SCIENCE CHINA
Information Sciences

• LETTER •

January 2018, Vol. 61 019101:1–019101:3
doi: 10.1007/s11432-016-9184-y

Integral cryptanalysis of SPN ciphers with binary permutations

Hailong SONG[1,2] & Yuechuan WEI[3*]

[1]*School of Information Science and Engineering, Central South University, Changsha* 410083*, China;*
[2]*School of Information Science and Engineering, Jishou University, Jishou* 416000*, China;*
[3]*Electronics Technology Department, Engineering University of Armed Police Force, Xi'an* 710086*, China*

Received 22 December 2016/Revised 20 March 2017/Accepted 21 June 2017/Published online 3 November 2017

Citation Song H L, Wei Y C. Integral cryptanalysis of SPN ciphers with binary permutations. Sci China Inf Sci, 2018, 61(1): 019101, doi: 10.1007/s11432-016-9184-y

Dear editor,

As one of the most powerful cryptanalytic vectors, integral cryptanalysis [1] exploits the simultaneous relationship between multiple encryptions. In [1], the integral of $f(x)$ over some subset V (V is not necessarily but often a linear subspace) is defined as follows:

$$\int_V f = \sum_{x \in V} f(x).$$

As the expansion of integral, several concepts such as bit-pattern-based integral [2], higher order integral and higher degree integral [3] are proposed respectively. Integrals are especially well-suited in analyzing ciphers with primarily bijective components. Consequently, they are applied to a lot of (round-reduced) ciphers which are not vulnerable to differential and linear cryptanalysis.

At EUROCRYPT 2016, Sun et al. [4] proved that the length of the impossible differential of an SPN cipher is upper bounded by the sum of the primitive indexes of both the diffusion layer and its inverse. This inspires us to characterize the integrals of ciphers using properties of diffusion layers.

Branch number of diffusion layer plays an important role in evaluating the security of block ciphers against differential and linear cryptanalysis. The larger a branch number is, the more resistant to differential and linear cryptanalysis the cipher is. In some papers, many people believe that the branch number can also be used to evaluate the security against integral attack. However, it seems that the branch number cannot characterize the security of block ciphers against integral cryptanalysis. For example, since the branch number of the linear layer of ARIA is 8, the designers believe that there does not exist any integral distinguisher which covers more than 3 rounds [5]. However, 3-round and 4-round integral distinguishers were constructed in [6] and [7], respectively.

In this letter, we mainly discuss the security of SPN ciphers with binary permutations against integral cryptanalysis. Firstly, it is pointed that the branch number of the linear transformations cannot properly characterize the security of ciphers against integral cryptanalysis, and we propose the *integral branch number* of binary linear transformations to evaluate the immunity of ciphers against integral cryptanalysis and these results can be successfully used to explain the existence of integrals of SPN ciphers such as ARIA. Secondly, some combinational properties of integral branch number are studied, we show that for an $n \times n$ non-singular binary matrix, the integral branch number is upper bounded by $n - 2$ and construction of binary matrix with optimal integral branch number is discussed. Note that this letter only presents the results, and the details of

* Corresponding author (email: wych004@163.com)
The authors declare that they have no conflict of interest.

the proof refer to the supplemental file.

Many block ciphers are designed based on the SPN structure. Let the input to a cipher $\mathcal{E}$ be $X = (X_0, \ldots, X_{n-1})^{\mathrm{T}} \in \mathbb{F}_{2^t}^n$, and the input and output of the ith round be $X^{(i)} = (X_0^{(i)}, \ldots, X_{n-1}^{(i)})^{\mathrm{T}} \in \mathbb{F}_{2^t}^n$ and $X^{(i+1)} = (X_0^{(i+1)}, \ldots, X_{n-1}^{(i+1)})^{\mathrm{T}} \in \mathbb{F}_{2^t}^n$, respectively. Let $K^{(i)} = (K_0^{(i)}, \ldots, K_{n-1}^{(i)})^{\mathrm{T}} \in \mathbb{F}_{2^t}^n$ be the ith round key. If the procedure of the round function is defined as follows, $\mathcal{E}$ is named as an SPN cipher:

$$X^{(i+1)} = \mathcal{PS}\left(X^{(i)} \oplus K^{(i)}\right),$$

where

$$\begin{aligned}&\mathcal{S}\left((T_0, \ldots, T_{n-1})^{\mathrm{T}}\right)\\ &= \left(S_0(T_0), \ldots, S_{n-1}(T_{n-1})\right)^{\mathrm{T}}\end{aligned}$$

and $S_i\,(0 \leqslant i \leqslant n-1)$ are nonlinear bijective transformations; $\mathcal{P}\left((T_0, \ldots, T_{n-1})^{\mathrm{T}}\right) = P(T_0, \ldots, T_{n-1})^{\mathrm{T}}$ is a linear transformation where $P \in \mathbb{F}_2^{n\times n}$.

The following definitions are essential in computing the integrals of $f(x)$ over some subsets.

Definition 1. A multi-set $A = \{a_i | a_i \in \mathbb{F}_{2^n}, 0 \leqslant i \leqslant 2^n - 1\}$ is *active*, if for any $0 \leqslant i < j \leqslant 2^n - 1$, $a_i \neq a_j$. A polynomial $p(x) \in \mathbb{F}_{2^t}[x]$ is active if $p(x)$ is a permutation over $\mathbb{F}_{2^t}$.

Definition 2. A multi-set $C = \{a_i | a_i \in \mathbb{F}_{2^n}, 0 \leqslant i \leqslant 2^n - 1\}$ is *passive*, if for any $0 < i \leqslant 2^n - 1$, $a_i = a_0$. A polynomial $p(x) \in \mathbb{F}_{2^t}[x]$ is passive if $p(x)$ is a constant over $\mathbb{F}_{2^t}$.

Definition 3. A multi-set $B = \{a_i | a_i \in \mathbb{F}_{2^n}, 0 \leqslant i \leqslant 2^n - 1\}$ is *balanced*, if $\sum_{i=0}^{2^n-1} a_i = 0$. A polynomial $p(x) \in \mathbb{F}_{2^t}[x]$ is balanced if $\sum_{x\in\mathbb{F}_{2^t}} p(x) = 0$.

Definition 4. For an iterated cipher $\mathcal{E}$, denote by $\mathcal{D}(i, j, r)$ an r-round integral distinguisher with only the ith byte of the input being active and the jth byte of the output being balanced.

In some cases, if r is known from the context, $\mathcal{D}(i, j, r)$ can be simplified by $\mathcal{D}(i, j)$.

Theorem 1. Let S be a bijective transformation over $\mathbb{F}_{2^t}$, $\alpha, \beta \in \mathbb{F}_{2^t}$, and $T(x) = S(x \oplus \alpha) \oplus S(x \oplus \beta)$. Then different values of $T(x)$ appear even times, thus $S(T(x))$ is balanced.

For a random function $f(x) \in \mathbb{F}_q[x]$, the probability that $\sum_{x\in V} f(x) = 0$ is q^{-1}. However, the following theorem tells that the probability that any different element appear even times is much lower than q^{-1}:

Theorem 2. Let $A = \{a_0, \ldots, a_{N-1}\}$ be a set with N different elements, B be a multi-set with $2M$ elements which are from A. Denote by $(a_i)_B$ the times that a_i appears in B. Then the probability that

$$(a_0)_B \equiv (a_1)_B \equiv \cdots \equiv (a_{N-1})_B \equiv 0 \mod 2$$

is

$$P_e(N, 2M) = \frac{C_{M+N-1}^{N-1}}{C_{2M+N-1}^{N-1}}.$$

Definition 5. The *Hamming Weight* of $X \in \mathbb{F}_{2^t}^n$ is defined as the number of non-zero components of X:

$$w(X) = \#\left\{i \,\middle|\, X = (x_0, \ldots, x_{n-1})^{\mathrm{T}}, x_i \neq 0\right\}.$$

Definition 6. Let L be a linear transformation over $\mathbb{F}_{2^t}^n$, then the branch number of L is defined as

$$\mathcal{B}(L) = \min_{0\neq X\in\mathbb{F}_{2^t}^n} \{w(X) + w(L(X))\}.$$

Definition 7. Let $X = (x_0, \ldots, x_{n-1})^{\mathrm{T}} \in \mathbb{F}_{2^t}^n$, $Y = (y_0, \ldots, y_{n-1})^{\mathrm{T}} \in \mathbb{F}_{2^t}^n$. Then $X \otimes Y$ is defined as

$$X \otimes Y = (x_0 y_0, \ldots, x_i y_i, \ldots, x_{n-1} y_{n-1})^{\mathrm{T}}.$$

Definition 8. Let P be an invertible element of $\mathbb{F}_{2^t}^{n\times n}$, $(P)_i\,(0 \leqslant i \leqslant n-1)$ be the ith column of P and P^{T} be the transpose of P. Then the *Integral Branch Number* of P is defined as

$$\mathcal{I}(P) = \min_{0\leqslant i,j\leqslant n-1} \left\{w\left((P)_i \otimes \left(P^{\mathrm{T}}\right)_j\right)\right\}.$$

To evaluate the security of ciphers against integral cryptanalysis, the following Theorem holds.

Theorem 3. Let $\mathcal{E}$ be an iterated SPN block cipher. Let $P \in \mathbb{F}_2^{n\times n}$ be the binary linear transformation that used in $\mathcal{E}$, and the confusion layer is defined as

$$S(X) = \left(S_0(X_0), \ldots, S_i(X_i), \ldots, S_{n-1}(X_{n-1})\right)^{\mathrm{T}},$$

where S_is are nonlinear function over $\mathbb{F}_{2^t}$. Assume $\mathcal{I}(P) = 2$, and the corresponding 2 non-zero positions are m_0 and m_1. If $S_{m_0} = S_{m_1}$, then $\mathcal{D}(m_0, m_1)$ is an integral distinguisher of SPSPS.

By Theorem 3, when designing an SPN cipher, $\mathcal{I}(P)$ should be 3 at least. However, this theorem does not imply that a larger integral branch number gives better security bound against integral attack.

Theorem 3 can be directly applied to SPN ciphers. The main observation of [6] is some 2.5-round integral distinguishers of ARIA, one of which can be simply denoted by $[0, (6, 9, 15)]$. By using Theorem 3, we can list all possible values where $[a, (b, c, d)]$ means that if only the ath byte of input takes all values of $\mathbb{F}_{2^8}$ and other bytes are constants, then $Z_{3,b}, Z_{3,c}$ and $Z_{3,d}$ are balanced. In [8], a 32×32 matrix is designed and

the authors proposed that there could not exist some integral distinguishers which cover more than 2 rounds, if the designer uses such 32×32 matrix. However, by Theorem 3, we find that if $S_{m_1} = S_{m_2}$, then some 2.5-round distinguishers $\mathcal{D}(i,j)$ of SPSPS could be found. For avoiding the existence of such 2.5-round integral distinguishers, one should use different S-boxes when design a cipher that adopts the linear transformation given by [8]. Distinguishers mentioned above are given in Appendix B.

Lemma 1. Let $P \in \mathbb{F}_2^{n\times n}$ be a nonsingular matrix, and $n \geqslant 2$. If $\mathcal{I}(P) \geqslant 2$, then

$$\mathcal{I}(P) \leqslant \min_{0\leqslant i\leqslant n-1} \left\{ w\left((P)_i\right), w\left(\left(P^{\mathrm{T}}\right)_i\right)\right\} - 1.$$

Theorem 4. Let $P \in \mathbb{F}_2^{n\times n}$ be an invertible matrix, and $n \geqslant 2$. Then $\mathcal{I}(P)$ is upper bounded by $n-2$.

In the following, we discuss how to construct P with $\mathcal{I}(P) = n-2$.

Definition 9. Let $P \in \mathbb{F}_2^{n\times n}$, if for any $0 \leqslant i,j \leqslant n-1$,

$$w\left((P)_i\right) = w\left(\left(P^{\mathrm{T}}\right)_j\right) = 1,$$

then P is called a permutation matrix.

Theorem 5. Let n be an even integer and $J_n = (a_{ij})_{n\times n}$ where $a_{ij} = 1$ for $0 \leqslant i,j \leqslant n-1$. Then $P \in \mathbb{F}_2^{n\times n}$ is an invertible matrix over $\mathbb{F}_2$ with $\mathcal{I}(P) = n-2$ if and only if: (1) $J_n \oplus P$ is a permutation matrix; or (2) There exist some integers $0 \leqslant t,k \leqslant n-1$, such that all components of $(P)_t$ and $(P^{\mathrm{T}})_k$ are 1 and $J_{n-1} \oplus P^*$ is a permutation matrix, where P^* is a sub-matrix of P by deleting the tth column and kth row.

Theorem 6. Let n be an odd integer and $J_{n-1} = (a_{ij})_{(n-1)\times(n-1)}$ where $a_{ij} = 1$ for $0 \leqslant i,j \leqslant n-2$. Then $P \in \mathbb{F}_2^{n\times n}$ is an invertible matrix over $\mathbb{F}_2$ with $\mathcal{I}(P) = n-2$ if and only if the following two conditions hold:

(1) There exist some integer $0 \leqslant t,k \leqslant n-1$, such that all components of $(P)_t$ and $(P^{\mathrm{T}})_k$ are 1.

(2) The $J_{n-1} \oplus P^*$ is a permutation matrix, where P^* is a sub-matrix of P by deleting the tth column and kth row.

Theorem 7. Let $P \in \mathbb{F}_2^{n\times n}$, and $n \geqslant 4$. Then if $\mathcal{I}(P) = n-2$, then $\mathcal{B}(P) = 4$.

Conclusion. This letter mainly discusses the security of SPN ciphers, especially those with binary matrices as linear transformations, against integral cryptanalysis. We first point that we may not use the branch number to efficiently evaluate the security against integral cryptanalysis.

It is given in this letter that the integral branch number of a non-singular $n \times n$ binary matrix is upper bounded by $n-2$. Also the construction of non-singular matrices with optimal integral branch number is discussed. However, though the integral branch number is optimal, the branch number is only 4. This tells that maybe we can construct some binary matrices whose integral branch number is a little smaller while the branch number grows larger. How to construct binary matrices with integral branch number greater than 2 whose branch number is also optimal is an open problem.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61572521), Foundation of Science and Technology on Information Assurance Laboratory (Grant No. KJ-15-010), Scientific Research Project of Education Department of Hunan Province (Grant No. 17B214), Natural Science Foundation of Shaanxi Province (Grant No. 2016JQ6030).

Supporting information Appendix A–D. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Knudsen L R, Wagner D. Integral cryptanalysis. In: Proceedings of International Workshop on Fast Software Encryption. Berlin/Heidelberg: Springer, 2002. 112–127
2 Z'aba M R, Raddum H, Henricksen H, et al. Bit-pattern based integral attack. In: Proceedings of International Workshop on Fast Software Encryption. Berlin/Heidelberg: Springer, 2008. 363–381
3 Sun B, Qu L J, Li C. New cryptanalysis of block ciphers with low algebraic degree. In: Proceedings of International Workshop on Fast Software Encryption. Berlin/Heidelberg: Springer, 2009. 180–192
4 Sun B, Liu M C, Guo J, et al. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin/Heidelberg: Springer, 2016. 196–213
5 Kwon D, Kim J, Park S, et al. New block cipher: ARIA. In: Proceedings of International Conference on Information Security and Cryptology. Berlin/Heidelberg: Springer, 2004. 432–445
6 Li P, Sun B, Li C. Integral cryptanalysis of ARIA. In: Proceedings of International Conference on Information Security and Cryptology. Berlin/Heidelberg: Springer, 2010. 1–14
7 Li Y J, Wu W L, Zhang L. Integral attacks on reduced-round ARIA block cipher. In: Proceedings of International Conference on Information Security, Practice and Experience. Berlin/Heidelberg: Springer, 2010. 19–29
8 Koo B, Jang H, Song J. On constructing of a 32×32 binary matrix as a diffusion layer for a 256-bit block cipher. In: Proceedings of International Conference on Information Security and Cryptology. Berlin/Heidelberg: Springer, 2006. 51–64