# A Link Between Integrals and Higher-Order Integrals of SPN Ciphers

Ruilin Li, Bing Sun, and Chao Li

**Integral cryptanalysis, which is based on the existence of (higher-order) integral distinguishers, is a powerful cryptographic method that can be used to evaluate the security of modern block ciphers. In this paper, we focus on substitution-permutation network (SPN) ciphers and propose a criterion to characterize how an *r*-round integral distinguisher can be extended to an (*r*+1)-round higher-order integral distinguisher. This criterion, which builds a link between integrals and higher-order integrals of SPN ciphers, is in fact based on the theory of direct decomposition of a linear space defined by the linear mapping of the cipher. It can be directly utilized to unify the procedure for finding 4-round higher-order integral distinguishers of AES and ARIA and can be further extended to analyze higher-order integral distinguishers of various block cipher structures. We hope that the criterion presented in this paper will benefit the cryptanalysts and may thus lead to better cryptanalytic results.**

**Keywords: Cryptanalysis, block ciphers, SPN, AES, ARIA, integral, higher-order integral.**

Manuscript received Oct. 6, 2011; revised Apr. 19, 2012; accepted May 3, 2012.

The work in this paper is supported by the National Natural Science Foundation of China (No: 61103192, 61070215), the Program for Changjiang Scholars and Innovative Research Team in University of Ministry of Education of China (No: IRT1012), and the Fund for Creative Research Groups of the Natural Science Foundation of Hunan Province, China (No: 11FH002).

Ruilin Li (phone: +86 13874976149, securitylrl@gmail.com) is with the School of Electronic Science and Engineering, National University of Defense Technology, Changsha, China.

Bing Sun (securitylrl@gmail.com) is with the Department of Mathematics and System Science, Science College, National University of Defense Technology, Changsha, China.

Chao Li (lichao_nudt@sina.com) is with the Department of Mathematics and System Science, Science College, and also with the School of Computer, National University of Defense Technology, Changsha, China.

http://dx.doi.org/10.4218/etrij.13.0111.0624

## I. Introduction

### 1. Backgrounds

Integral cryptanalysis, which considers the propagation of the sums of many values, was formally introduced by Knudsen and Wagner in [1]. As they pointed out [1], it is especially well suited for analyzing ciphers with primarily bijective components and is, in fact, a more generalized form of many specific attacks, including the square attack [2], saturation attack [3], and multiset attack [4]. These specific methods exploit the simultaneous relationships between many encryptions, in contrast to differential cryptanalysis [5], in which only pairs of encryptions are considered. Consequently, integral cryptanalysis can apply to a lot of block ciphers that are not vulnerable to differential cryptanalysis. These features have made integral cryptanalysis an increasingly popular tool in the field of cryptanalysis.

The substitution-permutation network (SPN) structure is one of the most widely used block cipher structures. Examples of algorithms that use the SPN structure are the well-known block cipher algorithms AES [6] and ARIA [7]. The SPN structure iterates the combination of a substitution and a permutation (or a linear transformation), and, thus, its resistance against differential and linear cryptanalysis [8] is well understood (for example, see [9]-[11]).

To apply integral cryptanalysis, adversaries should firstly find a (higher-order) integral distinguisher of the reduced-round cipher to distinguish it from a random permutation. The most well-known integral distinguisher of an SPN cipher is the 3-round integral distinguisher [12] of AES. This kind of distinguisher needs a special structure of $2^8$ plaintexts with the property that one byte of input is active (takes all possible 256 values), while all the other 15 bytes are constants. Feeding these $2^8$ plaintexts into a 3-round AES encryption procedure

  

will result in ciphertexts with the property that the bit-wise exclusive OR (XOR) of all values in any byte position is zero. This 3-round distinguisher can be used to attack AES reduced to four, five, and six rounds.

A new distinguishing property between the 4-round AES and a random permutation was constructed in [13], which enables 7-round attacks on AES. In [14], another observation was made on the 4-round AES, which led to an improvement in the running time of the attack. The main observation is that if one can obtain the $2^{32}$ plaintexts that take all possible values in the diagonal four bytes, then after one round of AES encryption, those $2^{32}$ plaintexts will correspond to another $2^{32}$ intermediate values, which form $2^{24}$ copies for the input of a 3-round integral distinguisher in the forthcoming 3-round encryption process (round 2 to round 4). Since the text in each integral sums to zero in any byte after the fourth round, so does the sum of all $2^{32}$ texts. This kind of distinguisher was later formalized in [1] and referred to as a 4-round *higher-order* (4th-order) integral distinguisher. Accordingly, the original 3-round integral distinguisher can be treated as a 1st-order integral distinguisher.

Let $n$ be the number of words (subblocks) in the plaintext and ciphertext and $m$ be the number of bits in a word. In the original paper [1], a higher-order integral is defined according to the number of active words. A $d$-th-order ($1 \le d \le n-1$) integral is the sum of ciphertexts whose corresponding plaintexts contain just $d$ active words (range over all possible $2^{md}$ values in the $d$-tuple position), while the traditional integral with one active word can be treated as a 1st-order integral. This kind of notation is suitable when explaining the 3/4-round integral distinguisher of AES as introduced in the previous paragraphs. Besides, the authors in [1] also demonstrated the feasibility of using higher-order integrals to analyze two block cipher structures: Nyberg's generalized Feistel networks and the Skipjack structure.

## 2. Motivation, Merit, and Outline of This Paper

Now that a 3-round 1st-order integral distinguisher of AES can be easily extended to a 4-round 4th-order integral distinguisher, what about other SPN ciphers?

Consider the block cipher ARIA, whose design is very similar to AES. The designers of ARIA believed that no integral distinguisher exists with more than two rounds due to the better avalanche effect of the diffusion layer. In fact, if the number of active bytes is limited to one, it is correct that there only exist 2-round distinguishers. However, these 2-round 1st-order integral distinguishers can be extended to many 3-round $d$-th-order integral distinguishers with $d \ge 7$ (as will be shown in subsection III.4). Unfortunately, these 3-round distinguishers are not the best ones since, in [15], 144 3-round 3rd-order integral distinguishers[1] of ARIA were found using the technique of counting method. Therefore, one may wonder whether this kind of 3-round integral distinguisher could be further extended to some 4-round distinguishers. However, it seems difficult to utilize the direct approach to extend the distinguisher of ARIA in a similar way to the distinguisher of AES. This problem was studied in [16], in which the 3-round 3rd-order integral distinguishers were modified to 3-round 4th-order integral distinguishers, and 24 4-round 12th-order integral distinguishers were thus obtained. It should be noted that these 4-round 12th-order integral distinguishers were used to mount a 7-round attack on ARIA [16], while the 3-round 3rd-order integral distinguishers only led to a 6-round attack [15].

As has been observed, higher-order integral distinguishers have been widely used to analyze many famous SPN ciphers, but there exist some related, yet unsolved, problems. A general problem is as follows.

Assume there is an $r$-round $u$-th-order integral (the basic integral) distinguisher of an SPN cipher, can this basic integral distinguisher be extended to some ($r$+1)-round $v$-th-order ($v \ge u$) integral (the extended higher-order integral) distinguisher? If so, how can we extend it?

To the best of our knowledge, no general solution to this problem is known, and previous techniques seem to be more empirical. In this paper, we borrow from linear algebra with the theory of *direct decomposition of a linear space* to build a link between the integrals and the higher-order integrals of SPN ciphers. We show that if the matrix of the linear transformation in the diffusion layer satisfies a rank property, then the basic integral distinguisher can be directly extended to a higher-order integral distinguisher[2]. This proposed criterion can be used to unify the procedure for finding 4-round higher-order integral distinguishers of AES and ARIA, and it can further be adopted to analyze higher-order integral distinguishers for various block cipher structures.

The remaining content of this paper is divided into four sections. A brief description of SPN ciphers is given in section II. The main result concerning the relationship between integral and higher-order integral distinguishers of SPN ciphers with application to AES and ARIA is presented in section III. Section IV extends the main result to other block cipher structures. Finally, section V contains the conclusion.

1) In fact, there are in total 176 integral distinguishers of the 3-round ARIA when the number of active bytes of the inputs is fixed to 3. Among these distinguishers, only 144 are listed in [15].

2) It should be emphasized that not all (extended) higher-order distinguishers of SPN ciphers can be obtained directly from the (basic) integral distinguishers only through a linear transformation. For instance, the 2-round first-order integral distinguishers [7] of ARIA cannot be directly extended to the 3-round third-order integral distinguishers [15], which are found by the counting method.

## II. SPN Ciphers

The class of SPN cipher considered in this paper iterates the combination of a substitution (a nonlinear transformation) and a linear transformation. Its block length is *mn*-bit (or *m*-word with a word being *n*-bit), and the round function consists of three basic operations: a substitution layer $\gamma$, a diffusion layer $\theta$, and a round key addition layer $\sigma$. Let us denote $\mathbb{F}_2$ as the finite field with elements 0 and 1. We briefly describe the three layers, as well as the whole cipher, as follows.

### 1. Substitution Layer $\gamma$

The substitution layer $\gamma$ is a nonlinear word-oriented substitution that applies parallel nonlinear bijective mappings on $\mathbb{F}_{2^m}$. At the *i*-th round, $\gamma_i : \mathbb{F}_{2^m}^n \to \mathbb{F}_{2^m}^n$ is defined as

$$\gamma_i(x_1, x_2, \ldots, x_n) = (s_{i,1}(x_1), s_{i,2}(x_2), \ldots, s_{i,n}(x_n)),$$

where each $s_{i,j}$ is an *m*-bit nonlinear substitution and the $s_{ij}$'s are not necessarily identical.

### 2. Diffusion Layer $\theta$

The diffusion layer $\theta$ is an invertible linear transformation on $\mathbb{F}_{2^m}^n$ that can be represented by an invertible matrix $P \in \mathbb{F}_{2^m}^{n \times n}$. That is, given an input *X*, the output can be obtained through *Y*=*P*(*X*).

### 3. Round Key Addition Layer $\sigma$

The round key additional layer $\sigma$ is defined simply by the bit-wise XOR of the input and the round key. Thus, at the *i*-th round, $\sigma_i(x) = X \oplus K_i$, where *X* is the input and $K_i$ is the *mn*-bit round key and may be generated from the key schedule of the cipher.

### 4. Whole Cipher

A typical *r*-round SPN cipher firstly applies a round key addition (also called the "whitening"), 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

$$E_k(\cdot) = \sigma_r \circ \gamma_r \circ \left( \bigcirc_{i=1}^{r-1} \sigma_i \circ \theta_i \circ \gamma_i \right) \circ \sigma_0(\cdot).$$

ARIA is a good example that belongs to the above SPN ciphers. For AES, the round function comprises SubBytes, ShiftRows, MixColumns, and RoundKeyAdditions. If we define a new linear transformation as the composition of ShiftRows and MixColumns, then AES could also be regarded as the kind of SPN ciphers described above.

## III. Link Between Integrals and Higher-Order Integrals of SPN Ciphers

In this section, we first give some preliminaries, particularly the definitions of "integral" and "higher-order integral," and then we present the main result that builds a link between an *r*-round integral (basic integral) and an (*r*+1)-round higher-order integral of an SPN cipher. We end this section by applying the result to the block cipher AES and ARIA.

### 1. Integrals and Higher-Order Integrals

An integral distinguisher considers the propagation of sums of many values, and, in general, it takes a special structure of plaintexts as input, in which each component (subblock or word) is *active* or *passive* (see definitions below) and its output has similar properties, that is, some components of the ciphertexts are active, passive, or *balanced*.

**Definition 1.** A set $\{a_i \mid a_i \in \mathbb{F}_{2^m}, 0 \le i \le 2^m - 1\}$ is active if for all $0 \le i < j \le 2^m - 1$, $a_i \ne a_j$. A set $\{a_i \mid a_i \in \mathbb{F}_{2^m}, 0 \le i \le 2^m - 1\}$ is passive or *constant* if for all $0 < i \le 2^m - 1$, $a_i = a_0$. A set $\{a_i \mid a_i \in \mathbb{F}_{2^m}, 0 \le i \le 2^m - 1\}$ is balanced if the bit-wise XOR sum of all elements of the set is 0, that is, $\bigoplus_{i=0}^{2^m-1} a_i = 0$. We use *A* to denote an active set, *C* to denote a passive or constant set, and *B* to denote a balanced set.

The above notation of "active" is defined for one word, and it can be extended to a more generalized case. For example, when referring to *d* active words, it means a set of $2^{md}$ values that range over $\mathbb{F}_{2^m}^d$ in the *d*-tuple position. According to this convention, we introduce the following definition of (higher-order) integral, as in [1].

**Definition 2.** A *d*-th-order integral of a block cipher is the sum of the ciphertexts whose corresponding plaintexts form a special structure with just *d* active words.

**Definition 3.** A *d*-th-order integral distinguisher of a block cipher takes a special structure with *d* active words as input; its output form is a *d*-th-order integral that can be predicted, that is, some components of the ciphertext are active, constant, or balanced.

For convenience, we will sometimes use "(higher-order) integral" as the short notation for "(higher-order) integral distinguisher."

Let

$$\{i_1, i_2, \ldots, i_d\}, \{j_1, j_2, \ldots, j_k\} \subseteq \{1, 2, \ldots, n\}.$$

Then, a typical *d*-th-order integral distinguisher of a block cipher can be represented by

$$A_{i_1, i_2, \ldots, i_d} \to B_{j_1, j_2, \ldots, j_k},$$

where $A_{i_1, i_2, \ldots, i_d}$ denotes that there are *d* active words of the input (plaintexts) with indices $i_1, i_2, \ldots, i_d$, and $B_{j_1, j_2, \ldots, j_k}$

denotes that the words of the output (ciphertexts) with indices $j_1, j_2, \ldots, j_k$ are all balanced.

As for an $r$-round block cipher, several (higher-order) integral distinguishers may exist, and the following definition is essential.

**Definition 4.** An $r$-round (higher-order) integral distinguisher of a block cipher is called optimal if the number of active words of the inputs is the minimum amount needed.

In the next subsection, we will solve the following problem: given an $r$-round $u$-th-order integral of an SPN cipher, which is referred to as the $r$-round *basic integral*, how can this $r$-round basic integral be extended to an ($r$+1)-round $v$-th-order ($v \geq u$) integral?

## 2. Main Result

We show the main theorem of this paper, which provides an approach to show how an $r$-round basic integral distinguisher of SPN ciphers can be extended to an ($r$+1)-round higher-order one. The link between a basic integral and a higher-order integral is built through the matrix of the linear transformation in the diffusion layer and is based on the decomposition of the linear space defined by the linear mapping of the block cipher.

Let us denote the matrix of the linear transformation of an SPN cipher by $P = (p_{i,j})_{n\times n}$, where $p_{i,j}$ is the $(i,j)$-entry of the matrix. Let $P_{A,B}$ be the matrix obtained from $P$ by selecting the rows from $A$ and the columns from $B$.

Since there is a correspondence between the vector space $\mathbb{F}_2^m$ and the finite field $\mathbb{F}_{2^m}$, we thus denote the bit-wise XOR "$\oplus$" between the elements simply by "+."

The main result is the following theorem.

**Theorem 1.** Given an $r$-round $u$-th-order integral (as the basic integral) distinguisher of an SPN cipher, for which the active word indices of the input form the set $U=\{r_1, r_2, \ldots, r_u\}$, let

$$\overline{U} = \{1,2,\ldots,n\} - U = \{s_1, s_2, \ldots, s_{n-u}\},$$

$$V = \{t_1, t_2, \ldots, t_v\}, v \geq u,$$

and

$$P_{\overline{U},V} = \left(p_{s_a,t_b}\right)_{(n-u)\times v}.$$

If

$$\operatorname{rank}(P_{\overline{U},V}) = v - u, \qquad (**)$$

then there will exist an ($r$+1)-round $v$-th-order integral (extended higher-order integral) distinguisher with the associated set formed by the active word indices of the inputs equal to $V$.

*Proof.* Let us consider a structure of plaintexts in the ($r$+1)-round SPN cipher, with active word positions $t_1, t_2, \ldots, t_v$ (and all the other $n$–$v$ words are passive). Thus, this structure consists of $2^{mv}$ plaintexts.

After the initial key whitening, these plaintexts will pass through a nonlinear bijective transformation. Let us denote these intermediate values by

$$X = (\ldots, X_{t_1}, \ldots, X_{t_2}, \ldots, X_{t_v}, \ldots)^T,$$

where the $v$ entries $X_{t_1}, X_{t_2}, \ldots, X_{t_v}$ range over $\mathbb{F}_{2^m}^v$ and the other $n$–$v$ entries are constants. These $2^{mv}$ values will then be fed into the linear transformation whose output can be represented by $Y=PX$. Note that $n$–$v$ indices of the constant components of $X$ form a set, $\overline{V} = \{1,2,\ldots,n\} - V$; thus,

$$Y = PX = \sum_{j\in V} P_j X_j + \sum_{j\in \overline{V}} P_j X_j \triangleq \sum_{b=1}^{v} P_{t_b} X_{t_b} + C, \qquad (1)$$

where $P_j$ is the $j$-th column vector of $P$, $X_j$ is the $j$-th component of $X$, and $C \in \mathbb{F}_{2^m}^n$ is a constant vector.

Let $(X_{t_1}, X_{t_2}, \ldots, X_{t_v}) = Z \triangleq (Z_1, Z_2, \ldots, Z_v) \in \mathbb{F}_{2^m}^v$ and $P_V = (p_{i,t_b})_{n\times v}$ or, equivalently, $P_V$ is the submatrix of $P$ composed of the $v$ column vectors $P_{t_1}, P_{t_2}, \ldots, P_{t_v}$; then, (1) becomes

$$Y = P_V Z + C \triangleq W + C. \qquad (2)$$

Equation (2) implies that all values of $Y$ will form an affine space $\mathbb{Y}$ defined by

$$\mathbb{Y} = \mathbb{W} + C = \{W + C \mid W = P_V Z, Z \in \mathbb{F}_{2^m}^v\},$$

where $\mathbb{W} \subseteq \mathbb{F}_{2^m}^n$ is a linear space over $\mathbb{F}_{2^m}$ defined by $\mathbb{W} = \{W \mid W = P_V Z, Z \in \mathbb{F}_{2^m}^v\}$, and $C$ is the offset.

Regarding linear space $\mathbb{W}$, one can see that $\dim(\mathbb{W}) = v$ since $\dim(\mathbb{W}) = \operatorname{rank}(P_V)$, and the result follows from the fact that $P$ is invertible, leading to the independent property of the $v$ column vectors of $P_V$.

Next, we will show that the linear space $\mathbb{W}$ is a direct sum ($\dot{+}$) of two other linear spaces, $\mathbb{W}_1$ and $\mathbb{W}_2$, with dimensions $u$ and $v$–$u$, respectively. Linear spaces $\mathbb{W}_1$ and $\mathbb{W}_2$ can be constructed as follows.

Let $P_{U,V} = (p_{r_a,t_b})_{u\times v}$ and set $\mathbb{W}_1 = \{(\alpha_1, \alpha_2, \ldots, \alpha_n)\}$, where each $\alpha_i$ is defined as

$$\alpha_i = \begin{cases} \sum_{b=1}^{v} p_{i,t_b} Z_b, & \text{if } i \in U, \\ 0, & \text{if } i \notin U. \end{cases}$$

Let $P_{\overline{U},V} = (p_{s_a,t_b})_{(n-u)\times v}$ and set $\mathbb{W}_2 = \{(\beta_1, \beta_2, \ldots, \beta_n)\}$, where each $\beta_i$ is defined as

$$\beta_i = \begin{cases} \sum_{b=1}^{v} p_{i,t_b} Z_b, & \text{if } i \in \overline{U}, \\ 0, & \text{if } i \notin \overline{U}. \end{cases}$$

According to the above definitions, $\mathbb{W}_1$ and $\mathbb{W}_2$ are linear spaces (subspaces of $\mathbb{W}$). Since $U \cup \bar{U} = \{1, 2 \ldots, n\}$, and $U \cap \bar{U} = \varnothing$, we have $\mathbb{W}_1 \cap \mathbb{W}_2 = \{0\}$, which implies that $\mathbb{W}_1 + \mathbb{W}_2 \subseteq \mathbb{W}$ is a direct sum of two linear spaces.

Further, we know that $P_V$ can be generated from $p_{U,V}$ and $P_{\bar{U},V}$; thus,

$$\text{rank}(P_V) \le \text{rank}(P_{U,V}) + \text{rank}(P_{\bar{U},V}).$$

According to the condition,

$$\text{rank}(P_{\bar{U},V}) = v - u,$$

and, as previously established,

$$\text{rank}(P_V) = v,$$

which results in

$$\text{rank}(P_{U,V}) \ge v - (v - u) = u.$$

Note that the matrix $P_{U,V}$ has $u$ rows and, thus,

$$\text{rank}(P_{U,V}) \le u.$$

It is concluded that

$$\text{rank}(P_{U,V}) = u.$$

Now, we get

$$\begin{cases} \dim(\mathbb{W}_1) = \text{rank}(P_{U,V}) = u, \\ \dim(\mathbb{W}_2) = \text{rank}(P_{\bar{U},V}) = v - u. \end{cases}$$

Thus,

$$\dim(\mathbb{W}) = \dim(\mathbb{W}_1) + \dim(\mathbb{W}_2),$$

which proves that

$$\mathbb{W} = \mathbb{W}_1 \dot{+} \mathbb{W}_2.$$

Since $\mathbb{Y} = \mathbb{W} + C$, we have

$$\mathbb{Y} = (\mathbb{W}_1 \dot{+} \mathbb{W}_2) + C. \quad (3)$$

Noting that $\#\mathbb{Y} = 2^{mv}$, $\#\mathbb{W}_1 = 2^{mu}$, and $\#\mathbb{W}_2 = 2^{m(v-u)}$, (3) means that all $2^{mv}$ values in $\mathbb{Y}$ can be divided into $2^{m(v-u)}$ (fixing each value in $C' \in \mathbb{W}_2 + C$) disjoint affine spaces $\mathbb{W}_1 + C'$, that is,

$$\mathbb{Y} = \bigcup_{C' \in \mathbb{W}_2 + C} \mathbb{W}_1 + C'.$$

This property is surely maintained for those $2^{mv}$ values after $\mathbb{Y}$ passes the round key addition layer in the first round.

In total, the above analysis shows that, after these special $2^{mv}$ plaintexts pass through the initial key whitening stage and the first round encryption, their corresponding $2^{mv}$ intermediate states can be divided into $2^{m(v-u)}$ disjoint affine spaces (each with $2^u$ elements) containing $u$ active words and $(n-u)$ constant words, and the indices of these $u$ active words form the set $U$.

Remember that there exists an $r$-round integral distinguisher whose inputs possess the same active set $U$; thus, each affine space forms the inputs for the $r$-round $u$-th-order integral distinguisher. Since each $u$-th-order integral distinguisher implies some predictable components of the ciphertexts after $r$ rounds, so are the ciphertexts for the $v$-th-order integral after ($r$+1) rounds. Thus, we get an ($r$+1)-round $v$-th-order integral distinguisher, which ends the proof. □

Theorem 1 tells us that, given an $r$-round known basic integral of an SPN cipher, let $U$ represent the active indices of inputs; then, if one can find a set $V$ such that the rank condition $\text{rank}(P_{\bar{U},V}) = v - u = \#V - \#U$ is satisfied, then one will obtain an ($r$+1)-round extended higher-order integral whose active indices of the inputs form the set $V$. Note that such rank condition can be simply checked with the *Gaussian elimination method*, either manually or automatically.

In the next two subsections, we will apply the criteria established in theorem 1 to the well-known block ciphers AES and ARIA, showing how to extend basic integral distinguishers to higher-order integral distinguishers. Note that when discussing integral distinguishers for these two example SPN ciphers, their last round function does not omit the diffusion layer.

## 3. Application to AES

According to [1], [13], there exists a 4-round 4th-order integral of AES. In the following, we characterize the existence of these higher-order integrals by checking the rank of the submatrix chosen from the matrix $P$ of the linear transformation.

According to [12], for all $1 \le i, j \le 16$, there exists the following form of a 3-round 1st-order integral of AES:

$$A_i \to B_j.$$

The matrix of the "linear transformation" of AES is

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

Now, if we choose $U$= {1} and $V$= {1, 6, 11, 16}, then $\overline{U}$ = {2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} and the submatrix $P_{\overline{U},V}$ is thus

$$P_{\overline{U},V} = \begin{pmatrix} 1&2&3&1\\ 1&1&2&3\\ 3&1&1&2\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0\\ 0&0&0&0 \end{pmatrix}.$$

Since

$$\text{rank}\left(P_{\overline{U},V}\right) = 3 = 4-1 = \#V - \#U,$$

it is concluded that the 3-round integral $A_1 \rightarrow B_j$ can be extended to a 4-round higher-order integral:

$$A_{1,6,11,16} \rightarrow B_j.$$

From the definition of $P$, we can further find the following 4-round higher-order integrals:

$$A_{2,7,12,13} \rightarrow B_j,\ A_{3,8,9,14} \rightarrow B_j,\ \text{and}\ A_{4,5,10,15} \rightarrow B_j.$$

**Remark 1.** The 4-round 4th-order integral distinguisher can be *intuitively* obtained from the 3-round 1st-order integral distinguisher; hence, it seems unnecessary to use a large matrix $P$ to check the rank condition. However, this simple deduction follows from the special structure of ShiftRows and MixColumns; it would not work for a more complex matrix $P$, for example, the one used in ARIA. In this case, the rank condition is very useful, as demonstrated below.

## 4. Application to ARIA

In this subsection, we apply the criterion to the 3/4-round ARIA.

### *A. From 2-Round 1st-Order Integral to 3-Round 7th-Order Integral*

According to [7], for all $1 \le i, j \le 16$, there exists a 2-round 1st-order integral of ARIA of the following form:

$$A_i \rightarrow B_j.$$

The matrix of the linear transformation of ARIA is

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

Now, if we choose $U$= {9} and $V$= {1, 2, 5, 8, 11, 14, 16}, then $\overline{U}$ = {1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 15, 16} and the submatrix $P_{\overline{U},V}$ is thus

$$P_{\overline{U},V} = \begin{pmatrix} 0&0&1&0&0&1&0\\ 0&0&0&1&0&0&1\\ 0&1&1&0&1&0&1\\ 1&0&0&1&1&1&0\\ 1&0&0&0&0&0&1\\ 0&1&1&0&1&0&1\\ 1&0&0&1&1&1&0\\ 0&1&0&0&0&1&0\\ 1&1&0&0&0&0&0\\ 0&0&0&0&0&1&1\\ 0&0&1&1&0&0&0\\ 0&1&0&1&0&0&0\\ 1&0&0&1&1&1&0\\ 1&0&1&0&0&0&0\\ 0&1&1&0&1&0&1 \end{pmatrix}.$$

Since

$$\text{rank}\left(P_{\overline{U},V}\right) = 6 = 7-1 = \#V - \#U,$$

it is concluded that the 2-round 1st-order integral $A_1 \rightarrow B_j$ can be extended to a 3-round 7th-order integral:

$$A_{1,2,5,8,11,14,16} \rightarrow B_j.$$

With the rank condition (**), we can find many other 3-round $d$-th-order integrals of ARIA based on the 2-round 1st-order integrals. Our results show that $d \ge 7$, and these 3-round 7th-order integrals are listed in Table 1.

**Remark 2**. These 3-round 7th-order integrals of ARIA are optimal under the hypothesis that these 3-round higher-order integrals are limited to be constructed from 2-round 1st-order integrals. However, they may not be optimal compared with other kinds of 3-round integrals found by other techniques. See the example in [15], where the inputs of 3-round integrals have only three active bytes.

Table 1. 3-round 7th-order integrals of ARIA.

| No. | Active bytes index $U$ | Active bytes index $V$ | Balanced bytes index |
|---|---|---|---|
| 1 | 9 | {1, 2, 5, 8, 11, 14, 16} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 2 | 10 | {1, 2, 6, 7, 12, 13, 15} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 3 | 5 | {1, 3, 6, 9, 12, 15, 16} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 4 | 7 | {1, 3, 8, 10, 11, 13, 14} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 5 | 15 | {1, 4, 5, 6, 10, 12, 15} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 6 | 14 | {1, 4, 7, 8, 9, 11, 14} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 7 | 4 | {1, 6, 8, 11, 12, 14, 15} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 8 | 16 | {2, 3, 5, 6, 9, 11, 16} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 9 | 13 | {2, 3, 7, 8, 10, 12, 13} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 10 | 6 | {2, 4, 5, 10, 11, 15, 16} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 11 | 8 | {2, 4, 7, 9, 12, 13, 14} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 12 | 3 | {2, 5, 7, 11, 12, 13, 16} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 13 | 12 | {3, 4, 5, 8, 10, 13, 15} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 14 | 11 | {3, 4, 6, 7, 9, 14, 16} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 15 | 2 | {3, 6, 8, 9, 10, 13, 16} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |
| 16 | 1 | {4, 5, 7, 9, 10, 14, 15} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16} |

**Remark 3**. These 3-round 7th-order integrals of ARIA can be further extended to many (16 in total) 4-round 15th-order integrals of the form $A_{\overline{\{i\}}} \rightarrow B_j$, where $\overline{\{i\}} = \{1,2,\ldots,16\} - \{i\}$. Yet, as will be explained later, compared with the 4-round 12th-order integrals, they are not optimal.

### *B. From 3-Round 3rd Order Integral to 4-Round 12th-Order Integral*

According to [15], there exists the following form of a 3-round 3rd-order integral of ARIA:

$$A_{9,11,14} \rightarrow B_{10,12,13,15}.$$

Now, if we choose $U$= {9, 11, 14} and $V$= {1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 14, 16}, then $\overline{U} = \{1,2,3,4,5,6,7,8,10,12,13,15,16\}$ and the submatrix $P_{\overline{U},V}$ is thus

$$P_{\overline{U},V} = \begin{pmatrix} 0&0&0&1&1&0&1&0&1&0&1&0 \\ 0&0&1&0&0&1&0&1&1&0&0&1 \\ 0&1&0&0&1&0&1&0&0&1&0&1 \\ 1&0&0&0&0&1&0&1&0&1&1&0 \\ 1&0&1&0&0&1&0&0&1&0&0&1 \\ 0&1&0&1&1&0&0&0&0&1&0&1 \\ 1&0&1&0&0&0&0&1&0&1&1&0 \\ 0&1&0&1&0&0&1&0&1&0&1&0 \\ 1&1&0&0&0&1&1&0&0&0&0&0 \\ 0&0&1&1&1&0&0&1&0&0&0&0 \\ 0&1&1&0&0&0&1&1&0&0&0&0 \\ 1&0&0&1&1&1&0&0&0&0&0&0 \\ 0&1&1&0&1&1&0&0&1&1&0&1 \end{pmatrix}.$$

Since

$$\operatorname{rank}\left(P_{\overline{U},V}\right) = 9 = 12 - 3 = \#V - \#U,$$

it is concluded that the 3-round 3rd-order integral $A_{9,11,14} \rightarrow B_{10,12,13,15}$ can be extended to a 4-round 12th-order integral:

$$A_{1,2,3,4,5,6,7,8,9,11,14,16} \rightarrow B_{10,12,13,15}.$$

According to the definition of $P$ and the 3-round integral distinguisher of ARIA in [15], we can find many 4-round higher-order integrals of ARIA, among which there exist 36 12th-order integrals, as listed in Table 2. These 36 integral distinguishers contain the 24 4-round integral distinguishers found in [16].

**Remark 4**. We point out that by testing the rank condition, these 4-round integrals of AES or ARIA cannot be further extended to 5-round integrals.

## IV. Application to Other Block Cipher Structures

The authors in [17], [18] developed the "$\mathcal{U}$-method" as an automated tool to find impossible differentials for various kinds of block cipher structures. They also pointed out that such a method can be converted to a tool for finding 1st-order integrals of block cipher structures.

In this section, we show that by adopting the notation of the "encryption matrix" as introduced in [17], [18], we can apply our proposed criterion to find higher-order integrals of other block cipher structures. Currently, we do not list all possible results on various kinds of block cipher structures; we present only the cryptanalytic results of Nyberg's generalized Feistel

Table 2. 4-round 12th-order integrals of ARIA.

| No. | Active bytes index $U$ | Active bytes index $V$ | Balanced bytes index |
|---|---|---|---|
| 1 | {9, 11, 14} {9, 11, 16} {9, 14, 16} {11, 14, 16} | {1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 14, 16} | {10, 12, 13, 15} |
| 2 | {10, 12, 13} {10, 12, 15} {10, 13, 15} {12, 13, 15} | {1, 2, 3, 4, 5, 6, 7, 8, 10, 12, 13, 15} | {9, 11, 14, 16} |
| 3 | {5, 6, 15} {5, 6, 16} {5, 15, 16} {6, 15, 16} | {1, 2, 3, 4, 5, 6, 9, 10, 11, 12, 15, 16} | {7, 8, 13, 14} |
| 4 | {6, 7, 9} {6, 7, 12} {6, 9, 12} {7, 9, 12} | {1, 2, 3, 4, 5, 8, 10, 11, 13, 14, 15, 16} | {6, 7, 9, 12} |
| 5 | {5, 8, 10} {5, 8, 11} {5, 10, 11} {8, 10, 11} | {1, 2, 3, 4, 6, 7, 9, 12, 13, 14, 15, 16} | {5, 8, 10, 11} |
| 6 | {7, 8, 13} {7, 8, 14} {7, 13, 14} {8, 13, 14} | {1, 2, 3, 4, 7, 8, 9, 10, 11, 12, 13, 14} | {5, 6, 15, 16} |
| 7 | {3, 5, 10} {3, 5, 16} {3, 10, 16} {5, 10, 16} | {1, 2, 3, 5, 6, 7, 9, 11, 12, 13, 15, 16} | {2, 6, 12, 16} |
| 8 | {2, 7, 9} {2, 7, 16} {2, 9, 16} {7, 9, 16} | {1, 2, 3, 5, 6, 8, 9, 10, 11, 13, 14, 16} | {3, 8, 11, 16} |
| 9 | {4, 5, 9} {4, 5, 16} {4, 9, 16} {5, 9, 16} | {1, 2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 16} | {4, 7, 10, 13} |
| 10 | {3, 7, 9} {3, 7, 13} {3, 9, 13} {7, 9, 13} | {1, 2, 3, 5, 7, 8, 10, 11, 12, 13, 14, 16} | {4, 6, 9, 15} |
| 11 | {2, 5, 10} {2, 5, 13} {2, 10, 13} {5, 10, 13} | {1, 2, 3, 6, 7, 8, 9, 10, 12, 13, 15, 16} | {4, 5, 11, 14} |
| 12 | {4, 7, 10} {4, 7, 13} {4, 10, 13} {7, 10, 13} | {1, 2, 3, 6, 7, 8, 10, 11, 12, 13, 14, 15} | {1, 8, 12, 13} |
| 13 | {1, 8, 10} {1, 8, 15} {1, 10, 15} {8, 10, 15} | {1, 2, 4, 5, 6, 7, 9, 10, 12, 13, 14, 15} | {4, 7, 12, 15} |
| 14 | {3, 6, 10} {3, 6, 15} {3, 10, 15} {6, 10, 15} | {1, 2, 4, 5, 6, 7, 10, 11, 12, 13, 15, 16} | {3, 8, 9, 14} |
| 15 | {4, 6, 9} {4, 6, 15} {4, 9, 15} {6, 9, 15} | {1, 2, 4, 5, 6, 8, 10, 11, 12, 14, 15, 16} | {1, 5, 11, 15} |
| 16 | {1, 6, 9} {1, 6, 14} {1, 9, 14} {6, 9, 14} | {1, 2, 4, 5, 7, 8, 9, 10, 11, 14, 15, 16} | {3, 6, 12, 13} |
| 17 | {3, 8, 9} {3, 8, 14} {3, 9, 14} {8, 9, 14} | {1, 2, 4, 5, 7, 8, 9, 11, 12, 13, 14, 16} | {2, 7, 11, 14} |
| 18 | {4, 8, 10} {4, 8, 14} {4, 10, 14} {8, 10, 14} | {1, 2, 4, 6, 7, 8, 9, 11, 12, 13, 14, 15} | {3, 5, 10, 16} |
| 19 | {3, 4, 9} {3, 4, 10} {3, 9, 10} {4, 9, 10} | {1, 2, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16} | {3, 4, 9, 10} |
| 20 | {1, 5, 11} {1, 5, 15} {1, 11, 15} {5, 11, 15} | {1, 3, 4, 5, 6, 7, 9, 10, 12, 14, 15, 16} | {2, 8, 11, 13} |
| 21 | {2, 5, 12} {2, 5, 15} {2, 12, 15} {5, 12, 15} | {1, 3, 4, 5, 6, 8, 9, 10, 12, 13, 15, 16} | {3, 6, 10, 15} |
| 22 | {4, 7, 12} {4, 7, 15} {4, 12, 15} {7, 12, 15} | {1, 3, 4, 5, 6, 8, 10, 11, 12, 13, 14, 15} | {2, 7, 9, 16} |
| 23 | {1, 7, 12} {1, 7, 14} {1, 12, 14} {7, 12, 14} | {1, 3, 4, 5, 7, 8, 9, 10, 11, 13, 14, 15} | {4, 8, 10, 14} |
| 24 | {2, 7, 11} {2, 7, 14} {2, 11, 14} {7, 11, 14} | {1, 3, 4, 6, 7, 8, 9, 10, 11, 13, 14, 16} | {2, 5, 12, 15} |
| 25 | {4, 5, 11} {4, 5, 14} {4, 11, 14} {5, 11, 14} | {1, 3, 4, 6, 7, 8, 9, 11, 12, 14, 15, 16} | {1, 6, 9, 14} |
| 26 | {2, 4, 5} {2, 4, 7} {2, 5, 7} {4, 5, 7} | {1, 3, 6, 8, 9, 10, 11, 12, 13, 14, 15, 16} | {2, 4, 5, 7} |
| 27 | {1, 4, 14} {1, 4, 15} {1, 14, 15} {4, 14, 15} | {1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 14, 15} | {2, 3, 13, 16} |
| 28 | {1, 6, 11} {1, 6, 16} {1, 11, 16} {6, 11, 16} | {2, 3, 4, 5, 6, 7, 9, 10, 11, 14, 15, 16} | {4, 5, 9, 16} |
| 29 | {3, 8, 11} {3, 8, 16} {3, 11, 16} {8, 11, 16} | {2, 3, 4, 5, 6, 7, 9, 11, 12, 13, 14, 16} | {1, 8, 10, 15} |
| 30 | {2, 6, 12} {2, 6, 16} {2, 12, 16} {6, 12, 16} | {2, 3, 4, 5, 6, 8, 9, 10, 11, 13, 15, 16} | {1, 7, 12, 14} |
| 31 | {1, 8, 12} {1, 8, 13} {1, 12, 13} {8, 12, 13} | {2, 3, 4, 5, 7, 8, 9, 10, 12, 13, 14, 15} | {1, 6, 11, 16} |
| 32 | {3, 6, 12} {3, 6, 13} {3, 12, 13} {6, 12, 13} | {2, 3, 4, 5, 7, 8, 10, 11, 12, 13, 15, 16} | {2, 5, 10, 13} |
| 33 | {2, 8, 11} {2, 8, 13} {2, 11, 13} {8, 11, 13} | {2, 3, 4, 6, 7, 8, 9, 10, 12, 13, 14, 16} | {3, 7, 9, 13} |
| 34 | {2, 3, 13} {2, 3, 16} {2, 13, 16} {3, 13, 16} | {2, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 16} | {1, 4, 14, 15} |
| 35 | { 1, 3, 6} {1, 3, 8} {1, 6, 8} {3, 6, 8} | {2, 4, 5, 7, 9, 10, 11, 12, 13, 14, 15, 16} | {1, 3, 6, 8} |
| 36 | {1, 2, 11} {1, 2, 12} {1, 11, 12} {2, 11, 12} | {3, 4, 5, 6, 7, 8, 9, 10, 13, 14, 15, 16} | {1, 2, 11, 12} |

network [19] and the generalized Feistel-nonlinear feedback shift register (GF-NLFSR) [20] as examples.

The idea is to introduce a substitution layer and a diffusion layer for block cipher structures. The substitution layer is just an identity transformation, while the diffusion layer can adopt the encryption matrix. Once these two layers are introduced, we can apply the criterion to extend a basic integral to a higher-order integral, as we do for SPN ciphers.

Considering the definition of the encryption matrix for a block cipher structure introduced in [17], [18], assume a block cipher structure with round function $F$ (or many different $F$'s) has $n$ data subblocks, and the input and the output of a round are $(X_0, X_1 \ldots, X_{n-1})$ and $(Y_0, Y_1 \ldots, Y_{n-1})$, respectively. We have the following definition:

**Definition 5** [17], [18]. For a block cipher structure, the $n \times n$ encryption matrix $M$ is defined as follows. If $Y_j$ is affected by $X_i$ (affected means $Y_j = X_i \oplus b$, where $b$ is a certain value), the $(i,j)$-entry of $M$ is set to 1. In particular, if $Y_j$ is affected by $F(X_i)$ or $F^{-1}(X_i)$, the $(i,j)$-entry of $M$ is set to $1_F$ instead of 1. If $Y_j$ is not affected by $X_i$, the $(i,j)$-entry of $M$ is set to 0.

A significant difference between the notation for the encryption matrix in this paper and that in [17], [18] is the definition of the multiplication of a vector and the matrix $M$.

In [17], [18], a vector is treated as a row-vector, and the

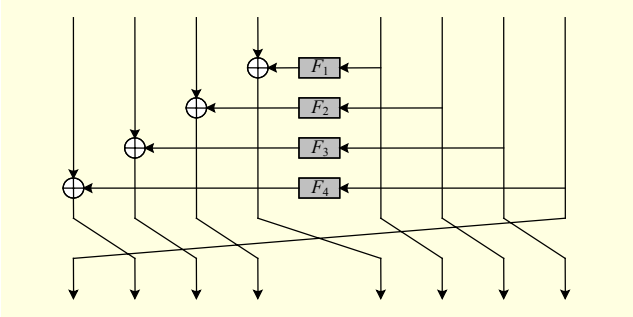


Fig. 1. Nyberg's generalized Feistel network with eight subblocks.

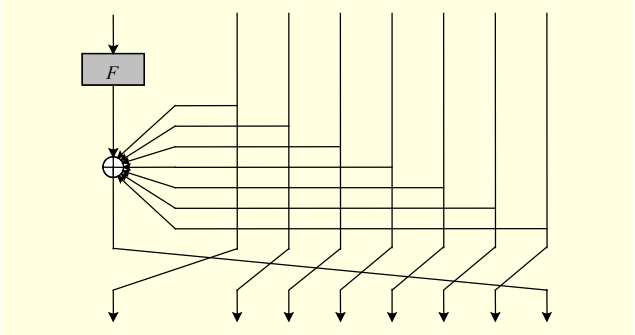


Fig. 2. GF-NLFSR structure with eight subblocks.

multiplication is thus defined by the product of a row-vector times the matrix $M$. However, using our approach, a vector is treated as a column-vector, and the multiplication is defined by the product of the matrix $M$ times a column-vector. This difference leads to the fact that the encryption matrix of a block cipher structure in this paper is the transpose of the corresponding matrix in [17], [18].

The definition of the rank for such an encryption matrix is important. Note that there are three kinds of elements in the encryption matrix: 0, 1, and $1_F$. In fact, as the definition of multiplication between a vector and a matrix, we can treat 0 and 1 as the traditional values, while treating the element $1_F$ as a non-zero and non-one value. Meanwhile, for different round functions $F$, the value $1_F$ should be different. According to the above convention, the rank of an encryption matrix can be defined as the traditional rank is defined.

## 1. Analysis of Nyberg's Generalized Feistel Network

A generalized Feistel network was proposed by Nyberg in [19], and it could provide provable security against differential and linear cryptanalysis. An evaluation of the security of this structure with eight subblocks against integral cryptanalysis [1] claims the existence of a 15-round 6th-order integral (the concrete distinguisher is not given). In this subsection, we show how to use our proposed criterion to construct the 15-round 6th-order integral.

The encryption procedure of Nyberg's generalized Feistel network structure with eight subblocks is described in Fig. 1, and the encryption matrix is

$$P=\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1_{F_4} \\ 0 & 1 & 0 & 0 & 0 & 0 & 1_{F_3} & 0 \\ 0 & 0 & 1 & 0 & 0 & 1_{F_2} & 0 & 0 \\ 0 & 0 & 0 & 1 & 1_{F_1} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Let us consider the 13-round 2nd-order integral of the form $A_{1,8} \to B_1$, as shown in [1]. Now, choose $U$= {1, 8} and $V$= {1, 2, 7, 8}; then, the submatrix is

$$P_{\overline{U},V}=\begin{pmatrix} 1 & 0 & 0 & 1_{F_4} \\ 0 & 1 & 1_{F_3} & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Since $\mathrm{rank}(P_{\overline{U},V}) = 2 = 4-2 = \#V - \#U$, we get a 14-round 4th-order integral of the form $A_{1,2,7,8} \to B_1$.

Based on the above 14-round 4th-order integral, let us further choose $U$= {1, 2, 7, 8} and $V$= {1, 2, 3, 6, 7, 8}; then, we will obtain the submatrix

$$P_{\overline{U},V}=\begin{pmatrix} 0 & 1 & 0 & 0 & 1_{F_3} & 0 \\ 0 & 0 & 1 & 1_{F_2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

The fact that $\mathrm{rank}(P_{\overline{U},V}) = 2 = 6-4 = \#V - \#U$ explains why there exists a 15-round 6th-order integral of the form $A_{1,2,3,6,7,8} \to B_1$.

## 2. Analysis of GF-NLFSR

The GF-NLFSR structure was proposed by Choy and others in [20]. Similar to Nyberg's generalized Feistel network, it can provide provable security against differential and linear cryptanalysis. The security of the GF-NLFSR containing $n$ subblocks against integral cryptanalysis was carefully studied in [21], which presents an $n^2$-round 1st-order integral and further an $(n^2+n-2)$-round $(n-1)$th-order integral. In this subsection, we consider the GF-NLFSR with eight subblocks as an example and show how the first-order integral of the GF-NLFSR can be easily extended to higher-order integrals by using theorem 1.

The encryption procedure of the GF-NLFSR with eight subblocks is described in Fig. 2, and the encryption matrix is

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

From [21], there exists a 64-round 1st-order integral of the form $A_1 \rightarrow A_{1\oplus 2\oplus \ldots \oplus 8}$, where $A_{1\oplus 2\oplus \ldots \oplus 8}$ means that the XOR sum of the eight words of the ciphertexts is active.

According to the encryption matrix $P$, for any $1 \le d \le 6$, let $U = \{1, 2, \ldots, d\}$ and $V = \{1, 2, \ldots, d, d+1\}$, and we can then prove $\mathrm{rank}(P_{\overline{U},V}) = 1 = d + 1 - d$. This observation shows that the above 64-round 1st-order integral can be iterated to construct a (64+$d$)-round ($d$+1)th-order integral. Thus, at last, we get the 70-round 7th-order integral:

$$A_{1,2,\ldots,7} \rightarrow B_{1\oplus 2\oplus \ldots \oplus 8},$$

where $B_{1\oplus 2\oplus \ldots \oplus 8}$ means that the XOR sum of the eight words of the ciphertexts is balanced.

## V. Conclusion

In this paper, we built a link between integrals and higher-order integrals of SPN ciphers. We showed that if the matrix of the linear transformation in the diffusion layer satisfies a rank condition that implies a direct decomposition of a linear space, then an $r$-round (basic) integral can be extended to an ($r$+1)-round higher-order integral. This proposed criterion unifies the procedure for finding 4-round higher-order integrals of the AES and ARIA. Additionally, it is suitable for detecting higher-order integrals of other block cipher structures. We hope that the criterion presented in this paper will benefit the cryptanalysts, and may thus lead to better cryptanalytic results.

## Reference


[1] L.R. Knudsen and D. Wagner, "Integral Cryptanalysis," *FSE*, *LNCS*, vol. 2365, Springer, 2002, pp. 112-127.

[2] J. Daemen, L.R. Knudsen, and V. Rijmen, "The Block Cipher SQUARE," *FSE*, *LNCS*, vol. 1267, Springer, 1997, pp. 149-165.

[3] S. Lucks, "The Saturation Attack – A Bait for Twofish," *FSE*, *LNCS*, vol. 2355, Springer, 2002, pp. 1-15.

[4] A. Biryukov and A. Shamir, "Structural Cryptanalysis of SASAS," *J. Cryptology*, vol. 23, Springer, 2010, pp. 505-518.

[5] E. Biham and A. Shamir. "Differential Cryptanalysis of DES-like Cryptosystems," *J. Cryptology*, *LNCS*, vol. 537, Springer, 1991, pp. 2-21.

[6] FIPS Publication 197, "Specification for the Advanced Encryption Standard (AES)," US Department of Commerce, National Institute of Standards and Technology (NIST), Information Technology Laboratory (ITL), Gaithersburg, MD, USA, 2001.

[7] D. Kwon et al., "New Block Cipher: ARIA," *ICISC*, *LNCS*, vol. 2971, Springer, 2004, pp. 432-445.

[8] M. Matsui, "Linear Cryptanalysis Method for DES Cipher," *EuroCrypt*, *LNCS* 765, Springer, 1994, pp. 386-397.

[9] S. Hong et al., "Provable Security Against Differential and Linear Cryptanalysis for the SPN Structure," *FSE*, *LNCS*, vol. 1978, Springer, 2001, pp. 273-283.

[10] J.-S. Kang et al., "Practical and Provable Security Against Differential and Linear Cryptanalysis for Substitution-Permutation Networks," *ETRI J.*, vol. 23, no. 4, Dec. 2001, pp. 158-167.

[11] S. Park et al., "Improving the Upper Bound on the Maximum Differential and the Maximum Linear Hull Probability for SPN Structures and AES," *FSE*, *LNCS*, vol. 2887, Springer, 2003, pp. 247-260.

[12] J. Daemen and V. Rijmen, *The Design of Rijndael: AES - The Advanced Encryption Standard*, Springer-Verlag, 2002.

[13] H. Gilbert and M. Minier, "A Collision Attack on 7 Rounds of Rijndael," *3rd Adv. Encryption Standard Candidate Conf.*, 2000, pp. 230-241.

[14] N. Ferguson et al., "Improved Cryptanalysis of Rijndael," *FSE*, *LNCS*, vol. 1978, Springer, 2001, pp. 213-230.

[15] P. Li, B. Sun, and C. Li, "Integral Cryptanalysis of ARIA," *INSCRYPT*, *LNCS*, vol. 6151, Springer, 2011, pp. 1-14.

[16] Y. Li, W. Wu, and L. Zhang. "Integral Attacks on Reduced-Round ARIA Block Cipher," *ISPEC*, *LNCS*, vol. 6047, Springer, 2010, pp. 19-29.

[17] J. Kim et al., "Impossible Differential Cryptanalysis for Block Cipher Structures," *INDOCRYPT*, *LNCS*, vol. 2904, Springer, 2003, pp. 82-96.

[18] J. Kim, S. Hong, and J. Lim, "Impossible Differential Cryptanalysis Using Matrix Method," *Discrete Mathematics*, vol. 310, no. 5, Elsevier, 2010, pp. 988-1002.

[19] K. Nyberg, "Generalized Feistel Networks," *ASIACRYPT*, *LNCS*, vol. 1163, Springer, 1996, pp. 91-104.

[20] J. Choy et al., "Cryptographic Properties and Application of a Generalized Unbalanced Feistel Network Structure," *ACISP*, *LNCS*, vol. 5594, Springer, 2009, pp. 73-89.

[21] R. Li et al., "Cryptanalysis of a Generalized Unbalanced Feistel Network Structure," *ACISP*, *LNCS*, vol. 6168, Springer, 2010, pp. 1-18.

**Ruilin Li** received his BS, MS, PhD in applied mathematics from the National University of Defense Technology, Changsha, Hunan, China, in 2005, 2007, and 2012, respectively. He is currently a lecturer with the School of Electronic Science and Engineering at the National University of Defense Technology. His research fields include cryptography and information security.

**Bing Sun** received his MS and PhD in applied mathematics from the National University of Defense Technology, Changsha, Hunan, China, in 2005 and 2009, respectively. He is now a lecturer with the Department of Mathematics and System Science at the National University of Defense Technology. His research fields include cryptography and information security.

**Chao Li** received his BS in mathematics in 1987 from the University of Information Engineering, Zhengzhou, Henan, China, his MS in mathematics in 1990 from the University of Science and Technology of China, Hefei, Anhui, China, and his PhD in engineering in 2002 from the National University of Defense Technology, Changsha, Hunan, China. Since December 2001, he has been a professor with the Department of Mathematics and System Science at the National University of Defense Technology. His research fields include coding theory, sequences, cryptography, and information security.