**A Design of Block Cipher Key using Cube**

Kim Min Ho\*, Jung Yun Sang\*, Lee Jun\*, Eun Jung Choi\*\*

\* Paul Math International School, Korea \*\*Dept. of Information Security, Seoul Women’s University, Seoul, Korea

*sansobonza@naver.com, fgf7404@naver.com, jkafa04@gmail.com, chej@swu.ac.kr*

**Abstract**

**The fiftyfour pieces of Rubik’s Cube change to totally different pieces depending on the number of rotation time and sequence. Also, when dissolving changed cube to an original shape, it could be done by rotating the cube in inverse order. These peculiarities are the same as the symmetry of decryption on the block cipher. This paper noticed the idea that if each piece of Rubik’s Cube could move, various kind of combination and also various keys can be obtained and created. Therefore we suggests the block cipher key using the mechanism of Rubik’s Cube.**

Information Security, Block Cipher, Cryptographic, Rubik’s Cube

**I. Introduction**

The Rubik's Cube which was originally called magic cube was invented in 1974 by Hungarian sculptor and professor of architecture Erno Rubik [1][2]. In a classic Rubik's Cube, each of the six faces is covered by nine stickers, each of one of six solid colours: white, red, blue, orange, green, and yellow. In currently sold models, white is opposite yellow, blue is opposite green, and orange is opposite red, and the red, white and blue are arranged in that order in a clockwise arrangement[3]. This cube is the famous puzzle toy which has 6 different colors of faces and each face has the rectangular of n x n pieces of the same color at its original state[4]. The purpose of this puzzle is to make the mixed color of face made by many times of rotation to the original state that each face has the same color.

A block cipher by itself is only suitable for the secure cryptographic transformation (encryption or decryption) of one fixed-length group of bits called a block[5]. Examples are DES[6], AES[7] and SEED[8]. This paper noticed the idea that if each piece of Rubik’s Cube could move, various kind of combination and also various keys can be obtained and created. This property of Rubik’s Cube can be used in creating block cipher keys.

**II. Definition of Cube**

 In this paper, the Cube which will be used has the dimension of 3 x 3 x 3, 54 faces and each faces of the Cube don’t have colors.

*A. Definition of Piece*

The pieces of Cube are defined as following Fig. 1. Assume that the Cube which will be utilized has 6 surfaces of 3 x 3 pieces , i.e. total 54 pieces, and the colors of 6 surfaces are the same. Each piece obtains sequence numbers as follows. The upper surface has the number of 1~9, and then right side surface has the number of 10~18, left side surface 19~27, front side surface 28~36, rear side surface 37~45, and the bottom surface 46~54.



Fig. 1 Definition of numbers

The definition of numbers according to its position and the rotation standard are as follows.

$B\_{i}$: Piece number $i$ of Rubik’s Cube.

Fixation: Fixed Piece is $B\_{5}$

*B. Definition of Axis*

$x\_{1}$: Axis which sets the standard as $B\_{5}, B\_{50}$ and rotates $B\_{35}$to left side $90°$. Can be expressed as $σ^{1}x\_{1}$.

$x\_{2}$: Axis which sets the standard as $B\_{5}, B\_{50}$and rotates $B\_{32}$to left side $90°$. Can be expressed as $σ^{1}x\_{2}$ .

$y\_{1}$: Axis which sets the standard as $B\_{32}, B\_{41}$and rotates $B\_{8}$to right side $90°$. Can be expressed as $σ^{1}y\_{1}$.

$y\_{2}$: Axis which sets the standard as $B\_{32}, B\_{41}$and rotates $B\_{2}$to right side $90°$. Can be expressed as $σ^{1}y\_{2}$.

$z\_{1}$: Axis which sets the standard as $B\_{14}, B\_{23}$and rotates $B\_{4}$to back side $90°$. Can be expressed as $σ^{1}z\_{1}$.

$z\_{2}$: Axis whichs sets the standard as $B\_{14}, B\_{23}$and rotates $B\_{35}$to back side $90°$. Can be expressed as$ σ^{1}z\_{2}$.

$σ^{i}a$: Rotate $a\_{i}$for $i$times.

($0\leq i \leq 3, a\in \{x\_{1}, x\_{2}, y\_{1}, y\_{2}, z\_{1}, z\_{2}\})$.

*C. Significant peculiarity of cube*

If the state of rubik’s cube such as in [Figure 1.] is S, the commutative law does not come into existence. In other words, different rotation sequence means different S.

$$\left\{\left(Sσ^{i}b\right)σ^{i}a\right\}\ne \left\{\left(Sσ^{i}b\right)σ^{i}b\right\}(a, b\in \left\{x\_{1}, x\_{2}, y\_{1}, y\_{2}, z\_{1}, z\_{2}\right\},$$

$$ i\in \left\{0, 1, 2, 3\right\}, a\ne b)$$

As the following equation shows, different rotation number means different S.

$$Sσ^{i}a\_{j}\ne Sσ^{k}a\_{j}(a\in \left\{x, y, z\right\}, j\in \left\{1, 2\right\}, i,$$

$$ k \in \left\{0, 1, 2, 3\right\}, k\ne i)$$

In other words, to recover the rotated cube to the original state, the process must be reverse of the rotation.

**III. Key Structure**

K can be divided into three parts. They are 128bit, 192bit, 256bit. When K is 128bit, there are 8 Round Keys, 192bit would be 12 and 256bit would be 16 Round Keys. As the Fig. 2 the number of Round Key is shown when K is $nb$.



Fig. 2 Number of Round Key

As Fig. 3 Round Key is a 16bits key which is formed with Rotation Key and Mix Key. Starting from the left, each 2bit means $x\_{1}, x\_{2}, y\_{1}, y\_{2}, z\_{1}, z\_{2}$ and these 12bits form Rotation Key. Mix Key is used to mix the rotation sequence of axis and TABLE I. shows the sequence applied to Mix Key.



Figure 3. Round Key

TABLE I. Mix Key Table when encryption

|  |  |
| --- | --- |
| Mix Key | Sequence |
| $$0000\_{(2)}$$ | $$σx\_{1}, σx\_{2}, σy\_{1}, σy\_{2}, σz\_{1}, σz\_{2}$$ |
| $$0001\_{(2)}$$ | $$σx\_{2}, σx\_{1}, σy\_{2}, σy\_{1}, σz\_{2}, σz\_{1}$$ |
| $$0010\_{(2)}$$ | $$σx\_{1}, σx\_{2}, σz\_{1}, σz\_{2}, σy\_{1}, σy\_{2}$$ |
| $$0011\_{(2)}$$ | $$σx\_{2}, σx\_{1}, σz\_{2}, σz\_{1}, σy\_{2}, σy\_{1}$$ |
| $$0100\_{(2)}$$ | $$σy\_{1}, σy, σx\_{1}, σx\_{2}, σz\_{1}, σz\_{2}$$ |
| $$0101\_{(2)}$$ | $$σy\_{2}, σy\_{1}, σx\_{2}, σx\_{1}, σz\_{2}, σz\_{1}$$ |
| $$0110\_{(2)}$$ | $$σy\_{1}, σy\_{2}, σz\_{1}, σz\_{2}, σx\_{1}, σx\_{2}$$ |
| $$0111\_{(2)}$$ | $$σy\_{2}, σy\_{1}, σz\_{2}, σz\_{1}, σx\_{2}, σx\_{1}$$ |
| $$1000\_{(2)}$$ | $$σz\_{1}, σz\_{2}, σx\_{1}, σx\_{2}, σy\_{1}, σy\_{2}$$ |
| $$1001\_{(2)}$$ | $$σz\_{2}, σz\_{1}, σx\_{2}, σx\_{1}, σy\_{2}, σy\_{1}$$ |
| $$1010\_{(2)}$$ | $$σz\_{1}, σz\_{2}, σy\_{1}, σy\_{2}, σx\_{1}, σx\_{2}$$ |
| $$1011\_{(2)}$$ | $$σz\_{2}, σz\_{1}, σy\_{2}, σy\_{1}, σx\_{2}, σx\_{1}$$ |
| $$1100\_{(2)}$$ | $$σz\_{2}, σx\_{1}, σx\_{2}, σy\_{1}, σy\_{2}, σz\_{1}$$ |
| $$1101\_{(2)}$$ | $$σx\_{1}, σy\_{2}, σy\_{1}, σz\_{1}, σx\_{2}, σz\_{2}$$ |
| $$1110\_{(2)}$$ | $$σy\_{2}, σz\_{1}, σz, σx\_{1}, σx\_{2}, σy\_{1}$$ |
| $$1111\_{(2)}$$ | $$σx\_{2}, σy\_{1}, σy\_{2}, σz\_{1}, σz\_{2}, σx\_{1}$$ |

**IV. Conclusion**

In this paper, we suggested a new key of block ciper which applied symmetry and miscarriage of commutative law for cube. The 54 pieces of 3X3X3 Rubik’s Cube change to totally different pieces depending on the number of rotation time and sequence. Also, when dissolving changed cube to an original shape, it could be done by rotating the cube in inverse order. These peculiarities are the same as the symmetry of decryption on the block cipher. In the next paper, we will implement of block cipher algorithm using cube and veridate safety probabilities and encryption speed.

**Acknowledgment**

This research was supported by the MISP(Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW) (R7116-16-1018) supervised by the IITP(Institute for Information & communications Technology Promotion) and by the MISP(Ministry of Science, ICT & Future Planning), Korea, under the National Program for Excellence in SW) (R7719-16-1002) supervised by the IITP(Institute for Information & communications Technology Promotion)

**References**

[1] de Castella, Tom. "The people who are still addicted to the Rubik's Cube". BBC News Magazine. bbc.com. Retrieved 28 April 2014.

[2] 'Driven mad' Rubik's nut weeps on solving cube... after 26 years of trying, Daily Mail Reporter, January 12, 2009.

[3] Michael W., Dempsey,"Growing up with science: The illustrated encyclopedia of invention. London", Marshall Cavendish, pp. 1245, 1988

[4] Ewing, John; Czes Kosniowski (1982). Puzzle it Out: Cubes, Groups and Puzzles. Cambridge: Press Syndiacte of the University of Cambridge. p. 4. ISBN 0 521 28924 6. Retrieved 19 May 2014.

[5] Ferguson, N., Schneier, B. and Kohno, T. Indianapolis, "Cryptography Engineering: Design Principles and Practical Applications", Wiley Publishing Inc, pp. 63-64, 2010

[6] IBM's (International Business Machines) Walter Tuchman, "A brief history of the data encryption standard", ACM Press/Addison-Wesley Publishing Co., pp. 275–280, 1997

[7] “Announcing the ADVANCED ENCRYPTION STANDARD (AES)", Federal Information Processing Standards Publication 197, United States National Institute of Standards and Technology (NIST), October 2, 2012.

[8] Sung, Jaechul, "Differential cryptanalysis of eight-round SEED", Information Processing Letters, 7 June 2016.