Impossible Differential Cryptanalysis of SPN Ciphers

Ruilin Li[1], Bing Sun[1] and Chao Li[1,2]

[1]Department of Mathematics and System Science, Science College, National University of Defense Technology, Changsha, 410073, China
securitylrl@gmail.com, happy_come@163.com
[2]State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, 100190, China
lichao_nudt@sina.com

Abstract. Impossible differential cryptanalysis is a very popular tool for analyzing the security of modern block ciphers and the core of such attack is based on the existence of impossible differentials. Currently, most methods for finding impossible differentials are based on the miss-in-the-middle technique and they are very ad-hoc. In this paper, we concentrate SPN ciphers and propose several criteria on the linear transformation P and its inversion P^{-1} to characterize the existence of 3/4-round impossible differentials. We further discuss the possibility to extend these methods to analyze 5/6-round impossible differentials. Using these criteria, impossible differentials for reduced-round Rijndael are found that are consistent with the ones found before. New 4-round impossible differentials are discovered for block cipher ARIA. And many 4-round impossible differentials are firstly detected for a kind of SPN cipher that employs a 32×32 binary matrix proposed at ICISC 2006 as its diffusion layer.

Keywords: block cipher, SPN, Rijndael, ARIA, linear transformation, impossible differential

1 Introduction

Many modern block ciphers are built using an iterative Substitution-Permutation Network (SPN), such as Shark, Square, Rijndael, Anubis, Khazad, ARIA, etc. These ciphers are generally designed to be immune against differential and linear cryptanalysis. However, they may be vulnerable to another powerful cryptanalytic method, the so called impossible differential cryptanalysis.

The idea of using impossible differentials (differentials with probability 0) to retrieve the secrete key of block cipehrs was firstly introduced by Knudsen [11] against the DEAL cipher and further by Biham et al. [1] to attack Skipjack. In fact, it is a kind of sieving attack that uses impossible differentials to exclude wrong key candidates. Since its emergence, impossible differential cryptanalysis has been used to attack many well-known block ciphers with very good results (see e.g. [4, 12, 13, 18, 19]).

The core of impossible differential cryptanalysis is based on the existence of impossible differentials. The longer the impossible differential is, the better the attack will be. Currently, most impossible differentials are found by miss-in-the-middle technique [2]. To find impossible differentials, firstly two differential characteristics from encryption and decryption directions both with probability 1 are constructed, and then they are connected together but with some inconsistence. Thus this combined long differential that consists of those two short ones is an impossible differential. Based on this idea, Kim et al. introduced $\mathcal{U}$-method [10] that could be used as an efficient tool to automatically find impossible differentials of many known block cipher structures. However, the disadvantage is that $\mathcal{U}$-method is too general to detect longer impossible differentials in some cases, because many information is lost during the calculation.

In a recent work [17], Wei et al. studied the impossible differential properties of Feistel ciphers with SP and SPS round functions, where the linear transformation P is defined over $\mathbb{F}_2^{n\times n}$. They characterized the existence of some 6/7/8-round impossible differentials (the hamming weights of both the input and output difference are 1) by presenting some sufficient conditions on P and its inversion P^{-1}. Using these criteria, impossible differentials of reduced-round Feistel ciphers, such as Camellia, E2, etc., could be studied in a unified approach.

In this paper, we concentrate SPN ciphers whose linear transformation P is defined over $\mathbb{F}_{2^d}^{n\times n}$. Based on the theory of matrix on finite field, we propose several criteria on P and its inversion P^{-1} to characterize the existence of 3/4-round impossible differentials. We also show that, due to the symmetry of the SPN structure, many similar criteria could be obtained. We further discuss the possibility to extend these methods to analyze 5/6-round impossible differentials. Using these criteria, impossible differentials for reduced-round Rijndael are found that are consistent with the ones found before. New 4-round impossible differentials are discovered for block cipher ARIA. And many 4-round impossible differentials are firstly detected for a kind of SPN cipher that employs a 32×32 binary matrix proposed at ICISC 2006 as its diffusion layer.

The advantage of the above two approaches is that one could discover some impossible differentials of reduced-round SPN (Feistel) ciphers just by observing the linear transformation, unlike the traditional ad-hoc approach, where one needs to follow the evolutional properties of the difference in both the encryption and decryption direction to detect some inconsistence by experience and intuition, according to the concrete components of the underlying block ciphers.

The outline of this paper is as follows: some preliminaries are introduced in Section 2. Section 3 and Section 4 present several criteria to characterize the existence of 3 and 4 rounds impossible differentials of SPN ciphers, respectively. Section 5 shows how to extend these methods to analyze 5/6-round SPN ciphers. Finally, Section 6 concludes this paper.

2 Preliminaries

In this section, we firstly describe SPN ciphers, and then introduce some notations that are used throughout this paper. Finally, we give the definition of χ-function that can be used as an useful tool to facilitate our cryptanalysis on the impossible differentials of SPN ciphers.

2.1 SPN Ciphers

Substitution-Permutation Network (SPN) structure can be seen as a direct realization of the concept of confusion and diffusion introduced by Shannon [16] to protect ciphers against statistical cryptanalysis. A classical SPN cipher is a kind of block cipher that alternatively iterates a substitution and a permutation (usually a bit-based shuffle), one such good example is the light-weight block cipher Present [3]. However, to achieve better and fast diffusion effects, many modern SPN ciphers adopt linear transformation with good branch number.

The class of SPN cipher considered in this paper is described below. Its block length is dn bits (or n-word with a word being d-bit), and the round function consists of three basic operations: a substitution layer, a diffusion layer and a round key addition layer.

The substitution layer is a non-linear transformation on $\mathbb{F}_{2^d}^n$ defined by n parallel non-linear bijective mappings on $\mathbb{F}_{2^d}$, i.e. $S : \mathbb{F}_{2^d}^n \rightarrow \mathbb{F}_{2^d}^n$ is defined by $S(x_1, x_2, \ldots, x_n) = (s_1(x_1), s_2(x_2), \ldots, s_n(x_n))$, where each s_i is a non-linear bijective mapping on $\mathbb{F}_{2^d}$ and all of them are not necessarily to be the same at different rounds. The diffusion layer is an invertible linear transformation P defined over $\mathbb{F}_{2^d}^{n \times n}$. The round key addition layer is defined simply by the exclusive or (XOR) of the round-key k_i and the input x, i.e. $\sigma_{k_i}(x) = x \oplus k_i$.

An r-round SPN cipher firstly applies a round key addition, and then iterates the round function $r-1$ times, the last round is the same but excludes the diffusion layer. We can describe the encryption procedure by

$$E_k(\cdot) = \sigma_{k_r} \circ S \circ \left(\bigcirc_{i=1}^{r-1} \sigma_{k_i} \circ P \circ S\right) \circ \sigma_{k_0}(\cdot),$$

where k_i is the dn-bit round-key that may be generated from the key schedule of the cipher. We omit the detail of the key schedule here since our impossible differential cryptanalysis is not relevant to it.

More precisely, in this paper, we consider SPN ciphers, where the differential branch number of the linear transformation doesn't achieve the maximum (n+1). In this situation, impossible differentials of any two-round SPN ciphers are easy to identify. Thus in the following sections, SPN ciphers with more than 2 rounds are in particular concentrated. We briefly describe three SPN ciphers in the appendices, including AES [15], ARIA [9], and a special kind of block cipher employing a binary matrix proposed in [8] as its diffusion layer.

2.2 Notations

We use $X = (x_{i,1}, x_{i,2}, \ldots, x_{i,n})$ to denote any n-word state, ΔX to denote the difference of X and X'. The difference used in this paper is the XOR($\oplus$)

difference, i.e. $\Delta X = X \oplus X'$. Particulary, e_j denotes an n-word state with the j-th position being non-zero and all other positions being zero, and $e_{j_1,j_2,\ldots,j_t}$ denotes an n-word state with the non-zero positions being $j_1, j_2, \ldots, j_t$. We use (α, β) to denote some differential, where α is the input difference and β is the output difference.

Note that the XOR difference is not influenced by the round-key addition layer, we thus omit this transformation when studying the evolutional property of difference in the encryption and decryption procedure. Moreover, it is well-known that given an input difference ΔX, after the linear transformation P, the output difference is $P(\Delta X)$. Now if we denote $S(X) \oplus S(X \oplus \Delta X)$ by $S(\Delta X)$, where S is the non-linear transformation in the substitution layer, then the output difference of an r-round SPN cipher could be represented by

$$S \circ \underbrace{P \circ S \circ \ldots \circ P \circ S \circ P \circ S}_{(r-1)-\text{round}} (\Delta X).$$

In fact, given ΔX, $S(\Delta X)$ represents several values according to the input X, however one can just choose one such value for his related discussion.

2.3 χ-Function

Definition 1. *(χ-function)* $\chi : \mathbb{F}_{2^d}^n \to \mathbb{F}_2$ *is defined as*

$$\chi(x_1, x_2, \ldots, x_n) = (\theta(x_1), \theta(x_2), \ldots, \theta(x_n)),$$

where $\theta : \mathbb{F}_{2^d} \to \mathbb{F}_2$ *is defined by*

$$\theta(x) = \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \neq 0 \end{cases}.$$

Given $X = (x_1, x_2, \ldots, x_n)$, define $\chi_s : \mathbb{F}_{2^d}^n \to \mathbb{F}_2$ by $\chi_s(X) = \theta(x_s)$, then $\chi_s(X) = 1 \Leftrightarrow x_s \neq 0$. This indicates that if we only consider whether there is a difference or not at some position while do not pay attention to its concrete value, then χ-function is an appropriate tool. Note that χ-function is well used in truncated differential cryptanalysis.

The following properties of χ-function has been pointed out in [17].

Property 1. [17] (1) For any difference $\Delta X \in \mathbb{F}_{2^d}^n$,

$$\chi(S(\Delta X)) = \chi(\Delta X).$$

(2) Let $P = (p_1, p_2, \ldots, p_n)$, where p_i is i-th column of P. If $\Delta X = e_i$, then

$$\chi(P \circ S(\Delta X)) = \chi(P(\Delta X)) = p_i.$$

(3) Let $X = (x_1, x_2, \ldots, x_n)$ and $Y = (y_1, y_2, \ldots, y_n)$. If $x_s = 0$, then

$$\chi_s(X \oplus Y) = \chi_s(Y).$$

Definition 2. *(Hamming Weight) Given* $X = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_{2^d}^n$*, the hamming weight of* X *is defined as the number of non-zero components of* X*:*

$$H_w(X) = \#\{i | x_i \neq 0, 1 \leq i \leq n\}.$$

3 Analysis of 3-Round SPN Ciphers

In this section, we present the following proposition to study the impossible differential property of 3-round SPN ciphers.

Proposition 1. *Given an SPN cipher with diffusion layer $P = (p_{ij})$, let the inversion of P be $P^{-1} = (q_{ij})$. If there exists $i_1, i_2, \ldots, i_r$, $j_1, j_2, \ldots, j_t$, and k, such that*

$$H_w(p_{k,i_1}, p_{k,i_2}, \ldots, p_{k,i_r}, q_{k,j_1}, q_{k,j_2}, \ldots, q_{k,j_t}) = 1,$$

then $(e_{i_1,i_2,\ldots,i_r}, e_{j_1,j_2,\ldots,j_t})$ is a 3-round impossible differential.

Proof. We finish this proof by contradiction. Assume $(e_{i_1,i_2,\ldots,i_r}, e_{j_1,j_2,\ldots,j_t})$ is a 3-round possible differential, then we have

$$S \circ P \circ S(e_{i_1,i_2,\ldots,i_r}) = P^{-1} \circ S^{-1}(e_{j_1,j_2,\ldots,j_t}). \tag{1}$$

Since

$$H_w(p_{k,i_1}, p_{k,i_2}, \ldots, p_{k,i_r}, q_{k,j_1}, q_{k,j_2}, \ldots, q_{k,j_t}) = 1,$$

without loss of generality, assume $p_{k,i_1} \neq 0$, $p_{k,l} = 0$, for $l = i_2, \ldots, i_r$, and $q_{k,l} = 0$, for $l = j_1, \ldots, j_t$.

Let $\alpha = S(e_{i_1,i_2,\ldots,i_r})$, then the k-th component of $P \circ \alpha$ is

$$\sum_{l=1}^{n} p_{kl}\alpha_l = \sum_{l \in \{i_1,i_2,\ldots,i_r\}} p_{kl}\alpha_l = p_{k,i_1}\alpha_{i_1} \neq 0,$$

Let $\beta = S^{-1}(e_{j_1,j_2,\ldots,j_t})$, then the k-th component of $P^{-1} \circ \beta$ is

$$\sum_{l=1}^{n} q_{kl}\alpha_l = \sum_{l \in \{j_1,j_2,\ldots,j_t\}} q_{kl}\alpha_l = 0.$$

According to Property 1,

$$\chi_k(S \circ P \circ S(e_{i_1,i_2,\ldots,i_r})) = \chi_k(P \circ \alpha) = 1,$$
$$\chi_k(P^{-1} \circ S^{-1}(e_{j_1,j_2,\ldots,j_t})) = \chi_k(P^{-1} \circ \beta) = 0,$$

which leads to a contradiction with Eq. (1). Thus $(e_{i_1,i_2,\ldots,i_r}, e_{j_1,j_2,\ldots,j_t})$ is a 3-round impossible differential. □

Example 1. (3-round impossible differential of AES) Given the following set $\{1, 2, 3, 4; 1, 2, 3, 4; 4\}$, we find that $p_{4,1} = \texttt{03}$, $p_{4,2} = p_{4,3} = p_{4,4} = 0$, and $q_{4,1} = q_{4,2} = q_{4,3} = q_{4,4} = 0$, thus according to Proposition 1, $(e_{1,2,3,4}, e_{1,2,3,4})$ is a 3-round impossible differential of AES.

Example 2. (3-round impossible differential of ARIA) Given the following set $\{1, 2, 4, 5, 7; 11, 12, 14, 15, 16; 2\}$, we find that $p_{2,1} = p_{2,2} = p_{2,4} = p_{2,5} = p_{2,7} = 0$, $q_{2,11} = q_{2,12} = q_{2,14} = q_{2,15} = 0$, and $q_{2,16} = 1$, thus $(e_{1,2,4,5,7}, e_{11,12,14,15,16})$ is a 3-round impossible differential of ARIA.

4 Analysis of 4-Round SPN Ciphers

This section concentrates 4-round SPN ciphers. We present three kinds of sufficient conditions to characterize the existence of 4-round impossible differentials, where the hamming weights of both the input and output difference are 1. We further show how to deal with the case when hamming weights exceed 1.

All proofs of the three propositions in the following sub-sections are finished by contradiction. To verify whether a given 4-round differential (e_i, e_j) is impossible, one firstly assume (e_i, e_j) is a possible one, then according to the encryption procedure, he get

$$P \circ S \circ P \circ S(e_i) = S^{-1} \circ P^{-1} \circ S^{-1}(e_j). \tag{2}$$

Using this equation, he could deduce some contradiction with the conditions that proposed in the proposition, and thus completes the proofs.

4.1 The First Criterion

The first criterion is the one that used especially in AES-like ciphers.

Proposition 2. *Given an SPN cipher with diffusion layer $P = (p_{ij})$, let the inversion of P be $P^{-1} = (q_{ij})$. For any $1 \leq i, j \leq n$, let*

$$U_j = \{r | q_{rj} = 0\} = \{r_1, r_2, \ldots, r_u\},$$
$$V_i = \{t | p_{ti} \neq 0\} = \{t_1, t_2, \ldots, t_v\},$$

and

$$M_{ij} = (p_{r_a, t_b})_{u \times v} = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_u \end{pmatrix},$$

where each m_i is the i-th row vector of M_{ij}.

If $U_j, V_i \neq \emptyset$, and there exists an $l \in \{1, 2, \ldots, u\}$, such that $H_w(m_l) = 1$, then (e_i, e_j) is a 4-round impossible differential.

Proof. Let $\lambda = S \circ P \circ S(e_i)$ and $\gamma = S^{-1} \circ P^{-1} \circ S^{-1}(e_j)$, then Eq. (2) becomes

$$P\lambda = \gamma. \tag{3}$$

According to the definition of V_i, for any $t \in V_i$, $\chi_t(\lambda) = 1$, and for $t \notin V_i$, $\chi_t(\lambda) = 0$, which implies that $\lambda_t \neq 0 \Leftrightarrow t \in V_i$, thus the left side of Eq. (3) becomes

$$P\lambda = \sum_{a=1}^{v} P_{t_a} \lambda_{t_a},$$

where P_i is the i-th column vector of P and λ_i is the i-th component of λ.

Now consider the right side of Eq.(3), according to the definition of U_j, for any $r \in U_j$, $\chi_r(\gamma) = 0$, which tells that $\chi_r(P \circ \lambda) = 0$. Thus,

$$\begin{aligned} p_{r_1,t_1}\lambda_{t_1} + p_{r_1,t_2}\lambda_{t_2} + \ldots + p_{r_1,t_v}\lambda_{t_v} &= 0 \\ p_{r_2,t_1}\lambda_{t_1} + p_{r_2,t_2}\lambda_{t_2} + \ldots + p_{r_2,t_v}\lambda_{t_v} &= 0 \\ \vdots \qquad\qquad\qquad\qquad & \quad \vdots \\ p_{r_u,t_1}\lambda_{t_1} + p_{r_u,t_2}\lambda_{t_2} + \ldots + p_{r_u,t_v}\lambda_{t_v} &= 0 \end{aligned} \tag{4}$$

The above linear equation system could be represented as

$$M_{ij}\widetilde{\lambda} = 0, \tag{5}$$

where $M_{ij} = (p_{r_a,t_b})_{u\times v}$, and $\widetilde{\lambda} = (\lambda_{t_1}, \ldots, \lambda_{t_v})^{\mathrm{T}}$, with each λ_{t_i} being non-zero.

Since there exists an $l \in \{1, 2, \ldots, u\}$, such that $H_w(m_l) = H_w(p_{r_l,t_1}, p_{r_l,t_2}, \ldots, p_{r_l,t_v}) = 1$, we have $m_l \cdot \widetilde{\lambda} \neq 0$ which is a contraction with the l-th equation of the linear system (4). □

Example 3. (4-round impossible differential of AES) Given $i = j = 1$, then $U_i = \{2, 3, 4, 5, 7, 8, 9, 10, 12, 13, 14, 15\}$, and $V_j = \{1, 2, 3, 4\}$, thus

$$M_{11} = \begin{pmatrix} 1&0&0&0 \\ 1&0&0&0 \\ 3&0&0&0 \\ 0&0&0&1 \\ 0&0&0&3 \\ 0&0&0&2 \\ 0&0&1&0 \\ 0&0&3&0 \\ 0&0&1&0 \\ 0&3&0&0 \\ 0&2&0&0 \\ 0&1&0&0 \end{pmatrix}.$$

Since for each $l \in \{1, 2, \ldots, 12\}$, $H_w(m_l) = 1$, (e_1, e_1) is a 4-round impossible differential of AES.

4.2 The Second Criterion

For many SPN ciphers, the sub-matrix M_{ij} usually doesn't satisfy the condition in Proposition 2, thus we propose the following criterion, which generalizes the idea in [17], to characterize the existence of 4-round impossible differentials.

Proposition 3. *Given an SPN cipher with diffusion layer $P = (p_{ij})$, let the inversion of P be $P^{-1} = (q_{ij})$. For any $1 \leq i, j \leq n$, let*

$$\begin{aligned} U_j &= \{r | q_{rj} = 0\} = \{r_1, r_2, \ldots, r_u\}, \\ V_i &= \{t | p_{ti} \neq 0\} = \{t_1, t_2, \ldots, t_v\}, \end{aligned}$$

and

$$M_{ij} = (p_{r_a,t_b})_{u\times v} = (m_1, m_2, \ldots, m_v),$$

where each m_i is the i-th column vector of M_{ij}.

If $U_j, V_i \neq \emptyset$, and there exists an $l \in \{1, 2, \ldots, v\}$, such that

$$\mathrm{rank}\{\{m_1, m_2, \ldots, m_v\} \backslash \{m_l\}\} < \mathrm{rank}\{m_1, m_2, \ldots, m_v\},$$

then (e_i, e_j) is a 4-round impossible differential.

Proof. According to Eq. (3), $\sum_{j=1}^{v} \lambda_{t_j} \cdot m_j = 0$, where each λ_{t_i} is non-zero. Since $\lambda_{t_l} \neq 0$, we get

$$m_l = \sum_{b=1, b\neq l}^{v} \frac{\lambda_{t_b}}{\lambda_{t_l}} \cdot m_j,$$

which implies that m_l could be represented by $\{m_1, \ldots, m_{l-1}, m_{l+1}, \ldots, m_v\}$, thus

$$\text{rank}\{\{m_1, m_2, \ldots, m_l\} \backslash \{m_l\}\} = \text{rank}\{m_1, m_2, \ldots, m_l\},$$

which is a contraction with the condition as described in the proposition. Thus we end the proof. □

Example 4. (4-round impossible differential of ARIA) Given $i = j = 1$, then $U_1 = \{1, 2, 3, 6, 8, 11, 12, 13, 16\}$, and $V_1 = \{4, 5, 7, 9, 10, 14, 15\}$, thus

$$M_{1,1} = \begin{pmatrix} \mathbf{1} & 1 & 1 & 1 & 1 & 1 & 1 \\ \mathbf{0} & 0 & 0 & 1 & 1 & 0 & 0 \\ \mathbf{0} & 1 & 1 & 0 & 0 & 0 & 0 \\ \mathbf{1} & 1 & 0 & 0 & 1 & 0 & 1 \\ \mathbf{1} & 0 & 1 & 1 & 0 & 1 & 0 \\ \mathbf{1} & 0 & 1 & 1 & 0 & 1 & 0 \\ \mathbf{1} & 1 & 0 & 0 & 1 & 0 & 1 \\ \mathbf{0} & 0 & 1 & 0 & 1 & 0 & 0 \\ \mathbf{0} & 1 & 0 & 1 & 0 & 0 & 0 \end{pmatrix} \triangleq (m_1, m_2, \ldots, m_7).$$

One can verify that

$$\text{rank}\{\{m_1, m_2, \ldots, m_7\} \backslash \{m_1\}\} = 5 < 6 = \text{rank}\{m_1, m_2, \ldots, m_7\},$$

thus (e_1, e_1) is a 4-round impossible differential of ARIA.

Using this method, we can further find many similar 4-round impossible differentials of ARIA, and the results are listed in Table 1.

Table 1. 4-Round Impossible Differential (e_i, e_j) of ARIA

i	j	i	j
1	1, 2, 3, 6, 8, 11, 12, 13, 16	9	3, 4, 6, 7, 9, 10, 12, 13, 15
2	1, 2, 4, 5, 7, 11, 12, 14, 15	10	3, 4, 5, 8, 9, 10, 11, 14, 16
3	1, 3, 4, 6, 8, 9, 10, 14, 15	11	1, 2, 5, 8, 10, 11, 12, 13, 15
4	2, 3, 4, 5, 7, 9, 10, 13, 16	12	1, 2, 6, 7, 9, 11, 12, 14, 16
5	2, 4, 5, 7, 8, 10, 11, 13, 14	13	1, 4, 5, 6, 9, 11, 14, 15, 16
6	1, 3, 6, 7, 8, 9, 12, 13, 14	14	2, 3, 5, 6, 10, 12, 13, 15, 16
7	2, 4, 5, 6, 7, 9, 12, 15, 16	15	2, 3, 7, 8, 9, 11, 13, 14, 16
8	1, 3, 5, 6, 8, 10, 11, 15, 16	16	1, 4, 7, 8, 10, 12, 13, 14, 15

4.3 The Third Criterion

We propose here another criterion to analyze 4-round impossible differentials.

Proposition 4. *Given an SPN cipher with diffusion layer $P = (p_{ij})$, let the inversion of P be $P^{-1} = (q_{ij})$. For any $1 \le i, j \le n$, let*

$$U_j = \{r | q_{rj} = 0\} = \{r_1, r_2, \ldots, r_u\},$$
$$W_j = \{s | q_{sj} \neq 0\} = \{s_1, s_2, \ldots, s_w\},$$
$$V_i = \{t | p_{ti} \neq 0\} = \{t_1, t_2, \ldots, t_v\},$$

and

$$M_{ij} = (p_{r_a,t_b})_{u\times v} = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_u \end{pmatrix}, \quad M'_{ij} = (p_{r_a,t_b})_{w\times v} = \begin{pmatrix} m'_1 \\ m'_2 \\ \vdots \\ m'_w \end{pmatrix},$$

where each m_i (resp. m'_i) denotes the i-th row vector of M_{ij} (resp. M'_{ij}).

If $U_j, W_j, V_i \neq \emptyset$, and there exists an $l \in \{1, 2, \ldots, w\}$, such that

$$\mathrm{rank}\{m_1, m_2, \ldots, m_u, m'_l\} = \mathrm{rank}\{m_1, m_2, \ldots, m_u\},$$

then (e_i, e_j) is a 4-round impossible differential.

Proof. According to Eq. (5), let $(\lambda_{t_1}, \lambda_{t_2}, \ldots, \lambda_{t_v})^{\mathrm{T}} = \widetilde{\lambda} \triangleq (\widetilde{\lambda}_1, \ldots, \widetilde{\lambda}_v)^{\mathrm{T}}$, with each $\widetilde{\lambda}_b \neq 0$, where $b = 1, 2, \ldots, v$, and let $m_a = (m_{a,1}, m_{a,2}, \ldots, m_{a,v})$, where $a = 1, 2, \ldots, u$. Then $m_a \cdot \widetilde{\lambda} = 0$.

Assume $m'_a = (m'_{a,1}, m'_{a,2}, \ldots, m'_{a,v})$, where $a = 1, 2, \ldots, w$, then according to the definition M'_{ij}, for any $a \in \{1, 2, \ldots, w\}$, $m'_a \cdot \widetilde{\lambda} \neq 0$.

Since there exists an $l \in \{1, 2, \ldots, w\}$, such that m'_l could be represented by $\{m_1, m_2, \ldots, m_u\}$, we have $m'_l = \sum_{a=1}^{u} c_a\ m_a$, where $c_1, c_2, \ldots, c_u$ are some constants, thus $m'_{lb} = \sum_{a=1}^{u} c_a\ m_{ab}$, where $b = 1, 2, \ldots, v$.

Now we get

$$\begin{aligned} m'_l \cdot \widetilde{\lambda} = \sum_{b=1}^{v} m'_{lb} \cdot \widetilde{\lambda}_b &= \sum_{b=1}^{v} \left(\sum_{a=1}^{u} c_a\ m_{ab} \right) \widetilde{\lambda}_b \\ &= \sum_{a=1}^{u} c_a \left(\sum_{b=1}^{v} m_{ab}\, \widetilde{\lambda}_b \right) \\ &= \sum_{a=1}^{u} c_a \cdot \left(m_a \cdot \widetilde{\lambda} \right) = \sum_{a=1}^{u} c_a \cdot 0 = 0, \end{aligned}$$

which leads to a contradiction. □

Example 5. (4-round Impossible Differential of ARIA) Given $i = j = 1$, then $U_1 = \{1, 2, 3, 6, 8, 11, 12, 13, 16\}$, $W_1 = \{4, 5, 7, 9, 10, 14, 15\}$, and $V_1 = \{4, 5, 7, 9, 10, 14, 15\}$, thus

$$M_{1,1} = \begin{pmatrix} 1&1&1&1&1&1&1 \\ 0&0&0&1&1&0&0 \\ 0&1&1&0&0&0&0 \\ 1&1&0&0&1&0&1 \\ \mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0} \\ 1&0&1&1&0&1&0 \\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1} \\ 0&0&1&0&1&0&0 \\ 0&1&0&1&0&0&0 \end{pmatrix}, \quad M'_{1,1} = \begin{pmatrix} 0&0&0&0&0&1&1 \\ 0&0&0&1&0&0&1 \\ 0&0&0&0&1&1&0 \\ 0&1&0&0&0&1&0 \\ 0&0&1&0&0&0&1 \\ \mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{1}&\mathbf{0} \\ \mathbf{1}&\mathbf{1}&\mathbf{0}&\mathbf{0}&\mathbf{1}&\mathbf{0}&\mathbf{1} \end{pmatrix}.$$

One can see that the last row vector of M'_{11} is equal to the seventh row vector of M_{11}, or the last second row vector of M'_{11} is equal to the fifth row vector of M_{11}, thus we obtain the same 4-round impossible differential (e_1, e_1).

An interesting result is that, by using the criterion as described in Proposition 4, we find the same impossible differentials as described in Table 1, which are found based on Proposition 3.

Example 6. (4-round Impossible Differential of a Kind of SPN Cipher) In [8], a special kind of 32×32 binary matrix was introduced that could be used to serve as the diffusion part of some 256-bit SPN ciphers. The designs showed that such binary matrix had good branch number and could be efficiently implemented. They further claimed that it could resist truncated and impossible differential cryptanalysis, especially that there would not exist any impossible differentials with more than 3-rounds. However, using the methods proposed in Proposition 3 or 4, we can demonstrate that for any given $1 \leq i, j \leq 32$, (e_i, e_j) is a 4-round impossible differential.

4.4 The Dual Case

We use the notion "dual case" to describe the phenomenon that, due to the symmetric property of the SPN structure, many similar criteria could be proposed to characterize the existence of impossible differentials. For example, Eq. (2) is equivalent to

$$S \circ P \circ S(e_i) = P^{-1} \circ S^{-1} \circ P^{-1} \circ S^{-1}(e_j),$$

which indicates that if we exchange the role of P and P^{-1} as well as i and j as shown in Proposition 2, 3 and 4, we could obtain another criterion. The same case exists when analyzing 5/6-round SPN ciphers.

4.5 The General Case

We show how to analyze 4-round impossible differentials whose input difference and (or) output difference are (is) with hamming weight(s) exceeding 1.

In general, given an input difference $\alpha \neq 0$ and an output difference $\beta \neq 0$, the criterion that we want to propose will be based on the following equation

$$P \circ S \circ P \circ S(\alpha) = S^{-1} \circ P^{-1} \circ S^{-1}(\beta),$$

or equivalently,

$$P\lambda = \gamma, \tag{6}$$

with $\lambda = S \circ P \circ S(\alpha)$ and $\gamma = S^{-1} \circ P^{-1} \circ S^{-1}(\beta)$.

Note that, the left side of Eq. (6) is equivalent to $\sum_{l=1}^{n} P_l \cdot \lambda_l$, thus if $\lambda_k = 0$, then the contribution of $P_k \cdot \lambda_k$ in the summation could be omitted.

Properties of $\boldsymbol{\lambda = S \circ P \circ S(\alpha)}$ and $\boldsymbol{\gamma = S^{-1} \circ P^{-1} \circ S^{-1}(\beta)}$. We concentrate the components of λ and γ. Take $\lambda = S \circ P \circ S(\alpha)$ as an example: each component of λ has three possible states, *the zero state* (**0**), *the non-zero state* (*****), and *the unknown state* (**?**). The unknown state is such state that one could not definitely determine whether its value is zero or non-zero, that is sometimes the value of the component could be non-zero, while sometimes it could be zero. In fact, we can classify the components of λ according to the input difference α.

(1) If $\alpha = e_i$, according to Property 1,

$$\chi_k(\lambda) = \chi_k(S \circ P \circ S(e_i)) = \chi_k(P \circ S(e_i)) = \chi_k(P(e_i)) = \theta(p_{ki}),$$

which implies that λ_k is either zero or non-zero, and thus the unknown state never appears in this situation.

(2) If $H_w(\alpha) > 1$, without loss of generality, assume $\alpha = e_{i_1,i_2,\ldots,i_r}$, then

$$\begin{aligned}\chi_k(\lambda) &= \chi_k(S \circ P \circ S(e_{i_1,i_2,\ldots,i_r})) \\ &= \chi_k(P \circ S(e_{i_1,i_2,\ldots,i_r})) \\ &= \theta\left(\sum_{l=1}^{r} p_{k,i_l} \cdot \delta_{i_l}\right),\end{aligned} \tag{7}$$

where δ_{i_l} is a possible output difference of the i_1-th s-box in the substitution layer. Thus λ_k could be either *****, **0**, or **?**. However, from Eq. (7), we can discuss the state of λ_k according to the hamming weight of $(p_{k,i_1}, p_{k,i_2}, \ldots, p_{k,i_r})$.

- If $H_w(p_{k,i_1}, p_{k,i_2}, \ldots, p_{k,i_r}) = 0$, then λ_k is 0,
- If $H_w(p_{k,i_1}, p_{k,i_2}, \ldots, p_{k,i_r}) = 1$, then λ_k is *,
- If $H_w(p_{k,i_1}, p_{k,i_2}, \ldots, p_{k,i_r}) > 1$, then λ_k is ?.

Similarly, we can analyze the component state of $\gamma = S^{-1} \circ P^{-1} \circ S^{-1}(\beta)$ when $\beta = (e_{j_1,j_2,\ldots,j_t})$.

Motivations of Proposition 2, 3 and 4. Let's further discuss why we could propose the former three criteria to characterize the existence of 4-round impossible differentials of SPN ciphers when $(\alpha, \beta) = (e_i, e_j)$. Recall that, in this situation, all components of both λ and γ are either 0 or $*$.

- Proposition 2 and 3 are based on the existence of two non-empty sets U_j and V_i. U_j chooses the positions of all zero difference of γ and V_i chooses the positions of all non-zero difference of λ. Then (U_j, V_i) is used to select a sub-matrix M_{ij} from P, where some inconsistence are detected which leads to some 4-round impossible differentials.
- Proposition 4 needs another non-empty set W_j to choose the positions of all non-zero difference of γ. Then (W_j, V_i) is used to select another sub-matrix M'_{ij} from P, and some inconsistence are detected between M_{ij} and M'_{ij}.

Generalized Methods. If we turn to the general case $(\alpha, \beta) = (e_{i_1,i_2,\ldots,i_r}, e_{j_1,j_2,\ldots,j_t})$, the components of both $\lambda = S \circ P \circ S(\alpha)$ and $\gamma = S^{-1} \circ P^{-1} \circ S^{-1}(\beta)$ will have three possible states. Thus, in order to generalize the former three propositions (Proposition 2, 3 and 4) into this situation, the definitions of U_j, W_j, and V_i must be modified to the followings:

$$\begin{aligned} U_\beta &= \{k | H_w(q_{k,j_1}, q_{k,j_2}, \ldots, q_{k,j_t}) = 0\}, \\ W_\beta &= \{k | H_w(q_{k,j_1}, q_{k,j_2}, \ldots, q_{k,j_t}) = 1\}, \text{ and} \\ V_\alpha &= \{1, 2, \ldots, n\} - \{k | H_w(p_{k,i_1}, p_{k,i_2}, \ldots, p_{k,i_r}) = 0\}. \end{aligned}$$

Now, (U_β, V_α) could be used to generalize Proposition 2 and 3, while $(U_\beta, W_\beta, V_\alpha)$ could be adopted to generalize Proposition 4.

However, a crucial stage when generalizing Proposition 2 and 3 must be emphasized. In these two situations, the following set should be defined in advance,

$$L = \{k | H_w(p_{k,i_1}, p_{k,i_2}, \ldots, p_{k,i_r}) = 1\}.$$

Once the sub-matrix $M_{\alpha,\beta} = \begin{pmatrix} m_1 \\ m_2 \\ \vdots \\ m_u \end{pmatrix}$ is selected by (U_β, V_α) from P, then to detect some inconsistence, the generalization of Proposition 2 should be

"If $L \neq \emptyset$, and there exists an $l \in \{1, 2, \ldots, u\}$, such that $H_w(m_l) = 1$ and the non-zero proposition of m_l belongs to L, then (α, β) is a 4-round impossible differential."

While, if the selected sub-matrix is $M_{\alpha,\beta} = (m_1, m_2, \ldots, m_v)$, then the generalization of Proposition 3 should be

"If $L \neq \emptyset$ and there exists a $l \in L$, such that

$$\text{rank}\{\{m_1, m_2, \ldots, m_v\} \backslash \{m_l\}\} = \text{rank}\{m_1, m_2, \ldots, m_v\},$$

then (α, β) is a 4-round impossible differential."

Example 7. (4-Round Impossible Differential of ARIA) Given $(\alpha, \beta) = (e_{1,6}, e_{1,7,9,11})$, one can calculate that $U_\beta = \{12\}$, $W_\beta = \{2, 4, 6, 13, 15\}$, and $V_\alpha = \{2, 4, 5, 7, 9, 10, 11, 14, 15, 16\}$, thus

$$M_{\alpha,\beta} = \begin{pmatrix} \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix}, \quad M'_{\alpha,\beta} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{0} \end{pmatrix}.$$

Since the last row vector of $M'_{\alpha,\beta}$ is equal to the only row vector of $M_{\alpha,\beta}$, (α, β) is a 4-round impossible differential of ARIA.

Remark 1. Ref. [14] proposed an efficient algorithm to find many 4-round impossible differentials of ARIA. In fact, this algorithm is based on a special case of the sufficient condition presented in Proposition 4 (and its generalized case as discussed in this sub-section) and thus could be seen as an application of our criteria. Note that for the SPN cipher as described in Appendix C, many impossible differentials with hamming weights of both the input and output difference exceeding 1 could also be found by adopting these generalized methods.

5 How to Extend to 5/6-Round SPN Ciphers?

In this section, we discuss the possibility to extend the above methods to analyze 5/6-round impossible differentials of SPN ciphers. Note that due to the diffusion effect of the linear transformation, we only focus on the differential (e_i, e_j).

5.1 Analysis of 5-Round SPN Ciphers

Case 1. We use the following equation

$$P \circ S \circ P \circ S \circ P \circ S(e_i) = S^{-1} \circ P^{-1} \circ S^{-1}(e_j), \tag{8}$$

to analyze 5-round SPN ciphers.

Let $\alpha = P \circ S(e_i)$, $\beta = e_j$, then Eq. (8) becomes

$$P \circ S \circ P \circ S(\alpha) = S^{-1} \circ P^{-1} \circ S^{-1}(\beta),$$

thus the analysis of 5-round impossible differentials is degenerated into the 4-round case through $(\alpha, \beta) = (P \circ S(e_i), e_j)$.

Case 2. We could also use the following equation

$$P \circ S \circ P \circ S(e_i) = S^{-1} \circ P^{-1} \circ S^{-1} \circ P^{-1} \circ S^{-1}(e_j), \tag{9}$$

to analyze 5-round impossible differentials of SPN ciphers.

Let $\alpha = e_i$, $\beta = P^{-1} \circ S(e_j)$, then Eq. (9) becomes

$$P \circ S \circ P \circ S(\alpha) = S^{-1} \circ P^{-1} \circ S^{-1}(\beta),$$

thus it is also equivalent to analyze 4-round impossible differentials through $(\alpha, \beta) = \big(e_i, P^{-1} \circ S^{-1}(e_j)\big)$.

5.2 Analysis of 6-Round SPN Ciphers

The following equation

$$P \circ S \circ P \circ S \circ P \circ S(e_i) = S^{-1} \circ P^{-1} \circ S^{-1} \circ P^{-1} \circ S^{-1}(e_j) \tag{10}$$

could be used to analyze 6-round SPN ciphers.

Let $\alpha = P \circ S(e_i)$ and $\beta = P^{-1} \circ S^{-1}(e_j)$, then Eq. (10) becomes

$$P \circ S \circ P \circ S(\alpha) = S^{-1} \circ P^{-1} \circ S^{-1}(\beta),$$

thus the analysis of 6-round impossible differentials is degenerated into the 4-round case through $(\alpha, \beta) = \big(P \circ S(e_i), P^{-1} \circ S^{-1}(e_j)\big)$.

Remark 2. According to the above analysis, we do some experiments on Rijndael-256, the large block version of the Rijndael block cipher family [5], and find many 5/6-round impossible differentials. These impossible differentials include the ones that found in [6] and [20].

6 Conclusion

This paper studies the impossible differential properties of SPN ciphers. It is shown that the existence of 3/4/5/6-round impossible differentials are strongly related to some properties of the linear transformation. Based on the theory of matrix on finite field, some sufficient conditions on linear transformations are proposed that can be used to verify whether a given differential is impossible. We point out that these properties should be carefully considered when designing the linear part of an SPN cipher.

Acknowledgment

The work in this paper is supported by the Natural Science Foundation of China (No: 60803156) and the open research fund of State Key Laboratory of Information Security(No: 01-07).

References

1. Eli Biham, Alex Biryukov, and Adi Shamir. Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials. EUROCRYPT 1999, LNCS 2595, pp.12-23, Springer-Verlag 1999.
2. Eli Biham, Alex Biryukov, and Adi Shamir. Miss in the Middle Attacks on IDEA, and Khufu. FSE 1999, LNCS 1636, pp. 124–138, Springer-Verlag, 1999.
3. A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin, and C. Vikkelsoe. PRESENT: An ultra-lightweight block cipher. CHES 2007, LNCS 4727, pp. 450–466. Springer-Verlag, 2007.
4. Orr Dunkelman and Nathan Keller. An Improved Impossible Differential Attack on MISTY1. Asiacrypt 2008. LNCS 5350, pp. 441-454, Springer-Verlag, 2008.
5. Joan Daemen, and Vincent Rijmen. The Desigh of Rijndael. Springer-Verlag, 2002.
6. Jorge Nakahara Jr. and Ivan Carlos Pavão. Impossible Differential Attacks on Large-Block Rijndael. ISC 2007, LNCS 4779, pp. 104–117, Springer-Verlag, 2007.
7. Bon Wook Koo, Hwan Seok Jang, and Jung Hwan Song. Constructing and Cryptanalysis of a 16×16 Binary Matrix as a Diffusion Layer. WISA 2003, LNCS 2908, pp.489–503, Springer-Verlag, 2004.
8. Bon Wook Koo, Hwan Seok Jang, and Jung Hwan Song. On Constructing of a 32×32 Binary Matrix as a Diffusion Layer for a 256-Bit Block Cipher ICISC 2006, LNCS 4296, pp. 51–64, Springer-Verlag, 2006.
9. Daesung Kwon, Jaesung Kim, Sangwoo Park, Soo Hak Sung et al. New Block Cipher: ARIA. ICISC 2003, LNCS 2971, pp.432–445, Springer-Verlag 2004.
10. Jongsung Kim, Seokhie Hong, Jaechul Sung, Sanjin Lee, Jonggin Lim, and Soohak Sung. Impossible Differential Cryptanalysis for Block Cipher Structures. Indocrypt 2003, LNCS 2904, pp. 82-96, Springer-Verlag, 2003.
11. Lars Ramkilde Knudsen. DEAL – A 128-bit Block Cipher. Technical Report 151, Department of Informatics, University of Bergen, Norway, Feb. 1998.
12. Jiqiang Lu, Orr Dunkelman, Nathan Keller and Jongsung Kim. New Impossible Differential Attacks on AES. Indocrypt 2008, LNCS 5365, pp. 279-293, Springer-Verlag, 2008.

13. Jiqiang Lu, Jongsung Kim, Nathan Keller and Orr Dunkelman. Improving the Efficiency of Impossible Differential Cryptanalysis of Reduced Camellia and MISTY1. CT-RSA 2008, LNCS 4904, pp. 370-386, Springer-Verlag, 2008.
14. Ruilin Li, Bing Sun, Peng Zhang and Chao Li. New Impossible Differential Cryptanalysis of ARIA. Cryptology ePrint Archive, Report 2008/227. Avaiable through http://eprint.iacr.org/2008/227.
15. National Institute of Standards and Technology. FIPS-197: Advanced Encryption Standard (AES) (November 2001).
16. Claude Elwood Shannon. Communication theory of secrecy systems, Bell System Technical Journal 28, 1949.
17. Yuechuan Wei, Ping Li, Bing Sun, Chao Li. Impossible Differential Cryptanalysis on Feistel Ciphers with SP and SPS Round Functions. To appear in ACNS 2010.
18. Wenling Wu, Wentao Zhang and Dengguo Feng. Impossible differential cryptanalysis of Reduced-Round ARIA and Camellia. Journal of Compute Science and Technology 22(3): 449-456, Springer-Verlag, 2007.
19. Wentao Zhang, Wenling Wu, and Dengguo Feng. New Results on Impossible Differential Cryptanalysis of Reduced AES. ICISC 2007, LNCS 4817, pp.239-250, Springer-Verlag 2007.
20. Lei Zhang, Wenling Wu, Je Hong Park, Bon Wook Koo, and Yongjin Yeom. Improved Impossible Differential Attacks on Large-Block Rijndael. ISC 2008, LNCS 5222, pp. 298–315, Springer-Verlag, 2008.

A Brief Description of AES

AES [15] is a well-known SPN block ciphe with 128-bit block length, and 128/192/256-bit key length. The basic round function of AES consists of four operations: SubBytes, ShiftRows, MixColumns, and AddRoundKey. Here we give an equivalent description of AES, where the SubBytes and AddRoundKey are the same as the original one, while ShitRows and Mixcolumns are combined together to form a new linear transformation as the diffusion layer.

It should be noted that this equivalent description is a bit different from the original one, since the last round in the former does not contain the ShitRows transformation while the latter one does. However, this doesn't influence our analysis of impossible differentials, since any impossible differential could be easily transformed with each other. Thus, we only focus on the equivalent cipher in this paper and remain to denote it by AES.

Given an input $X = (x_1, x_2, \ldots, x_{16}) \in \mathbb{F}_{2^8}^{16}$, if we treat X as the following 4×4 state,

x_1	x_5	x_9	x_{13}
x_2	x_6	x_{10}	x_{14}
x_3	x_7	x_{11}	x_{15}
x_4	x_8	x_{12}	x_{16}

then the linear transformation P and its inversion P^{-1} of AES could be represented by

$$P = \begin{pmatrix}
02\ 00\ 00\ 00\ 00\ 03\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 01 \\
01\ 00\ 00\ 00\ 00\ 02\ 00\ 00\ 00\ 00\ 03\ 00\ 00\ 00\ 00\ 01 \\
01\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 02\ 00\ 00\ 00\ 00\ 03 \\
03\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 02 \\
00\ 00\ 00\ 01\ 02\ 00\ 00\ 00\ 00\ 03\ 00\ 00\ 00\ 00\ 01\ 00 \\
00\ 00\ 00\ 01\ 01\ 00\ 00\ 00\ 00\ 02\ 00\ 00\ 00\ 00\ 03\ 00 \\
00\ 00\ 00\ 03\ 01\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 02\ 00 \\
00\ 00\ 00\ 02\ 03\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 01\ 00 \\
00\ 00\ 01\ 00\ 00\ 00\ 00\ 01\ 02\ 00\ 00\ 00\ 00\ 03\ 00\ 00 \\
00\ 00\ 03\ 00\ 00\ 00\ 00\ 01\ 01\ 00\ 00\ 00\ 00\ 02\ 00\ 00 \\
00\ 00\ 02\ 00\ 00\ 00\ 00\ 03\ 01\ 00\ 00\ 00\ 00\ 01\ 00\ 00 \\
00\ 00\ 01\ 00\ 00\ 00\ 00\ 02\ 03\ 00\ 00\ 00\ 00\ 01\ 00\ 00 \\
00\ 03\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 01\ 02\ 00\ 00\ 00 \\
00\ 02\ 00\ 00\ 00\ 00\ 03\ 00\ 00\ 00\ 00\ 01\ 01\ 00\ 00\ 00 \\
00\ 01\ 00\ 00\ 00\ 00\ 02\ 00\ 00\ 00\ 00\ 03\ 01\ 00\ 00\ 00 \\
00\ 01\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 02\ 03\ 00\ 00\ 00
\end{pmatrix},$$

$$P^{-1} = \begin{pmatrix}
0e\ 0b\ 0d\ 09\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00 \\
00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 09\ 0e\ 0b\ 0d \\
00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 0d\ 09\ 0e\ 0b\ 00\ 00\ 00\ 00 \\
00\ 00\ 00\ 00\ 0b\ 0d\ 09\ 0e\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00 \\
00\ 00\ 00\ 00\ 0e\ 0b\ 0d\ 09\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00 \\
09\ 0e\ 0b\ 0d\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00 \\
00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 0d\ 09\ 0e\ 0b \\
00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 0b\ 0d\ 09\ 0e\ 00\ 00\ 00\ 00 \\
00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 0e\ 0b\ 0d\ 09\ 00\ 00\ 00\ 00 \\
00\ 00\ 00\ 00\ 09\ 0e\ 0b\ 0d\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00 \\
0d\ 09\ 0e\ 0b\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00 \\
00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 0b\ 0d\ 09\ 0e \\
00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 0e\ 0b\ 0d\ 09 \\
00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 09\ 0e\ 0b\ 0d\ 00\ 00\ 00\ 00 \\
00\ 00\ 00\ 00\ 0d\ 09\ 0e\ 0b\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00 \\
0b\ 0d\ 09\ 0e\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00
\end{pmatrix}.$$

B Brief Description of ARIA

ARIA [9] is an SPN style block cipher, and the number of the rounds are 12/14/16 corresponding to key of 128/192/256-bit. The substitution layer of ARIA consists of two kinds of non-linear transformations in order to get a similar encryption and decryption. The linear transformation in the diffusion layer is an involutional binary matrix [7] defined by

$$P = \begin{pmatrix}
0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0 \\
0\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1 \\
0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 1 \\
1\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1\ 1\ 0 \\
1\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1 \\
0\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 1 \\
1\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0 \\
0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0 \\
1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0\ 1 \\
1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0 \\
0\ 0\ 1\ 1\ 0\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1 \\
0\ 0\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 0 \\
0\ 1\ 1\ 0\ 0\ 0\ 1\ 1\ 0\ 1\ 0\ 1\ 1\ 0\ 0\ 0 \\
1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0 \\
1\ 0\ 0\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 0 \\
0\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 0\ 0\ 1
\end{pmatrix}.$$

C A Kind of SPN Cipher

This kind of SPN cipher is described below: the substitution layer is not definitively given, i.e., it could be arbitrary 32 parallel bijective non-linear mappings, while a specially designed binary matrix P as introduced in [8] is employed as the diffusion layer. The definition of P and P^{-1} are

$$P = \begin{pmatrix}
1&0&1&1&1&1&0&0&1&1&1&0&1&1&0&0&0&1&1&1&0&0&0&0&1&1&0&0&0&1&0&1\\
1&1&0&1&0&1&1&0&0&1&1&1&0&1&1&0&1&0&1&1&0&0&0&0&0&1&1&0&1&0&1&0\\
1&1&1&0&0&0&1&1&1&0&1&1&0&0&1&1&1&1&0&1&0&0&0&0&0&0&1&1&0&1&0&1\\
0&1&1&1&1&0&0&1&1&1&0&1&1&0&0&1&1&1&1&0&0&0&0&0&1&0&0&1&1&0&1&0\\
1&1&0&0&0&0&0&1&0&1&0&0&1&0&1&1&0&0&0&0&1&0&1&0&0&0&0&1&1&0&0&0\\
0&1&1&0&1&0&0&0&0&0&1&0&1&1&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0&1&0&0\\
0&0&1&1&0&1&0&0&0&0&0&1&1&1&1&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&1&0\\
1&0&0&1&0&0&1&0&1&0&0&0&0&1&1&1&0&0&0&0&0&1&0&1&0&0&1&0&0&0&0&1\\
1&1&1&0&0&1&0&0&1&1&1&0&1&0&0&1&0&1&0&0&0&0&0&0&0&1&1&1&0&0&0&0\\
0&1&1&1&0&0&1&0&0&1&1&1&1&1&0&0&0&0&1&0&0&0&0&0&1&0&1&1&0&0&0&0\\
1&0&1&1&0&0&0&1&1&0&1&1&0&1&1&0&0&0&0&1&0&0&0&0&1&1&0&1&0&0&0&0\\
1&1&0&1&1&0&0&0&1&1&0&1&0&0&1&1&1&0&0&0&0&0&0&0&0&1&1&1&0&0&0&0\\
1&1&0&0&1&0&1&1&1&0&0&1&0&1&1&1&1&1&0&0&1&1&0&0&0&0&0&0&1&1&1&0\\
0&1&1&0&1&1&0&1&1&1&0&0&1&0&1&1&0&1&1&0&0&1&1&0&0&0&0&0&0&1&1&1\\
0&0&1&1&1&1&1&0&0&1&1&0&1&1&0&1&0&0&1&1&0&0&1&1&0&0&0&0&1&0&1&1\\
1&0&0&1&0&1&1&1&0&0&1&1&1&1&1&1&0&1&0&0&1&1&0&0&1&0&0&0&0&1&1&0&1\\
0&1&1&1&0&0&0&0&0&1&0&0&1&1&0&0&0&0&0&1&0&0&0&1&0&1&1&0&1&0&0&0\\
1&0&1&1&0&0&0&0&0&0&0&1&0&0&1&1&0&1&0&1&0&0&0&1&0&0&0&0&1&1&0&1&0\\
1&1&0&1&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&0&0&1&0&0&1&0&1&0&0&1&0&1&0\\
1&1&1&0&0&0&0&0&1&0&0&0&0&1&0&0&1&1&1&0&0&0&0&0&1&1&1&0&0&0&1&1&1\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&1&1&0&1&0&0&0&1&1&0&1&0&1&1&0&1&1&0&1\\
0&0&0&0&0&1&0&1&0&0&0&0&0&0&0&1&1&0&1&0&0&1&1&1&0&0&0&1&1&1&1&1&0\\
0&0&0&0&0&1&0&1&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&1&1&1&1&0&0&1&0&1&1\\
1&1&0&0&0&0&0&1&0&1&1&1&0&0&0&0&0&1&1&0&1&1&0&0&0&1&1&1&0&0&0&0&0\\
0&1&1&0&1&0&0&0&1&0&1&1&0&0&0&0&0&0&0&1&1&0&1&1&0&1&0&1&1&0&0&0&0\\
0&0&1&1&0&1&0&0&1&1&0&1&0&0&0&0&1&1&0&1&0&0&1&0&0&1&1&1&1&0&1&0&0\\
1&0&0&1&0&0&1&0&1&1&1&0&0&0&0&0&1&1&0&0&1&0&0&1&1&1&1&0&0&0&0&0\\
0&1&0&1&1&0&0&0&0&0&0&0&1&1&1&0&1&0&0&0&1&0&1&1&0&0&0&0&1&1&1&0\\
1&0&1&0&0&1&0&0&0&0&0&0&0&1&1&1&0&1&0&0&1&1&0&1&0&0&0&0&0&1&1&1\\
0&1&0&1&0&0&1&0&0&0&0&0&1&0&1&1&0&0&1&0&1&1&1&0&0&0&0&0&1&0&1&1\\
1&0&1&0&0&0&0&1&0&0&0&0&1&1&0&1&0&0&0&1&0&1&1&1&0&0&0&0&1&1&0&1
\end{pmatrix},$$

$$P^{-1} = \begin{pmatrix}
1&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&1&0&1&1&0&1&1&1&1&0&1&0&1&0&1\\
0&1&0&0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&1&1&0&1&1&0&1&1&1&1&0&1&0&1&0\\
0&0&1&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&1&1&1&1&1&1&1&0&0&1&1&1&0&1&0\\
0&0&0&1&0&0&0&0&0&1&1&0&1&0&0&0&0&0&1&0&1&1&0&1&1&1&1&0&1&1&1&0&1&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&1&1&0&0&1&0&0&1&1&0&1&1&1&0&0&0&0&0\\
0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&0&1&0&0&1&1&0&1&1&0&0&0&0&0\\
0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&1&0&1&1&0&0&1&1&0&0&1&1&0&1&0&0&0&0\\
0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0&1&1&0&1&1&0&1&1&1&0&0&0&0\\
1&1&1&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&1&0&1&1&1&0&0&1\\
0&1&1&1&0&0&0&0&0&0&0&0&1&0&1&1&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&0&0\\
1&0&1&1&0&0&0&0&1&0&0&0&0&0&1&1&0&0&0&0&0&0&0&0&0&1&1&1&0&0&1&1&0&0\\
1&1&0&1&0&0&0&0&0&1&0&0&1&0&0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&0&0&1&1&0\\
0&0&0&0&1&1&0&1&1&1&0&0&0&0&0&1&0&0&0&0&1&1&0&1&1&0&1&1&0&1&1&1&1&1\\
0&0&0&0&1&1&1&0&0&1&1&0&1&0&0&0&0&0&0&0&1&1&1&0&1&1&0&1&1&0&1&1&0&1\\
0&0&0&0&0&1&1&1&0&0&1&1&0&1&0&0&0&0&0&0&0&1&1&1&1&1&1&0&1&1&0&1&1&0\\
0&0&0&0&1&0&1&1&1&0&0&1&0&0&1&0&0&0&0&0&0&1&0&1&1&0&1&1&1&1&1&1&1&0\\
1&1&1&0&1&1&0&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&0&1&0&1&0&0&0&0&0\\
1&1&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&1&1&1&0&1&0&1&0&0&0&0\\
0&1&1&1&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&1&0&1&1&1&0&1&0&0&0&0&0\\
1&0&1&1&0&0&1&1&0&0&0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&1&0&1&0&1&0&0&0&0\\
1&0&1&1&0&0&1&1&0&0&0&0&1&1&0&1&1&1&1&0&1&0&0&0&0&0&0&0&0&1&0&1&1&1\\
1&1&0&1&1&0&0&1&0&0&0&1&1&0&0&1&1&1&0&1&0&1&1&0&0&0&0&0&0&0&1&1&0&1\\
1&1&1&0&1&1&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&0&1&0&0&0&0&0&0&1&1&1&1&0\\
0&1&1&1&0&1&1&0&0&0&0&0&1&0&1&1&1&0&1&0&0&0&1&0&0&0&0&0&1&1&0&1&1&0\\
1&1&0&1&0&1&1&1&1&0&1&1&1&0&1&0&1&0&1&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&1&1&0&1&1&1&1&0&1&1&1&0&1&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&1&1&1&1&1&0&0&1&1&1&0&1&1&1&0&1&0&1&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&0&1&0&0&0&0&1&0&0&1&0&1&1&1&0&0&0&0&1&0&1&1&0&0&0&0&0&0&1&0&0&0\\
1&0&1&0&0&0&0&0&0&1&1&0&0&1&0&1&1&0&0&0&0&1&1&0&1&0&0&0&0&0&0&0&0&1\\
0&1&0&1&0&0&0&0&0&0&1&1&0&1&1&0&1&0&0&0&0&1&1&1&0&0&0&0&0&1&0&0&0&0\\
1&0&1&0&0&0&0&0&0&0&1&1&1&1&1&1&0&0&0&0&0&0&1&1&1&0&0&0&0&0&1&0&0&0
\end{pmatrix}.$$