Weak Keys of Reduced-Round PRESENT for Linear Cryptanalysis

Kenji Ohkuma[1,2]

[1] Corporate R & D Center, Toshiba Corporation
[2] IT Security Center, Information-technology Promotion Agency, Japan

Abstract. The block cipher PRESENT designed as an ultra-light weight cipher has a 31-round SPN structure in which the S-box layer has 16-parallel 4-bit S-boxes and the diffusion layer is a bit permutation. The designers claimed that the maximum linear characteristic deviation is not more than 2^{-43} for 28 rounds and concluded that PRESENT is not vulnerable to linear cryptanalysis. But we have found that 32% of PRESENT keys are weak for linear cryptanalysis, and the linear deviation can be much larger than the linear characteristic value by the multi-path effect. And we discovered a 28-round path with a linear deviation of $2^{-39.3}$ for the weak keys. Furthermore, we found that linear cryptanalysis can be used to attack up to 24 rounds of PRESENT for the weak keys.

1 Introduction

The block cipher PRESENT designed as an ultra-light weight cipher has a 31-round SPN structure in which the S-box layer has 16-parallel 4-bit S-boxes and the diffusion layer is a bit permutation. The data randomizing part has a 31-round SPN structure of 64-bit block size, where each round consists of a key addition layer (addKeyLayer), an S-box layer (sBoxLayer) with 16 parallel 4-bit S-boxes, and a bit permutation layer (pLayer) as shown in Figure 1. Two key lengths, 80 bits and 128 bits, are supported. We consider 80-bit key in this paper.

PRESENT is similar to AES in structure, as the S-box layer consists of 16 S-boxes and each S-box is connected to 4 S-boxes in the next round. But there is a big difference in design philosophy between the two ciphers. The MDS matrices in AES's mixColumn operations are based on the wide-trail strategy, and there are 25 or more active S-boxes in 4 successive rounds for both linear and differential cryptanalyses. On the contrary, PRESENT's pLayer only permutes the order of bits and the trail can be very narrow. As a matter of fact, we can easily find a linear path with only one active S-box per round. We call such a path a single-bit path.

There are some security evaluations of PRESENT. The designers insist that the differential characteristic is upper-bounded by $2^{-100} (< 2^{-64})$ for 25 rounds, and that the absolute value of linear characteristic deviation are upper-bounded by $2^{-43} (< 2^{-32})$ for 28 rounds [1]. These evaluations are very loose, and do not show how many rounds are vulnerable to attack.

M.J. Jacobson Jr., V. Rijmen, and R. Safavi-Naini (Eds.): SAC 2009, LNCS 5867, pp. 249–265, 2009.

M.R. Z'aba et al. applied an integral attack for bit-patterns, and showed that 7-round PRESENT can be attacked [7]. M. Wang demonstrates 16-round PRESENT can be attacked by differential cryptanalysis [6]. M. Albrecht and C. Cid applied the differential cryptanalysis strengthened by algebraic techniques, and found 16-round PRESENT can be attacked [8]. B. Collard and F.-X. Standaert applied a statistical saturation attack which works up to 24 rounds in theory [**?**].

The designers evaluated the resistance of PRESENT against linear cryptanalysis by using linear characteristic deviation [1]. But, the absolute value of linear deviation can be much larger than is that of linear characteristic deviation as T. Shimoyama et al. showed for RC6 in FSE 2002 [5]. In fact, we found that PRESENT has many linear single-bit paths with the same input/output masks for 4 or more rounds, and that the linear deviation can be very large for some portion of keys, which we call weak keys. We show that 24-round reduced round PRESENT can be cryptanalysed with $2^{63.5}$ known plaintexts for 32% of the 80-bit keys.

The construction of this paper is as follows. Section 2 describes the structure of PRESENT and some notations. In Section 3, some properties of linear single-bit paths are analyzed. In Section 4, reduced round PRESENTs are attacked with linear cryptanalysis. Section 5 is devoted to concluding remarks.

2 Description of PRESENT Encryption

Fig. 1 shows the structure of encryption for PRESENT. The data radomizing part consists of 31 iterations of key addition (addRoundKey), S-box layer (sBoxLayer), bit permutation (pLayer) followed by the final addRoundKey.

sBoxLayer consists of 16 parallel 4-bit S-boxes described in Table 1.

pLayer permutates the output bits of sBoxLayer. When the rightmost bit is 0-th and the leftmost bit is 63rd, the ℓ-th bit moves to $P(\ell)$-th where P is given by the following equation.

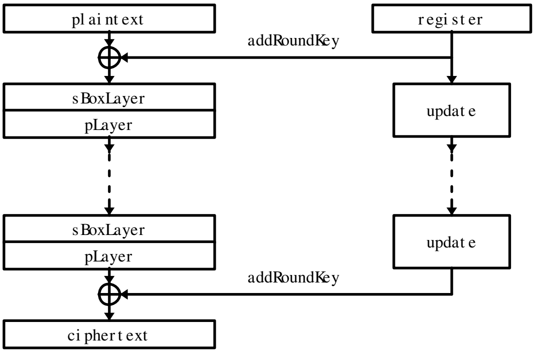

Fig. 1. Structure of PRESENT

Table 1. S-box

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
$S[x]$	C	5	6	B	9	0	A	D	3	E	F	8	4	7	1	2

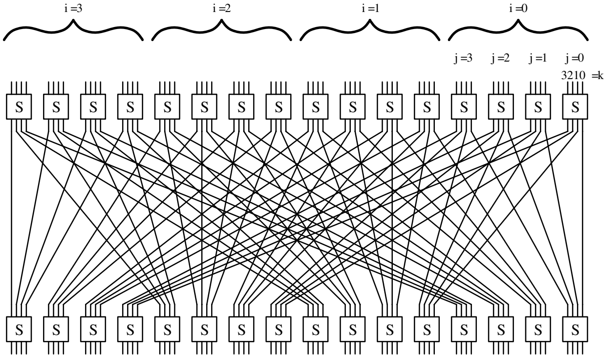

Fig. 2. Round structure

$$P(16*i+4*j+k) = 16*k+4*i+j, \qquad 0 \le i,j,k \le 3 \tag{1}$$

Successive sBoxLayers connected by pLayer are shown in Fig. 2. Here, addRoundKeys just before sBoxLayer is not shown for simplicity.

As we focus on linear single-bit paths where only one bit is active in all masks, we represent the location of a bit using i, j, k as in Equation 1. The ℓ-th key bit in the r-th round[1] is denoted $k^{(r)}_{i,j,k}$, and the bit just before is denoted $x^{(r)}_{i,j,k}$. Therefore, the ℓ-th bit of the plaintext is $x^{(0)}_{i,j,k}$ and the ℓ-th bit of the ciphertext is $x^{(31)}_{i,j,k}$. A variable without the 3rd subscript k, such as $x^{(0)}_{i,j}$ means a 4-bit set for the $4*i+j$-th S-box.

The key schedule of PRESENT for an 80-bit key is as follows. 80-bit key variables for the r-th round($0 \le r \le 31$) is denoted $\kappa^{(r)}_{79}\kappa^{(r)}_{78}\dots\kappa^{(r)}_{0}$. The encryption key is used as $\kappa^{(0)}(r=0)$, and its leftmost 64 bits are used as the 1st round key. The 80-bit key variable is updated 31 times according to the following steps, and its leftmost 64 bits are used as each round key.

$$k^{(r)}_{63} \mid k^{(r)}_{62} \mid \dots \mid k^{(r)}_{0} = \kappa^{(r)}_{79} \mid \kappa^{(r)}_{78} \mid \dots \mid \kappa^{(r)}_{16}$$

After a 19-bit right rotation, the leftmost 4 bits are transformed by an S-box, and 5 bits from the 15-th to the 19-th positions are XORed with a counter value.

$$\kappa'^{(r)}_{79}\kappa'^{(r)}_{78}\dots\kappa'^{(r)}_{0}$$

$$\kappa'^{(r)}_{i} = \kappa^{(r)}_{i+19 (\mathrm{mod}\ 80)}$$

[1] $r = 0$ for the round key just after the plaintext.

$$\kappa_{79}^{(r+1)} \mid \kappa_{78}^{(r+1)} \mid \kappa_{77}^{(r+1)} \mid \kappa_{76}^{(r+1)} = S(\kappa_{79}^{'(r)} \mid \kappa_{78}^{'(r)} \mid \kappa_{77}^{'(r)} \mid \kappa_{76}^{'(r)})$$

$$\kappa_{19}^{(r+1)} \mid \kappa_{18}^{(r+1)} \mid \kappa_{17}^{(r+1)} \mid \kappa_{16}^{(r+1)} \mid \kappa_{15}^{(r+1)} = \kappa_{19}^{'(r)} \mid \kappa_{18}^{'(r)} \mid \kappa_{17}^{'(r)} \mid \kappa_{16}^{'(r)} \mid \kappa_{15}^{'(r)} \oplus (r+1)$$
$$\kappa_{i}^{(r+1)} = \kappa_{i}^{'(r)} \ (i \in \{0, \ldots, 14, 20, \ldots, 75\})$$

3 Single-Bit Paths

The most important part of linear cryptanalysis is to find the paths with the largest linear deviation in absolute value. And a path with fewer active S-boxes tends to have a larger absolute linear deviation. As the linear layer of PRESENT pLayer only permutes the bits, it is easy to find linear paths in which only one active S-box appears per round. Thus, we focus on paths where only one bit is active in every round.

3.1 Single-Bit Masks for S-Box

Table 2 shows the linear deviation for the S-box of PRESENT.

There are 36 masks with the largest absolute linear deviation 2^{-2}, which do not include those with only one bit active in both input and output. Figure 3 shows 8 masks with one bit active in both input and output, which have non-zero absolute linear deviation(2^{-3}). Note that the 0-th bit is never active in the figure, but all combinations of the other 3 input and output bits appear, except for the combination in which the 3rd input bit and the 2nd output bit are active.

Table 2. Linear deviation of S-box(with sign)

	input masks														
	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
1_x	0	0	0	0	0	0	0	0	$\frac{1}{4}$	0	$-\frac{1}{4}$	0	$\frac{1}{4}$	0	$\frac{1}{4}$
2_x	0	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{4}$	0	0	$\frac{1}{4}$	$\frac{1}{8}$	$-\frac{1}{8}$
3_x	0	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{4}$	$\frac{1}{4}$	$-\frac{1}{8}$	$-\frac{1}{8}$	0	0	0	0	$\frac{1}{8}$	$\frac{1}{8}$
4_x	0	$-\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	0	$\frac{1}{4}$	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{4}$	0
5_x	$-\frac{1}{4}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	0	0	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{4}$	0
6_x	0	0	$-\frac{1}{4}$	0	0	$-\frac{1}{4}$	0	$-\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$
7_x	$-\frac{1}{4}$	0	0	$\frac{1}{4}$	0	0	0	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$
8_x	0	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	0	0	$-\frac{1}{8}$	$-\frac{1}{8}$	0	$-\frac{1}{4}$	$\frac{1}{4}$	0	$-\frac{1}{8}$	$-\frac{1}{8}$
9_x	0	$-\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{4}$	$-\frac{1}{4}$	$\frac{1}{8}$	$-\frac{1}{8}$	0	0	0	0	$-\frac{1}{8}$	$\frac{1}{8}$
A_x	0	0	$-\frac{1}{4}$	0	$-\frac{1}{4}$	0	0	0	$-\frac{1}{4}$	0	0	0	0	0	$\frac{1}{4}$
B_x	0	$\frac{1}{4}$	0	$-\frac{1}{4}$	0	0	0	0	0	$-\frac{1}{4}$	0	$-\frac{1}{4}$	0	0	0
C_x	0	0	0	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$
D_x	$-\frac{1}{4}$	$\frac{1}{4}$	0	0	0	0	0	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$
E_x	0	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	0	$\frac{1}{4}$	$\frac{1}{4}$	0	$-\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	0	0
F_x	$\frac{1}{4}$	$\frac{1}{8}$	$-\frac{1}{8}$	$\frac{1}{8}$	$\frac{1}{8}$	0	0	$\frac{1}{4}$	0	$\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	$-\frac{1}{8}$	0	0

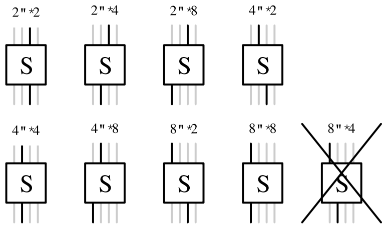

Fig. 3. Single-bit masks for S-box (absolute linear deviation: 2^{-3})

3.2 Continuable 1-Round Single-Path

As we saw in the previous subsection, S-box's single-bit masks do not contain the 0-th bit in both input and output. From this property it follows that the 1-round single-bit paths that can be included in single-bit paths with 3 or more rounds are limited to the 72 shown in Figure 4.

That is, single-bit paths with an arbitrary number of rounds can be constructed by connecting paths in Figure 4.

The above 72 masks have the property that none of i, j, k is 0 when the position of an active input or output bit is denoted (i, j, k). The reason that 0 does not appear for an active input bit can be explained as follows.

$i = 0$ *case.* Input bit $(0, j, k)$ proceeds to $(j', k', 0)$ after 2 rounds, and the single-bit path can not continue any more. That means the single-bit path can not continue to 3 or more rounds in the case of $i = 0$.

$j = 0$ *case.* Input bit $(i, 0, k)$ proceeds to $(k', i, 0)$ after 1 round, and the single-bit path can not continue any more. That means the single-bit path can not continue to 2 or more rounds in the case of $j = 0$.

$k = 0$ *case.* The active input bit is the rightmost for the S-box, and the single-bit path terminates here.

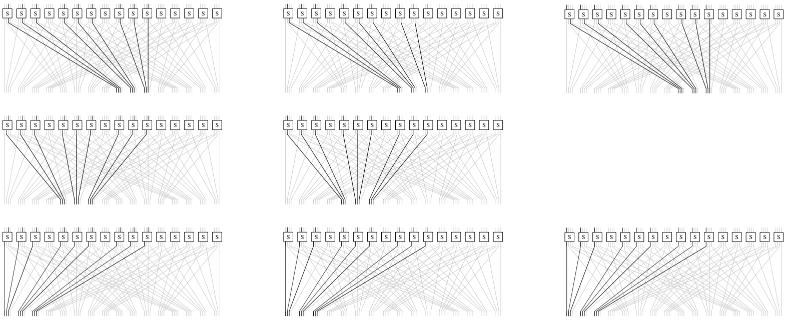

Fig. 4. Continuable 1-Round Single-bit Paths

Table 3. The number of single-bit paths for optimal input-output masks

# rounds	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
# paths	1	1	1	3	9	27	72	192	512	1,344	3,528	9,261	24,255	63,525	166,375

# rounds	16	17	18	19	20	21	22
# paths	435,600	1,140,480	2,985,984	7,817,472	20,466,576	53,582,633	140,281,323

# rounds	23	24	25	26	27
# paths	367,261,713	961,504,803	2,517,252,696	6,590,254,272	17,253,512,704

# rounds	28	29	30	31
# paths	45,170,283,840	118,257,341,400	309,601,747,125	810,547,899,975

3.3 Single-Bit Paths with the Same Input-Output Mask

In the previous subsection, we show that single-bit paths with 3 or more rounds can be made by connecting 1-round paths in Figure 4. For 4 or more rounds, there appear more than 1 single-bit paths with the same input-output mask. Figure 5 shows single-bit paths with the same input-output mask $\Gamma_{2,1,2}$-$\Gamma_{3,3,3}$. There are 3 paths for 4 rounds. The number of paths increases rapidly, as the number of rounds goes up (Table 3).

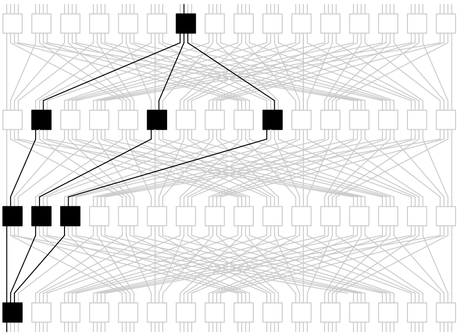

Fig. 5. 4-round single-bit paths with the same input-output mask ($\Gamma_{2,1,2}$-$\Gamma_{3,3,3}$)

The above case is for the input-output mask $\Gamma_{2,1,2}$-$\Gamma_{3,3,3}$, and we found this input-output mask has the maximum number of single-bit paths for all rounds. If we call this propery as optimal, there are 64 optimal input-output masks including the above one, which are given as arbitrary combinations of the 8 input masks

$$\Gamma_{1,1,1}, \Gamma_{1,1,2}, \Gamma_{1,2,1}, \Gamma_{1,2,2}, \Gamma_{2,1,1}, \Gamma_{2,1,2}, \Gamma_{2,2,1}, \Gamma_{2,2,2},$$

and the 8 output masks

$$\Gamma_{1,1,1}, \Gamma_{1,1,3}, \Gamma_{1,3,1}, \Gamma_{1,3,3}, \Gamma_{3,1,1}, \Gamma_{3,1,3}, \Gamma_{3,3,1}, \Gamma_{3,3,3}.$$

Table 3 shows the number of single-bit paths for R rounds $L(R)$ for the optimal input-output masks.

Table 4. Linear deviations with multiple-path effects for weak keys

R	16	17	18	19	20	21	22	23
$\log_2(\epsilon^{(R)})$	-23.634	-24.939	-26.245	-27.551	-28.857	-30.162	-31.468	-32.774

R	24	25	26	27	28	29	30	31
$\log_2(\epsilon^{(R)})$	-34.080	-35.385	-36.691	-37.997	-39.303	-40.608	-41.914	-43.220

3.4 Multiple-Path Effect and Weak Keys

As shown in the previous subsection, there are more than 1 single-bit paths for 4 or more rounds. For the case of R rounds, the absolute value of linear deviation for each path is evaluated as 2^{-2R-1} by using Matsui's Piling-up lemma [4]. It should be noted that the sign of each path depends on the S-box's single-bit approximation and the encryption key. Denote the number of positive paths by N^+, and the number of negative paths by N^-. Then, the linear deviation for the mask is approximated by $2^{-2R-1}(N^+ - N^-)$, which has been confirmed by computer simulations with random plaintexts. This is the multiple-path effect. Appendix A shows the theoretical analysis for the 3 single-bit path case, which can be regarded as a simplification of Figure 5.

Multiple-path effect depends on the extended key. If we assume the extended key distributes uniformly, the sign of each single-bit path follows the binary distribution of probability 1/2. When the number of paths $L(R)$ is sufficiently large, the binary distribution is approximated by the normal distribution with the deviation $\sqrt{L(R)}$. Then the absolute deviation is considered to be not less than $\sqrt{L(R)}$ times larger than the deviation for a single-path for 32% of keys. In fact, by a computer simulation, we confirmed that the standard deviation of $(N^+ - N^-)$ and the rate where $\mid N^+ - N^- \mid$ is larger than the standard deviation are well fitted to the theoretical results.

We call the 32% of keys satisfying $\mid N^+ - N^- \mid >= \sqrt{L(R)}$ weak keys. The lower bound of absolute value of linear deviation for the weak keys is evaluated as follows.

$$\epsilon^{(R)} = 2^{-2R-1}\sqrt{L^{(R)}} \tag{2}$$

Table 4 shows their logarithms. For 28 rounds, linear deviation is about $2^{-39.3}$. This is larger than 2^{-43} which is the upper bound estimated by the designers using the linear characteristic deviations.

4 Key Recovery Attack

In the linear cryptanalysis with the linear deviation ϵ and the number of known plaintexts N, we assume the number of guessed keys is m-bits and they are independent. Then, the success rate of key guess p is denoted as follows (Appendix B).

Table 5. The number of known plaintexts needed for an $(R+1)$-round attack of upper 1-round elimination type

R	18	19	20	21	22
# plaintexts($\log_2$)	55.384	57.996	60.607	63.219	65.830

$$p = \left\{ \mathrm{erf} \left(\sqrt{N} \epsilon \right) \right\}^{2^m} \tag{3}$$

erf() is the Gaussian error function defined as follows here.

$$\mathrm{erf}(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-y^2/2} dy \tag{4}$$

In reverse, the number of plaintexts N needed for the success rate p is evaluated as follows.

$$N = \left\{ \mathrm{erf}^{-1} \left(p^{1/2^m} \right) \ / \ \epsilon \right\}^2 \tag{5}$$

By taking the logarithm with base 2, the equation transforms as follows.

$$\log_2 N = 2 \log_2 \left\{ \mathrm{erf}^{-1} \left(p^{1/2^m} \right) \right\} + 4R + 2 - \log_2 \left\{ L(R) \right\} \tag{6}$$

In the following, we apply linear cryptanalysis for 80-bit key PRESENT, with the linear approximation for an optimal single-bit path $\mathit{\Gamma}_{1,1,1} - \mathit{\Gamma}_{1,1,1}$. More specifically, 5 types of key guesses shown in Figures 7∼11 of Appendix C have been applied.

4.1 Upper 1-Round Elimination Attack ($\mathit{\Gamma}_{1,1,1}$-$\mathit{\Gamma}_{1,1,1}$)

Figure 7 shows the $(R+1)$-round attack for R-round optimal single-bit path ($\mathit{\Gamma}_{1,1,1}$-$\mathit{\Gamma}_{1,1,1}$) in which we guess key bits for 1 preceding round. We search for the 4-bit key which gives the largest absolute linear deviation.

$$\Pr \left(x_{1,1,1}^{(1)} \oplus x_{1,1,1}^{(R+1)} = 0 \right) - 1/2$$

Let γ_1 be a mask which takes 1st bit(2nd rightmost bit), then the above equation is transformed as follows.

$$\Pr \left(\gamma_1 \cdot S \left(x_{1,1}^{(0)} \oplus k_{1,1}^{(0)} \right) \oplus \ x_{1,1,1}^{(R+1)} = 0 \right) - 1/2 \tag{7}$$

Round key $k_{1,1}^{(0)}$ is selected such that the absolute value of the above equation is the largest. In this case, the number of guessed bits m is 4 for one S-box. Table 5 shows the logarithm of the number of plaintexts needed for 95% successful key guessing $2 \log_2(\mathrm{erf}(0.95^{1/2^4})/\epsilon)$. The attack in Figure 7 is available

Table 6. The number of known plaintexts needed for an $(R+2)$-round attack for upper 1-round & lower 1-round elimination type

R	18	19	20	21	22
# plaintexts($\log_2$)	56.137	58.749	61.360	63.972	66.583

up to 22 rounds, and $2^{63.219}$ known texts are needed. The exhaustive search for the remaining key bits requires the calculation of 2^{76} encryptions.

4.2 Upper 1-Round & Lower 1-Round Elimination Attack ($\Gamma_{1,1,1}$-$\Gamma_{1,1,1}$)

Figure 8 shows the $(R+2)$-round attack for R-round optimal single-bit path ($\Gamma_{1,1,1}$-$\Gamma_{1,1,1}$) in which we guess keys bits for 1 preceding and 1 following rounds. We search for the 8-bit key which gives the largest absolute linear deviation.

$$\Pr\left(x^{(1)}_{1,1,1} \oplus x^{(R+1)}_{1,1,1} = 0\right) - 1/2$$

Using γ_1, the above equation is transformed as follows.

$$\Pr\left(\gamma_1 \cdot S\left(x^{(0)}_{1,1} \oplus k^{(0)}_{1,1}\right) \oplus\ \gamma_1 \cdot S^{-1}\left(x^{(R+2)}_{1,1} \oplus k^{(R+2)}_{1,1}\right) = 0\right) - 1/2 \qquad (8)$$

Round key $\left(k^{(0)}_{1,1}\ ,\ k^{(R+2)}_{1,1}\right)$ is selected such that the absolute value of the above equation is the largest. In this case, the number of guessed bits m is 8 for 2 S-boxes. Table 6 shows the logarithm of the number of plaintexts needed for 95% successful key guessing $2\log_2(\mathrm{erf}(0.95^{1/2^8})/\epsilon)$. The attack in Figure 8 is available up to 23 rounds, and $2^{63.972}$ known texts are needed. The exhaustive search for the remaining key bits requires the calculation of 2^{72} encryptions.

4.3 Upper 2-Round Elimination Attack ($\Gamma_{1,1,1}$-$\Gamma_{1,1,1}$)

Figure 9 shows the $(R+2)$-round attack for R-round optimal single-bit path ($\Gamma_{1,1,1}$-$\Gamma_{1,1,1}$) in which we guess keys bits for 2 preceding rounds. We search for the 20-bit key which gives the largest absolute linear deviation.

$$\Pr\left(x^{(2)}_{1,1,1} \oplus x^{(R+2)}_{1,1,1} = 0\right) - 1/2$$

Using γ_1, the above equation is transformed as follows.

$$\Pr\Big(S\Big(\gamma_1 \cdot S(x^{(0)}_{1,3} \oplus k^{(0)}_{1,3}) \mid \gamma_1 \cdot S(x^{(0)}_{1,2} \oplus k^{(0)}_{1,2}) \mid \gamma_1 \cdot S(x^{(0)}_{1,1} \oplus k^{(0)}_{1,1}) \mid$$
$$\gamma_1 \cdot S(x^{(0)}_{1,0} \oplus k^{(0)}_{1,0}) \oplus\ k^{(1)}_{1,1}\Big) \oplus x^{(R+2)}_{1,1,1} = 0\Big) - 1/2 \qquad (9)$$

Table 7. The number of known plaintexts needed for an $(R+2)$-round attack of upper 2-round elimination type

R	18	19	20	21	22
# plaintexts($\log_2$)	57.319	59.930	62.542	65.153	67.765

Table 8. The number of known plaintexts needed for an $(R+3)$-round attack for upper 2-round & lower 1-round elimination type

R	18	19	20	21	22
# plaintexts($\log_2$)	57.569	60.181	62.792	65.404	68.015

Round key $\left(k_{1,0}^{(0)}\ ,\ k_{1,1}^{(0)}\ ,\ k_{1,2}^{(0)}\ ,\ k_{1,3}^{(0)}\ ,\ k_{1,1}^{(1)}\right)$ is selected such that the absolute value of the above equation is the largest. In this case, the number of guessed bits m is 20 for 5 S-boxes. Table 7 shows the logarithm of the number of plaintexts needed for 95% successful key guessing $2\log_2(\mathrm{erf}(0.95^{1/2^{20}})/\epsilon)$. The attack in Figure 9 is available up to 22 rounds, and $2^{62.542}$ known texts are needed. The exhaustive search for the remaining key bits requires the calculation of 2^{60} encryptions.

4.4 Upper 2-Round & Lower 1-Round Elimination Attack ($\boldsymbol{\Gamma_{1,1,1}}$-$\boldsymbol{\Gamma_{1,1,1}}$)

Figure 10 shows the $(R+3)$-round attack for R-round optimal single-bit path ($\Gamma_{1,1,1}$-$\Gamma_{1,1,1}$) in which we guess key bits for 2 preceding and 1 following round. We search for the 24-bit key which gives the largest absolute linear deviation.

$$\Pr\left(x_{1,1,1}^{(2)} \oplus x_{1,1,1}^{(R+2)} = 0\right) - 1/2$$

Using γ_1, the above equation is transformed as follows.

$$\Pr\Big(\gamma_1 \cdot S\Big(\gamma_1 \cdot S(x_{1,3}^{(0)} \oplus k_{1,3}^{(0)}) \mid \gamma_1 \cdot S(x_{1,2}^{(0)} \oplus k_{1,2}^{(0)}) \mid \gamma_1 \cdot S(x_{1,1}^{(0)} \oplus k_{1,1}^{(0)}) \mid$$

$$\gamma_1 \cdot S(x_{1,0}^{(0)} \oplus k_{1,0}^{(0)}) \oplus\ k_{1,1}^{(1)}\Big) \oplus\ \gamma_1 \cdot S^{-1}\left(x_{1,1}^{(R+3)} \oplus k_{1,1}^{(R+3)}\right) = 0\Big) - 1/2 \qquad (10)$$

Round key $\left(k_{1,0}^{(0)}\ ,\ k_{1,1}^{(0)}\ ,\ k_{1,2}^{(0)}\ ,\ k_{1,3}^{(0)}\ ,\ k_{1,1}^{(1)}\ ,\ k_{1,1}^{(R+3)}\right)$ is selected such that the absolute value of the above equation is the largest. In this case, the number of guessed bits m is 24 for 6 S-boxes. Table 8 shows the logarithm of the number of plaintexts needed for 95% successful key guessing $2\log_2(\mathrm{erf}(0.95^{1/2^{24}})/\epsilon)$. The attack in Figure 10 is available up to 23 rounds, and $2^{62.792}$ known texts are

Table 9. The number of known plaintexts needed for an $(R+4)$-round attack for upper 2-round & lower 2-round elimination type

R	18	19	20	21	22
# plaintexts($\log_2$)	58.285	60.897	63.508	66.120	68.731

needed. The exhaustive search for the remaining key bits requires the calculation of 2^{56} encryptions.

4.5 Upper 2-Round & Lower 2-Round Elimination Attack ($\boldsymbol{\Gamma_{1,1,1}}$-$\boldsymbol{\Gamma_{1,1,1}}$)

Figure 11 shows the $(R+4)$-round attack for R-round optimal single-bit path ($\Gamma_{1,1,1}$-$\Gamma_{1,1,1}$) with 2 preceeding and 2 following rounds for key guess. We search for the 40-bit key which gives the largest absolute linear deviation.

$$\Pr\left(x^{(2)}_{1,1,1} \oplus x^{(R+2)}_{1,1,1} = 0\right) - 1/2$$

Using γ_1, the above equation is transformed as follows.

$$\begin{aligned}
&\Pr\Big(\gamma_1 \cdot S\Big(\gamma_1 \cdot S(x^{(0)}_{1,3} \oplus k^{(0)}_{1,3}) \mid \gamma_1 \cdot S(x^{(0)}_{1,2} \oplus k^{(0)}_{1,2}) \mid \gamma_1 \cdot S(x^{(0)}_{1,1} \oplus k^{(0)}_{1,1}) \mid \\
&\qquad \gamma_1 \cdot S(x^{(0)}_{1,0} \oplus k^{(0)}_{1,0}) \oplus\ k^{(1)}_{1,1}\Big) \\
&\quad \oplus \gamma_1 \cdot S^{-1}\Big(\gamma_1 \cdot S^{-1}(x^{(R+4)}_{1,3} \oplus k^{(R+4)}_{1,3}) \mid \gamma_1 \cdot S^{-1}(x^{(R+4)}_{1,2} \oplus k^{(R+4)}_{1,2}) \mid \\
&\gamma_1 \cdot S^{-1}(x^{(R+4)}_{1,1} \oplus k^{(R+4)}_{1,1}) \mid \gamma_1 \cdot S^{-1}(x^{(R+4)}_{1,0} \oplus k^{(R+4)}_{1,0})\ \oplus\ k^{(R+3)}_{1,1}\Big) = 0\Big) - 1/2 \quad (11)
\end{aligned}$$

Round key $\Big(k^{(0)}_{1,0}\ ,\ \ k^{(0)}_{1,1}\ ,\ k^{(0)}_{1,2}\ ,\ k^{(0)}_{1,3}\ ,\ k^{(1)}_{1,1}\ ,\ k^{(R+3)}_{1,1}\ ,\ k^{(R+4)}_{1,0}\ ,\ k^{(R+4)}_{1,1}\ ,\ k^{(R+4)}_{1,2}\ ,$ $k^{(R+4)}_{1,3}\Big)$ is selected such that the absolute value of the above equation is the largest. In this case, the number of guessed bits m is 40 for 10 S-boxes. Table 9 shows the logarithm of the number of plaintexts needed for 95% successful key guessing $2\log_2(\mathrm{erf}(0.95^{1/2^{40}})/\epsilon)$. The attack in Figure 11 is available up to 24 rounds, and $2^{63.508}$ known texts are needed. The exhaustive search for the remaining key bits requires the calculation of 2^{40} encryptions.

5 Concluding Remarks

The block cipher PRESENT is designed so that the implementation is very small. As a bit permutation is used in the linear layer, the avalanche effect is very low, and it is easy to find single-bit paths with only one bit active in every round. We found that there are many such paths with the same input-output mask for 4 or more rounds.

Each single-bit path for the same input-output mask has its sign, and the absolute value of linear deviation is large when the portion of one sign is much larger than 1/2. Let $L(R)$ be the number of single-bit paths for R rounds. Under the assumption that the signs follows the binary distribution, we determined that for 32% of all keys, which we call weak keys, the absolute linear deviation is not less than $\sqrt{L(R)}$ times of single path linear deviation. This phenomenon is called the multi-path effect.

By considering the multi-path effect, the linear deviation for 28 rounds is evaluated as $2^{-39.3}$ for weak keys, which is larger than 2^{-43} given by the designers with sigle-path evaluation. We applied 5 types of linear cryptanalysis to PRESENT, and 24-round reduced PRESENT is vulnerable with $2^{63.5}$ known plaintexts.

In this paper 32% key is weak keys for PRESENT, but the evaluation is for only one input-output mask. There are 64 masks with the same number of single-bit paths, and if a key is weak at least for one mask, it can be regarded as a weak key.

References

1. Bogdanov, A., Knudsen, L.R., Leander, G., Paar, C., Poschmann, A., Robshaw, M.J.B., Seurin, Y., Vikkelsoe, C.: PRESENT: An Ultra-Lightweight Block Cipher. In: Paillier, P., Verbauwhede, I. (eds.) CHES 2007. LNCS, vol. 4727, pp. 450–466. Springer, Heidelberg (2007)
2. Kaliski Jr., B.S., Robshaw, M.J.B.: Linear Cryptanalysis Using Multiple Approximations. In: Desmedt, Y.G. (ed.) CRYPTO 1994. LNCS, vol. 839, pp. 26–39. Springer, Heidelberg (1994)
3. Kaliski Jr., B.S., Robshaw, M.J.B.: Linear Cryptanalysis Using Multiple Approximations and FEAL. In: Preneel, B. (ed.) FSE 1994. LNCS, vol. 1008, pp. 249–264. Springer, Heidelberg (1995)
4. Matsui, M.: Linear Cryptanalysis Method for DES Cipher. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 386–397. Springer, Heidelberg (1994)
5. Shimoyama, T., Takenaka, M., Koshiba, T.: Multiple Linear Cryptanalysis of a Reduced Round RC6. In: Daemen, J., Rijmen, V. (eds.) FSE 2002. LNCS, vol. 2365, pp. 76–88. Springer, Heidelberg (2002)
6. Wang, M.: Differential Cryptanalysis of Reduced-Round PRESENT. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 40–49. Springer, Heidelberg (2008)
7. Z'aba, M.R., Raddum, H., Henricksen, M., Dawson, E.: Bit-Pattern Based Integral Attack. In: Nyberg, K. (ed.) FSE 2008. LNCS, vol. 5086, pp. 363–381. Springer, Heidelberg (2008)
8. Collard, B., Standaert, F.-X.: A Statistical Saturation Attack against the Block Cipher PRESENT. In: Fischlin, M. (ed.) CT-RSA 2009. LNCS, vol. 5473, pp. 195–210. Springer, Heidelberg (2009)

A Analysis of 3 Single-Bit Path Model

In this Appendix, multiple-path effect is analyzed for the simplest case.

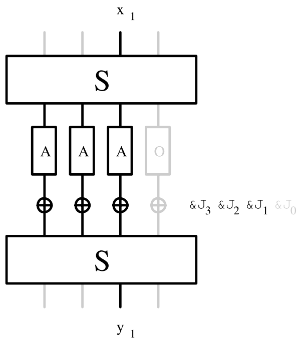

Fig. 6. 3 single-bit path model

Table 10. Linear deviation for 3-path model

$\kappa_1 + \kappa_2 + \kappa_3$	0	1	2	3
η	$3\epsilon - 4\epsilon^3$	$\epsilon + 4\epsilon^3$	$-\epsilon - 4\epsilon^3$	$-3\epsilon + 4\epsilon^3$

Figure 6 is a simplified model for Figure 5. 2 S's are the S-boxes of PRESENT, 3 A's are mutually independent paths with a positive linear deviation ϵ, and O is a path with 0 deviation. The deviation of A can take both positive and negative signs. But, without loss of generality, we can assume the positive sign, as the sign can be absorbed in the key bits κ's.

$$\Pr(x \oplus A(x) = 0) = 1/2 + \epsilon$$

$$\Pr(x \oplus O(x) = 0) = 1/2$$

Table 10 shows the deviation η for an equation $x_1 \oplus y_1$.

$$\Pr(x_1 \oplus y_1 = 0) = 1/2 + \eta$$

$\kappa_1 + \kappa_2 + \kappa_3$ means the number of paths with negative correlation for $x_1 \oplus y_1$. When $\kappa_1 + \kappa_2 + \kappa_3 = 0$, all 3 paths induce positive correlations. To the contrary, when $\kappa_1 + \kappa_2 + \kappa_3 = 3$, all 3 paths induce negative correlations. When $\kappa_1 + \kappa_2 + \kappa_3 = 1$ or $\kappa_1 + \kappa_2 + \kappa_3 = 2$, one positive and one negative are canceled out, one positive or negative correlation remains.

The 1st order terms of ϵ in Table 10 shows an effect which agrees with the above consideration. The 3rd order terms of ϵ is regarded as shifts from the simple sum of 3 correlations, which can be negligible for a sufficiently small ϵ. Let the number of $\kappa_i = 0$ as N^+ and the number of $\kappa_i = 1$ as N^- in Figure 6, then, the linear deviation η is approximated as follows.

$$\eta \simeq (N^+ - N^-)\epsilon. \tag{12}$$

B Evaluation of Successful Key Recovery Rate

Let ϵ be the absolute value of linear deviation. Then, the probability that a linear approximation is satisfied is considered to be $1/2 \pm \epsilon$ for the correct key guess, and $1/2$ for the wrong key guess. Without loss of generality, we assume the sign is negative.

When known plaintexts are assumed to be uniformly distributed, both valid linear approximation rates are considered to follow the binary distribution. When the number of plaintexts is N, the average and the variance for both rates are evaluated as follows

$$\begin{aligned} &\mathit{correctkey\ average} : \mu_{\mathrm{T}} = 1/2 - \epsilon \\ &\qquad\qquad \mathit{standarddeviation} : \sigma_{\mathrm{T}} = \sqrt{(1/4 - \epsilon^2)/N} \\ &\mathit{wrongkeys\ average} : \mu_{\mathrm{F}} = 1/2 \\ &\qquad\qquad \mathit{standarddeviation} : \sigma_{\mathrm{F}} = 2/\sqrt{N} \end{aligned}$$

When N is sufficiently large, the 2 distributions can be approximated by the normal distributions. Let x_0 be the value for the cross point. When we compare the correct key and one wrong key, and choose the key with the probability which is more distant from 1/2, the probability to choose the correct key p_{s} is given as follows.

$$p_{\mathrm{s}} = \int_{-\infty}^{x_0 - \mu_{\mathrm{T}}} \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{T}}} e^{-(x-\mu_{\mathrm{T}})^2/2\sigma_{\mathrm{T}}^2} dx \tag{13}$$

When ϵ is sufficiently small, terms of order ϵ^2 are negligible, and the next approximated equations are given.

$$\sigma_{\mathrm{T}} = 1/2\sqrt{N}$$

$$x_0 = 1/2 - \epsilon/2$$

From the above equations and the next transform

$$y = (x - \mu_{\mathrm{T}})/\sigma_{\mathrm{T}},$$

p_{s} is evaluated as follows.

$$\begin{aligned} p_{\mathrm{s}} &= \int_{-\infty}^{(x_0-\mu_{\mathrm{T}})/\sigma_{\mathrm{T}}} \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{T}}} e^{-y^2/2}\ \sigma_{\mathrm{T}}\ dy \\ &= \int_{-\infty}^{\sqrt{N}\epsilon} \frac{1}{\sqrt{2\pi}} e^{-y^2/2} dy = \mathrm{erf}\left(\sqrt{N}\epsilon\right) \end{aligned}$$

When m-bit key is guessed, $2^m - 1$ keys are wrong, and the probability of correct key selection p is $(2^m - 1)$-th power of p_{s}

$$p = p_{\mathrm{s}}^{2^m-1} = \left\{\mathrm{erf}\left(\sqrt{N}\epsilon\right)\right\}^{2^m-1}$$

When m is sufficiently large, deleting -1 is a good approximation for this equation.

C Figures of Key Recovery Attacks

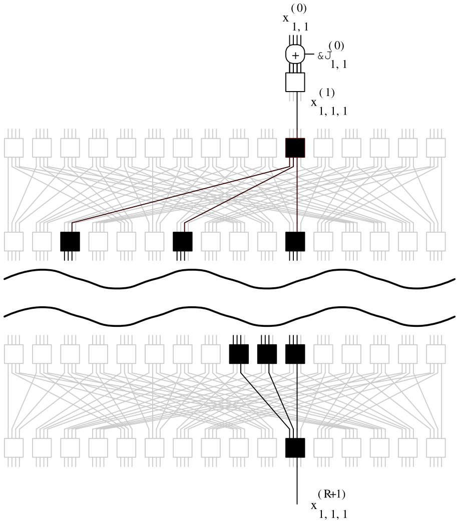

Fig. 7. Upper 1-round elimination attack

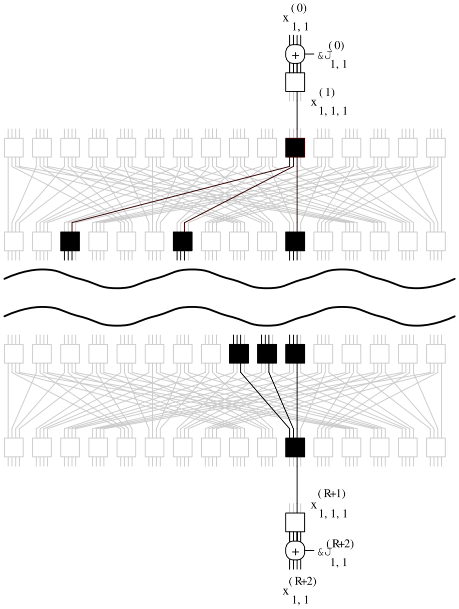

Fig. 8. Upper 1-round & lower 1-round elimination attack

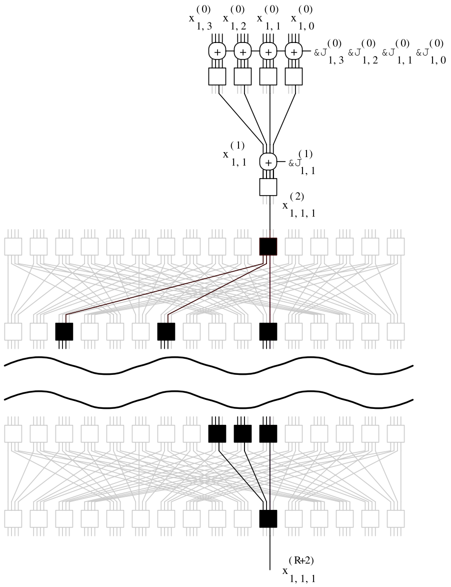

Fig. 9. Upper 2-round elimination attack

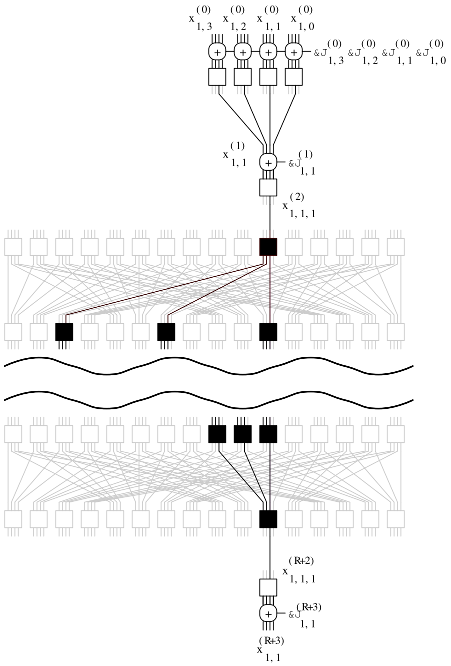

Fig. 10. Upper 2-round & lower 1-round elimination attack

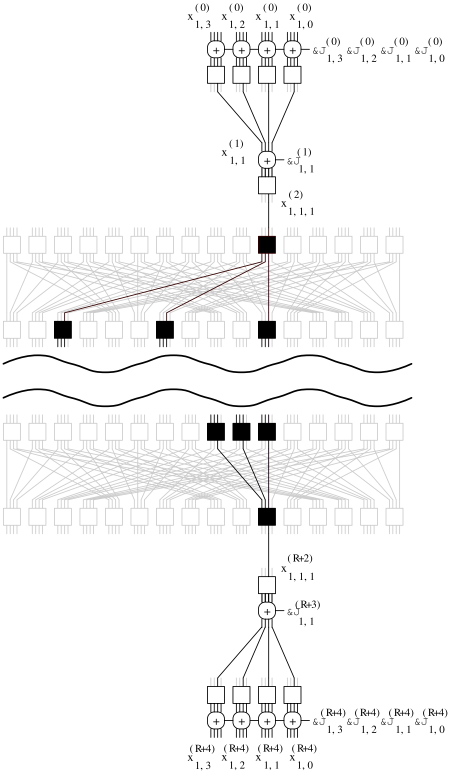

Fig. 11. Upper 2-round & lower 2-round elimination attack