# A New Higher Order Differential of RAGHAV

Naoki Shibayama

*Japan Air Self-Defense Force*
*Ministry of Defense*
Tokyo, Japan

Yasutaka Igarashi
*Faculty of Science and Technology*
*Tokyo University of Science*
Chiba, Japan

***Abstract*—RAGHAV is a 64-bit block cipher proposed by Bansod in 2021. It supports 80-, and 128-bit secret keys. The designer evaluated its security against typical attack, such as differential cryptanalysis, linear cryptanalysis, and so on. On the other hand, it has not been reported the security of RAGHAV against higher order differential attack, which is one of the algebraic attacks. In this paper, we applied higher order differential cryptanalysis to RAGHAV. As a results, we found a new full-round higher order characteristic of RAGHAV using 1-st order differential. Exploiting this characteristic, we also show that the full-round of RAGHAV is attackable by distinguishing attack with 2 chosen plaintexts.**

***Index Terms*—Cryptanalysis, Higher order differential, Saturation property, Block cipher, RAGHAV**

## I. Introduction

Bansod proposed a block cipher RAGHAV[1] supporting secret key length of 80-, and 128-bit in 2021. A data processing part of RAGHAV consists of specified round of Substitute-Permutation Network structure, which operates on 64-bit plaintext. The numbers of rounds are 31 for 80-bit and 128-bit keys respectively. In this paper, we analyze RAGHAV with 128-bit secret key.

The designer evaluated the security of RAGHAV against linear cryptanalysis, differential cryptanalysis, biclique analysis, zero correlation cryptanalysis and related key cryptanalysis. They argued that RAGHAV is secure enough against these attacks. On the other hand, it has not been reported the security of RAGHAV against higher order differential attack. Higher order differential attack is a powerful and versatile attack on block ciphers. It exploits the properties of higher order differentials of functions, defined by Lai, and derives an attack equation to estimate the key, and then determines the key by solving a formula.

This paper shows a new higher order differential of RAGHAV. By focusing on the structure of RAGHAV, we found the 31-round, i.e. full-round higher order differential characteristic of RAGHAV, in which 1-st order differential of the 32-bit output of the 31-st round equals to 0. As far as we know, this is the first report which investigates the higher order differential of RAGHAV. We also describe the distinguishing attack to full-round RAGHAV by using this characteristic. It needs 2 chosen plaintexts and encryption operations. Furthermore, by using the synchronous 1-st order differential, it is possible to apply the higher order differential attack to 9-round RAGHAV with $2^{5.9}$ blocks for chosen plaintext and $2^{59.9}$ times of encryption operation.

The rest of this paper is organized as follows. In Section II, we explain the specification of RAGHAV. Section III presents the general theory of the higher order differential attack. In Section IV, we show the results of the obtained higher order differential of RAGHAV. Then, we describe the attack using higher order differential in Section V, and conclude the paper in Section VI.

## II. Specification of RAGHAV

This section briefly describes the structure of RAGHAV. RAGHAV consists of 4/16 bits swaps, a 8-bit permutation, and the S-box transformation. Fig.1 shows the data processing part of RAGHAV. A symbol ' BP ' denotes bit permutation (Table I) and the ' S ' denotes 4-bit S-box (Table II), which is bijective and non-linear. The symbol ' $\oplus$ ' represents an XOR operation and $\lll m$ ($\ggg m$) denotes $m$-bit rotation to the left (right). Its input plaintext and output ciphertext are represented by $\mathbf{X}_1 = (X_1^{\mathrm{L}} \parallel X_1^{\mathrm{R}})$ and $\mathbf{C}_{31} = (C_{31}^{\mathrm{L}} \parallel C_{31}^{\mathrm{R}})$, where $X_i^{\mathrm{J}} = (x_{i,0}^{\mathrm{J}}, x_{i,1}^{\mathrm{J}}, \cdots, x_{i,7}^{\mathrm{J}})$, $C_i^{\mathrm{J}} = (c_{i,0}^{\mathrm{J}}, c_{i,1}^{\mathrm{J}}, \cdots, c_{i,7}^{\mathrm{J}})$, $1 \leq i \leq 31$, J$\in\{$L, R$\}$. A bit length of $X_i^j$ and $C_i^j$ is 32. $\mathbf{RK}_i = (RK_i^{\mathrm{L}} \parallel RK_i^{\mathrm{R}})$, $RK_i^{\mathrm{J}} = (rk_{i,0}^{\mathrm{J}}, rk_{i,1}^{\mathrm{J}}, \cdots, rk_{i,7}^{\mathrm{J}})$, $rk_{i,\ell}^{\mathrm{J}} \in \mathrm{GF}(2)^4$ are 64-bit round keys. The numbers of iterated rounds of data processing part are 31.

The key schedule consists of a left circular shift by 13-bit, an XORing of the counter, and 2 S-boxes shown in Fig.2. The input key is stored into the key register which is given as $\mathbf{K} = (k_0, k_1, \cdots, k_{127})$. For $i$-th round of encryption, $\mathbf{RK}_i$ is

TABLE I
Bit Permutation

| $x$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| BP[$x$] | 2 | 4 | 6 | 0 | 7 | 1 | 3 | 5 |

TABLE II
S-box

| $x$ | 0x0* | 0x1 | 0x2 | 0x3 | 0x4 | 0x5 | 0x6 | 0x7 |
|---|---|---|---|---|---|---|---|---|
| S[$x$] | 0x1 | 0x2 | 0x4 | 0xd | 0x6 | 0xf | 0xb | 0x8 |

| $x$ | 0x8 | 0x9 | 0xa | 0xb | 0xc | 0xd | 0xe | 0xf |
|---|---|---|---|---|---|---|---|---|
| S[$x$] | 0xa | 0x5 | 0xe | 0x3 | 0x9 | 0xc | 0x7 | 0x0 |

*0x denotes the subsequent number is a hexadecimal format.

[1]This paper has been accepted for publication at proceeding of the Tenth International Symposium on Computing and Networking Workshops (CANDARW 2022), which is published by IEEE. It has been further edited by IEEE, and the final version is appearing at https://doi.org/10.1109/CANDARW57323.2022.00016.

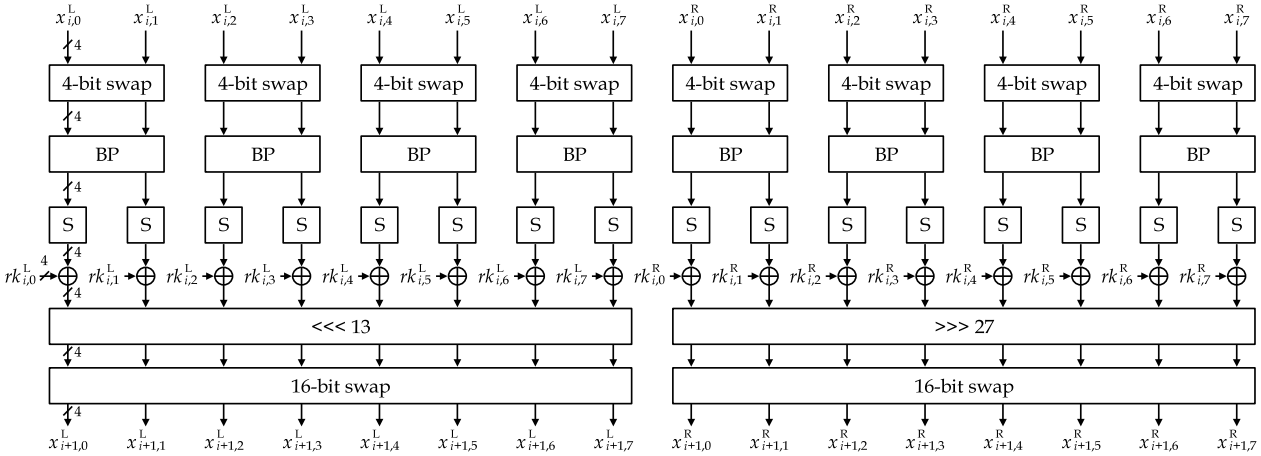


Fig. 1. Data processing part of RAGHAV

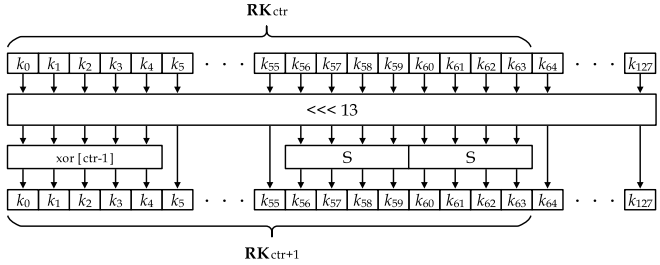


Fig. 2. Key schedule

generated by the following procedure, where ctr = 1.
(1) If $i = 1$, $\mathbf{RK}_i$ = ($k_0$, $k_1$, $\cdots$, $k_{63}$).
(2) The key register is circularly left shifted by 13-bit;

$$\mathbf{K} \lll 13.$$

(3) The 8-bit ($k_{56}$, $k_{57}$, $k_{58}$, $k_{59}$) and ($k_{60}$, $k_{61}$, $k_{62}$, $k_{63}$) are passed through the S-box;

$$(k_{56}, k_{57}, k_{58}, k_{59}) \leftarrow \mathrm{S}(k_{56}, k_{57}, k_{58}, k_{59}),$$
$$(k_{60}, k_{61}, k_{62}, k_{63}) \leftarrow \mathrm{S}(k_{60}, k_{61}, k_{62}, k_{63}).$$

(4) Apply the round counter, i.e. XOR the 5-bit round counter (ctr) of respective round with the key bits ($k_0$, $k_1$, $k_2$, $k_3$, $k_4$);

$$(k_0, k_1, k_2, k_3, k_4) \leftarrow (k_0, k_1, k_2, k_3, k_4) \oplus (\mathrm{ctr}{-}1).$$

(5) Increment the value of ctr, and if ctr $\leq$ 31, then $\mathbf{RK}_{\mathrm{ctr}}$ = ($k_0$, $k_1$, $\cdots$, $k_{63}$).

## III. Higher Order Differential

In this section, we describe the definition of higher order differential and some of its properties, and we consider an attack equation using these properties.

### A. Higher Order Differential [2]

Let $E(\cdot)$ be an encryption function as follows:

$$Y = E(X; K), \tag{1}$$

where $X \in \mathrm{GF}(2)^n$, $Y \in \mathrm{GF}(2)^m$, and $K \in \mathrm{GF}(2)^s$. For a block cipher, $X$, $K$, and $Y$ denote plaintext, key, and ciphertext respectively. Let $\{\mathbf{a}_1, \mathbf{a}_2, \cdots, \mathbf{a}_i\}$ be a set of linearly independent vectors in $\mathrm{GF}(2)^n$ and $V^{(i)}$ be a sub-space spanned by these vectors. The $i$-th order differential of $E(X; K)$ with respect to $X$ is defined as follows.

$$\Delta^{(i)}_{V^{(i)}} E(X; K) = \bigoplus_{\alpha \in V^{(i)}} E(X \oplus \alpha; K) \tag{2}$$

In the following, we abbreviate $\Delta^{(i)}_{V^{(i)}}$ as $\Delta^{(i)}$, when it is clearly understood.

In this paper, we use the following properties of the higher order differential.

**Property 1** : If the algebraic degree of $E(X; K)$ with respect to $X$ equals to $N\,(\leq n)$, then the following equation holds.

$$deg_X\{E(X;K)\} = N \rightarrow \begin{cases} \Delta^{(N)} E(X;K) & = const, \\ \Delta^{(N+1)} E(X;K) & = 0. \end{cases} \tag{3}$$

**Property 2** : Higher order differential has a linear property on Exclusive-OR sum.

$$\begin{aligned} &\Delta^{(N)} \{E_0(X; K_0) \oplus E_1(X; K_1)\} \\ &\quad = \Delta^{(N)} E_0(X; K_0) \oplus \Delta^{(N)} E_1(X; K_1) \end{aligned} \tag{4}$$

### B. Saturation Properties

We describe some definitions of saturation properties related to this paper.

Let a set of $2^N$ elements of $N$-bit values be $\mathbf{X} = \{X_i | X_i \in \{0,1\}^N, 0 \leq i < 2^N\}$. Now we first categorize saturation properties of the set $\mathbf{X}$ into four types depending on conditions defined as follows.

- **Constant** ( C ) : if $\forall_{i,j}$ , $X_i = X_j$
- **All** ( A ) : if $\forall_{i,j}$ , $i \neq j \Leftrightarrow X_i \neq X_j$
- **Even** ( E ) : if $\forall_i$ , $Y_i \equiv 0 \pmod 2$

- **Balance** ( B ) : $\bigoplus_i X_i = 0$,

where $Y_i$ denotes the number of occurrences of $X{=}i$.

If the saturation property of $2^\ell$ elements of $\ell$-bit values is ' A ', it is expressed as $\mathrm{A}_{(\ell)}$. Further, when $\mathrm{A}_{(\ell)}$ is divided into $m\,(\geq 2)$-nibble or $(m+1)$-nibble, it is written as follows.

$$\mathrm{A}_{(\ell)} = \begin{cases} (\mathrm{A}^0\,\mathrm{A}^1\,\cdots\,\mathrm{A}^{m-1}), & (\ell = 4m) \\ (\mathrm{A}^0\,\mathrm{A}^1\,\cdots\,\mathrm{A}^{m-1}\,\mathrm{A}^m_{(n)}), & (\ell = 4m+n) \end{cases}$$

where $0 < n < 4$. For example, 8-th order differential $\mathrm{A}_{(8)}$ is written as $(\mathrm{A}^0\,\mathrm{A}^1)$.

*1) Definition of Synchronous:* Let $(X_0, X_1)$ be $2^N$ elements of $2N$-bit values, and the saturation property of $X_0$ be $\mathrm{A}_{(N)}$. We define a saturation property for $X_1$ as follows.

- **Synchronous** ( S ) : if Eq.(5) holds.

$$X_0 \oplus X_1 = const. \tag{5}$$

In this paper, the property which synchronizes with $\mathrm{A}_{(\ell)}$ is written as '$\mathrm{S}_{(\ell)}$', and the characteristic using $\mathrm{A}_{(\ell)}$ and $\mathrm{S}_{(\ell)}$ is called synchronous higher order differential characteristic.

*2) Others:*

- **Unknown** ( U ) : No specific condition is known.

In the following, the symbol '$c$', '$\mathrm{A}_{(1)}$', '$\mathrm{S}_{(1)}$', '$b$', and '$u$' denote the saturation property of 1-bit value which are ' C ', ' A ', ' S ', ' B ', and ' U ' respectively. Then, if the saturation property of 1-nibble values $X_i$ is ' A ', we express this as

$$\{X_i\} = \mathrm{A}.$$

For multiple-nibble values, it is expressed as a similar manner. For example, if the saturation property of 4-nibble values $(X_0, X_1, X_2, X_3)$ is $(\mathrm{A}^0\ \mathrm{A}^1\ \mathrm{C}\ \mathrm{C})$, we express this as

$$\{(X_0, X_1, X_2, X_3)\} = (\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{C}\,\mathrm{C}).$$

We also use the following abbreviation.

$$\{(X_0, X_1, X_2, X_3)\} = (\mathrm{C}\,\mathrm{C}\,\mathrm{C}\,\mathrm{C}) = \mathbf{C},$$
$$\{(X_0, X_1, X_2, X_3)\} = (\mathrm{A}^0\,\mathrm{A}^1\,\mathrm{A}^2\,\mathrm{A}^3) = \mathbf{A},$$

where $\mathbf{A}$ follows expression rule of $\mathrm{A}_{(\ell)}$.

**Property 3** : If the saturation property of ciphertext $Y$ is ' C ', ' A ', ' E ', ' B ', or ' S ' using $\ell$-th order differential, $\Delta^{(\ell)}Y = 0$. Then, if the saturation property of its 1-bit value is '$\mathrm{A}_{(1)}$', or '$\mathrm{S}_{(1)}$' using 1-st order differential, $\Delta^{(1)}Y = 1$.

### C. Attack Equation

Consider an $r$-round iterative block cipher. Let $H_{r-1}(X) \in \mathrm{GF}(2)^m$ be a part of the $(r-1)$-th round output and $C(X) \in \mathrm{GF}(2)^n$ be the ciphertext corresponding to the plaintext $X \in \mathrm{GF}(2)^n$. $H_{r-1}(X)$ is expressed as follows.

$$H_{r-1}(X) = F_{r-1}(X; K_1, K_2, \cdots, K_{r-1}), \tag{6}$$

where $K_i \in \mathrm{GF}(2)^s$ be the $i$-th round key and $F_i(\cdot)$ be a function of $\mathrm{GF}(2)^n \times \mathrm{GF}(2)^{s\times i} \to \mathrm{GF}(2)^m$.

If the algebraic degree of $F_{r-1}(\cdot)$ with respect to $X$ is less than $N$, we have the following from Property 1.

$$\Delta^{(N)} H_{r-1}(X) = 0 \tag{7}$$

Let $\widetilde{F}(\cdot)$ be a decoding function that calculates $H_{r-1}(X)$ from a ciphertext $C(X) \in \mathrm{GF}(2)^n$.

$$H_{r-1}(X) = \widetilde{F}(C(X); K_r), \tag{8}$$

where $K_r \in \mathrm{GF}(2)^s$ denotes the $r$-th round key to decode $H_{r-1}(X)$ from $C(X)$. From Eqs.(2), (7), and (8), we can derive following equation and can determine $K_r$ by solving it.

$$\bigoplus_{\alpha \in V^{(N)}} \widetilde{F}(C(X \oplus \alpha); K_r) = 0 \tag{9}$$

In the following, we refer to Eq.(9) as an attack equation.

## IV. Higher Order Differential of RAGHAV

By computer experiment, we searched for the distinguisher of RAGHAV using higher order differential. As a results, we found that RAGHAV has the 31-round, i.e. full-round higher order differential characteristics.

### A. 1-st order differential

The higher order differential characteristics from input to 31-st round output can be written as follows.

$$\begin{aligned}
(\mathrm{A}1{-}i)\quad & (((c\mathrm{A}_{(1)}cc)\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\,\mathbf{C} \parallel \mathbf{C}\,\mathbf{C}) \\
& \xrightarrow{4r} (((cccu)\,\mathrm{U}\,\mathrm{U}\,\mathrm{U})\,(\mathrm{U}\,\mathrm{U}\,(uuuc)\,\mathrm{C}) \parallel \mathbf{C}\,\mathbf{C}) \\
& \xrightarrow{5\sim 31r} (\mathbf{U}\,\mathbf{U} \parallel \mathbf{C}\,\mathbf{C}), \\
(\mathrm{A}1{-}ii)\quad & ((\mathrm{C}\,\mathrm{C}\,(c\mathrm{A}_{(1)}ccc)\,\mathrm{C})\,\mathbf{C} \parallel \mathbf{C}\,\mathbf{C}) \\
& \xrightarrow{4r} (((uuuc)\,\mathrm{C}\,(cccu)\,\mathrm{U})\,\mathbf{U} \parallel \mathbf{C}\,\mathbf{C}) \\
& \xrightarrow{5\sim 31r} (\mathbf{U}\,\mathbf{U} \parallel \mathbf{C}\,\mathbf{C}), \\
(\mathrm{A}1{-}iii)\quad & (\mathbf{C}\,\mathbf{C} \parallel ((c\mathrm{A}_{(1)}cc)\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\,\mathbf{C}) \\
& \xrightarrow{4r} (\mathbf{C}\,\mathbf{C} \parallel ((cccu)\,\mathrm{U}\,\mathrm{U}\,\mathrm{U})\,(\mathrm{U}\,\mathrm{U}\,(uuuc)\,\mathrm{C})) \\
& \xrightarrow{5\sim 31r} (\mathbf{C}\,\mathbf{C} \parallel \mathbf{U}\,\mathbf{U}), \\
(\mathrm{A}1{-}iv)\quad & (\mathbf{C}\,\mathbf{C} \parallel (\mathrm{C}\,\mathrm{C}\,(c\mathrm{A}_{(1)}cc)\,\mathrm{C})\,\mathbf{C}) \\
& \xrightarrow{4r} (\mathbf{C}\,\mathbf{C} \parallel ((uuuc)\,\mathrm{C}\,(cccu)\,\mathrm{U})\,\mathbf{U}) \\
& \xrightarrow{5\sim 31r} (\mathbf{C}\,\mathbf{C} \parallel \mathbf{U}\,\mathbf{U}).
\end{aligned}$$

In the above characteristics, the left hand side of the formula expresses the input property and the right hand side means the output property. Although we found many other characteristics easily by changing the position $\mathrm{A}_{(1)}$ in the input property, we omit the description of them. The path of the upper 32-bit of the characteristic $(\mathrm{A}1{-}i)$ is depicted in Fig.3. We omit the input of the keys in the figure, because they have no influence on the characteristic. Then, the saturation properties of the bit position shown in white and gray are ' C ' and ' U ', respectively. In addition, the 1-st order differential of the bit position represented in red equals to 1.

In the structure of RAGHAV, since there is no diffusion between the upper 32-bit $X_1^{\mathrm{L}}$ and lower 32-bit $X_1^{\mathrm{R}}$ of the input plaintext, a fixed value is always propagated in $X_1^{\mathrm{L}}$ or $X_1^{\mathrm{R}}$, in which 1-st order differential is not inputted. Therefore,

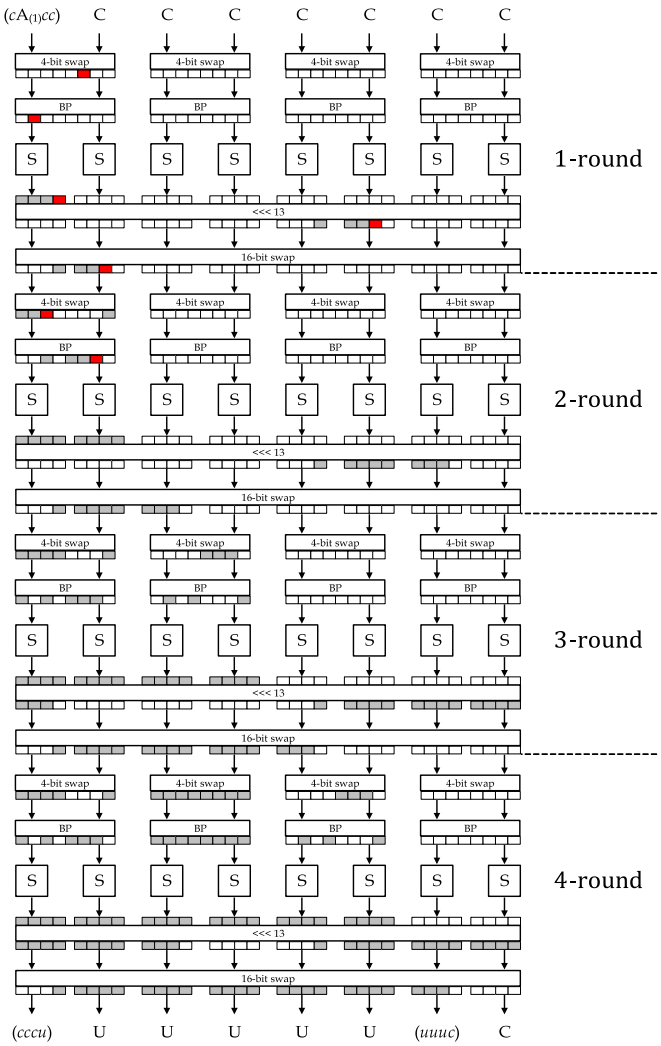


Fig. 3. Path of the upper 32-bit using 1-st order differential

the saturation property of the its 32-bit output of each round turn to be $(\mathbf{C}\,\mathbf{C})$.

And then, we can obtain the following 4-round higher order differential characteristic by inputting synchronous 1-st order differential.

$$\begin{aligned}(\mathrm{A1}{-}v)\quad & ((((c\mathrm{A}_{(1)}cc)\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\,\mathbf{C}\;\|\;((c\mathrm{S}_{(1)}cc)\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\,\mathbf{C})\\ &\xrightarrow{4r}((((cccu)\,\mathrm{U}\,\mathrm{U}\,\mathrm{U})\,(\mathrm{U}\,\mathrm{U}\,(uuuc)\,\mathrm{C})\;\|\\ &\qquad((cccu)\,\mathrm{U}\,\mathrm{U}\,\mathrm{U})\,(\mathrm{U}\,\mathrm{U}\,(uuuc)\,\mathrm{C}))\end{aligned}$$

This characteristic consists of the upper 32-bit and lower 32-bit of the similar characteristics $(\mathrm{A1}{-}i)$ and $(\mathrm{A1}{-}iii)$ respectively.

### B. 2-nd order differential

Using 2-nd order differential, we also found the 31-round higher order differential characteristics;

$$\begin{aligned}(\mathrm{A2}{-}i)\quad & (((((c\mathrm{A}^0_{(1)}cc)\,\mathrm{C}\,(c\mathrm{A}^1_{(1)}cc)\,\mathrm{C})\,\mathbf{C}\;\|\;\mathbf{C}\,\mathbf{C})\\ &\xrightarrow{5r}((\mathrm{U}\,(uubu)\,(uubu)\,\mathrm{U})\,\mathbf{U}\;\|\;\mathbf{C}\,\mathbf{C})\\ &\xrightarrow{6\sim31r}(\mathbf{U}\,\mathbf{U}\;\|\;\mathbf{C}\,\mathbf{C}),\\ (\mathrm{A2}{-}ii)\quad & (\mathbf{C}\,\mathbf{C}\;\|\;(((c\mathrm{A}^0_{(1)}cc)\,\mathrm{C}\,(c\mathrm{A}^1_{(1)}cc)\,\mathrm{C})\,\mathbf{C})\\ &\xrightarrow{5r}(\mathbf{C}\,\mathbf{C}\;\|\;(\mathrm{U}\,\mathrm{U}\,\mathrm{U}\,(uubu))\,((uubu)\,\mathrm{U}\,\mathrm{U}\,\mathrm{U}))\\ &\xrightarrow{6\sim31r}(\mathbf{C}\,\mathbf{C}\;\|\;\mathbf{U}\,\mathbf{U}),\\ (\mathrm{A2}{-}iii)\quad & (((((c\mathrm{A}^0_{(1)}cc)\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\,\mathbf{C}\;\|\;((c\mathrm{A}^1_{(1)}cc)\,\mathrm{C}\,\mathrm{C}\,\mathrm{C})\,\mathbf{C})\\ &\xrightarrow{5\sim31r}(\mathbf{E}\,\mathbf{E}\;\|\;\mathbf{E}\,\mathbf{E}).\end{aligned}$$

By inputting independent differentials to each of the upper 32-bit and lower 32-bit, the 2-nd order differential of the 64-bit output of the 31-st round becomes zero. Consequently, we found a new 31-round higher order differential characteristic using 1-st, 2-nd order differential respectively.

### C. 31-st order differential

If we use 31-st order differential, the higher order differential characteristics from input to 9-th round output can be written as follows.

$$\begin{aligned}(\mathrm{A31}{-}i)\quad & (\mathbf{A}^0\,(\mathrm{A}^1\,\mathrm{A}^2\,\mathrm{A}^3\,(\mathrm{A}^4_{(1)}\mathrm{A}^5_{(1)}\mathrm{A}^6_{(1)}c))\;\|\;\mathbf{C}\,\mathbf{C})\\ &\xrightarrow{9r}(\mathbf{U}\,(\mathrm{U}\,(uubu)\,(uubu)\,\mathrm{U})\;\|\;\mathbf{C}\,\mathbf{C})\\ &\xrightarrow{10\sim31r}(\mathbf{U}\,\mathbf{U}\;\|\;\mathbf{C}\,\mathbf{C}),\\ (\mathrm{A31}{-}ii)\quad & (\mathbf{C}\,\mathbf{C}\;\|\;\mathbf{A}^0\,(\mathrm{A}^1\,\mathrm{A}^2\,\mathrm{A}^3\,(\mathrm{A}^4_{(1)}\mathrm{A}^5_{(1)}\mathrm{A}^6_{(1)}c)))\\ &\xrightarrow{9r}(\mathbf{C}\,\mathbf{C}\;\|\;((uubu)\,\mathrm{U}\,\mathrm{U}\,\mathrm{U})\,(\mathrm{U}\,\mathrm{U}\,\mathrm{U}(uubu)))\\ &\xrightarrow{10\sim31r}(\mathbf{C}\,\mathbf{C}\;\|\;\mathbf{U}\,\mathbf{U}).\end{aligned}$$

Thus, if we consider that RAGHAV consists of 2-type of 32-bit block cipher algorithms, they have a 9-round higher order differential characteristics.

## V. Higher Order Differential Attack on RAGHAV

In this section, we describe the attack exploiting the characteristic of RAGHAV we found using 1-st order differential.

### A. Distinguishing Attack

From the results of the above simulations, we found a new 31-round higher order differential characteristics using 1-st order differential. Let $\mathbf{C}_i = (C_i^{\mathrm{L}} \parallel C_i^{\mathrm{R}})$ be an $i$-th round ciphertext. By exploiting the characteristic $(\mathrm{A1}{-}i)$, for instance, we can derive the following attack equation as

$$\bigoplus C_{31}^{\mathrm{R}} = 0. \tag{10}$$

We use this equation as a distinguisher and claim that the attack is successful if Eq.(10) is satisfied. Therefore, it is possible to apply the distinguishing attack to full-round of RAGHAV with 2 blocks for chosen plaintext and times of encryption operation.

### B. Higher Order Differential Attack

In the structure of RAGHAV, since the upper 32-bit and lower 32-bit of plaintext are independent, it can be considered to consist of 2-type of 32-bit block cipher algorithms. Furthermore, they are inputted to the round keys generated from the same secret key. Thus, by independently determining the round keys from these algorithms and using the relation among the round keys analyzed for the key schedule, we can efficiently recover all keys.

*1) Attack Equation:* Let $\mathbf{H}_i$=($H_i^{\mathrm{L}} \parallel H_i^{\mathrm{R}}$), $H_i^{\mathrm{J}}$=($h_{i,0}^{\mathrm{J}}$, $h_{i,1}^{\mathrm{J}}$, $\cdots$, $h_{i,7}^{\mathrm{J}}$), $h_{i,\ell}^{\mathrm{J}} \in \mathrm{GF}(2)^4$ be an output of the bit permutation in $i$-th round, where $1 \le i \le 31$, J$\in\{\mathrm{L},\mathrm{R}\}$, and $0 \le \ell \le 7$. Let $\mathbf{Z}_i$=($Z_i^{\mathrm{L}} \parallel Z_i^{\mathrm{R}}$), $Z_i^{\mathrm{J}}$=($z_{i,0}^{\mathrm{J}}$, $z_{i,1}^{\mathrm{J}}$, $\cdots$, $z_{i,7}^{\mathrm{J}}$), $z_{i,\ell}^{\mathrm{J}} \in \mathrm{GF}(2)^4$ be the variable after the round key is added. Let us denote $(m+1)$-th bit (to $(n+1)$-th bit) of the variable $x$ by $x[m]$ ($x[m,\cdots,n]$). In the upper 32-bit of the characteristic (A1$-v$), since the saturation properties of $c_{4,0}^{\mathrm{L}}[0,1,2]$, $c_{4,6}^{\mathrm{L}}[3]$, and $c_{4,7}^{\mathrm{L}}$ are ‘C’, we focus on the saturation properties ‘C’ which appear in the output $h_{5,0}^{\mathrm{L}}[1,3]$, $h_{5,1}^{\mathrm{L}}[3]$, $h_{5,6}^{\mathrm{L}}[0,2]$, and $h_{5,7}^{\mathrm{L}}[0,1,2]$ of the bit permutation in 5-th round. Fig.4 shows the equivalent circuit which calculates $C_4^{\mathrm{L}}$ from $Z_9^{\mathrm{L}}$. From Fig.4, we derive the following equations corresponding to Eq.(9).

$$\bigoplus h_{5,0}^{\mathrm{L}}[1,3] = 0, \tag{11}$$

$$\bigoplus h_{5,1}^{\mathrm{L}}[3] = 0, \tag{12}$$

$$\bigoplus h_{5,6}^{\mathrm{L}}[0,2] = 0, \tag{13}$$

$$\bigoplus h_{5,7}^{\mathrm{L}}[0,1,2] = 0, \tag{14}$$

$$\begin{aligned}
h_{5,0}^{\mathrm{L}}[1,3] &= \mathrm{S}^{-1}(z_{5,0}^{\mathrm{L}} \oplus rk_{5,0}^{\mathrm{L}})[1,3],\\
h_{5,1}^{\mathrm{L}}[3] &= \mathrm{S}^{-1}(z_{5,1}^{\mathrm{L}} \oplus rk_{5,1}^{\mathrm{L}})[3],\\
h_{5,6}^{\mathrm{L}}[0,2] &= \mathrm{S}^{-1}(z_{5,6}^{\mathrm{L}} \oplus rk_{5,6}^{\mathrm{L}})[0,2],\\
h_{5,7}^{\mathrm{L}}[0,1,2] &= \mathrm{S}^{-1}(z_{5,7}^{\mathrm{L}} \oplus rk_{5,7}^{\mathrm{L}})[0,1,2],
\end{aligned}$$

where $\mathrm{S}^{-1}$ denotes the inverse function of S-box.

*2) Analysis of Key schedule:* In Eq.(13), the unknown keys are 84-bit shown in red letters in Fig.4;

$$\begin{aligned}
&rk_{5,6}^{\mathrm{L}}, rk_{6,6}^{\mathrm{L}}, rk_{6,7}^{\mathrm{L}}, rk_{7,0}^{\mathrm{L}}, rk_{7,1}^{\mathrm{L}}, rk_{7,6}^{\mathrm{L}}, rk_{7,7}^{\mathrm{L}},\\
&rk_{8,0}^{\mathrm{L}}, rk_{8,1}^{\mathrm{L}}, rk_{8,2}^{\mathrm{L}}, rk_{8,3}^{\mathrm{L}}, rk_{8,6}^{\mathrm{L}}, rk_{8,7}^{\mathrm{L}}, RK_9^{\mathrm{L}}.
\end{aligned}$$

By using the relation among the round keys, we can drive these keys efficiently. Fig.5 shows these relations in the key schedule, where the keys of the bit position shown in white represent unknown. The 27-bit keys have the following relations.

$$\begin{aligned}
&rk_{5,6}^{\mathrm{L}}[2,3] = rk_{7,0}^{\mathrm{L}}[0,1],\ rk_{6,6}^{\mathrm{L}}[2,3] = rk_{8,0}^{\mathrm{L}}[0,1],\\
&rk_{6,7}^{\mathrm{L}} = ((rk_{8,0}^{\mathrm{L}}[2,3] \oplus \mathtt{0x3}) \parallel rk_{8,1}^{\mathrm{L}}[0,1]),\\
&rk_{7,6}^{\mathrm{L}} = (rk_{8,2}^{\mathrm{L}}[3] \parallel rk_{8,3}^{\mathrm{L}}[0] \parallel rk_{9,0}^{\mathrm{L}}[0,1]),\\
&rk_{7,7}^{\mathrm{L}} = ((rk_{9,0}^{\mathrm{L}}[2,3] \oplus \mathtt{0x3}) \parallel (rk_{9,1}^{\mathrm{L}}[0,1] \oplus \mathtt{0x2})),\\
&rk_{8,3}^{\mathrm{L}}[1,2,3] = (rk_{9,0}^{\mathrm{L}}[0,1,2] \oplus \mathtt{0x1}),\\
&rk_{8,6}^{\mathrm{L}} = (rk_{9,2}^{\mathrm{L}}[3] \parallel rk_{9,3}^{\mathrm{L}}[0,1,2]),\\
&rk_{8,7}^{\mathrm{L}} = (rk_{9,3}^{\mathrm{L}}[3] \parallel rk_{9,4}^{\mathrm{L}}[0,1,2]).
\end{aligned}$$

Because of these relations, the number of bit of unknowns can be reduced from 84-bit to 57-bit.

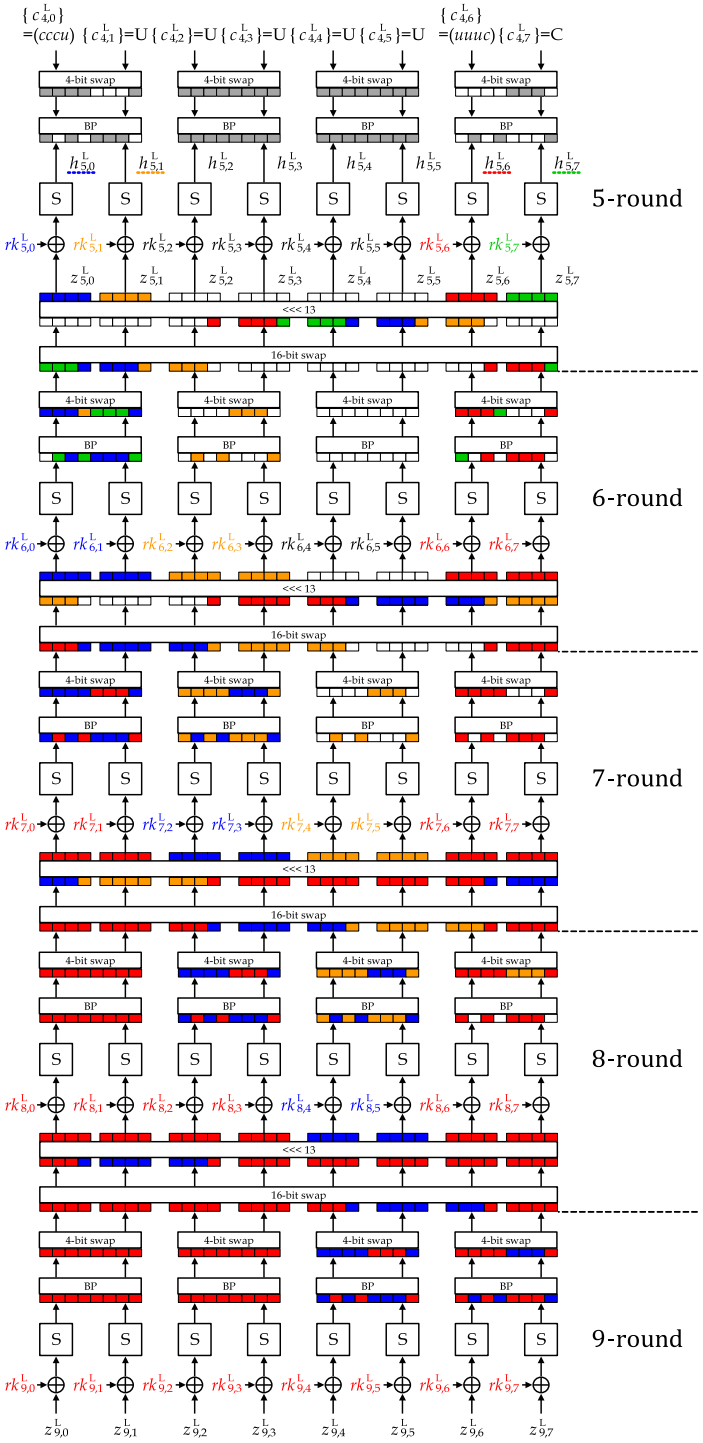


Fig. 4. Equivalent circuit which calculates $C_4^{\mathrm{L}}$ from $Z_9^{\mathrm{L}}$

From Fig.4, by solving Eqs.(11)∼(13), we can determine the 136-bit keys;

$$\begin{aligned}
&rk_{5,0}^{\mathrm{L}}, rk_{5,1}^{\mathrm{L}}, rk_{5,6}^{\mathrm{L}}, rk_{5,7}^{\mathrm{L}}, rk_{6,0}^{\mathrm{L}}, rk_{6,1}^{\mathrm{L}}, rk_{6,2}^{\mathrm{L}},\\
&rk_{6,3}^{\mathrm{L}}, rk_{6,6}^{\mathrm{L}}, rk_{6,7}^{\mathrm{L}}, RK_7^{\mathrm{L}}, RK_8^{\mathrm{L}}, RK_9^{\mathrm{L}}.
\end{aligned}$$

Similarly, these relations are shown in Fig.6, where the keys of the bit position shown in white, gray, and black are unknown.

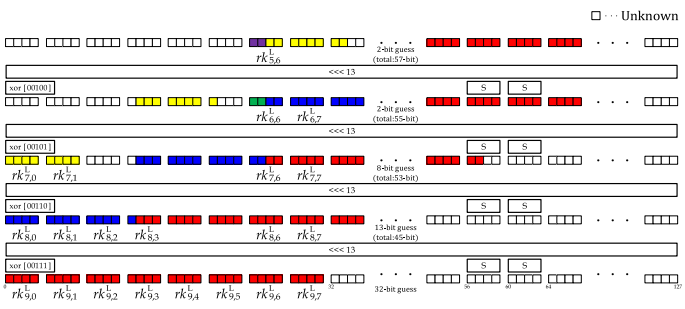


Fig. 5. Relation of the keys which are added from 5-round to 9-round

Therefore, based on Fig.6, it is necessary to determine the remaining total of 49-bit keys;

$$rk^{\mathrm{L}}_{4,0}[1,2,3], rk^{\mathrm{L}}_{4,1}, rk^{\mathrm{L}}_{4,2}, rk^{\mathrm{L}}_{4,3}[0], rk^{\mathrm{L}}_{5,2}, rk^{\mathrm{L}}_{5,3}[0], RK^{\mathrm{R}}_{9}.$$

*3) Attack Algorithm:* Attacker executes the following procedure to recover all keys.

**Step1** By solving Eq.(13), we can determine the 57-bit keys $rk^{\mathrm{L}}_{5,6}[0,1]$, $rk^{\mathrm{L}}_{6,6}[0,1]$, $rk^{\mathrm{L}}_{7,0}$, $rk^{\mathrm{L}}_{7,1}$, $rk^{\mathrm{L}}_{8,0}$, $rk^{\mathrm{L}}_{8,1}$, $rk^{\mathrm{L}}_{8,2}$, $rk^{\mathrm{L}}_{8,3}[0]$, and $RK^{\mathrm{L}}_{9}$ without the dependent keys.

First, the 32-bit mod 2 frequency distribution table (MFDT) of $Z^{\mathrm{L}}_{9}$ derives from 2 ciphertexts corresponding to the input a set of 2 plaintexts. Next, the 4-bit MFDT of $h^{\mathrm{L}}_{5,6}$ is derived by calculating (1)-(6) using the partial sum technique [3]. Finally, we calculate $\bigoplus h^{\mathrm{L}}_{5,6}[0,2]$ from the 4-bit MFDT of $h^{\mathrm{L}}_{5,6}$, and confirm if Eq.(13) holds.

(1) By assuming 16-bit $rk^{\mathrm{L}}_{9,4}$, $rk^{\mathrm{L}}_{9,5}$, $rk^{\mathrm{L}}_{9,6}$ and $rk^{\mathrm{L}}_{9,7}$, the 24-bit MFDT (`MFDT(1)`) of ($z^{\mathrm{L}}_{8,3}[1,2,3]$, $z^{\mathrm{L}}_{8,6}$, $z^{\mathrm{L}}_{8,7}[1]$, $z^{\mathrm{L}}_{9,0}$, $z^{\mathrm{L}}_{9,1}$, $z^{\mathrm{L}}_{9,2}$, $z^{\mathrm{L}}_{9,3}$) can calculate from the 32-bit MFDT of $Z^{\mathrm{L}}_{9}$.

(2) By assuming 16-bit $rk^{\mathrm{L}}_{9,0}$, $rk^{\mathrm{L}}_{9,1}$, $rk^{\mathrm{L}}_{9,2}$ and $rk^{\mathrm{L}}_{9,3}$, the 21-bit MFDT (`MFDT(2)`) of ($z^{\mathrm{L}}_{7,6}$, $z^{\mathrm{L}}_{7,7}[0]$, $z^{\mathrm{L}}_{8,0}$, $z^{\mathrm{L}}_{8,1}$, $z^{\mathrm{L}}_{8,2}$, $z^{\mathrm{L}}_{8,3}$) can calculate from `MFDT(1)`.

(3) By assuming 13-bit $rk^{\mathrm{L}}_{8,0}$, $rk^{\mathrm{L}}_{8,1}$, $rk^{\mathrm{L}}_{8,2}$ and $rk^{\mathrm{L}}_{8,3}[0]$, the 13-bit MFDT (`MFDT(3)`) of ($z^{\mathrm{L}}_{6,6}$, $z^{\mathrm{L}}_{6,7}[0]$, $z^{\mathrm{L}}_{7,0}$, $z^{\mathrm{L}}_{7,1}$) can calculate from `MFDT(2)`.

(4) By assuming 8-bit $rk^{\mathrm{L}}_{7,0}$ and $rk^{\mathrm{L}}_{7,1}$, the 7-bit MFDT (`MFDT(4)`) of ($z^{\mathrm{L}}_{5,6}[0,2,3]$, $z^{\mathrm{L}}_{6,6}$) can calculate from `MFDT(3)`.

(5) By assuming 2-bit $rk^{\mathrm{L}}_{6,6}[0,1]$, the 4-bit MFDT (`MFDT(5)`) of $z^{\mathrm{L}}_{5,6}$ can calculate from `MFDT(4)`.

(6) By assuming 2-bit $rk^{\mathrm{L}}_{5,6}[0,1]$, the 4-bit MFDT of $h^{\mathrm{L}}_{5,6}$ can calculate from `MFDT(5)`.

**Step2** By solving Eq.(11), we can determine 15-bit $rk^{\mathrm{L}}_{5,0}$, $rk^{\mathrm{L}}_{6,0}$, $rk^{\mathrm{L}}_{6,1}$ and $rk^{\mathrm{L}}_{7,2}[0,1,2]$ (total:72-bit), where

$$\begin{aligned}
rk^{\mathrm{L}}_{7,2}[3] &= rk^{\mathrm{L}}_{6,6}[0],\\
rk^{\mathrm{L}}_{7,3} &= (rk^{\mathrm{L}}_{6,6}[1] \parallel (rk^{\mathrm{L}}_{8,0}[0,1,2] \oplus \texttt{0x1})),\\
rk^{\mathrm{L}}_{8,4} &= ((rk^{\mathrm{L}}_{9,0}[3] \oplus \texttt{0x1}) \parallel (rk^{\mathrm{L}}_{9,1}[0,1,2] \oplus \texttt{0x4})),\\
rk^{\mathrm{L}}_{8,5} &= (rk^{\mathrm{L}}_{9,1}[3] \parallel rk^{\mathrm{L}}_{9,2}[0,1,2]).
\end{aligned}$$

**Step3** By solving Eq.(12), we can determine 7-bit $rk^{\mathrm{L}}_{5,1}$ and $rk^{\mathrm{L}}_{6,2}[0,1,2]$ (total:79-bit), where

$$\begin{aligned}
rk^{\mathrm{L}}_{6,2}[3] &= rk^{\mathrm{L}}_{5,6}[0],\\
rk^{\mathrm{L}}_{6,3} &= (rk^{\mathrm{L}}_{5,6}[1] \parallel (rk^{\mathrm{L}}_{7,0}[0,1,2] \oplus \texttt{0x1})),\\
rk^{\mathrm{L}}_{7,4} &= ((rk^{\mathrm{L}}_{8,0}[3] \oplus \texttt{0x1}) \parallel rk^{\mathrm{L}}_{8,1}[0,1,2]),\\
rk^{\mathrm{L}}_{7,5} &= (rk^{\mathrm{L}}_{8,1}[3] \parallel rk^{\mathrm{L}}_{8,2}[0,1,2]).
\end{aligned}$$

**Step4** In the lower 32-bit of the characteristic (A1$-v$), since the saturation properties of $c^{\mathrm{R}}_{4,6}[3]$, $c^{\mathrm{R}}_{4,7}[1,2]$ are 'C', we can determine 32-bit $RK^{\mathrm{R}}_{9}$ (total:111-bit) by solving $\Delta^{(1)}h^{\mathrm{R}}_{5,7}[0,1,2]=0$.

**Step5** In the upper 32-bit of the characteristic (A1$-ii$), since the saturation properties of $c^{\mathrm{L}}_{4,2}[0,1,2]$ are 'C', we can determine 5-bit $rk^{\mathrm{L}}_{5,2}$, $rk^{\mathrm{L}}_{5,3}[0]$ (total:116-bit) by solving $\Delta^{(1)}h^{\mathrm{L}}_{5,2}[1,3]=0$, $\Delta^{(1)}h^{\mathrm{L}}_{5,3}[3]=0$.

**Step6** In the upper 32-bit of the characteristic (A1$-v$), since the saturation properties of $c^{\mathrm{L}}_{3,0}[0,1,2]$ are 'C', we can determine 7-bit $rk^{\mathrm{L}}_{4,0}[1,2,3]$, $rk^{\mathrm{L}}_{4,1}$ (total:123-bit) by solving $\Delta^{(1)}h^{\mathrm{L}}_{4,0}[1,3]=0$, $\Delta^{(1)}h^{\mathrm{L}}_{4,1}[3]=0$.

**Step7** In the upper 32-bit of the characteristic (A1$-ii$), since the saturation properties of $c^{\mathrm{L}}_{3,2}[0,1,2]$ are 'C', we can determine 5-bit $rk^{\mathrm{L}}_{4,2}$, $rk^{\mathrm{L}}_{4,3}[0]$ (total:128-bit) by solving $\Delta^{(1)}h^{\mathrm{L}}_{4,2}[1,3]=0$, $\Delta^{(1)}h^{\mathrm{L}}_{4,3}[3]=0$.

*4) Complexity Estimation:* In Step1, if the assumed value of the 57-bit keys is true, Eq.(13) hold with probability 1. Because Eq.(13) is an equation of 2-bit, it is satisfied with probability $2^{-2}$ even if the assumed keys false. Therefore we need to solve $30\,(>\lceil\frac{57}{2}\rceil)$ sets of Eq.(13) with different $\mathbf{X}_1$ which need $30\times 2\approx 2^{5.9}$ chosen plaintexts in order to identify the true key. If we reuse the chosen plaintexts and ciphertexts, the number of chosen plaintexts required to identity the keys in Step2-7 can be reduced.

From the attack algorithm, since the procedure which required the most computational complexity is to identify the 57-bit keys by solving Eq.(13), other computational complexities are negligibly smaller than this and are omitted. Therefore, the computational complexity is as follows.

$$\mathbf{T} = T_0 + T_1 \approx 2^{67.1}\,(\text{S-box}),$$

$$\begin{aligned}
T_0 &= 2^{5,9},\\
T_1 &= 2^{16}(2^{32}+2^{16}(2^{24}+2^{13}\,(2^{21}+2^{8}(2^{13}+2^{2}(2^{7}+2^{2}\,(2^{4}))))))),
\end{aligned}$$

where $T_0$ is the computational complexity of 30-set of synchronous 1-st order differential, $T_1$ is the computational complexity required to determine the keys. In addition, the computational complexity required to determine the keys for the 9-round RAGHAV attack is $\mathbf{T} \approx 2^{67.1}$ times of S-box operation. Since 9-round RAGHAV consists of $144\,(=16\times 9)$ S-boxes, this computational complexity is equivalent to $2^{67.1}/144 \approx 2^{59.9}$ encryptions.

## VI. Conclusion

We have studied a higher order differential of RAGHAV. By focusing on the structure of RAGHAV, we found the full-round higher order differential characteristic of RAGHAV using 1-st order differential. If we use it, it is possible to apply the

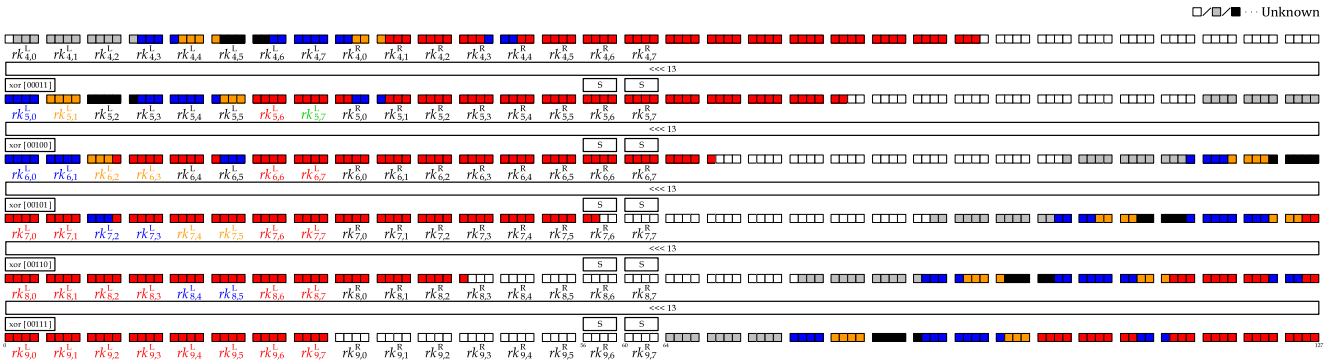


Fig. 6. Relation between the keys determined by solving Eqs.(11)∼(13) and the remaining keys

distinguishing attack to full-round RAGHAV with 2 blocks of chosen plaintext and times of encryption operation. Furthermore, using exhaustive key search, it is possible to apply the higher order differential attack to 9-round RAGHAV with $2^{5.9}$ blocks of chosen plaintext and $2^{59.9}$ times of encryption operation.

Our future work is to attack exploiting the 9-round higher order differential characteristic.

## REFERENCES


[1] G.Bansod, "RAGHAV : A new low power S-P network encryption design for resource constrained environment," https://eprint.iacr.org/2021/364.pdf, 2021.

[2] X.Lai, "Higher Order Derivatives and Differential Cryptanalysis," Communications and Cryptography, pp.227–233, Kluwer Academic Publishers, 1994.

[3] N.Ferguson, J.Kelsey, S.Lucks, B.Schneier, M.Stay, D.Wanger, and D.Whiting, "Improved Cryptanalysis of Rijndael," FSE2000, LNCS1978, pp.213–230, Springer, Heidelberg, 2001.