = 2^{192} or approximately $(10^3)^{19.6} = 10^{58.8}$ keys.

Key generation technique for HC is computationally secure and having the large key space that makes the brute-force attack difficult and time-consuming. The number of keys used in the key generation technique can determine the practical feasibility of conducting a brute-force key.

The brute force and entropy test were carried out to demonstrate that the proposed technique is suitable for the generation of encryption and decryption key and secure for a non-binary block cipher. The proposed technique of creating a layer of order 4 matrix and the rotation of HCs makes it difficult for predicting keys pattern. Even one rotation of HCs able to show the reflection of all faces of HC. So, the new combination of layer entries through key generation technique is used to enhance the complexity in the overall construction of encryption algorithm.

V. Conclusion and Future Work

In this paper, the key generation technique based on TCE for HC of order 4 matrices is presented which can be used to generate the keys during rotation of HCs. Security is the major concern in the design of key generation technique. In this technique, the four key matrices are employed in the generation of one TKM matrix using the concept of TCE. The modulo-16 operation used to calculate the value of TKM by

utilizing the rotation points and then the rotation of HCs increases the complexity in the design of RCM. It creates a difficulty to predict the pattern of keys which ensure the protection of message from cryptanalysts. This research can be further analyzed in the future by implementing the non-binary block cipher based on 3-dimensional key generation algorithm.

ACKNOWLEDGEMENT

The authors would like to thank the Universiti Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia and Ministry of Higher Education Malaysia for supporting this research under Project Vot No. U493.

REFERENCES

[1] N. Kumar and P. Chaudhary, "Performance evaluation of encryption/decryption mechanisms to enhance data security," *Indian Journal of Science and Technology*, vol. 9, no. 20, 2016.

[2] M. Ebrahim, S. Khan, and U. Bin Khalid, "Symmetric Algorithm Survey: A Comparative Analysis," *International Journal of Computer Applications*, vol. 61, no. 20, pp. 12–19, 2013.

[3] Disina, A. H., Pindar, Z. A., & Jamel, S., "Enhanced Caeser Cipher to Exclude Repetition and Withstand Frequency Cryptanalysis," In *Proceedings of the International Conference on Information Science and Security (ICISS)*, 2015.

[4] S. H. Jamel and M. M. Deris, "Diffusive primitives in the design of modern cryptographic algorithms," in *Proceedings of the International Conference on Computer and Communication Engineering*, 2008, pp. 707–710.

[5] National Institute of Standards (NIST), *Federal Information Processing Standards Publication197: Advanced encryption standard (AES)*. 2001.

[6] R. R. Rachh, P. V. A. Mohan, and B. S. Anami, "Implementation of AES Key Schedule Using Look-Ahead Technique," *Circuits, Systems, and Signal Processing*, vol. 33, no. 11, pp. 3663–3670, 2014.

[7] A. H. Disina, S. Jamel, Z. A. Pindar, and M. M. Deris, "All-or-nothing Key Derivation Function Based on Quasigroup String," in *Proceedings of the International Conference on Information Science and Security (ICISS*), 2016, pp. 6–10.

[8] M. Trenkler, "An algorithm for making magic cubes," *The Pi ME Journal*, vol. 12, no. 2, pp. 105–106, 2005.

[9] L. Zhang, X. Tian, and S. Xia, "Scrambling algorithm of image encryption based on Rubik's cube rotation and logistic sequence," in *Proceedings of the International Conference on Multimedia and Signal Processing, CMSP*, 2011, vol. 1, pp. 312–315.

[10] B. Nini and D. Bouteldja, "Virtual Cylindrical View of a Color Image for its Permutation for an Encryption Purpose," *International Journal of Computer Applications*, vol. 16, no. 1, pp. 11–17, 2011.

[11] J. Shen, X. Jin, and C. Zhou, "A color image encryption algorithm based on magic cube transformation and modular arithmetic operation," *Advances in Multimedia Information Processing*, vol. 3768, pp. 270–280, 2005.

[12] L. Zhang, S. Ji, Y. Xie, Q. Yuan, Y. Wan, and G. Bao, "Principle of image encrypting algorithm based on magic cube transformation," *Computational Intelligence and Security*, vol. 3802, pp. 977–982, 2005.

[13] Q. Wu, C. Zhu, J. J. Li, C. C. Chang, and Z. H. Wang, "A magic cube based information hiding scheme," *Journal of information security and application*, vol. 26, pp. 1–7, 2016.

[14] S. Jamel, T. Herawan, and M. M. Deris, "A cryptographic algorithm based on hybrid cubes," *Computational Science and Its Applications ICCSA*, vol. 6019, pp. 175–187, 2010.

[15] S. Jamel, M. M. Deris, I. T. R. Yanto, and T. Herawan, "The hybrid cubes encryption algorithm (HiSea)," *Communications in Computer and Information Science*, vol. 154, pp. 191–200, 2011.

[16] D. Rajavel and S. P. Shantharajah, "Cryptography Based on Combination of Hybridization and Cube's Rotation," *International Journal of Computational Intelligence and Informatics*, vol. 1, no. 4, pp. 294–299, 2012.

[17] P. R. Kumar, S.S.Dhenakaran, K.L.Sailaja, and P.SaiKishore, "CHAKRA: A New Approach for Symmetric Key Encryption," in *Proceedings of the 2012 World Congress on Information and Communication Technologies, WICT*, 2012, pp. 727–732.

[18] N. Anghel, "Determinant Identities and the Geometry of Lines and Circles," *The Journal of Ovidius University of Constanta, Versita*, vol. 22, pp. 37–49, 2014.

[19] M. F. Mushtaq, S. Jamel, and M. M. Deris, "Triangular Coordinate Extraction (TCE) for Hybrid Cubes," *Journal of Engineering and Applied Sciences*, vol. 12, no. 8, pp. 2164-2169, 2017.

[20] D. Hearn and M. P. Baker, *Computer Graphics - C version*. Pearson Education, 2005.

[21] E. B. Barker and A. Roginsky, "Recommendation for Cryptographic Key Generation," *NIST Special Publication 800-133*, pp. 1–26, 2012.

[22] L. May, M. Henricksen, W. Millan, G. Carter, and E. Dawson, "Strengthening the Key Schedule of the AES," in *Proceedings of the 7th Australian Conference on Information Security and Privacy*, 2002, pp. 226–240.

[23] S. Jamel, *The Hybrid Cubes Encryption Algorithm (HiSea)*. Ph.D Thesis, University Tun Hussein Onn Malaysia (UTHM), Johor, Malaysia, pp. 1–138, 2012.