

Impossible Differential Cryptanalysis of SPN Ciphers

Ruilin Li¹, Bing Sun¹ and Chao Li^{1,2}

¹Department of Mathematics and System Science, Science College,
National University of Defense Technology, Changsha, 410073, China
securitylrl@gmail.com, happy_come@163.com

²State 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 whose diffusion layer is defined by a linear transformation P . Based on the theory of linear algebra, we propose several criteria on 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. It is concluded that the linear transformation should be carefully designed in order to protect the cipher against impossible differential cryptanalysis.

Keywords: Block ciphers, SPN, Rijndael, ARIA, linear transformation, impossible differential

1 Introduction

1.1 Backgrounds

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 secret key of block ciphers was firstly introduced by Knudsen [11] against the DEAL cipher and further by Biham et al. [1] to attack Skipjack. 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 inconsistency. 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.

1.2 Motivation, Merit and Outline of This Paper

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 6/7/8-round impossible differentials (the hamming weights of both the input and output differences are 1) by presenting some sufficient conditions on P and its inversion P^{-1} . According to 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 diffusion layer employs a linear transformation P defined over $\mathbb{F}_{2^d}^{n \times n}$. Based on the theory of linear algebra, we propose several criteria on P and 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. Note that the procedure for finding these impossible differentials could be implemented either manually or automatically aided by the algebraic software Magma.

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 evolutionary properties of the differences in both the encryption and decryption directions to deduce some inconsistency by experience and intuition, according to the concrete components of the underlying block ciphers. Also such traditional method will be surely boring, especially when the number of sub-blocks is increasing.

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 transformations 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 (sub-block) 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 $S(x_1, x_2, \dots, x_n) = (s_1(x_1), s_2(x_2), \dots, s_n(x_n))$, where each s_i is a non-linear bijective mapping on \mathbb{F}_{2^d} and all of them are not necessarily to be identical 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 whose diffusion layer employs a binary matrix proposed in [8]. Remind that the linear transformation of AES is defined as the composition of ShiftRows and MixColumns.

2.2 Notations

We use $X = (x_1, x_2, \dots, x_n)$ 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., $\Delta X = X \oplus X'$. Particularly, 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, \dots, j_t} denotes an n -word state with the non-zero positions being j_1, j_2, \dots, j_t . We use (α, β) to denote a differential, where α is the input difference and β is the output difference. Further, $\alpha \rightarrow \beta$ denotes a possible differential and $\alpha \nrightarrow \beta$ denotes an impossible differential.

Note that the XOR difference is not influenced by the round-key addition layer, we thus omit this transformation when studying the evolutionary property of the difference in the encryption and decryption procedure. Moreover, 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 given an input difference ΔX , the output difference of an r -round SPN cipher could be represented by

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

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) $\chi : \mathbb{F}_{2^d}^n \rightarrow \mathbb{F}_2^n$ is defined as

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

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

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

Given $X = (x_1, x_2, \dots, x_n)$, define $\chi_s : \mathbb{F}_{2^d}^n \rightarrow \mathbb{F}_2$ 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.

Let the bijective transformations S and P be defined as above, then the χ -function has the following properties.

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

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

(2) Let $P = (P_1, P_2, \dots, P_n)$, where P_i is i -th column of P . If $\Delta X = e_i$, then

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

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

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

Definition 2. (*Hamming Weight*) Given $X = (x_1, x_2, \dots, x_n) \in \mathbb{F}_{2^d}^n$, 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 $P = (p_{i,j})$, let the inversion of P be $P^{-1} = (q_{i,j})$. If there exists a set $\{i_1, i_2, \dots, i_r; j_1, j_2, \dots, j_t; k\}$, such that

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

then $e_{i_1, i_2, \dots, i_r} \not\rightarrow e_{j_1, j_2, \dots, j_t}$ is a 3-round impossible differential.

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

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

Since

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

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

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

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

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

$$\sum_{l=1}^n q_{k,l} \beta_l = \sum_{l \in \{j_1, j_2, \dots, j_t\}} q_{k,l} \beta_l = 0.$$

According to Property 1,

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

which leads to a contradiction with Eq. (1). Thus $e_{i_1, i_2, \dots, i_r} \not\rightarrow e_{j_1, j_2, \dots, j_t}$ is a 3-round impossible differential. \square

Example 1. (3-round impossible differential of AES) Given the following set $\{1, 2, 3, 4; 1, 2, 3, 4; 4\}$, we find that $p_{4,1} = 03$, $p_{4,2} = p_{4,3} = p_{4,4} = 0$, and $q_{4,1} = q_{4,2} = q_{4,3} = q_{4,4} = 0$, thus according to Proposition 1, $e_{1,2,3,4} \not\rightarrow e_{1,2,3,4}$ 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 $e_{1,2,4,5,7} \not\rightarrow e_{11,12,14,15,16}$ 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 criteria (sufficient conditions) to characterize the existence of 4-round impossible differentials, where the hamming weights of both the input and output differences 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 $e_i \rightarrow e_j$ is a possible one, then according to the encryption (decryption) procedure, the following equation must hold:

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

Using this equation, he could deduce some contradictions, and thus complete the proofs.

One may observe that, for some SPN ciphers (e.g., AES), it is easy to detect 4-round impossible differentials using the direct analysis, i.e., from the encryption direction, the difference of one sub-block is non-zero, while from the decryption direction, the corresponding difference of the sub-block is zero, which leads to a contradiction. However, there exist some other block ciphers (e.g., ARIA) in which 4-round impossible differentials are hard to detect just by this direct approach.

According to the above discussion, we point out here that, the first criterion presented in this section is, in fact, the basis of the direct approach, while the second and third criterion, which are based on the theory of linear algebra, are two new methods that are significantly different from the first one. Utilizing these two new criteria, many impossible differentials could be detected.

4.1 The First Criterion

As mentioned above, our first criterion is the basis of the direct approach.

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

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

and

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

where each m_a is the a -th row vector of $M_{i,j}$, $a = 1, 2, \dots, u$.

If $U_j, V_i \neq \emptyset$, and there exists an $l \in \{1, 2, \dots, u\}$, such that $H_w(m_l) = 1$, then $e_i \rightarrow e_j$ 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

$$P\lambda = \gamma. \quad (3)$$

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

$$P\lambda = \sum_{b=1}^v P_{t_b} \lambda_{t_b},$$

where P_{t_b} is the t_b -th column vector of P and λ_{t_b} is the t_b -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,

$$\begin{aligned} p_{r_1, t_1} \lambda_{t_1} + p_{r_1, t_2} \lambda_{t_2} + \dots + p_{r_1, t_v} \lambda_{t_v} &= 0 \\ p_{r_2, t_1} \lambda_{t_1} + p_{r_2, t_2} \lambda_{t_2} + \dots + p_{r_2, t_v} \lambda_{t_v} &= 0 \\ &\vdots \\ p_{r_u, t_1} \lambda_{t_1} + p_{r_u, t_2} \lambda_{t_2} + \dots + p_{r_u, t_v} \lambda_{t_v} &= 0 \end{aligned} \quad (4)$$

The above linear equation system could be represented as

$$M_{i,j} \tilde{\lambda} = 0, \quad (5)$$

where $M_{i,j} = (p_{r_a, t_b})_{u \times v}$, and $\tilde{\lambda} = (\lambda_{t_1}, \dots, \lambda_{t_v})^T$, with each λ_{t_b} being non-zero, where $b = 1, 2, \dots, v$.

Since there exists an $l \in \{1, 2, \dots, u\}$, such that $H_w(m_l) = H_w(p_{r_1, t_1}, p_{r_1, t_2}, \dots, p_{r_1, t_v}) = 1$, we have $m_l \cdot \tilde{\lambda} \neq 0$ which is a contradiction with the l -th equation of the linear equation system (4). \square

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

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

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

4.2 The Second Criterion

For many SPN ciphers, the sub-matrix $M_{i,j}$ 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 $P = (p_{i,j})$, let the inversion of P be $P^{-1} = (q_{i,j})$. For any $1 \leq i, j \leq n$, let*

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

and

$$M_{i,j} = (p_{r_a, t_b})_{u \times v} = (m_1, m_2, \dots, m_v),$$

where each m_b is the b -th column vector of $M_{i,j}$, $b = 1, 2, \dots, v$.

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

$$\text{rank}\{m_1, m_2, \dots, m_v\} \setminus \{m_l\} < \text{rank}\{m_1, m_2, \dots, m_v\},$$

then $e_i \rightarrow e_j$ is a 4-round impossible differential.

Proof. According to Eq. (5), $\sum_{b=1}^v \lambda_{t_b} \cdot m_b = 0$, where each λ_{t_b} is non-zero. Since $\lambda_{t_l} \neq 0$, we get

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

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

$$\text{rank}\{\{m_1, m_2, \dots, m_l\} \setminus \{m_l\}\} = \text{rank}\{m_1, m_2, \dots, m_l\},$$

which is a contradiction with the condition as described in the proposition. \square

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

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

One can verify that

$$\text{rank}\{\{m_1, m_2, \dots, m_7\} \setminus \{m_1\}\} = 5 < 6 = \text{rank}\{m_1, m_2, \dots, m_7\},$$

thus $e_1 \rightarrow e_1$ 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 $e_i \rightarrow e_j$ 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 $P = (p_{i,j})$, let the inversion of P be $P^{-1} = (q_{i,j})$. For any $1 \leq i, j \leq n$, let

$$\begin{aligned} U_j &= \{r | q_{r,j} = 0\} = \{r_1, r_2, \dots, r_u\}, \\ W_j &= \{s | q_{s,j} \neq 0\} = \{s_1, s_2, \dots, s_w\}, \\ V_i &= \{t | p_{t,i} \neq 0\} = \{t_1, t_2, \dots, t_v\}, \end{aligned}$$

and

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

where each m_a (resp. m'_a) denotes the a -th row vector of $M_{i,j}$ (resp. $M'_{i,j}$).

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

$$\text{rank}\{m_1, m_2, \dots, m_u, m'_l\} = \text{rank}\{m_1, m_2, \dots, m_u\},$$

then $e_i \rightarrow e_j$ is a 4-round impossible differential.

Proof. According to Eq. (5), let $(\lambda_{t_1}, \lambda_{t_2}, \dots, \lambda_{t_v})^T = \tilde{\lambda} \triangleq (\tilde{\lambda}_1, \dots, \tilde{\lambda}_v)^T$, with each $\tilde{\lambda}_b \neq 0$, where $b = 1, 2, \dots, v$, and let $m_a = (m_{a1}, m_{a2}, \dots, m_{av})$, where $a = 1, 2, \dots, u$, then $m_a \cdot \tilde{\lambda} = 0$.

Assume $m'_a = (m'_{a1}, m'_{a2}, \dots, m'_{av})$, where $a = 1, 2, \dots, w$, then according to the definition $M'_{i,j}$, for any $a \in \{1, 2, \dots, w\}$, $m'_a \cdot \tilde{\lambda} \neq 0$.

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

Now we get

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

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

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

One can see that the last row vector of $M'_{1,1}$ is equal to the seventh row vector of $M_{1,1}$, or the last second row vector of $M'_{1,1}$ is equal to the fifth row vector of $M_{1,1}$, thus we obtain the same 4-round impossible differential $e_1 \rightarrow e_1$.

Remark 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. However, even so, we point out here that in general, impossible differentials detected by those two propositions (or their generalized versions, see Section 4.5) are not necessarily to be the same, since these two sub-matrices corresponds to two different linear equation systems. One can refer Example 7 as a counter example.

Example 6. (4-round Impossible Differentials 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 designers 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 $1 \leq i, j \leq 32$, $e_i \nrightarrow e_j$ 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 the general case and 5/6-round SPN ciphers.

Remark 2. There exist many “dual cases” when analyzing 4-round impossible differentials of ARIA. In fact, due to the involutorial property of the linear transformation P in the diffusion layer, we can easily identify these dual cases. For instance, given a 4-round impossible differential of ARIA, if we exchange the role of its input difference and output difference, the result differential is also impossible. This indicates that 4-round impossible differentials of ARIA are huge.

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,

$$P\lambda = \gamma,$$

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

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

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

which implies that λ_k is either zero or non-zero depending on $p_{k,i}$, and thus the unknown state never appears in this situation.

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

$$\begin{aligned}\chi_k(\lambda) &= \chi_k(S \circ P \circ S(e_{i_1, i_2, \dots, i_r})) \\ &= \chi_k(P \circ S(e_{i_1, i_2, \dots, i_r})) \\ &= \theta \left(\sum_{l=1}^r p_{k, i_l} \cdot \delta_{i_l} \right),\end{aligned}\tag{6}$$

where δ_{i_l} is a possible output difference of the i_l -th s-box in the substitution layer. Thus λ_k could be either $\mathbf{0}$, $*$, or $?$. However, from Eq. (6), we can discuss the state of λ_k according to the hamming weight of $(p_{k, i_1}, p_{k, i_2}, \dots, p_{k, i_r})$.

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

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

Motivations of Proposition 2, 3 and 4. Let's 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 $*$. Thus one can just consider the truncated form of the linear equation system $P\lambda = \gamma$.

- Consider the left side of the linear equation system, $P\lambda = \sum_{k=1}^n P_k \cdot \lambda_k$, thus according to the component of λ , if $\lambda_k = 0$, then the contribution of $P_k \cdot \lambda_k$ in the summation could be omitted. This indicates that the size of the linear equation system could be reduced, namely, some column vectors of P (the coefficient matrix of the linear equation system) can be deleted.
- Consider the right side of the linear equation system, according to the component of γ , this reduced linear equation system could be further divided into two parts: one is the zero linear equation system and the other is the non-zero linear equation system. These two sub-linear equation systems can be represented by their corresponding coefficient matrices $M_{i,j}$ and $M'_{i,j}$, that are selected from P .

Now we can summarize the motivations of these criteria as follows:

- 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 $M_{i,j}$ from P , where some inconsistency are detected.
- 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 $M'_{i,j}$ from P , and some inconsistency are detected between $M_{i,j}$ and $M'_{i,j}$.

Generalized Methods. If we turn to the general case $(\alpha, \beta) = (e_{i_1, i_2, \dots, i_r}, e_{j_1, j_2, \dots, j_t})$, 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 following:

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

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,

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

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 inconsistency, the generalization of Proposition 2 should be

“If $\Omega \neq \emptyset$, and there exists an $l \in \{1, 2, \dots, u\}$, such that $H_w(m_l) = 1$ and the non-zero proposition of m_l belongs to Ω , then $\alpha \nrightarrow \beta$ is a 4-round impossible differential.”

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

“If $\Omega \neq \emptyset$ and there exists a $l \in \Omega$, such that

$$\text{rank}\{\{m_1, m_2, \dots, m_v\} \setminus \{m_l\}\} < \text{rank}\{m_1, m_2, \dots, m_v\},$$

then $\alpha \nrightarrow \beta$ 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

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

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

Remark 3. This example shows that, by using only the sub-matrix $M_{\alpha,\beta}$, one couldn't detect any 4-round impossible differentials.

Remark 4. 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 conditions presented in Proposition 4 (and its generalized case as discussed in this sub-section) and thus could be seen as an application of our criterion. For the SPN cipher as described in Appendix C, many impossible differentials with hamming weights of both the input and output differences 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 to analyze 5-round impossible differentials.

$$P \circ S \circ P \circ S \circ P \circ S(e_i) = S^{-1} \circ P^{-1} \circ S^{-1}(e_j) \quad (7)$$

Let $\alpha = P \circ S(e_i)$, $\beta = e_j$, then Eq. (7) 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 to analyze 5-round impossible differentials.

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

Let $\alpha = e_i$, $\beta = P^{-1} \circ S(e_j)$, then Eq. (8) 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 $(\alpha, \beta) = (e_i, P^{-1} \circ S^{-1}(e_j))$.

5.2 Analysis of 6-Round SPN Ciphers

The following equation could be used to analyze 6-round impossible differentials.

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

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

Remark 5. 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 linear algebra, some criteria on the linear transformation are proposed that can be used to verify whether a given differential is impossible. As application, we utilize these criteria to detect large class of many well-known block ciphers. We hope that the techniques in the present paper will also be beneficial when finding impossible differentials in some other block cipher structures with SP round function.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable suggestions and comments. The work in this paper is supported by the Natural Science Foundation of China (No: 60803156, 61070215) 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 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, 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, 2007.

4. Orr Dunkelman and Nathan Keller. An Improved Impossible Differential Attack on MISTY1. Asiacrypt 2008. LNCS 5350, pp. 441-454, Springer, 2008.
5. Joan Daemen, and Vincent Rijmen. The Design of Rijndael–AES, the advanced encryption standard. Springer, 2002.
6. Jorge Nakahara Jr. and Ivan Carlos Pavão. Impossible Differential Attacks on Large-Block Rijndael. ISC 2007, LNCS 4779, pp. 104–117, Springer, 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, 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, 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, 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, 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, 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, 2008.
14. Ruilin Li, Bing Sun, Peng Zhang and Chao Li. New Impossible Differential Cryptanalysis of ARIA. Cryptology ePrint Archive, Report 2008/227. Available 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 Secrete System, Bell System Technical Journal, 28(4), 656–715.
17. Yuechuan Wei, Ping Li, Bing Sun, Chao Li. Impossible Differential Cryptanalysis on Feistel Ciphers with SP and SPS Round Functions. ACNS 2010, LNCS 6123, pp. 105–122, Springer, 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, 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, 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, 2008.

A Brief Description of AES

AES [15] is a well-known SPN block cipher 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 ShiftRows 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 one does not contain the ShiftRows 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 $X = (x_1, x_2, \dots, x_{16}) \in \mathbb{F}_{2^8}^{16}$, 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

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

$$P = \begin{pmatrix} 1011110011101100011100000110000101 \\ 11010110011101101011000001101010 \\ 11100011101100111101000000110101 \\ 01111001110110011110000010011010 \\ 11000001010010110000101000011000 \\ 01101000001011010000010110000100 \\ 00110100000111100000101001000010 \\ 10010010100001110000010100100001 \\ 11100100111010010100000001110000 \\ 01110010011111000010000010110000 \\ 10110001101101100001000011010000 \\ 11011000110100111000000011100000 \\ 11001011100101111100110000001110 \\ 01101101110010110110011000000111 \\ 00111110011011010011001100001011 \\ 10010111001111101001100100001101 \\ 01110000010011000001000101101000 \\ 10110000001001101000100000110100 \\ 11010000000100110100010010010010 \\ 111000001000100100100010111000001 \\ 00001010000011000001101111001011 \\ 00000101000001101000110101101101 \\ 00001010000000110100111000111110 \\ 0000010100001001001001001111001011 \\ 11000001011100000110110001110000 \\ 011010001011100000011011010110000 \\ 00110100110100001001001111010000 \\ 10010010111000001100100111100000 \\ 01011000000011101000101100001110 \\ 1010010000001110100110100000111 \\ 01010010000010110010111000001011 \\ 10100001000011010001011100001101 \end{pmatrix},$$

$$P^{-1} = \begin{pmatrix} 10000000111000001101101111010101 \\ 01000000011100001110110111101010 \\ 00100000101100000111111001110101 \\ 00010000110100001011011110111010 \\ 00000100000011011001001101110000 \\ 00000010000011101100100110110000 \\ 00000001000001110110110011010000 \\ 0000100000010110011011011100000 \\ 111000000101100000000010111001 \\ 0111000000101100000000011011100 \\ 10110000100000110000000011100110 \\ 11010000010010010000000001110011 \\ 00001101110000010000110110110111 \\ 00001110011010000000111011011011 \\ 00000111001101000000011111101101 \\ 0000101110010010000010110111110 \\ 11101100000000000100111010100000 \\ 11101100000000000100111010100000 \\ 01110110000000000001101110100000 \\ 10110011000000001000110101010000 \\ 10110011000011011110100000001011 \\ 11011001000011100111010000001101 \\ 11101100000001111011001000001110 \\ 01110110000010111101000100000111 \\ 1101011110111011101000000010000 \\ 11101011110111010101000010000000 \\ 01111101111011101010000001000000 \\ 10111110011101110101000000100000 \\ 01010000100101110000101100000010 \\ 10100000110010110000110100000001 \\ 01010000011011010000111000001000 \\ 10100000001111100000011100000100 \end{pmatrix}.$$