SCIENCE CHINA
Information Sciences

• **Supplementary File** •

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*, P. R. China;*
[2] *School of Information Science and Engineering, Jishou University, Jishou,* 416000 *, P.R. China;*
[3] *Electronics Technology Department, Engineering University of Armed Police Force, Xi'an,* 710086*, P. R. China*

Appendix A Proof of Theorem 3

Assume $(P)_i = (a_0, \ldots, a_{n-1})$, $\left(P^T\right)_j = (b_0, \ldots, b_{n-1})$. If the input is of the form

$$(c_0, \ldots, c_{i-1}, x_i, c_{i+1}, \ldots, c_{n-1})^T$$

where c_ms are constants. Let $y = S_i\left(x_i \oplus k_i^{(1)}\right)$, then the output of the first round is

$$(a_0 y \oplus d_0, \ldots, a_{n-1} y \oplus d_{n-1})^T$$

where d_ms are some constants. Let $q_m = d_m \oplus k_m^{(2)}$, then the j-th byte of the output of second round is

$$T(y) = b_0 S_0 (a_0 y \oplus q_0) \oplus \cdots \oplus b_{n-1} S_{n-1} (a_{n-1} y \oplus q_{n-1}).$$

Now, $a_m b_m = 0$ implies that $b_m S_m (a_m y \oplus q_0)$ is a constant. Taking $\mathcal{I}(P) = 2$ and $a_{m_0} = b_{m_0} = a_{m_1} = b_{m_1} = 1$ into consideration, we have

$$T(y) = S_{m_0}(y \oplus q_{m_0}) \oplus S_{m_1}(y \oplus q_{m_1}) \oplus \alpha,$$

where α is a constant. From Theorem 1, different values of $S_j\left(T(y) \oplus k_j^{(3)}\right)$ appear even times, which ends our proof. □

Appendix B Distinguishers of ARIA and SPN Ciphers Using 32×32 Matrix of [1] as Linear Layer

Distinguishers of ARIA obtained by Theorem 3 are listed in Table B1.

Table B1 2.5-Round Integral Distinguishers of ARIA

Active byte	Balanced bytes	Active byte	Balanced bytes
0	6, 9, 15	8	1, 7, 14
1	7, 8, 14	9	0, 6, 15
2	4, 11, 13	10	3, 5, 12
3	5, 10, 12	11	2, 4, 13
4	2, 11, 13	12	3, 5, 10
5	3, 10, 12	13	2, 4, 11
6	0, 9, 15	14	1, 7, 8
7	1, 8, 14	15	0, 6, 9

When using 32×32 matrix of [1] as linear layer, by Theorem 3, if $S_{m_1} = S_{m_2}$, some 2.5-round distinguishers $\mathcal{D}(i,j)$ of SPSPS could be found which are listed in Table B2.

* Corresponding author (email: wych004@163.com)

Table B2 Distinguishers of SPSPS

(i, j)	m_1, m_2	(i, j)	m_1, m_2
(4, 7)	12,15	(18,22)	14,30
(4,27)	9,22	(19,23)	15,31
(5, 4)	12,13	(20,10)	24,25
(5,24)	10,23	(20,16)	12,28
(6, 5)	13,14	(21,11)	25,26
(6,25)	11,20	(21,17)	13,29
(7, 6)	14,15	(22, 8)	26,27
(7,26)	8,21	(22,18)	14,30
(8,22)	25,26	(23, 9)	24,27
(8,30)	1,12	(23,19)	15,31
(9,23)	26,27	(24, 7)	10,21
(9,31)	2,13	(25, 4)	11,22
(10,20)	24,27	(26, 5)	8,23
(10,28)	3,14	(27, 6)	9,20
(11,21)	24,25	(28,10)	1,14
(11,29)	0,15	(29,11)	2,15
(16,20)	12,28	(30, 8)	3,12
(17,21)	13,29	(31, 9)	0,13

Appendix C Proof of Theorem 5 and Theorem 6

Assume $J_n \oplus P$ is a permutation. Then for any $0 \leqslant i, j \leqslant n-1$, $w\left((P)_i\right) = w\left(\left(P^T\right)_j\right) = n-1$, thus there exist at least one j, such that $w\left((P_i) \otimes \left(P^T\right)_j\right) = n-2$. Since for any $\alpha, \gamma \in \mathbb{F}_2^n$ with $w(\alpha) = w(\beta) = n-1$, $w(\alpha \otimes \beta) \geqslant n-2$. So $\mathcal{I}(P) = n-2$.

Now, assume the second condition is satisfied. Since we have:

$$w\left((P)_t \otimes (P^T)_j\right) = \begin{cases} n & j = k \\ n-1 & j \neq k \end{cases}$$

and

$$w\left((P)_i \otimes (P^T)_k\right) = \begin{cases} n & i = t \\ n-1 & i \neq t. \end{cases}$$

For $i \neq t$ and $j \neq k$, we always have $w\left((P)_t \otimes (P^T)_k\right) = n-2$. Therefore, $\mathcal{I}(P) = n-2$.

Next, assume $\mathcal{I}(P) = n-2$. According to Theorem **??**, for any $0 \leqslant i \leqslant n-1$, $w\left((P)_i\right) \geqslant n-1$. Thus there exist at most one column all of whose components are 1. If $w\left((P)_0\right) = \cdots = w\left((P)_{n-1}\right) = n-1$, taking non-singularity into consideration, $J_n \oplus P$ is obviously a permutation matrix. If there is a column and row all of whose components are 1, then P^*, the sub-matrix of P by deleting the correspondence column and row, satisfies that $J_{n-1} \oplus P^*$ is a permutation matrix. This ends our proof of Theorem 5. □

Since for an odd integer n, if $J_n \oplus P$ is a permutation matrix, the sum of all rows (columns) is 0, which tells that P is singular, thus we have Theorem 6.

Appendix D Proof of Theorem 7

We only give the proof of the case that $J_n \oplus P$ is a permutation matrix.

Notice the fact that a permutation matrix is corresponding to a permutation π on $\{0, 1, \ldots, n-1\}$, thus

$$(J_n \oplus P) \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{n-1} \end{pmatrix} = \begin{pmatrix} X_{\pi(0)} \\ X_{\pi(1)} \\ X_{\pi(2)} \\ \vdots \\ X_{\pi(n-1)} \end{pmatrix}.$$

Let $T = X_0 \oplus X_1 \oplus \cdots \oplus X_{n-1}$, then

$$P \begin{pmatrix} X_0 \\ X_1 \\ X_2 \\ \vdots \\ X_{n-1} \end{pmatrix} = \begin{pmatrix} T \oplus X_{\pi(0)} \\ T \oplus X_{\pi(1)} \\ T \oplus X_{\pi(2)} \\ \vdots \\ T \oplus X_{\pi(n-1)} \end{pmatrix}.$$

(1) If the weight of the input is 1, then $T \neq 0$, thus the weight of the output is at least $n-1$;

(2) If the weight of the input is 2, there are following 2 cases: $T = 0$ and $T \neq 0$. If $T = 0$, the weight of the output is exactly 2; and if $T \neq 0$, the weight of the output is at least $n-2$;

(3) If the weight of the input is 3, there are also following 2 cases: $T = 0$ and $T \neq 0$. If $T = 0$, the weight of the output is exactly 3, and if $T \neq 0$, the weight of the output is at least $n-3$.

According to the definition of branch number, $\mathcal{B}(P) = 4$, which ends our proof. □

References

1 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 ICISC 2006, LNCS 4296, pp. 51–64, Springer–Verlag, 2006.