Mathematical Problems of Computer Science 45, 127--137, 2016.

Linear Cryptanalysis of SAFER-256

Knarik M. Kyuregyan

Institute for Informatics and Automation Problems of NAS RA
e-mail: knarikyuregyan@gmail.com

Abstract

In this paper linear cryptanalysis of 256-bit block cipher SAFER-256 is presented. SAFER-256 is secure against differential cryptanalysis after 5 rounds.

Keywords: Linear cryptanalysis.

1. Introduction

In paper [1] the detailed construction and security analysis against differential analysis of block cipher SAFER-256 is introduced. In this paper the result of linear cryptanalysis [2] of SAFER-256 is presented. We follow the terminology and notation in [2].

The round function is applied to 256 bit plaintext $X = X1X2 \dots X32$ with 6 times. The round function consists of the following four layers:

1. XOR/ADD, the first round key is "added" to the round input. Bytes 1,2,3,4,9,10,11,12,17,18,19,20,25,26,27,28 are added together bit-by-bit modulo 2 (XOR) bytes 5,6,7,8,13,14,15,16,21,22,23,24,29,30,31,32 are added together modulo 256 (ADD): $U = XOR/ADD(X, K_{2i-1})$.
2. Non-Linear (NL), where the values of bytes 1,2,3,4,9,10,11,12,17,18,19,20,25,26,27,28 are converted to $45^x \text{modulo} 257$ (with the convention that 45^{128} is represented as 0) and the values of bytes 5,6,7,8,13,14,15,16,21,22,23,24,29,30,31,32 are converted to $\log_{45} x$ (with the convention that the output $\log_{45} 0$ is represented by 128): $V = NL(U)$.
3. ADD/XOR, by this layer the second round key is inserted. The round key bytes 1,2,3,4,9,10,11,12,17,18,19,20,25,26,27,28 are added to the corresponding output bytes of linear layer modulo 256 (ADD) while the round key bytes 5,6,7,8,13, 14,15,16,21, 22,23,24, 29,30,31,32 are added to the corresponding output bytes of linear layer modulo 2 (XOR): $W = ADD/XOR(V, K_{2i})$.
4. Invertible Linear Transform or Pseudo-Hadamard Transform (PHT) consisting of four times applied $Armenian\ shuffle$ and four times applied eight 2-PHT boxes: $Y = PHT(W)$, is equivalent to $Y = WM$, where M is called an invertible linear transformation matrix of SAFER-256 introduced in Fig 1.

$$M=\begin{vmatrix}
8 & 8 & 1 & 1 & 2 & 2 & 8 & 4 & 4 & 2 & 1 & 1 & 1 & 1 & 4 & 4 & 8 & 4 & 4 & 2 & 2 & 1 & 2 & 2 & 32 & 16 & 2 & 1 & 8 & 4 & 2 & 2 \\
4 & 2 & 4 & 2 & 8 & 4 & 2 & 2 & 1 & 1 & 16 & 8 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 4 & 4 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 4 & 2 \\
4 & 2 & 8 & 4 & 8 & 4 & 4 & 4 & 1 & 1 & 32 & 16 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 8 & 8 & 2 & 1 & 1 & 1 & 2 & 2 & 2 & 2 & 8 & 4 \\
4 & 4 & 1 & 1 & 1 & 1 & 8 & 4 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 4 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 16 & 8 & 2 & 1 & 4 & 2 & 2 & 2 \\
2 & 2 & 2 & 2 & 1 & 1 & 32 & 16 & 2 & 1 & 4 & 4 & 2 & 2 & 1 & 1 & 2 & 1 & 8 & 4 & 8 & 4 & 1 & 1 & 8 & 4 & 4 & 2 & 4 & 2 & 8 & 8 \\
4 & 2 & 4 & 2 & 16 & 8 & 1 & 1 & 2 & 2 & 8 & 4 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 2 & 4 & 2 & 1 & 1 & 1 & 1 & 4 & 4 & 2 & 1 \\
8 & 4 & 4 & 2 & 32 & 16 & 1 & 1 & 4 & 4 & 8 & 4 & 2 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 2 & 2 & 8 & 4 & 2 & 2 & 1 & 1 & 8 & 8 & 2 & 1 \\
2 & 2 & 1 & 1 & 1 & 1 & 16 & 8 & 2 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 1 & 4 & 2 & 4 & 2 & 1 & 1 & 8 & 4 & 2 & 1 & 4 & 2 & 4 & 4 \\
2 & 2 & 1 & 1 & 8 & 8 & 4 & 2 & 8 & 4 & 1 & 1 & 2 & 2 & 2 & 2 & 4 & 2 & 8 & 4 & 2 & 1 & 4 & 4 & 8 & 4 & 2 & 1 & 32 & 16 & 1 & 1 \\
8 & 4 & 16 & 8 & 4 & 2 & 1 & 1 & 1 & 1 & 4 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 1 & 2 & 2 & 4 & 4 & 1 & 1 & 2 & 1 \\
8 & 4 & 32 & 16 & 4 & 2 & 2 & 2 & 1 & 1 & 8 & 4 & 8 & 4 & 2 & 1 & 1 & 1 & 4 & 4 & 2 & 2 & 2 & 1 & 2 & 2 & 8 & 8 & 1 & 1 & 4 & 2 \\
1 & 1 & 1 & 1 & 4 & 4 & 4 & 2 & 4 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 2 & 1 & 8 & 4 & 2 & 1 & 2 & 2 & 4 & 2 & 2 & 1 & 16 & 8 & 1 & 1 \\
1 & 1 & 4 & 4 & 2 & 2 & 8 & 4 & 2 & 1 & 2 & 2 & 8 & 8 & 1 & 1 & 2 & 1 & 32 & 16 & 4 & 2 & 1 & 1 & 4 & 2 & 8 & 4 & 8 & 4 & 2 & 2 \\
16 & 8 & 8 & 4 & 4 & 2 & 1 & 1 & 1 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 2 & 1 & 4 & 4 & 2 & 2 & 1 & 1 & 2 & 1 \\
32 & 16 & 8 & 4 & 8 & 4 & 1 & 1 & 2 & 2 & 4 & 2 & 2 & 1 & 8 & 4 & 4 & 4 & 1 & 1 & 1 & 1 & 4 & 2 & 8 & 8 & 2 & 2 & 2 & 2 & 2 & 1 \\
1 & 1 & 2 & 2 & 2 & 2 & 4 & 2 & 2 & 1 & 1 & 1 & 4 & 4 & 1 & 1 & 2 & 1 & 16 & 8 & 2 & 1 & 1 & 1 & 4 & 2 & 4 & 2 & 8 & 4 & 1 & 1 \\
1 & 1 & 2 & 2 & 1 & 1 & 8 & 4 & 4 & 2 & 8 & 8 & 2 & 2 & 2 & 2 & 8 & 4 & 4 & 2 & 32 & 16 & 1 & 1 & 2 & 1 & 8 & 4 & 2 & 1 & 4 & 4 \\
2 & 1 & 4 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 16 & 8 & 8 & 4 & 2 & 2 & 4 & 4 & 1 & 1 & 4 & 2 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 \\
2 & 1 & 8 & 4 & 2 & 1 & 2 & 2 & 1 & 1 & 4 & 2 & 32 & 16 & 8 & 4 & 2 & 2 & 8 & 8 & 2 & 2 & 4 & 2 & 1 & 1 & 4 & 4 & 1 & 1 & 8 & 4 \\
1 & 1 & 1 & 1 & 1 & 1 & 4 & 2 & 4 & 2 & 4 & 4 & 1 & 1 & 2 & 2 & 8 & 4 & 2 & 1 & 16 & 8 & 1 & 1 & 2 & 1 & 4 & 2 & 2 & 1 & 2 & 2 \\
4 & 4 & 1 & 1 & 2 & 2 & 2 & 1 & 8 & 4 & 2 & 2 & 1 & 1 & 8 & 8 & 32 & 16 & 2 & 1 & 8 & 4 & 2 & 2 & 8 & 4 & 4 & 2 & 4 & 2 & 1 & 1 \\
4 & 2 & 2 & 1 & 2 & 1 & 1 & 1 & 1 & 1 & 2 & 1 & 8 & 4 & 16 & 8 & 4 & 4 & 2 & 2 & 1 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 1 & 1 & 4 & 2 \\
8 & 4 & 2 & 1 & 4 & 2 & 1 & 1 & 2 & 2 & 2 & 1 & 8 & 4 & 32 & 16 & 8 & 8 & 2 & 2 & 1 & 1 & 8 & 4 & 4 & 4 & 1 & 1 & 2 & 2 & 4 & 2 \\
2 & 2 & 1 & 1 & 1 & 1 & 2 & 1 & 4 & 2 & 2 & 2 & 1 & 1 & 4 & 4 & 16 & 8 & 2 & 1 & 8 & 4 & 1 & 1 & 4 & 2 & 4 & 2 & 2 & 1 & 1 & 1 \\
1 & 1 & 8 & 8 & 1 & 1 & 4 & 2 & 8 & 4 & 2 & 2 & 4 & 4 & 1 & 1 & 4 & 2 & 8 & 4 & 8 & 4 & 2 & 2 & 2 & 1 & 32 & 16 & 2 & 1 & 2 & 2 \\
2 & 1 & 2 & 1 & 2 & 1 & 4 & 4 & 2 & 2 & 4 & 2 & 4 & 2 & 4 & 2 & 1 & 1 & 1 & 1 & 2 & 2 & 8 & 4 & 1 & 1 & 1 & 1 & 1 & 1 & 16 & 8 \\
2 & 1 & 4 & 2 & 2 & 1 & 8 & 8 & 2 & 2 & 8 & 4 & 8 & 4 & 4 & 2 & 1 & 1 & 2 & 2 & 4 & 4 & 8 & 4 & 1 & 1 & 2 & 2 & 1 & 1 & 32 & 16 \\
1 & 1 & 4 & 4 & 1 & 1 & 2 & 1 & 8 & 4 & 1 & 1 & 2 & 2 & 1 & 1 & 4 & 2 & 4 & 2 & 4 & 2 & 2 & 2 & 2 & 1 & 16 & 8 & 2 & 1 & 1 & 1 \\
2 & 2 & 2 & 2 & 4 & 4 & 2 & 1 & 32 & 16 & 1 & 1 & 1 & 1 & 2 & 2 & 8 & 4 & 2 & 1 & 4 & 2 & 8 & 8 & 4 & 2 & 8 & 4 & 8 & 4 & 1 & 1 \\
2 & 1 & 2 & 1 & 4 & 2 & 2 & 2 & 4 & 4 & 2 & 1 & 4 & 2 & 4 & 2 & 1 & 1 & 1 & 1 & 1 & 1 & 16 & 8 & 1 & 1 & 1 & 1 & 2 & 2 & 8 & 4 \\
4 & 2 & 2 & 1 & 8 & 4 & 2 & 2 & 8 & 8 & 2 & 1 & 4 & 2 & 8 & 4 & 2 & 2 & 1 & 1 & 1 & 1 & 32 & 16 & 2 & 2 & 1 & 1 & 4 & 4 & 8 & 4 \\
1 & 1 & 2 & 2 & 2 & 2 & 2 & 1 & 16 & 8 & 1 & 1 & 11 & 1 & 1 & 1 & 4 & 2 & 2 & 1 & 4 & 2 & 4 & 4 & 2 & 1 & 8 & 4 & 4 & 2 & 1 & 1
\end{vmatrix}$$

Fig. 1. Invertible linear transformation matrix of SAFER-256..

2. Linear Cryptanalysis of SAFER-256

We will find effective homomorphic I/O sums to a cascade of half-rounds of SAFER-256.

At first we find all binary-valued homomorphisms for ADD/XOR and for XOR/ADD. There are $2^8 - 1$ binary-valued homomorphisms for 8 bit XOR, namely the functions defined as $l_{a2}(V2) := a2 \circ V2$, where $a2$ is a non-zero binary 8-tuple " $\circ$ " operation denotes the modulo two "dot product". There is only one binary-valued homomorphism for modulo 256 addition, namely the function l_{a1} where $a1 = 0000\ 0001 = 01$ (hex notation of byte). Hence, there exist $2^{144} - 1$ balanced homomorphisms for ADD/XOR, namely the functions l_a defined as $l_a(V) = a \circ V$ where a lies in the set of 256-tuples.

$$\mathcal{A} = \{a: a \in \{0,1\}^{256} \backslash \{00\}; a1, a2, a3, a4, a9, a10, a11, a12, a17, a18, a19, a20, a25, a26, a27, a28\} \in \{00, 01\}\}.$$

Similarly, there are $2^{144} - 1$ balanced homomorphism for XOR/ADD, namely the functions $l_b(V) = b * V$, where b lies in the set

$$\mathcal{B} = \{b: b \in \{0,1\}^{256} \backslash \{00\}; b5, b6, b7, b8, b13, b14, b15, b16, b21, b22, b23, b24, b29, b30, b31, b32\} \in \{00, 01\}\}.$$

The set of all homomorphic functions for XOR/ADD and the set of all homomorphic functions for ADD/XOR are subsets of the set of all linear binary-valued functions.

At first we consider the part of round (half-round) containing the PHT function. The following lemma specifies all homomorphic I/O sums that have non-zero imbalance. The input function must be balanced and homomorphic for ADD/XOR; the output function must be balanced and homomorphic for XOR/ ADD. There are $(2^{144} - 1)^2$ such I/O sums, namely

$$S_{a,b}^{\mathrm{PHT-hr}} := l_a(\mathrm{V}) \oplus l_b(\mathrm{Y}) \quad a \in \mathcal{A}, b \in \mathcal{B}.$$

Lemma 1: *For the PHT-half-round, the only homomorphic I/O sums that have non-zero imbalance are the* $2^{32} - 1$ *guaranteed I/O sums obtained by XOR-ing together any positive number of the 32 guaranteed I/O sums listed in Table 1.*

Since $I\left(S_{a,b}^{\mathrm{PHT-hr}} | k_{2i}\right) = I\left(S_{a,b}^{\mathrm{PHT}}\right)$ for any $k_{2i} \in \{0,1\}^{256}$, where $S_{a,b}^{\mathrm{PHT}} := l_a(W) \oplus l_b(Y)$, $(a \in \mathcal{A}$ and $b \in \mathcal{B})$ is an I/O sum for the PHT function alone, we will look for I/O sums $S_{a,b}^{\mathrm{PHT}}$ with non-zero imbalance instead of looking for $S_{a,b}^{\mathrm{PHT-hr}}$ with non-zero imbalance. So, our main purpose is to find $a \in \mathcal{A}$ and $b \in \mathcal{B}$ such that $S_{a,b}^{\mathrm{PHT}}$ sum has the form $W_\alpha \oplus \phi(W_{256}, \dots, W_{\alpha+1}, W_{\alpha-1}, \dots, W_0)$ for some input bit W_α, since this implies that the I/O sum imbalance is 0.

First we consider PHT function. Table 2 shows three kind of dependences for some input and output bits. By using Table 2 we can iteratively show that I/O sums $S_{a,b}^{\mathrm{PHT}}$ with none-zero imbalance cannot contain any of the output bits Yi_j, where $i = 1,2,3,4,9,10,11,12,17,18,19,20,25,26,27,28$ and $j = 1,2,3,4,5,6,7$.

Finally, we consider the $2^{32} - 1$ balanced output functions obtained as linear combinations of the remaining 32 output bits that might occur if $b \in \mathcal{B}$. For each of these output functions, we found all input functions such that $S_{a,b}^{\mathrm{PHT}}$ doesn't depend linearly on any input bit. It is easy to show that $\left((a,b); a,b \in \{0,1\}^{256}, I\left(\mathrm{S}_{a,b}^{\mathrm{PHT}}\right) = 1\right)$ is a subgroup of $(\mathcal{A} \times \mathcal{B}, \oplus_{256\mathrm{bits}})$. (In fact if $I\left(\mathrm{S}_{a,b}^{\mathrm{PHT}}\right) = 1$ and $I\left(\mathrm{S}_{a',b'}^{\mathrm{PHT}}\right) = 1$ for some 256 tuples a' and b', then $I\left(\mathrm{S}_{a\oplus a',b\oplus b'}^{\mathrm{PHT}}\right) = I\left(\mathrm{S}_{a,b}^{\mathrm{PHT}} \oplus \mathrm{S}_{a',b'}^{\mathrm{PHT}}\right) = I\left(\mathrm{S}_{a,b}^{\mathrm{PHT}}\right) \cdot I\left(\mathrm{S}_{a',b'}^{\mathrm{PHT}}\right) = 1$ as well, whch shows that $\mathcal{A} \times \mathcal{B}$ is closed under "$\oplus$".) Thus, we obtain all I/O sums with non-zero imbalance, as is done in the statement of the lemma.

Table 1. Effective I/O sums for the PHT-function.

(a,b)	$l_b(Y)$	$l_a(W)$	$I(S_{a,b}^{\mathrm{PHT}})$
(00000000000110011001000010010001, 10000000000000000000000000000000)	$Y1_0$	$W12_0 \oplus W13_0 \oplus W16_0 \oplus W17_0 \oplus W20_0 \oplus W25_0 \oplus W28_0 \oplus W32_0$	1
(00000000000110011111000011110101, 01000000000000000000000000000000)	$Y2_0$	$W12_0 \oplus W13_0 \oplus W16_0 \oplus W17_0 \oplus W18_0 \oplus W19_0 \oplus W20_0 \oplus W25_0 \oplus W26_0 \oplus W27_0 \oplus W28_0 \oplus W30_0 \oplus W32_0$	1
(10010001100100000001100100000000, 00100000000000000000000000000000)	$Y3_0$	$W1_0 \oplus W4_0 \oplus W8_0 \oplus W9_0 \oplus W12_0 \oplus W20_0 \oplus W21_0 \oplus W24_0$	1
(10010001100100000001111101000110, 00010000000000000000000000000000)	$Y4_0$	$W1_0 \oplus W4_0 \oplus W8_0 \oplus W9_0 \oplus W12_0 \oplus W20_0 \oplus W21_0 \oplus W22_0 \oplus W23_0 \oplus W24_0 \oplus W26_0 \oplus W30_0 \oplus W31_0$	1
(00011001000000001001000110010000, 00001000000000000000000000000000)	$Y5_0$	$W4_0 \oplus W5_0 \oplus W8_0 \oplus W17_0 \oplus W20_0 \oplus W24_0 \oplus W25_0 \oplus W28_0$	1
(00011001000000001111010111110000, 00000100000000000000000000000000)	$Y6_0$	$W4_0 \oplus W5_0 \oplus W8_0 \oplus W17_0 \oplus W18_0 \oplus W19_0 \oplus W20_0 \oplus W22_0 \oplus W24_0 \oplus W25_0 \oplus W26_0 \oplus W27_0 \oplus W28_0$	1
(00000110010001100100011000000000, 00000010000000000000000000000000)	$Y7_0$	$W6_0 \oplus W7_0 \oplus W10_0 \oplus W14_0 \oplus W15_0 \oplus W18_0 \oplus W22_0 \oplus W23_0$	1
(00000110010001100100111100011001, 00000001000000000000000000000000)	$Y8_0$	$W6_0 \oplus W7_0 \oplus W10_0 \oplus W14_0 \oplus W15_0 \oplus W18_0 \oplus W21_0 \oplus W22_0 \oplus W23_0 \oplus W24_0 \oplus W28_0 \oplus W29_0 \oplus W32_0$	1
(01100000011001000110010000000000, 00000000100000000000000000000000)	$Y9_0$	$W2_0 \oplus W3_0 \oplus W10_0 \oplus W11_0 \oplus W14_0 \oplus W18_0 \oplus W19_0 \oplus W22_0$	1
(01111001011011010110010000000000, 00000000010000000000000000000000)	$Y10_0$	$W2_0 \oplus W3_0 \oplus W4_0 \oplus W5_0 \oplus W8_0 \oplus W10_0 \oplus W11_0 \oplus W13_0 \oplus W14_0 \oplus W16_0 \oplus W18_0 \oplus W19_0 \oplus W22_0$	1
(10010000100100010000000000011001, 00000000001000000000000000000000)	$Y11_0$	$W1_0 \oplus W4_0 \oplus W9_0 \oplus W12_0 \oplus W16_0 \oplus W28_0 \oplus W29_0 \oplus W32_0$	1
(10010000100100010100011000011111, 00000000000100000000000000000000)	$Y12_0$	$W1_0 \oplus W4_0 \oplus W9_0 \oplus W12_0 \oplus W16_0 \oplus W18_0 \oplus W22_0 \oplus W23_0 \oplus W28_0 \oplus W29_0 \oplus W30_0 \oplus W31_0 \oplus W32_0$	1
(10010001000000000001100100001001, 00000000000010000000000000000000)	$Y13_0$	$W1_0 \oplus W4_0 \oplus W8_0 \oplus W20_0 \oplus W21_0 \oplus W24_0 \oplus W29_0 \oplus W32_0$	1
(11010111000001100001100100001001, 00000000000001000000000000000000)	$Y14_0$	$W1_0 \oplus W2_0 \oplus W4_0 \oplus W6_0 \oplus W7_0 \oplus W8_0 \oplus W14_0 \oplus W15_0 \oplus W20_0 \oplus W21_0 \oplus W24_0 \oplus W29_0 \oplus W32_0$	1
(00001001000110010000000010010001, 00000000000000100000000000000000)	$Y15_0$	$W5_0 \oplus W8_0 \oplus W12_0 \oplus W13_0 \oplus W16_0 \oplus W25_0 \oplus W28_0 \oplus W32_0$	1
(01101101011110010000000010010001, 00000000000000010000000000000000)	$Y16_0$	$W2_0 \oplus W3_0 \oplus W5_0 \oplus W6_0 \oplus W8_0 \oplus W10_0 \oplus W11_0 \oplus W12_0 \oplus W13_0 \oplus W16_0 \oplus W25_0 \oplus W28_0 \oplus W32_0$	1
(01100100011000000000000001100100, 00000000000000001000000000000000)	$Y17_0$	$W2_0 \oplus W3_0 \oplus W6_0 \oplus W10_0 \oplus W11_0 \oplus W26_0 \oplus W27_0 \oplus W30_0$	1
(01101101011110010000000001100100, 00000000000000000100000000000000)	$Y18_0$	$W2_0 \oplus W3_0 \oplus W5_0 \oplus W6_0 \oplus W8_0 \oplus W10_0 \oplus W11_0 \oplus W12_0 \oplus W13_0 \oplus W16_0 \oplus W26_0 \oplus W27_0 \oplus W30_0$	1
(01000110000001100000000001000110, 00000000000000000010000000000000)	$Y19_0$	$W2_0 \oplus W6_0 \oplus W7_0 \oplus W14_0 \oplus W15_0 \oplus W26_0 \oplus W30_0 \oplus W31_0$	1
(01000110000001100001100101001111, 00000000000000000001000000000000)	$Y20_0$	$W2_0 \oplus W6_0 \oplus W7_0 \oplus W14_0 \oplus W15_0 \oplus W20_0 \oplus W21_0 \oplus W24_0 \oplus W26_0 \oplus W29_0 \oplus W30_0 \oplus W31_0 \oplus W32_0$	1
(00000000010001100100011000000110, 00000000000000000000100000000000)	$Y21_0$	$W10_0 \oplus W14_0 \oplus W15_0 \oplus W18_0 \oplus W22_0 \oplus W23_0 \oplus W30_0 \oplus W31_0$	1
(10010000110101110100011000000110, 00000000000000000000010000000000)	$Y22_0$	$W1_0 \oplus W4_0 \oplus W9_0 \oplus W10_0 \oplus W12_0 \oplus W14_0 \oplus W15_0 \oplus W16_0 \oplus W18_0 \oplus W22_0 \oplus W23_0 \oplus W30_0 \oplus W31_0$	1
(00011001000010011001000100000000, 00000000000000000000001000000000)	$Y23_0$	$W4_0 \oplus W5_0 \oplus W8_0 \oplus W13_0 \oplus W16_0 \oplus W17_0 \oplus W20_0 \oplus W24_0$	1
(01111001011011011001000100000000, 00000000000000000000000100000000)	$Y24_0$	$W2_0 \oplus W3_0 \oplus W4_0 \oplus W5_0 \oplus W8_0 \oplus W10_0 \oplus W11_0 \oplus W13_0 \oplus W14_0 \oplus W16_0 \oplus W17_0 \oplus W20_0 \oplus W24_0$	1
(01100100000000000110000001100100, 00000000000000000000000010000000)	$Y25_0$	$W2_0 \oplus W3_0 \oplus W6_0 \oplus W18_0 \oplus W19_0 \oplus W26_0 \oplus W27_0 \oplus W30_0$	1
(01100100000000001111000011110101, 00000000000000000000000001000000)	$Y26_0$	$W2_0 \oplus W3_0 \oplus W6_0 \oplus W17_0 \oplus W18_0 \oplus W19_0 \oplus W20_0 \oplus W25_0 \oplus W26_0 \oplus W27_0 \oplus W28_0 \oplus W30_0 \oplus W32_0$	1
(01000110000000000000011001000110, 00000000000000000000000000100000)	$Y27_0$	$W2_0 \oplus W6_0 \oplus W7_0 \oplus W22_0 \oplus W23_0 \oplus W26_0 \oplus W30_0 \oplus W31_0$	1
(11010111100100000000011001000110, 00000000000000000000000000010000)	$Y28_0$	$W1_0 \oplus W2_0 \oplus W4_0 \oplus W6_0 \oplus W7_0 \oplus W8_0 \oplus W9_0 \oplus W12_0 \oplus W22_0 \oplus W23_0 \oplus W26_0 \oplus W30_0 \oplus W31_0$	1
(00000000011001000110010001100000, 00000000000000000000000000001000)	$Y29_0$	$W10_0 \oplus W11_0 \oplus W14_0 \oplus W18_0 \oplus W19_0 \oplus W22_0 \oplus W26_0 \oplus W27_0$	1
(00000000011001001111010111110000, 00000000000000000000000000000100)	$Y30_0$	$W10_0 \oplus W11_0 \oplus W14_0 \oplus W17_0 \oplus W18_0 \oplus W19_0 \oplus W20_0 \oplus W22\_0 \oplus W24\_0 \oplus W25_0 \oplus W26_0 \oplus W27_0 \oplus W28_0$	1
(00000000100100010000100100011001, 00000000000000000000000000000010)	$Y31_0$	$W9_0 \oplus W12_0 \oplus W16_0 \oplus W21_0 \oplus W24_0 \oplus W28_0 \oplus W29_0 \oplus W32_0$	1
(00000110110101110000100100011001, 00000000000000000000000000000001)	$Y32_0$	$W6_0 \oplus W7_0 \oplus W9_0 \oplus W10_0 \oplus W12_0 \oplus W14_0 \oplus W15_0 \oplus W16_0 \oplus W21_0 \oplus W24_0 \oplus W28_0 \oplus W29_0 \oplus W32_0$	1

Table 2. Dependencies for certain bits of the PHT output Y on certain bits of the PHT input W ("0"-no dependence, "1"-binary linear dependence (i.e., complementing this input bit complements the corresponding output bit), "n"- non-linear binary dependence.

Input bit / Output bit		$W1$	$W2$	$W3$	$W4$	$W9$	$W10$	$W11$	$W12$	$W17$	$W18$	$W19$	$W20$	$W25$	$W26$	$W27$	$W28$
		7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321	7654321
$Y1$	7	0001nnn	001nnnn	001nnnn	001nnnn	01nnnnn	0001nnn	0001nnn	1nnnnnn	1nnnnnn	01nnnnn	01nnnnn	1nnnnnn	1nnnnnn	01nnnnn	01nnnnn	1nnnnnn
	6	0001nnn	0001nnn	0001nnn	0001nnn	001nnnn	0000101	0000101	01nnnnn	01nnnnn	001nnnn	001nnnn	01nnnnn	01nnnnn	001nnnn	001nnnn	01nnnnn
	5	0000101	0000101	0000101	0000101	0001nnn	0001nnn	0001nnn	001nnnn	001nnnn	0001nnn	0001nnn	001nnnn	001nnnn	0001nnn	0001nnn	001nnnn
	4	0000010	0000010	0000010	0000010	0000101	0000101	0000101	0001nnn	0001nnn	0000101	0000101	0001nnn	0001nnn	0000101	0000101	0001nnn
	3	0000000	0000000	0000000	0000000	0000010	0000000	0000000	0000101	0000101	0000010	0000010	0000101	0000101	0000010	0000010	0000101
	2	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000010	0000010	0000000	0000000	0000010	0000010	0000000	0000000	0000010
	1	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y2$	7	0001nnn	01nnnnn	01nnnnn	001nnnn	01nnnnn	001nnnn	001nnnn	1nnnnnn	1nnnnnn	1nnnnnn	1nnnnnn	1nnnnnn	1nnnnnn	1nnnnnn	1nnnnnn	1nnnnnn
	6	0001nnn	001nnnn	001nnnn	0001nnn	001nnnn	0001nnn	0001nnn	01nnnnn	01nnnnn	01nnnnn	01nnnnn	01nnnnn	01nnnnn	01nnnnn	01nnnnn	01nnnnn
	5	0000101	0001nnn	0001nnn	0000101	0001nnn	0000101	0000101	001nnnn	001nnnn	001nnnn	001nnnn	001nnnn	001nnnn	001nnnn	001nnnn	001nnnn
	4	0000010	0000101	0000101	0000010	0000101	0000010	0000010	0001nnn	0001nnn	0001nnn	0001nnn	0001nnn	0001nnn	0001nnn	0001nnn	0001nnn
	3	0000000	0000010	0000010	0000000	0000010	0000000	0000000	0000101	0000101	0000101	0000101	0000101	0000101	0000101	0000101	0000101
	2	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000010	0000010	0000010	0000010	0000010	0000010	0000010	0000010	0000010
	1	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y3$	7	1nnnnnn	001nnnn	0001nnn	1nnnnnn	1nnnnnn	0001nnn	000001n	1nnnnnn	01nnnnn	001nnnn	0001nnn	1nnnnnn	0001nnn	01nnnnn	001nnnn	001nnnn
	6	01nnnnn	0001nnn	0001nnn	01nnnnn	01nnnnn	0000101	0000010	01nnnnn	001nnnn	0001nnn	0000101	01nnnnn	0000101	0001nnn	0001nnn	0001nnn
	5	001nnnn	0000101	0000101	001nnnn	001nnnn	0001nnn	0000000	001nnnn	0001nnn	0000101	0000010	001nnnn	0000010	0000101	0000101	0000101
	4	0001nnn	0000010	0000010	0001nnn	0001nnn	0000101	0000000	0001nnn	0000101	0000010	0000000	0001nnn	0000000	0000010	0000010	0000010
	3	0000101	0000000	0000000	0000101	0000101	0000010	0000000	0000101	0000010	0000000	0000000	0000101	0000000	0000000	0000000	0000000
	2	0000010	0000000	0000000	0000010	0000010	0000000	0000000	0000010	0000000	0000000	0000000	0000010	0000000	0000000	0000000	0000000
	1	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y4$	7	1nnnnnn	01nnnnn	001nnnn	1nnnnnn	1nnnnnn	0001nnn	00001nn	1nnnnnn	01nnnnn	01nnnnn	001nnnn	1nnnnnn	0001nnn	1nnnnnn	01nnnnn	001nnnn
	6	001nnnn	001nnnn	0001nnn	01nnnnn	01nnnnn	0000101	0000001	001nnnn	001nnnn	001nnnn	0001nnn	01nnnnn	0000101	0001nnn	001nnnn	0001nnn
	5	0001nnn	0001nnn	0000101	001nnnn	001nnnn	0001nnn	0000000	0001nnn	0001nnn	0001nnn	0000101	001nnnn	0000010	0000101	0001nnn	0000101
	4	0000101	0000101	0000010	0001nnn	0001nnn	0000101	0000000	0000101	0000101	0000101	0000010	0001nnn	0000000	0000010	0000101	0000010
	3	0000010	0000010	0000000	0000101	0000101	0000010	0000000	0000010	0000010	0000010	0000000	0000101	0000000	0000000	0000010	0000000
	2	0000000	0000000	0000000	0000010	0000010	0000000	0000000	0000000	0000000	0000000	0000000	0000010	0000000	0000000	0000000	0000000
	1	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y5$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y6$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y7$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y8$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000

$Y9$	7	001nnnn	1nnnnnn	01nnnnn	1nnnnnn	0001nnn	1nnnnnn	01nnnnn	1nnnnnn	w001nnn	001nnnn	1nnnnnn	0001nnn	001nnnn	0001nnn	01nnnnn	0001nnn
	6	0001nnn	01nnnnn	001nnnn	01nnnnn	0001nnn	01nnnnn	001nnnn	01nnnnn	0001nnn	0001nnn	01nnnnn	0001nnn	001nnnn	0001nnn	001nnnn	0001nnn
	5	0000111n	001nnnn	0001nnn	001nnnn	0000111n	001nnnn	0001nnn	001nnnn	0000111n	0000111n	001nnnn	0000111n	0001nnn	0000111n	0001nnn	0000111n
	4	000001n	0001nnn	0000111n	0001nnn	000001n	0001nnn	0000111n	0001nnn	000001n	000001n	0001nnn	000001n	0000111n	000001n	0000111n	000001n
	3	0000001	000011nn	000001nn	000011nn	0000001	000011nn	000001nn	000011nn	0000001	0000001	000011nn	0000001	000001nn	0000001	000001nn	0000001
	2	0000000	0000111n	0000001n	0000111n	0000000	0000111n	0000001n	0000111n	0000000	0000000	0000111n	0000000	0000001n	0000000	0000001n	0000000
	1	0000000	0000001	0000000	0000001	0000000	0000001	0000000	0000001	0000000	0000000	0000001	0000000	0000000	0000000	0000000	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y10$	7	01nnnnn	1nnnnnn	01nnnnn	1nnnnnn	001nnnn	1nnnnnn	01nnnnn	1nnnnnn	001nnnn	001nnnn	1nnnnnn	001nnnn	001nnnn	001nnnn	01nnnnn	001nnnn
	6	001nnnn	01nnnnn	001nnnn	01nnnnn	001nnnn	01nnnnn	001nnnn	01nnnnn	001nnnn	001nnnn	01nnnnn	001nnnn	001nnnn	001nnnn	001nnnn	001nnnn
	5	0001nnn	001nnnn	0001nnn	001nnnn	0001nnn	001nnnn	0001nnn	001nnnn	0001nnn	0001nnn	001nnnn	0001nnn	0001nnn	0001nnn	0001nnn	0001nnn
	4	0000111n	0001nnn	0000111n	0001nnn	0000111n	0001nnn	0000111n	0001nnn	0000111n	0000111n	0001nnn	0000111n	0000111n	0000111n	0000111n	0000111n
	3	0000001	000011nn	000001nn	000011nn	0000001	000011nn	000001nn	000011nn	0000001	0000001	000011nn	0000001	000001nn	0000001	000001nn	0000001
	2	0000000	0000111n	0000001n	0000111n	0000000	0000111n	0000001n	0000111n	0000000	0000000	0000111n	0000000	0000001n	0000000	0000001n	0000000
	1	0000000	0000001	0000000	0000001	0000000	0000001	0000000	0000001	0000000	0000000	0000001	0000000	0000000	0000000	0000000	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y11$	7	1nnnnnn	0000111n	0000001n	0000111n	0001nnn	0000111n	0000001n	0000111n	0001nnn	0001nnn	0000111n	0001nnn	0000001n	0001nnn	0000001n	0001nnn
	6	01nnnnn	000001n	0000001	000001n	0001nnn	000001n	0000001	000001n	0001nnn	0001nnn	000001n	0001nnn	0000001	0001nnn	0000001	0001nnn
	5	001nnnn	0000001	0000000	0000001	0001nnn	0000001	0000000	0000001	0001nnn	0001nnn	0000001	0001nnn	0000000	0001nnn	0000000	0001nnn
	4	0001nnn	0000000	0000000	0000000	0001nnn	0000000	0000000	0000000	0001nnn	0001nnn	0000000	0001nnn	0000000	0001nnn	0000000	0001nnn
	3	0000111	0000000	0000000	0000000	0000111	0000000	0000000	0000000	0000111	0000111	0000000	0000111	0000000	0000111	0000000	0000111
	2	0000001	0000000	0000000	0000000	0000001	0000000	0000000	0000000	0000001	0000001	0000000	0000001	0000000	0000001	0000000	0000001
	1	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y12$	7	1nnnnnn	0001nnn	1nnnnnn	0001nnn	001nnnn	1nnnnnn	0001nnn	1nnnnnn	0001nnn	0001nnn	1nnnnnn	0001nnn	001nnnn	0001nnn	001nnnn	0001nnn
	6	01nnnnn	0000111n	01nnnnn	0000111n	001nnnn	01nnnnn	0000111n	01nnnnn	0000111n	0000111n	01nnnnn	0000111n	001nnnn	0000111n	001nnnn	0000111n
	5	001nnnn	000001n	001nnnn	000001n	0001nnn	001nnnn	000001n	001nnnn	000001n	000001n	001nnnn	000001n	0001nnn	000001n	0001nnn	000001n
	4	0001nnn	0000001	0001nnn	0000001	0001nnn	0001nnn	0000001	0001nnn	0000001	0000001	0001nnn	0000001	0001nnn	0000001	0001nnn	0000001
	3	0000111	0000000	0000111	0000000	0000111	0000111	0000000	0000111	0000000	0000000	0000111	0000000	0000111	0000000	0000111	0000000
	2	0000001	0000000	0000001	0000000	0000001	0000001	0000000	0000001	0000000	0000000	0000001	0000000	0000001	0000000	0000001	0000000
	1	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y13$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y14$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y15$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y16$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000

*Y*17	7	0001nnnn	1nnnnnnn	001nnnnn	1nnnnnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	001nnnnn	1nnnnnnn	001nnnnn	1nnnnnnn	001nnnnn	1nnnnnnn	001nnnnn	1nnnnnnn
	6	00001nnn	01nnnnnn	0001nnnn	01nnnnnn	001nnnnn	00001nnn	001nnnnn	00001nnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn
	5	00000 1n	001nnnnn	00001nnn	001nnnnn	0001nnnn	000001nn	0001nnnn	000001nn	00001nnn	001nnnnn	00001nnn	001nnnnn	00001nnn	001nnnnn	00001nnn	001nnnnn
	4	00000001	0001nnnn	000001nn	0001nnnn	00001nnn	0000001n	00001nnn	0000001n	000001nn	0001nnnn	000001nn	0001nnnn	000001nn	0001nnnn	000001nn	0001nnnn
	3	00000000	00001nnn	0000001n	00001nnn	000001nn	00000001	000001nn	00000001	0000001n	00001nnn	0000001n	00001nnn	0000001n	00001nnn	0000001n	00001nnn
	2	00000000	00000 1n	00000001	000001nn	0000001n	00000000	0000001n	00000000	00000001	000001nn	00000001	000001nn	00000001	000001nn	00000001	000001nn
	1	00000000	00000001	00000000	0000001n	00000001	00000000	00000001	00000000	00000000	0000001n	00000000	0000001n	00000000	0000001n	00000000	0000001n
	0	00000000	00000000	00000000	00000001	00000000	00000000	00000000	00000000	00000000	00000001	00000000	00000001	00000000	00000001	00000000	00000001
*Y*18	7	001nnnnn	1nnnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn
	6	0001nnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn	00001nnn	001nnnnn	00001nnn	001nnnnn	00001nnn	001nnnnn	00001nnn	001nnnnn
	5	00001nnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn	00001nnn	0001nnnn	00001nnn	000001nn	0001nnnn	000001nn	0001nnnn	000001nn	0001nnnn	000001nn	0001nnnn
	4	00000 1n	0001nnnn	00001nnn	0001nnnn	00001nnn	000001nn	00001nnn	000001nn	0000001n	00001nnn	0000001n	00001nnn	0000001n	00001nnn	0000001n	00001nnn
	3	00000001	00001nnn	000001nn	00001nnn	000001nn	0000001n	000001nn	0000001n	00000001	000001nn	00000001	000001nn	00000001	000001nn	00000001	000001nn
	2	00000000	00000 1n	0000001n	000001nn	0000001n	00000001	0000001n	00000001	00000000	0000001n	00000000	0000001n	00000000	0000001n	00000000	0000001n
	1	00000000	00000001	00000001	0000001n	00000001	00000000	00000001	00000000	00000000	00000001	00000000	00000001	00000000	00000001	00000000	00000001
	0	00000000	00000000	00000000	00000001	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
*Y*19	7	001nnnnn	1nnnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn
	6	0001nnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn	00001nnn	001nnnnn	00001nnn	001nnnnn	00001nnn	001nnnnn	00001nnn	001nnnnn
	5	00001nnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn	00001nnn	0001nnnn	00001nnn	000001nn	0001nnnn	000001nn	0001nnnn	000001nn	0001nnnn	000001nn	0001nnnn
	4	00000 1n	0001nnnn	00001nnn	0001nnnn	00001nnn	000001nn	00001nnn	000001nn	0000001n	00001nnn	0000001n	00001nnn	0000001n	00001nnn	0000001n	00001nnn
	3	00000001	00001nnn	000001nn	00001nnn	000001nn	0000001n	000001nn	0000001n	00000001	000001nn	00000001	000001nn	00000001	000001nn	00000001	000001nn
	2	00000000	00000 1n	0000001n	000001nn	0000001n	00000001	0000001n	00000001	00000000	0000001n	00000000	0000001n	00000000	0000001n	00000000	0000001n
	1	00000000	00000001	00000001	0000001n	00000001	00000000	00000001	00000000	00000000	00000001	00000000	00000001	00000000	00000001	00000000	00000001
	0	00000000	00000000	00000000	00000001	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
*Y*2 0	7	01nnnnnn	1nnnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	01nnnnnn
	6	001nnnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn	00001nnn	001nnnnn	00001nnn	001nnnnn	00001nnn	001nnnnn	00001nnn	001nnnnn
	5	0001nnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn	00001nnn	0001nnnn	00001nnn	000001nn	0001nnnn	000001nn	0001nnnn	000001nn	0001nnnn	000001nn	0001nnnn
	4	00001nnn	0001nnnn	00001nnn	0001nnnn	00001nnn	000001nn	00001nnn	000001nn	0000001n	00001nnn	0000001n	00001nnn	0000001n	00001nnn	0000001n	00001nnn
	3	00000001	00001nnn	000001nn	00001nnn	000001nn	0000001n	000001nn	0000001n	00000001	000001nn	00000001	000001nn	00000001	000001nn	00000001	000001nn
	2	00000000	00000 1n	0000001n	000001nn	0000001n	00000001	0000001n	00000001	00000000	0000001n	00000000	0000001n	00000000	0000001n	00000000	0000001n
	1	00000000	00000001	00000001	0000001n	00000001	00000000	00000001	00000000	00000000	00000001	00000000	00000001	00000000	00000001	00000000	00000001
	0	00000000	00000000	00000000	00000001	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
*Y*21	0	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
*Y*22	0	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
*Y*23	0	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
*Y*24	0	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000

$Y25$	7	0000001n	1nnnnnnn	1nnnnnnn	0000001n	01nnnnnn	0001nnnn	001nnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	01nnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn
	6	0000001	01nnnnnn	01nnnnnn	000001nn	001nnnnn	0001nnnn	001nnnnn	001nnnnn	01nnnnnn	001nnnnn	001nnnnn	001nnnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn
	5	0000000	001nnnnn	001nnnnn	00001nnn	0001nnnn	00001nnn	0001nnnn	0001nnnn	001nnnnn	0001nnnn	0001nnnn	0001nnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn
	4	0000000	0001nnnn	0001nnnn	000001nn	001nnnnn	000001nn	00001nnn	00001nnn	0001nnnn	00001nnn	00001nnn	00001nnn	0001nnnn	00001nnn	0001nnnn	00001nnn
	3	0000000	00001nnn	00001nnn	000000 1n	0001nnnn	000000 1n	000001nn	000001nn	00001nnn	000001nn	000001nn	000001nn	00001nnn	000001nn	00001nnn	000001nn
	2	0000000	000001nn	000001nn	0000001n	00001nnn	0000001n	000000 1n	000000 1n	000001nn	0000001n	0000001n	0000001n	000001nn	0000001n	000001nn	0000001n
	1	0000000	0000001n	0000001n	0000001	000001nn	0000000	0000001n	0000001n	000000 1n	0000000	0000000	0000000	0000001n	0000000	0000001n	0000000
	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y26$	7	0000 1nn	1nnnnnnn	1nnnnnnn	0001nnnn	01nnnnnn	0001nnnn	001nnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	01nnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn
	6	000001n	01nnnnnn	01nnnnnn	0000 1nn	001nnnnn	0000 1nnn	001nnnnn	001nnnnn	01nnnnnn	001nnnnn	001nnnnn	001nnnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn
	5	0000001	001nnnnn	001nnnnn	0000 1nnn	0001nnnn	0000 1nnn	0001nnnn	0001nnnn	001nnnnn	0001nnnn	0001nnnn	0001nnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn
	4	0000000	0001nnnn	0001nnnn	0000 01n	001nnnnn	0000 01nn	00001nnn	00001nnn	0001nnnn	00001nnn	00001nnn	00001nnn	0001nnnn	00001nnn	0001nnnn	00001nnn
	3	0000000	00001nnn	00001nnn	0000 001n	0001nnnn	0000 001n	000001nn	000001nn	00001nnn	000001nn	000001nn	000001nn	00001nnn	000001nn	00001nnn	000001nn
	2	0000000	000001nn	000001nn	0000 0001	00001nnn	0000 0001	000000 1n	000000 1n	000001nn	0000001n	0000001n	0000001n	000001nn	0000001n	000001nn	0000001n
	1	0000000	0000001n	0000001n	0000 0000	000001nn	0000 0000	0000001n	0000001n	000000 1n	0000000	0000000	0000000	0000001n	0000000	0000001n	0000000
	0	0000000	0000000	0000000	0000 0000	0000000	0000 0000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y27$	7	01nnnnnn	1nnnnnnn	01nnnnnn	0001nnnn	01nnnnnn	0001nnnn	001nnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	01nnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn
	6	001nnnnn	01nnnnnn	001nnnnn	0000 1nnn	001nnnnn	0000 1nnn	0001nnnn	0001nnnn	001nnnnn	0001nnnn	0001nnnn	0001nnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn
	5	0001nnnn	001nnnnn	0001nnnn	0000 01nn	0001nnnn	0000 01nn	00001nnn	00001nnn	0001nnnn	00001nnn	00001nnn	00001nnn	0001nnnn	00001nnn	0001nnnn	00001nnn
	4	0000 1nnn	0001nnnn	00001nnn	0000 001n	00001nnn	0000 001n	000001nn	000001nn	00001nnn	000001nn	000001nn	000001nn	00001nnn	000001nn	00001nnn	000001nn
	3	0000 01nn	00001nnn	000001nn	0000 0001	000001nn	0000 0001	0000001n	0000001n	000001nn	0000001n	0000001n	0000001n	000001nn	0000001n	000001nn	0000001n
	2	0000 001n	000001nn	0000001n	0000 0000	0000001n	0000 0000	0000000 1	0000000 1	0000001n	0000000 1	0000000 1	0000000 1	0000001n	0000000 1	0000001n	0000000 1
	1	0000 0001	0000001n	0000000 1	0000 0000	0000000 1	0000 0000	0000000 0	0000000 0	0000000 1	0000000 0	0000000 0	0000000 0	0000000 1	0000000 0	0000000 1	0000000 0
	0	0000 0000	0000000 0	0000000 0	0000 0000	0000000 0	0000 0000	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0
$Y28$	7	1nnnnnnn	1nnnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	0001nnnn	001nnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	01nnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn	1nnnnnnn	01nnnnnn
	6	01nnnnnn	01nnnnnn	001nnnnn	01nnnnnn	001nnnnn	0000 1nnn	0001nnnn	0001nnnn	001nnnnn	0001nnnn	0001nnnn	0001nnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn
	5	001nnnnn	001nnnnn	0001nnnn	001nnnnn	0001nnnn	0000 01nn	00001nnn	00001nnn	0001nnnn	00001nnn	00001nnn	00001nnn	0001nnnn	00001nnn	0001nnnn	00001nnn
	4	0001nnnn	0001nnnn	00001nnn	0001nnnn	00001nnn	0000 001n	000001nn	000001nn	00001nnn	000001nn	000001nn	000001nn	00001nnn	000001nn	00001nnn	000001nn
	3	0000 1nnn	00001nnn	000001nn	00001nnn	000001nn	0000 0001	0000001n	0000001n	000001nn	0000001n	0000001n	0000001n	000001nn	0000001n	000001nn	0000001n
	2	0000 01nn	000001nn	0000001n	000001nn	0000001n	0000 0000	0000000 1	0000000 1	0000001n	0000000 1	0000000 1	0000000 1	0000001n	0000000 1	0000001n	0000000 1
	1	0000 001n	0000001n	0000000 1	0000001n	0000000 1	0000 0000	0000000 0	0000000 0	0000000 1	0000000 0	0000000 0	0000000 0	0000000 1	0000000 0	0000000 1	0000000 0
	0	0000 0000	0000000 0	0000000 0	0000000 0	0000000 0	0000 0000	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0	0000000 0
$Y29$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y30$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y31$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000
$Y32$	0	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000	0000000

The half round containing the nonlinear function NL and find homomorphic I/O sums for NL that have non-zero imbalance. Here the input function is homomorphic for XOR/ADD and the output function is homomorphic for ADD/XOR. Such I/O sums can be obtained by summing I/O sums for its EXP and LOG blocks. For the function EXP with the input byte U1 and output byte V1, the only homomorphic I/O sums are

$$S^{\mathrm{EXP}}_{a1,b1} = l_{a1}(\mathrm{U1}) \oplus l_{b1}(\mathrm{V1}),\ \text{for } a1 \in B^8 \backslash \{00\};\ b1 = 01.$$

The most effective ones are obtained when $(a1, b1)$ is equal to $(cd, 01)$ or $(ff, 01)$ (the imbalance being $\frac{28}{128}$) or to $(86{,}01), (bf, 01), (c0, 01)$ or $(f7{,}01)$ (the imbalance being $\frac{24}{128}$). Computing all these I/O sums for EXP, establishes the following.

Remark 1: $I\left(S^{EXP}_{01,01}\right) = I\left(S^{EXP}_{02,01}\right) = I\left(S^{EXP}_{03,01}\right) = 0$. *Furthermore, for all* $a1$ *and* $b1$ *in* B^8, *if* $a1_7 = 0$, *then* $I\left(S^{EXP}_{a1,b1}\right) = 0$.

For the function LOG with the input U2 and output V2, the only homomorphic I/O sums are

$$S^{\mathrm{LOG}}_{a2,b2} = l_{a2}(\mathrm{U2}) \oplus l_{b2}(\mathrm{V2}),\ \text{for } a2 = 01;\ b2 \in B^8 \backslash \{00\}.$$

Their imbalance is easily deduced since $I\left(S^{\mathrm{EXP}}_{a1,b1}\right) = I\left(S^{\mathrm{LOG}}_{b1,a1}\right)$.

Remark 2: *For all* $a1$ *and* $b1$ *in* B^8, *if* $b1_7 = 0$, *then* $I\left(S^{LOG}_{a1,b1}\right) = 0$.

Finally we have link I/O sums for successive half rounds.

Theorem 1: *The procedure for finding effective homomorphic I/O sums doesn't find an I/O sum with non-zero imbalance for cascade of half rounds taken in the same order as they are used in SAFER-256 and containing at least two PHT-layers.*

Proof: Let $T^{\mathrm{PHT-hr}}_{a,b}$, $T^{\mathrm{NL}}_{b,c}$ and $T^{\mathrm{PHT-hr}}_{c,d}$ be linked homomorphic half-round threefold sums with maximizing key function. If $T^{\mathrm{PHT-hr}}_{a,b}$ and $T^{\mathrm{PHT-hr}}_{c,d}$ have none zero imbalance, the 256 bit none zero masks a, b, c, d, can have a 1 only in the two least significant bits of each byte (bits of byte are numbered from 7 for the most significant bit to 0 for the least significant bit) (Lemma 1). Then $I\left(T^{\mathrm{NL}}_{b,c}\right) = 0$ since the I/O sum average key imbalance is also 0 (Remark 1) Therefore, the sum of the three half-round threefold sums has imbalance 0.
One of the most effective I/O sums is $S^{\mathrm{NL-PHT-NL}}_{a,b}$, where $a2, a10$ and $b13, b14, b31, b32$ are either cd or ff and other bytes of a and b are zero. Their imbalance is $\left(\frac{28}{128}\right)^6$, because

$$I\left(S^{\mathrm{EXP}}_{ff,01}\right) = I\left(S^{\mathrm{EXP}}_{cd,01}\right) = I\left(S^{\mathrm{LOG}}_{01,ff}\right) = I\left(S^{\mathrm{LOG}}_{01,cd}\right) = \frac{28}{128}$$

and because

$I\left(S^{\mathrm{PHT}}_{a,b}\right) = I\left(S^{\mathrm{PHT}}_{a1\oplus a2\oplus a3\oplus a4,b1\oplus b2\oplus b3\oplus b4}\right) = I\left(S^{\mathrm{PHT}}_{a1,b1}\right) \cdot I\left(S^{\mathrm{PHT}}_{a2,b2}\right) = I\left(S^{\mathrm{PHT}}_{a3,b3}\right) = I\left(S^{\mathrm{PHT}}_{a4,b4}\right) = 1$, if

$a1 \oplus a2 \oplus a3 \oplus a4 =$
(01 00 00 01 00 00 00 01 00 00 00 00 00 00 00 00 00 00 01 01 00 00 01 00 00 00 00 01 00 00 01)⊕
(01 01 00 01 00 01 01 01 00 00 00 00 00 01 01 00 00 00 00 01 01 00 00 01 00 00 00 00 01 00 00 01) ⊕
(00 00 00 00 00 00 00 00 01 00 00 01 00 00 00 01 00 00 00 00 01 00 00 01 00 00 00 01 01 00 00 01) ⊕
(00 00 00 00 00 01 01 00 01 01 00 01 00 01 01 01 00 00 00 00 01 00 00 01 00 00 00 01

$01\ 00\ 00\ 01) =$
$(00\ 01\ 00\ 00\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$00\ 00\ 00\ 00) = a$ (hex notation),

$b1 \oplus b2 \oplus b3 \oplus b4 =$
$(00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$00\ 00\ 00\ 00) \oplus$
$(00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 01\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$00\ 00\ 00\ 00) \oplus$
$(00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$00\ 00\ 01\ 00) \oplus$
$(00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$00\ 00\ 00\ 01$
$(00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 01\ 01\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\ 00$
$00\ 00\ 01\ 01) = b$ (hex notation).

Thus, we have proved that SAFER-256 is secure against the linear cryptanalysis after only three of its suggested six rounds.

Acknowledgement

The author is thankful to Prof. Gurgen Khachatrian and Dr. Melsik Kureghyan for very useful discussions and comments.

References

[1] G. H. Khachatrian, M. K. Kyureghyan, K. M. Kyuregyan, Design and Cryptanalysis of a New Encryption Algorithm SAFER-256. Transactions of IIAP NAS RA, Mathematical Problems of Computer Science Vol. 42, pp. 97-106, 2014.

[2] H. Carlo, Cryptanalysis of iterated Block Ciphers, ETH Series In Information Processing (Ed Massey), v. 7, Konstanz: Hartung-Gorre Verlag, 1996.

Submitted 05.11.2016, accepted 03.02.2016

SAFER-256 համակարգի գծային վերլուծությունը

Ք.Կյուրեղյան

Ամփոփում

Այս հոդվածում ներկայացված է 256 բիթ բլոկի երկարության SAFER-256 բլոկային ծածկագրական համակարգի գծային վերլուծությունը, որը դիֆերենցիալ վերլուծության նկատմամբ կայուն է 5 ռաունդից հետո:

Линейнный криптоанализ алгоритма SAFER-256

К. Кюрегян

Аннотация

В данной статье представлен линейный криптоанализ блочного шифра SAFER-256, которая устойчива по отношению к дифференциальному анализу после 5 раындов.