Differential Cryptanalysis of PRESENT

Meiqin Wang

Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education,
Shandong University,
Jinan, 250100, China
{mqwang}@sdu.edu.cn**

Abstract. PRESENT is proposed by A.Bogdanov et al. in CHES 2007 for extremely constrained environments such as RFID tags and sensor networks. In this paper, we find out the differential characteristics for r-round($5 \leq r \leq 15$), then give the differential cryptanalysis on reduced-round variants of PRESENT. We attack 16-round PRESENT using 2^{64} chosen plaintexts, 2^{32} 6-bit counters, and 2^{65} memory accesses.

1 Introduction

RFID systems and sensor networks have been aggressively deployed in a variety of applications, but their further pervasive usage is mainly limited by lots of security and privacy concerns. As RFID tags and sensor networks are low cost with limited resources, the present cryptographic primitives can not be feasible. So the security primitives suitable for these environments must be designed.

PRESENT is an Ultra-Lightweight block cipher proposed by A.Bogdanov, L.R.Knudsen and G.Leander et al.[3] and has implementation requirements similar to many compact stream ciphers. Compared to other current block ciphers for low-cost implementation requirements such as TEA[12, 13], MCRYPTON[7], HIGHT[5], SEA[11] and CGEN[9], PRESENT has the lowest implementation costs.

PRESENT is a 31-round SP-network with block length 64 bits and 80 bits or 128 bits key length. Serpent[1] and DES have excellent performance in hardware, so the design of PRESENT makes use of the characteristics of the two block ciphers. The non-linear substitution layer S-box of PRESENT is similar to that of Serpent and the linear permutation layer pLayer of PRESENT is similar to that of DES.

Differential cryptanalysis, proposed by Biham and Shamir[4], has been one of the most general cryptanalytic techniques. Although the original PRESENT proposal provided theoretical upper bounds for the highest probability characteristics of 25-round PRESENT[3], the proposal did not give the concrete differential results.

In this paper, we consider actual differential attack against reduced-round PRESENT. First we give some differential characteristics for PRESENT. 14-round differential characteristics occur with the probability of 2^{-62} and 15-round differential characteristics occur with the probability of 2^{-66}. Second, we attack 16-round PRESENT with 14-round differential characteristics using 2^{64} chosen plaintexts, 2^{32} 6-bit counters, and 2^{65} memory accesses.

The paper is organized as follows. Section 2 introduces the description of PRESENT. In Section 3, we give some notations used in this paper. In Section 4, we present the best differential characteristics we found for PRESENT, and give the differential attack on 16-round PRESENT-80. Section 5 concludes this paper.

** supported by the National "973" Program of China under Grant No.2007CB807902, Natural Science Foundation of China under Grant No.90604036

2 Description of PRESENT

2.1 The Encryption Process

PRESENT is a 31-round Ultra-Lightweight block cipher. The block length is 64-bit. PRESENT uses only one 4-bit S-box S which is applied 16 times in parallel in each round. The cipher is described in Figure 1. As in Serpent, there are three stages involved in PRESENT. The first stage is addRoundKey described as follows,

$$b_j \rightarrow b_j \bigoplus {k^i}_j$$

where $b_j, 0 \leq j \leq 63$ is the current state and ${k^i}_j, 1 \leq i \leq 32, 0 \leq j \leq 63$ is the $j-th$ subkey bit of round key K_i.

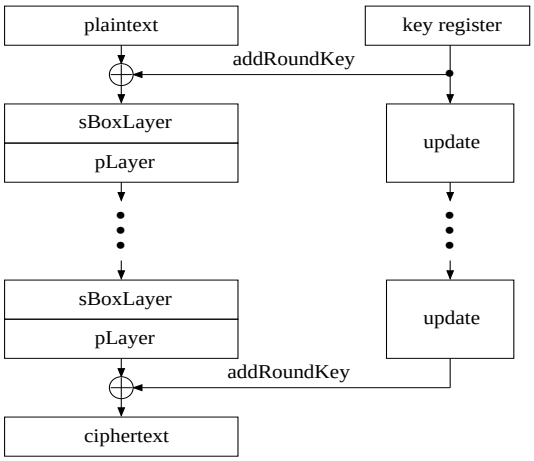

Fig. 1. 31-round PRESENT Encryption Algorithm.

The second stage is sBoxLayer which is 16 times implementation of 4-bit to 4-bit S-box, which is given in Table 1.

Table 1. Table of 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

The third stage is the bit permutation pLayer, which is given by Table 2. From pLayer, bit i of stage is moved to bit position $P(i)$.

2.2 The Key Schedule

PRESENT's key schedule can take key sizes as 80 bits or 128 bits. We will cryptanalyze 80 bits version, so we will only give the schedule algorithm for 80 bits version.

Table 2. Table of pLayer

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

Firstly, the 80-bit key will be stored in a key register K denoted as $K = k_{79}k_{78}\dots k_0$. In round j, PRESENT firstly extracts 64-bit subkeys K_j as the following ways,

$$K_j = \kappa_{63}\kappa_{62}\dots\kappa_0 = k_{79}k_{78}\dots k_{16}$$

Then it updates key register $K = k_{79}k_{78}\dots k_0$ as follows,

$$[k_{79}k_{78}\dots k_1k_0] = [k_{18}k_{17}\dots k_{20}k_{19}]$$

$$[k_{79}k_{78}k_{77}k_{76}] = S[k_{79}k_{78}k_{77}k_{76}]$$

$$[k_{19}k_{18}k_{17}k_{16}k_{15}] = [k_{19}k_{18}k_{17}k_{16}k_{15}] \oplus round\_counter$$

3 Some Notations

In the remainder of the paper, we use $X = x_0, x_1, \dots, x_{15}$ to denote the intermediate difference in each step. $x_0, x_1, \dots, x_{15}$ are 16 nibble differences. x_0 is the least significant nibble difference. We denote K_i as the subkey for the $i-th$ round, $K_{i,j}$ as the $j-th$ nibble subkey for the $i-th$ round and $k_{i,j}$ as the $j-th$ bit subkey for the $i-th$ round.

4 Differential Characteristics for PRESENT

Firstly, we give the XORs differential distribution of S-box in Table 3. From the XOR's distribution table for S-box, one bit input difference will cause at least two bits output difference, which will cause two active S-boxes in the next round. Then each of the two active S-boxes will have at least two bits output difference, which will cause at least four active S-boxes in the next round.

4.1 Searching for differential characteristics

The differential cryptanalysis of DES[4] makes use of 2-round iterative characteristics to form 13-round differential characteristics. Knudsen has searched the better iterative characteristics for DES[6], which is an efficient method to find the differential characteristics for more rounds. We have searched for the differential characteristic in the following way:

– We searched the iterative characteristics from 2-round to 7-round, which are more advantage than the 2-round iterative characteristic given in [3]. As the maximum probability in the differential distribution table for PRESENT S-box is 2^{-2}, we only consider the maximum number of active S-boxes from 2-round to 4-round are 4, 7 and 9 respectively. The possible distribution of the number of active S-boxes in them is listed in Table 4. As a result, only 4-round iterative characteristics with the probability 2^{-18} have been found, one of which is given in Table 5.

Table 3. Differential Distribution Table of S-box

	0_x	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
0_x	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2_x	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3_x	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4_x	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5_x	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6_x	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7_x	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8_x	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9_x	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A_x	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B_x	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C_x	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D_x	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E_x	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F_x	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

– We searched the best differential characteristics from 5-round to 10-round which are more advantage than the characteristics based on 4-round iterative characteristics we have found.
– Based on 4-round iterative characteristic, we have found the differential characteristics from round-11 to round-15.

Table 4. Possible Distribution of Active S-box for Iterative Characteristics

Rounds	2	3	4
Possible Distribution of Active S-box	2-2	2-2-2	2-2-2-2
		3-2-2	3-2-2-2
		2-3-2	2-3-2-2
		2-2-3	2-2-3-2
			2-2-2-3

The differential characteristics we found in the way are given in Table 6. It is noted that the number of active S-boxes in each round are all 2.

We have found 24 14-round differential characteristics with the probability 2^{-62}, among which 20 differential characteristics with different input differences but the same output difference and 4 pairs of differential characteristic with the same input differences in the first round and the different difference from the output of round 2 to the input of round 8. All the characteristics have the same differences after the $8-th$ round, and all have the same probability 2^{-62}. Table 7 gives one of the 14-round characteristics we have found.

4.2 Attacking 16-round PRESENT

We will attack 16-round PRESENT using the 14-round differential characteristics with probability of 2^{-62}.

Table 5. 4-round Iterative Differential of PRESENT

Rounds		Differences	Pr
I		$x_0 = 4, x_3 = 4$	1
R1	S	$x_0 = 5, x_3 = 5$	$\frac{1}{2^4}$
R1	P	$x_0 = 9, x_8 = 9$	1
R2	S	$x_0 = 4, x_8 = 4$	$\frac{1}{2^4}$
R2	P	$x_8 = 1, x_{10} = 1$	1
R3	S	$x_8 = 9, x_{10} = 9$	$\frac{1}{2^4}$
R3	P	$x_2 = 5, x_{14} = 5$	1
R4	S	$x_2 = 1, x_{14} = 1$	$\frac{1}{2^6}$
R4	P	$x_0 = 4, x_3 = 4$	1

Table 6. Probability of the Best Characteristics

Rounds	Differential Probability	Number of Active S-box
5	2^{-20}	10
6	2^{-24}	12
7	2^{-28}	14
8	2^{-32}	16
9	2^{-36}	18
10	2^{-42}	20
11	2^{-46}	22
12	2^{-52}	24
13	2^{-56}	26
14	2^{-62}	28
15	2^{-66}	30

Table 7. The 14-round Differential of PRESENT

Rounds		Differences	Pr
I		$x_2 = 7, x_{14} = 7$	
R1	S	$x_2 = 1, x_{14} = 1$	$\frac{1}{2^4}$
R1	P	$x_0 = 4, x_3 = 4$	1
R2	S	$x_0 = 5, x_3 = 5$	$\frac{1}{2^4}$
R2	P	$x_0 = 9, x_8 = 9$	1
R3	S	$x_0 = 4, x_8 = 4$	$\frac{1}{2^4}$
R3	P	$x_8 = 1, x_{10} = 1$	1
R4	S	$x_8 = 9, x_{10} = 9$	$\frac{1}{2^4}$
R4	P	$x_2 = 5, x_{14} = 5$	1
R5	S	$x_2 = 1, x_{14} = 1$	$\frac{1}{2^6}$
R5	P	$x_0 = 4, x_3 = 4$	1
R6	S	$x_0 = 5, x_3 = 5$	$\frac{1}{2^4}$
R6	P	$x_0 = 9, x_8 = 9$	1
R7	S	$x_0 = 4, x_8 = 4$	$\frac{1}{2^4}$
R7	P	$x_8 = 1, x_{10} = 1$	1
R8	S	$x_8 = 9, x_{10} = 9$	$\frac{1}{2^4}$
R8	P	$x_2 = 5, x_{14} = 5$	1
R9	S	$x_2 = 1, x_{14} = 1$	$\frac{1}{2^6}$
R9	P	$x_0 = 4, x_2 = 4$	1
R10	S	$x_0 = 5, x_2 = 5$	$\frac{1}{2^4}$
R10	P	$x_0 = 9, x_8 = 9$	1
R11	S	$x_0 = 4, x_8 = 4$	$\frac{1}{2^4}$
R11	P	$x_8 = 1, x_{10} = 1$	1
R12	S	$x_8 = 9, x_{10} = 9$	$\frac{1}{2^4}$
R12	P	$x_2 = 5, x_{14} = 5$	1
R13	S	$x_2 = 1, x_{14} = 1$	$\frac{1}{2^6}$
R13	P	$x_0 = 4, x_2 = 4$	1
R14	S	$x_0 = 5, x_2 = 5$	$\frac{1}{2^4}$
R14	P	$x_0 = 9, x_8 = 9$	1

As the 24 differential characteristics we found have 2 active S-boxes in the first round which locate in S-box 0, 1, 2, 12, 13 and 14, which must be non-active S-box from 3 to 11 and 15 in the first round. This attack requires 2^{40} structures of 2^{24} chosen plaintexts each. In each structure, the inputs in 10 non-active S-boxes can take 2^{40} possible values, and the inputs to any two active S-boxes in each characteristic among the six active S-boxes have 2^{24} possible values. There are $2^{40} * 2^{16} * 2^7 = 2^{63}$ pairs for each possible characteristics, $2^{63} * 20 = 2^{67.32}$ pairs satisfy 24 characteristics. Each characteristic has the possibility 2^{-62}, so the number of right pairs is $2^{63} * 2^{-62} * 24 = 48$ satisfying any one characteristic. For each structure, there are about 2^{47} pairs of plaintext to be considered in total.

According to the output difference of 14-round differential characteristics, there are two active S-boxes in round-15 which are x_0 and x_8 whose input difference is 9 and output difference will be 2, 4, 6, 8, 12 or 14. The least significant bit of their output difference must be zero, so at most 6 bits are non-zero for the output difference of S-boxes in round 15. After the pLayer of round 15, the maximum number of active S-boxes for round 16 is 6 and the active S-boxes will be $x_4, x_6, x_8, x_{10}, x_{12}$ and x_{14}, and the minimum number of active S-boxes for round 16 is 2.

For each structure, each pair satisfying each characteristic should have 10 non-active S-boxes in round 16, so the wrong pairs should be discarded. Thus about $2^{47} * 2^{-40} = 2^7$ candidates for right pairs remain from each structure.

Among 16 S-boxes in round 16, 10 S-boxes must be non-active, 2 S-boxed must be active and 4 S-boxes can be active or non-active. If it is active, the input difference must be 1, and the output difference will be 3, 7, 9 or 13. Discarding any pair with a wrong output difference using the above filter should keep only a fraction of $\frac{5}{16}^6 = 2^{-10.07}$. So only about $2^7 * 2^{-10.07} = 2^{-3.07}$ pairs remain for each structure.

For each structure, we check if the remaining pairs satisfy one of the 24 possible plaintext differences corresponding to 24 characteristics. As there are about 2^{24} possible input differences, only a fraction of about $2^{-24} * 20 = 2^{-19.68}$ of the pairs remain. So the expected number of remaining pairs in all the 2^{40} structures is $2^{40} * 2^{-3.07} * 2^{-19.68} = 2^{17.25}$.

During the decryption process, 8 bits of round subkey K_{16} and 24 bits of round subkey K_{17} will be involved during decrypt from round 16 to round 14, which are $k_{16,0}$,$k_{16,8}$,$k_{16,16}$,$k_{16,24}$,$k_{16,32}$,$k_{16,40}$,$k_{16,48}$ $k_{16,56}$,$k_{17,4}$,$k_{17,20}$,$k_{17,36}$,$k_{17,52}$,$k_{17,6}$,$k_{17,22}$, $k_{17,38}$,$k_{17,54}$,$k_{17,8}$,$k_{17,24}$,$k_{17,40}$,$k_{17,56}$,$k_{17,10}$, $k_{17,26}$, $k_{17,42}$,$k_{17,58}$,$k_{17,12}$,$k_{17,28}$,$k_{17,44}$,$k_{17,60}$, $k_{17,14}$,$k_{17,30}$,$k_{17,46}$ and $k_{17,62}$ respectively. After deriving the subkey K_{16} and K_{17} from the master key K, the 24-bit subkey from K_{17} above are independent from the 8-bit subkey from K_{16}, so the total number of subkey bits involved in the decryption from round 16 to round 14 is 32.

For each remaining pair, we guess the 24-bit subkey of K_{17} and 8-bit subkey of K_{16} in round 16, and decrypt the remaining ciphertext pairs from round 16 to round 14. According to the differential distribution table of S-box for PRESENT, given the input difference and output difference, there will be at most 4 pairs occurrences, so the average count per counted pair of the subkey nibble corresponding to one active S-box will be 4. According to the number of active S-boxes in round 16 denoted as $t(2 \leq t \leq 6)$ for the remaining ciphertext pairs, we will consider 5 cases according to the value of t:

- If $t = 2$, only $2^{17.25} * 2^{-16} = 2^{1.25}$ pairs of ciphertext satisfy the condition of 2 active S-boxes, so the total counted times of subkeys are about $2^{1.25} * 4^4 = 2^{9.25}$ for the remaining pairs.
- If $t = 3$, about $2^{17.25} * (2^{-12} - 2^{-16}) = 2^{5.16}$ pairs of ciphertext satisfy the condition of 3 active S-boxes, so the total counted times of subkeys are about $2^{5.16} * 4^5 = 2^{15.16}$ for the remaining pairs.
- If $t = 4$, about $2^{17.25} * (2^{-8} - 2^{-12}) = 2^{9.16}$ pairs of ciphertext satisfy the condition of 4 active S-boxes, so the total counted times of subkeys are about $2^{9.16} * 4^6 = 2^{21.16}$ for the remaining pairs.

- If $t = 5$, about $2^{17.25} * (2^{-4} - 2^{-8}) = 2^{13.16}$ pairs of ciphertext satisfy the condition of 5 active S-boxes, so the total counted times of subkeys are about $2^{13.16} * 4^7 = 2^{27.16}$ for the remaining pairs.
- If $t = 6$, the remained pairs satisfying the condition of 6 active S-box will be $2^{17.25} * (1 - 2^{-4}) = 2^{17.16}$, so the total counted times of subkeys are about $2^{17.16} * 4^8 = 2^{33.16}$ for the remaining pairs.

The total counted times of the subkeys are $2^{33.16} + 2^{27.16} + 2^{21.16} + 2^{15.16} + 2^{9.25} = 2^{33.18}$, so the wrong subkey hits are average about $2^{33.18}/2^{32} = 2^{1.18} = 2.27$ times, but the right subkey is counted for the right pairs about 48 times, so it can be easily identified. In total, we retrieve 32 subkey bits using at most $2^{33.18}$ times 2-round PRESENT encryptions and 2^{32} 6-bit counters.

We take another set of 14-round characteristics, whose difference from the above set characteristics is from the output difference of S-box for round 13 to the output difference for round 14 given in Table 8. The active S-boxes in round 15 will be x_2 and x_{10}, and the active S-boxes in round 16 are $x_4, x_6, x_8, x_{10}, x_{12}$ and x_{14} which are the same as that of the above set of characteristic. As we already know the common 24 subkey bits of K_{17}, so we can easily discard wrong pairs. We can get 8 additional subkey bits of K_{16}.

Table 8. The 14-round Differential of PRESENT

Rounds		Differences	Pr
I		$x_2 = 7, x_{14} = 7$	
⋮	⋮	⋮	⋮
R12	P	$x_2 = 5, x_{14} = 5$	1
R13	S	$x_2 = 4, x_{14} = 4$	$\frac{1}{2^6}$
R13	P	$x_8 = 4, x_{11} = 4$	1
R14	S	$x_8 = 5, x_{11} = 5$	$\frac{1}{2^4}$
R14	P	$x_2 = 9, x_{10} = 9$	1

As the above description, 6 active S-boxes involved in the first round for 24 characteristics. In the 6 active S-boxes, 6 nibbles of subkey of the first round are involved, which are $K_{1,0}, K_{1,1}, K_{1,2}, K_{1,12}, K_{1,13}$ and $K_{1,14}$ respectively. According to the key schedule of PRESENT, 7 bits subkey information is related with the derived 40 bits subkey, so 17 additional bits of subkey in round 1 can be obtained by analyzing the first round. Averagely the result is that the 17 bits of K_1 have 32 possible values. So we can deduce the 57-bit master key according to the key schedule. By exhaustively searching the remaining 23 bits master key, we can find out 80-bit master key. In this step, the time complexity is $32 * 2^{23} = 2^{28}$ times of 16-round PRESENT encryption.

In order to reduce the time of analysis we perform the follow algorithm [11]:

1. For each structure:
   (a) Insert all the ciphertext into the hash table according to the 40-bit ciphertext'bit of the non-active S-boxes in the last round.
   (b) For each entry with collision(a pair of ciphertext with equal 40-bit values) check whether the plaintexts'difference(in round 1) is one of the 24 characteristics's input difference.
   (c) If a pair passes the above test, check whether the difference(in the 24 bits) can be caused by the output difference of the characteristics.

(d) For each possible subkey of K_{17}, we decrypt the last round to obtain the output difference of 2 two active S-boxes for round 15 , and check whether the difference(in the 8 bits) can be caused by the output difference of the characteristics. If a pair passes the above test, add 1 to the counter related to 24 bits of K_{17} and 8 bits of K_{16}.

2. Collect all the subkeys whose counter has at least 48 hits. With the high probability the correct subkey is in this list.
3. Using another set of characteristics, execute from step 1 to step 2, and derive additional 8-bit K_{16}.(It's no need to guess K_{17} for it is known.)
4. For each pair suggesting a value in the list, we complete the subkey of 6 S-boxes of round 1.
5. Exhaustive searching the remaining 23-bit master key, we can obtain the whole 80-bit master key.

4.3 Complexity Estimations

In step (a), the time complexity is 2^{24} memory accesses. In step (b), about 2^7 pairs remain through the filter of step (a), so the time complexity is 2^8 memory accesses. The time complexity of step (c) (d) (e) and step 2 can be ignored for the fewer remaining pairs for each structure. In all, the time in step 1 is 2^{64} memory accesses.

In step 3, the time complexity is also 2^{64} memory accesses.

In step 5, the time complexity is about 2^{28} times of 16-round PRESENT encryption.

According to the relationship between the memory accesses and the encryption time in [4], 2^{65} memory accesses is the main term in the implementing time, so the time complexity is about 2^{65} memory accesses.

In our attack, the ratio of signal to noise is as follows:

$$S/N = \frac{p*2^k}{\alpha*\beta} = \frac{2^{-62}*2^{32}}{2^{33.18-17.25}*2^{17.25-67.32}} = 17.63$$

The success probability is as follows:

$$Ps = \int_{-\frac{\sqrt{\mu S_N}-\Phi^{-1}(1-2^{-a})}{\sqrt{S_N+1}}}^{\infty} \Phi(x)dx = 0.999999939$$

where $a = 32$ is the number of subkey bits involved in the decryption and μ is the number of right pairs which can be obtained

$$\mu = pN = 2^{-62} * 2^{63} * 24 = 48$$

In all, our attack needs 2^{64} chosen plaintexts. The time complexity is 2^{65} memory accesses. The memory requirements are about 2^{32} 6-bit counters and 2^{24} cells for hash table. We can obtain the right key with the probability 0.999999939.

5 Summary

In this paper, we give the differential cryptanalysis on reduced-round variants of PRESENT. We attack 16-round PRESENT using 2^{64} chosen plaintexts, 2^{32} 6-bit counters and 2^{24} hash cells, the time complexity in our attack is about 2^{65} memory accesses.

Although we can't break the whole 32-round PRESENT, but the result provides the starting point for the further research on PRESENT.

References

1. R.J. Anderson, E. Biham and L.R. Knudsen, Serpent: A Proposal for the Advanced Encryption Standard. Available at: http://www.cs.technion.ac.il/biham/Reports/Serpent.
2. E. Biham, O. Dunkelman, N. Keller, The Rectangle Attack - Rectangling the Serpent, Eurocrypt 2001, LNCS2045, pp.340-357, Springer, 2001.
3. A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M.J.B. Robshaw, Y. Seurin and C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher, CHES 2007, LNCS4727, pp.450-466, Springer, 2007.
4. E. Biham and A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, vol.4, no.1, pp.3-72, Springer, 1991.
5. D. Hong, J. Sung, S. Hong, J. Lim, S. Lee, B.-S; Koo, C. Lee, D. Chang, J. Lee, K. Jeong, H. Kim, J. Kim and S. Chee. HIGHT: A New Block Cipher Suitable for Low-Resource Device. In L. Goubin and M. Matsui, editors, Proceedings of CHES 2006, LNCS4249, pp.46-59, Springer, 2006.
6. L.R. Knudsen, Iterative Characteristics of DES and s2-DES, Crypto 1992, LNCS740, pp.497-511, Springer, 1992.
7. C. Lim and T. Korkishko, mCrypton - A Lightweight Block Cipher for Security of Low-cost RFID Tags and Sensors. In J. Song, T. Kwon, and M. Yung, editors, Workshop on Information Security Applications - WISA05, LNCS3786, pp.243-258, Springer, 2005.
8. NIST, A Request for Candidate Algorithm Nominations for the AES, available on-line at http://www.nist.gov/aes/.
9. M.J.B. Robshaw, Searching for Compact Algorithms: cgen. In P.Q. Nguyen, editor, Proceedings of Vietcrypt 2006, LNCS4341, pp.37-49, Springer, 2006.
10. A.A. Selcuk and A. Bicak, On Probability of Success in Linear and Differential Cryptanalysis, SCN 2002, LNCS2576, pp.174-185, Springer, 2003.
11. F.-X. Standaert, G. Piret, N. Gershenfeld and J.-J. Quisquater. SEA: A Scalable Encryption Algorithm for Small Embedded Applications. In J. Domingo-Ferrer, J. Posegga, and D. Schreckling, editors, Smart Card Research and Applications, Proceedings of CARDIS 2006, LNCS3928, pp.222-236, Springer, 2006.
12. D. Wheeler and R. Needham. TEA, a Tiny Encryption Algorithm. In B. Preneel, editor, Proceedings of FSE 1994, LNCS1008, pp.363-366, Springer, 1994.
13. D. Wheeler and R. Needham. TEA extensions. October, 1997. (Also Correction to XTEA. October, 1998.) Available via www.ftp.cl.cam.ac.uk/ftp/users/djw3/.