SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Algebraic Techniques in Slender-set Differential Cryptanalysis of PRESENT-like Cipher

LIU Guo-Qiang[1,2*] & JIN Chen-Hui[2]

[1]*Department of Mathematic and System Science, College of Science, National University of Defense Technology, Changsha, Hunan* 410073*, China;*
[2]*Information Engineering University, Zhengzhou, Henan* 450000*, China*

Appendix A Description of PRESENT-like Cipher

Assuming that the block size of the PRESENT-like is nm-bit and the number of rounds is N. Each round of the cipher has three layers of operations: the key addition layer, the S-box layer and the permutation layer. However, being different from PRESENT cipher, the PRESENT-like cipher contains secret components which may be the secret S-boxes and secret permutations. In this paper, we focus on the PRESENT-like cipher with secret S-boxes, which can be described as Algorithm A1. The cipher Maya corresponds to the PRESENT-like cipher with $n = 16$ and $m = 4$.

```
Algorithm A1 $N$-rounds PRESENT-like cipher
Require: $nm$-bit plaintext $X$; main key $K$
Ensure: $nm$-bit ciphertext $C = E_K(X)$
Derive $n$ $m$-bit S-boxes $S_j$ $(0 \leqslant j \leqslant n-1)$ and round keys $K_i$ $(1 \leqslant i \leqslant N)$ from the main key $K$
$STATE = X$
for $i = 1$ to $N$ do
    Parse $STATE$ as $STATE_0||STATE_1||\cdots||STATE_{n-1}$
    for $j = 0$ to $n-1$ do
        $STATE_j = S_j(STATE_j)$
    end for
    Apply the bit permutation to $STATE$
    Add round key $K_i$ to $STATE$
end for
return
```

Appendix B Description of slender-set differential cryptanalysis

Definition 1. Given $e \in \mathbb{F}_2^m$ and $S : \mathbb{F}_2^m \rightarrow \mathbb{F}_2^m$, we denote the set of all pairs $\{x, y\}$ such that $S(x) \oplus S(y) = e$ by D_e. Here, we consider the pairs $\{x, y\}$ and $\{y, x\}$ to be identical. A pair $\{x, y\}$ belonging to a set D_e where e has Hamming weight '1' is called a *slender-pair*. A set consisting of slender-pairs is called a *slender-set*. We denote $wt_1(e)$ as the Hamming weight of e.

It holds that there are m slender-sets and $|D_e| = 2^{m-1}$ for each $e \neq 0$ according to Definition 1. We focus on the PRESENT-like cipher Maya. The block size is $nm = 64$ and the size of S-box is $m = 4$ in cipher Maya. Without loss of generality, we explain how to recover the leftmost 4-bit secret S-box. In order to determine the slender-sets, we encrypt a certain number of plaintexts P_{r_i} with the form of $P_{r_i} = \{(x||r_i) : x \in \mathbb{F}_2^4\}$, where each $r_i \in \mathbb{F}_2^{60}$ is chosen randomly. The different plaintexts $(x||r_i)$, $(y||r_i)$ in the set P_{r_i} is the right pair arising the input difference with the form of $(x||r_i) \oplus (y||r_i) = (?||0^{60})$. And the output difference after leftmost secret S-box S in the first S-box layer is $S(x) \oplus S(y) = e$. We denote $p(\{x, y\})$ as the probability of which only one S-box is active in the ciphertext difference when the plaintext pair is $\{x||r_i, y||r_i\}$. As

[*] Corresponding author (email: liuguoqiang87@hotmail.com)

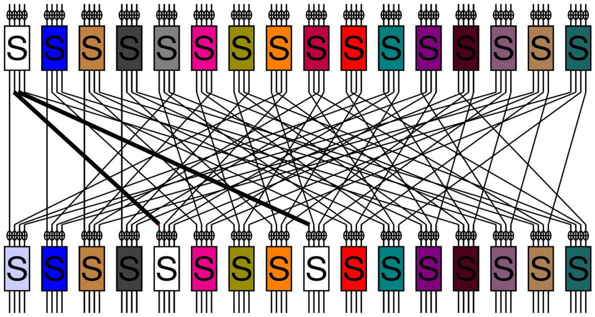

Figure B1 The differential path with weight two

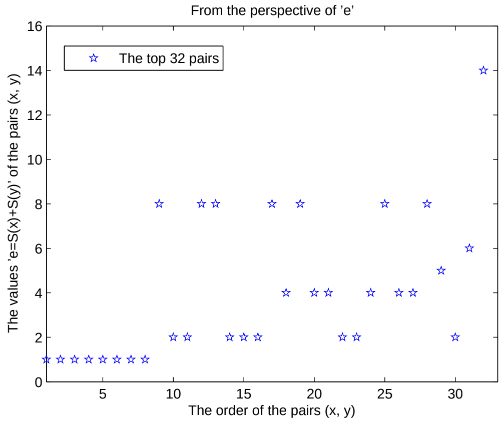

Figure B2 The candidate slender-set from the perspective of the value e.

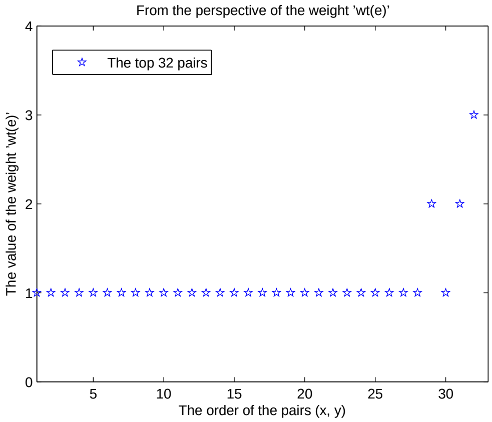

Figure B3 The candidate slender-set from the perspective of the value $wt(e)$.

mentioned above, the weight of the output difference $S(x) \oplus S(y) = e$ will determine the number of active S-boxes in the second round. Thus the probability $p(\{x, y\})$ is determined by the pairs $\{x||r_i, y||r_i\}$. Hence, given $S(x) \oplus S(y) = e$, we can denote this probability $p_e = p(\{x, y\})$. The lower weight output difference $S(x) \oplus S(y) = e$ will cause active S-boxes in the next round. The Borghoff's method is based on the following two assumptions.

Assumption 1. The probability $p(\{x, y\})$ only depends on the value of $S(x) \oplus S(y)$, not on the pair $\{x, y\}$ specifically. Hence, given $S(x) \oplus S(y) = e$, we can denote this probability $p_e = p(\{x, y\})$.

Assumption 2. The probability p_e is higher when e has Hamming weight 1, than when e has Hamming weight greater than 1.

Borghoff *et al.* estimated the probabilities p_e by the counter described as follows:

$$C(\{x, y\}) = \#\{r_i : \exists j, s.t. E(x||r_i) \oplus E(y||r_i) = 0^{4j}||?||0^{60-4j}\}$$

where $r_i \in \mathbb{F}_2^{60}$ is chosen randomly and $0 \leqslant j \leqslant 15$. For every pair $\{x, y\}$, $0 \leqslant x \neq y \leqslant 15$, there are $C_{16}^2 = 120$ counters totally. After encrypting enough number of plaintexts with the form of $(x||r_i)$, $(y||r_i)$, we sort the counters $C(\{x, y\})$ in descending order. Then we can partition the 120 pairs $\{x, y\}$ into several sets up to the descending order of the counters. The top four sets (contain 32 pairs) can be treated as the slender-sets. For the 16-round Maya, we give an example in the data collection phase by using Liu's improving method with 2^{28} data complexity (see Table B1). One can see that the first 8 pairs in the descending order is the correct slender-set from the perspective of the value $S(x) \oplus S(y) = e$. And the second to fourth slender-set consist of the remaining pairs are incorrect (see Figure B2). More correct slender-sets require higher data complexity. In order to reduce the data complexity, Liu *et al.* pointed out that they can swap the elements in the incorrect pairs properly to construct the correct slender-sets by a pruning search algorithm. However, we note that the values of the weight $wt(e)$ corresponding to the top 32 pairs in the descending order are almost equal to weight one using the same data complexity (see Figure B3). In this paper, we consider recovering the 4-bit secret S-box by algebraic techniques directly instead of dividing the slender-sets into four partitions accurately.

Table B1 The top 32 pairs in the descending order with 2^{28} data complexity

$\{x,y\}$	Order	e	$wt(e)$	$\{x,y\}$	Order	e	$wt(e)$
{5,14}	10.87	(1)	$< 1 >$	{0,12}	3.58	(8)	$< 1 >$
{6,12}	10.78	(1)	$< 1 >$	{0,2}	3.55	(4)	$< 1 >$
{2,9}	10.41	(1)	$< 1 >$	{1,7}	3.54	(8)	$< 1 >$
{13,15}	9.83	(1)	$< 1 >$	{4,8}	3.48	(4)	$< 1 >$
{1,4}	8.07	(1)	$< 1 >$	{6,14}	3.37	(4)	$< 1 >$
{8,11}	7.30	(1)	$< 1 >$	{2,11}	3.30	(2)	$< 1 >$
{0,10}	6.63	(1)	$< 1 >$	{4,10}	3.18	(2)	$< 1 >$
{3,7}	6.43	(1)	$< 1 >$	{1,11}	3.17	(4)	$< 1 >$
{11,13}	4.41	(8)	$< 1 >$	{6,10}	3.06	(8)	$< 1 >$
{0,1}	4.23	(2)	$< 1 >$	{5,12}	3.00	(4)	$< 1 >$
{5,13}	4.21	(2)	$< 1 >$	{3,15}	3.00	(4)	$< 1 >$
{9,14}	4.05	(8)	$< 1 >$	{2,5}	2.90	(8)	$< 1 >$
{3,4}	3.91	(8)	$< 1 >$	{4,11}	2.84	(5)	$< 2 >$
{3,6}	3.90	(2)	$< 1 >$	{8,9}	2.82	(2)	$< 1 >$
{7,12}	3.88	(2)	$< 1 >$	{8,10}	2.81	(6)	$< 2 >$
{14,15}	3.66	(2)	$< 1 >$	{4,14}	2.78	(14)	$< 3 >$

Appendix C Experimental results

Table C1 shows the list of one possible solution.

Table C1 The list of one possible solution for the equations system

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$s_0(x)$	0	0	1	0	0	1	0	0	1	1	0	1	0	1	1	1
$s_1(x)$	0	0	0	1	0	1	1	1	0	0	0	0	1	1	1	1
$s_2(x)$	0	1	0	1	1	0	0	1	1	0	0	1	0	1	0	1
$s_3(x)$	0	0	0	1	1	0	1	0	1	1	1	0	0	0	1	1

Table C2 shows the average data complexities and success rates of our attack.

Table C2 The average data complexity to 9-16 rounds PRESENT-like with randomly chosen secret S-boxes in this paper

Round	9	10	11	12	13	14	15	16
Data complexity	$2^{12.5}$	2^{16}	2^{18}	$2^{20.5}$	2^{22}	$2^{24.2}$	$2^{25.8}$	2^{28}
Success rate	100%	100%	100%	100%	100%	100%	100%	100%

Table C3 The 184 equations for recovering secret S-box

$x[6] \oplus x[15] \oplus x[22] \oplus x[31] \oplus x[38] \oplus x[47] \oplus x[54] \oplus x[63] = 1;$
$(x[6] \oplus x[15]) \ast (x[22] \oplus x[31]) \oplus (x[38] \oplus x[47]) \ast (x[54] \oplus x[63]) = 0;$
$x[7] \oplus x[13] \oplus x[23] \oplus x[29] \oplus x[39] \oplus x[45] \oplus x[55] \oplus x[61] = 1;$
$(x[7] \oplus x[13]) \ast (x[23] \oplus x[29]) \oplus (x[39] \oplus x[45]) \ast (x[55] \oplus x[61]) = 0;$
$x[3] \oplus x[10] \oplus x[19] \oplus x[26] \oplus x[35] \oplus x[42] \oplus x[51] \oplus x[58] = 1;$
$(x[3] \oplus x[10]) \ast (x[19] \oplus x[26]) \oplus (x[35] \oplus x[42]) \ast (x[51] \oplus x[58]) = 0;$
$x[14] \oplus x[16] \oplus x[30] \oplus x[32] \oplus x[46] \oplus x[48] \oplus x[62] \oplus x[64] = 1;$
$(x[14] \oplus x[16]) \ast (x[30] \oplus x[32]) \oplus (x[46] \oplus x[48]) \ast (x[62] \oplus x[64]) = 0;$
$x[2] \oplus x[5] \oplus x[18] \oplus x[21] \oplus x[34] \oplus x[37] \oplus x[50] \oplus x[53] = 1;$
$(x[2] \oplus x[5]) \ast (x[18] \oplus x[21]) \oplus (x[34] \oplus x[37]) \ast (x[50] \oplus x[53]) = 0;$
$x[9] \oplus x[12] \oplus x[25] \oplus x[28] \oplus x[41] \oplus x[44] \oplus x[57] \oplus x[60] = 1;$
$(x[9] \oplus x[12]) \ast (x[25] \oplus x[28]) \oplus (x[41] \oplus x[44]) \ast (x[57] \oplus x[60]) = 0;$
$x[1] \oplus x[11] \oplus x[17] \oplus x[27] \oplus x[33] \oplus x[43] \oplus x[49] \oplus x[59] = 1;$
$(x[1] \oplus x[11]) \ast (x[17] \oplus x[27]) \oplus (x[33] \oplus x[43]) \ast (x[49] \oplus x[59]) = 0;$
$x[4] \oplus x[8] \oplus x[20] \oplus x[24] \oplus x[36] \oplus x[40] \oplus x[52] \oplus x[56] = 1;$
$(x[4] \oplus x[8]) \ast (x[20] \oplus x[24]) \oplus (x[36] \oplus x[40]) \ast (x[52] \oplus x[56]) = 0;$
$x[12] \oplus x[14] \oplus x[28] \oplus x[30] \oplus x[44] \oplus x[46] \oplus x[60] \oplus x[62] = 1;$
$(x[12] \oplus x[14]) \ast (x[28] \oplus x[30]) \oplus (x[44] \oplus x[46]) \ast (x[60] \oplus x[62]) = 0;$
$x[1] \oplus x[2] \oplus x[17] \oplus x[18] \oplus x[33] \oplus x[34] \oplus x[49] \oplus x[50] = 1;$
$(x[1] \oplus x[2]) \ast (x[17] \oplus x[18]) \oplus (x[33] \oplus x[34]) \ast (x[49] \oplus x[50]) = 0;$
$x[6] \oplus x[14] \oplus x[22] \oplus x[30] \oplus x[38] \oplus x[46] \oplus x[54] \oplus x[62] = 1;$
$(x[6] \oplus x[14]) \ast (x[22] \oplus x[30]) \oplus (x[38] \oplus x[46]) \ast (x[54] \oplus x[62]) = 0;$
$x[10] \oplus x[15] \oplus x[26] \oplus x[31] \oplus x[42] \oplus x[47] \oplus x[58] \oplus x[63] = 1;$
$(x[10] \oplus x[15]) \ast (x[26] \oplus x[31]) \oplus (x[42] \oplus x[47]) \ast (x[58] \oplus x[63]) = 0;$
$x[4] \oplus x[5] \oplus x[20] \oplus x[21] \oplus x[36] \oplus x[37] \oplus x[52] \oplus x[53] = 1;$
$(x[4] \oplus x[5]) \ast (x[20] \oplus x[21]) \oplus (x[36] \oplus x[37]) \ast (x[52] \oplus x[53]) = 0;$
$x[4] \oplus x[7] \oplus x[20] \oplus x[23] \oplus x[36] \oplus x[39] \oplus x[52] \oplus x[55] = 1;$
$(x[4] \oplus x[7]) \ast (x[20] \oplus x[23]) \oplus (x[36] \oplus x[39]) \ast (x[52] \oplus x[55]) = 0;$
$x[8] \oplus x[13] \oplus x[24] \oplus x[29] \oplus x[40] \oplus x[45] \oplus x[56] \oplus x[61] = 1;$
$(x[8] \oplus x[13]) \ast (x[24] \oplus x[29]) \oplus (x[40] \oplus x[45]) \ast (x[56] \oplus x[61]) = 0;$
$x[15] \oplus x[16] \oplus x[31] \oplus x[32] \oplus x[47] \oplus x[48] \oplus x[63] \oplus x[64] = 1;$
$(x[15] \oplus x[16]) \ast (x[31] \oplus x[32]) \oplus (x[47] \oplus x[48]) \ast (x[63] \oplus x[64]) = 0;$
$x[1] \oplus x[13] \oplus x[17] \oplus x[29] \oplus x[33] \oplus x[45] \oplus x[49] \oplus x[61] = 1;$
$(x[1] \oplus x[13]) \ast (x[17] \oplus x[29]) \oplus (x[33] \oplus x[45]) \ast (x[49] \oplus x[61]) = 0;$
$x[1] \oplus x[3] \oplus x[17] \oplus x[19] \oplus x[33] \oplus x[35] \oplus x[49] \oplus x[51] = 1;$
$(x[1] \oplus x[3]) \ast (x[17] \oplus x[19]) \oplus (x[33] \oplus x[35]) \ast (x[49] \oplus x[51]) = 0;$
$x[2] \oplus x[8] \oplus x[18] \oplus x[24] \oplus x[34] \oplus x[40] \oplus x[50] \oplus x[56] = 1;$
$(x[2] \oplus x[8]) \ast (x[18] \oplus x[24]) \oplus (x[34] \oplus x[40]) \ast (x[50] \oplus x[56]) = 0;$
$x[5] \oplus x[9] \oplus x[21] \oplus x[25] \oplus x[37] \oplus x[41] \oplus x[53] \oplus x[57] = 1;$
$(x[5] \oplus x[9]) \ast (x[21] \oplus x[25]) \oplus (x[37] \oplus x[41]) \ast (x[53] \oplus x[57]) = 0;$
$x[7] \oplus x[15] \oplus x[23] \oplus x[31] \oplus x[39] \oplus x[47] \oplus x[55] \oplus x[63] = 1;$
$(x[7] \oplus x[15]) \ast (x[23] \oplus x[31]) \oplus (x[39] \oplus x[47]) \ast (x[55] \oplus x[63]) = 0;$
$x[3] \oplus x[12] \oplus x[19] \oplus x[28] \oplus x[35] \oplus x[44] \oplus x[51] \oplus x[60] = 1;$
$(x[3] \oplus x[12]) \ast (x[19] \oplus x[28]) \oplus (x[35] \oplus x[44]) \ast (x[51] \oplus x[60]) = 0;$
$x[5] \oplus x[11] \oplus x[21] \oplus x[27] \oplus x[37] \oplus x[43] \oplus x[53] \oplus x[59] = 1;$
$(x[5] \oplus x[11]) \ast (x[21] \oplus x[27]) \oplus (x[37] \oplus x[43]) \ast (x[53] \oplus x[59]) = 0;$
$x[2] \oplus x[12] \oplus x[18] \oplus x[28] \oplus x[34] \oplus x[44] \oplus x[50] \oplus x[60] = 1;$
$(x[2] \oplus x[12]) \ast (x[18] \oplus x[28]) \oplus (x[34] \oplus x[44]) \ast (x[50] \oplus x[60]) = 0;$
$x[7] \oplus x[11] \oplus x[23] \oplus x[27] \oplus x[39] \oplus x[43] \oplus x[55] \oplus x[59] = 1;$
$(x[7] \oplus x[11]) \ast (x[23] \oplus x[27]) \oplus (x[39] \oplus x[43]) \ast (x[55] \oplus x[59]) = 0;$
$x[6] \oplus x[13] \oplus x[22] \oplus x[29] \oplus x[38] \oplus x[45] \oplus x[54] \oplus x[61] = 1;$
$(x[6] \oplus x[13]) \ast (x[22] \oplus x[29]) \oplus (x[38] \oplus x[45]) \ast (x[54] \oplus x[61]) = 0;$
$x[4] \oplus x[16] \oplus x[20] \oplus x[32] \oplus x[36] \oplus x[48] \oplus x[52] \oplus x[64] = 1;$
$(x[4] \oplus x[16]) \ast (x[20] \oplus x[32]) \oplus (x[36] \oplus x[48]) \ast (x[52] \oplus x[64]) = 0;$
$x[3] \oplus x[6] \oplus x[19] \oplus x[22] \oplus x[35] \oplus x[38] \oplus x[51] \oplus x[54] = 1;$
$(x[3] \oplus x[6]) \ast (x[19] \oplus x[22]) \oplus (x[35] \oplus x[38]) \ast (x[51] \oplus x[54]) = 0;$
$x[9] \oplus x[16] \oplus x[25] \oplus x[32] \oplus x[41] \oplus x[48] \oplus x[57] \oplus x[64] = 1;$
$(x[9] \oplus x[16]) \ast (x[25] \oplus x[32]) \oplus (x[41] \oplus x[48]) \ast (x[57] \oplus x[64]) = 0;$
$x[9] \oplus x[10] \oplus x[25] \oplus x[26] \oplus x[41] \oplus x[42] \oplus x[57] \oplus x[58] = 1;$
$(x[9] \oplus x[10]) \ast (x[25] \oplus x[26]) \oplus (x[41] \oplus x[42]) \ast (x[57] \oplus x[58]) = 0;$
$x[8] \oplus x[14] \oplus x[24] \oplus x[30] \oplus x[40] \oplus x[46] \oplus x[56] \oplus x[62] = 1;$
$(x[8] \oplus x[14]) \ast (x[24] \oplus x[30]) \oplus (x[40] \oplus x[46]) \ast (x[56] \oplus x[62]) = 0;$
$x[10] \oplus x[11] \oplus x[26] \oplus x[27] \oplus x[42] \oplus x[43] \oplus x[58] \oplus x[59] = 1;$
$(x[10] \oplus x[11]) \ast (x[26] \oplus x[27]) \oplus (x[42] \oplus x[43]) \ast (x[58] \oplus x[59]) = 0;$
$(x[1] \oplus x[2] \oplus 1) \ast (x[17] \oplus x[18] \oplus 1) \ast (x[33] \oplus x[34] \oplus 1) \ast (x[49] \oplus x[50] \oplus 1) = 0;$
$(x[1] \oplus x[3] \oplus 1) \ast (x[17] \oplus x[19] \oplus 1) \ast (x[33] \oplus x[35] \oplus 1) \ast (x[49] \oplus x[51] \oplus 1) = 0;$
$(x[1] \oplus x[4] \oplus 1) \ast (x[17] \oplus x[20] \oplus 1) \ast (x[33] \oplus x[36] \oplus 1) \ast (x[49] \oplus x[52] \oplus 1) = 0;$
$\vdots$
$(x[14] + x[16] + 1) \ast (x[30] + x[32] + 1) \ast (x[46] + x[48] + 1) \ast (x[62] + x[64] + 1) = 0;$
$(x[15] + x[16] + 1) \ast (x[31] + x[32] + 1) \ast (x[47] + x[48] + 1) \ast (x[63] + x[64] + 1) = 0.$