Flaws in Differential Cryptanalysis of Reduced Round PRESENT

Manoj Kumar*, Pratibha Yadav, Meena Kumari
SAG, DRDO, Metcalfe House, Delhi-110054, India
*mktalyan@yahoo.com

Abstract: In this paper, we have presented flaws in differential cryptanalysis of reduced round variant of PRESENT given by M.Wang in [3] [4] for 80 bits key length and we have shown that it is not possible to recover 32 subkey bits by differential cryptanalysis of 16-round PRESENT as claimed in [3] [4].We have also shown that at the most 30 subkey bits can be recovered by the attack given in [4] after some modifications in the algorithm presented in [3][4].

Keywords: block ciphers, differential cryptanalysis, PRESENT

1. Introduction

PRESENT [2] was proposed by A.Bogdanov et al. in CHES 2007 for extremely constrained environments such as RFID tags and sensor networks. In [3] [4], M. Wang has attacked 16-round PRESENT using 2^{64} chosen plaintexts, 2^{32} 6-bit counters and 2^{64} memory accesses. M.Wang has presented the differential characteristics for r-rounds ($5 \leq r \leq 15$) and she has given differential cryptanalysis of reduced round variant of PRESENT. In this paper, we consider the actual implementation of differential attack against reduced round variant of PRESENT with key length 80 bits and show that the attack can not be implemented practically to recover 32 subkey bits of 80 bit master key. We also show that at the most 30 subkey bits of the 80 bit master key can be recovered after some modifications in the algorithm given in [4].

In this paper, section 2 gives a brief description of PRESENT with key length 80 bits and key schedule for key length 80 bits is also described. In section 3, the differential attack on 16 round PRESENT given by M.Wang [3] [4] is discussed. In section 4, the flaws in differential attack given by M.Wang [3] [4] are presented and it is shown that 32 bits of round subkey can not be recovered practically as claimed in [4] but after some modification in algorithm at the most 30 subkey bits can be recovered by this attack and finally section 5 concludes the paper.

2. Description of PRESENT

PRESENT is an Ultra-Lightweight block cipher. It consists of 31 rounds. It takes plaintext block of length 64 bits and produced ciphertext block of the same length. It supports two key sizes of length 80 bits and 120 bits. Based on the key sizes there are two variants of PRESENT, one is PRESEST-80 with 80-bits key length and other is PRESENT-128 with 128-bits key length. The cipher is described in Figure 1.

2.1 The Encryption Process

Each round of the PRESENT has three layers of operations: *addRoundKey*, *sBoxLayer*, and *pLayer*. The first layer of operations is *addRoundKey* described as follows,

$$b_j \rightarrow b_j \oplus k_{i,j}$$

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

The second layer of operations is *sBoxLayer*. PRESENT uses only one S-box S of length 4-bit which is applied 16 times in parallel in each round. This is given in Table 1.

Figure 1: 31-round PRESENT Encryption Algorithm

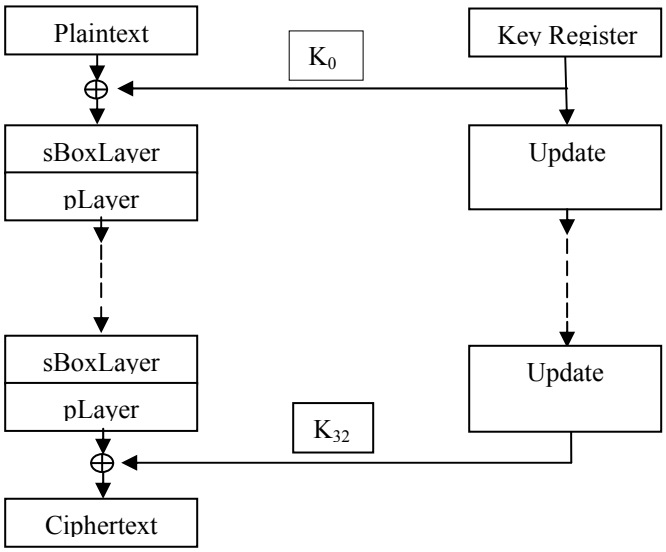


Table 1: Table of S-box

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 layer of operations is *player*, the pLayer is a bit-by-bit permutation given by Table 2. Bit *i* of a stage is moved to bit position P(*i*).

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	38	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

2.2 Key Schedule for Key Length 80 bits

Key register stores the 80 bit key K supplied by the user denoted as $K = k_{79}k_{78}\ldots\ldots k_0$. At round i the 64-bit round subkey K^i consist of the 64 leftmost bits of the current contents of register K, extracted as follows

$$K^i = k^i_{63}\, k^i_{62}\ldots\ldots k^i_0 = k_{79}k_{78}\ldots\ldots k_{16}$$

Then key register $K= k_{79}k_{78}\ldots\ldots k_0$ is updated in the following three steps,

1. $[\, k_{79}k_{78}\ldots\ldots k_0\,] = [\, k_{18}k_{17}\ldots\ldots\ldots k_{20}k_{19}\,]$ left Rotation by 61 bits
2. $[\, k_{79}k_{78}k_{77}k_{76}\,] = S[\, k_{79}k_{78}k_{77}k_{76}\,]$ 4x4 S-box substitution
3. $[\, k_{19}k_{18}k_{17}k_{16}k_{15}\,] = [\, k_{19}k_{18}k_{17}k_{16}k_{15}\,] \oplus$ round_counter

3. Differential Cryptanalysis of Reduced Round PRESENT [4]

M.Wang [3][4] has given differential cryptanalysis for reduced round variant of PRESENT with key length 80 bits with best probability 2^{-62} for 14 rounds differential characteristics.

3.1 Difference pairs of the S-box

The difference distribution table for the S-box of PRESENT is given in Table 3, in which the rows represent ΔX value (in hexadecimal) and columns represent ΔY values (in hexadecimal). Each element of the table represents the number of occurrences of the corresponding output difference ΔY value given the input difference ΔX, besides the special case of both input and output values being 0, the largest value in the table is 4.The smallest value in the table is 0 and occurs for many difference pairs. From table 3, we see that the maximum differential probability is 1/4.

Table 3: Difference distribution table of S-box

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

3.2 Differential Characteristics [4]

M.Wang [3][4] attacked 16-round PRESENT using 14-round differential characteristics. She found 24 14-round differential characteristics. All the characteristics have the same probability 2^{-62}. Out of the 24 differential characteristics, 20 differential characteristics have different input differences but same output difference [5] and 4 pairs of differential characteristics have same input difference but different difference from the output of round 2 to the input of round 8. All the characteristics have the same difference after 8^{th} round. All of the 24 differential characteristics have 2 active S-boxes located in the position 0,1,2,12,13 &14, so the S-boxes in position from 3 to 11 and 15 are all non-active. 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 differences will be 2, 4, 6, 8, 12 or 14. In all possible output differences the least significant bit of their output differences is zero, so at most 6 bits are non zero for the output difference of S-boxes in round 15. After pLayer of round 15, the maximum number of active S-boxes for round 16 is 6 and minimum number of active S-boxes is 2.

Considering 6 S-boxes in round 16 namely x_4, x_6, x_8, x_{10}, x_{12} and x_{14}, Wang[3][4] has claimed to recover 24 bits of round subkey K^{17} namely $k_{17,4}$, $k_{17,20}$, $k_{17,36}$, $k_{17,52}$, $k_{17,6}$, $k_{17,22}$, $k_{17,38}$, $k_{17,54}$, $k_{17,8}$, $k_{17,24}$, $k_{17,40}$, $k_{17,56}$, $k_{17,10}$, $k_{17,26}$, $k_{17,42}$, $k_{17,58}$, $k_{17,12}$, $k_{17,28}$, $k_{17,44}$, $k_{17,60}$, $k_{17,14}$, $k_{17,30}$, $k_{17,46}$, $k_{17,62}$ and 8 bits of round subkey K^{16} namely $k_{16,0}$, $k_{16,8}$, $k_{16,16}$, $k_{16,24}$, $k_{16,32}$, $k_{16,40}$, $k_{16,48}$, $k_{16,56}$ taking one set of differential characteristic and taking another set of differential characteristics it has been claimed to recover additional 8 subkey bits $k_{16,2}$, $k_{16,10}$, $k_{16,18}$, $k_{16,26}$, $k_{16,34}$, $k_{16,42}$, $k_{16,50}$, $k_{16,58}$ of round subkey K_{16}. In total, it has been claimed to recover 57 bits of 80-bit master key on the basis of these 40 bits of subkey K_{16} and K_{17}.

For getting right pairs for cryptanalysis, xor of ciphertext bits corresponding to non-active S-boxes x_0, x_1, x_2, x_3, x_5, x_7, x_9, x_{11}, x_{13}, x_{15} should be zero. After finding right pairs, ciphertext bits of right pairs corresponding to active S-boxes in the last two rounds will be decrypted. 24 bits of round subkey K_{17} and 8 bits of round subkey K_{16} will be involved during decryption from round 16 to round 14.

4. Flaws in Differential Cryptanalysis

We have found that 32 subkey bits as claimed in [4] can not be recovered by the attack described in [4]. We can recover 24 bits of round subkey K^{17} and 6 bits of round subkey K^{16}. At the most 30 subkey bits can be recovered by this attack given in [4].

4.1 Recovery of 32 Subkey bits-an impossible task

In round 16, 24 ciphertext bits corresponding to 24 bits of round subkey K_{17} are extracted and x-ored with all possible values of 24 bits of round subkey K_{17}, after that inverse pLayer is applied.

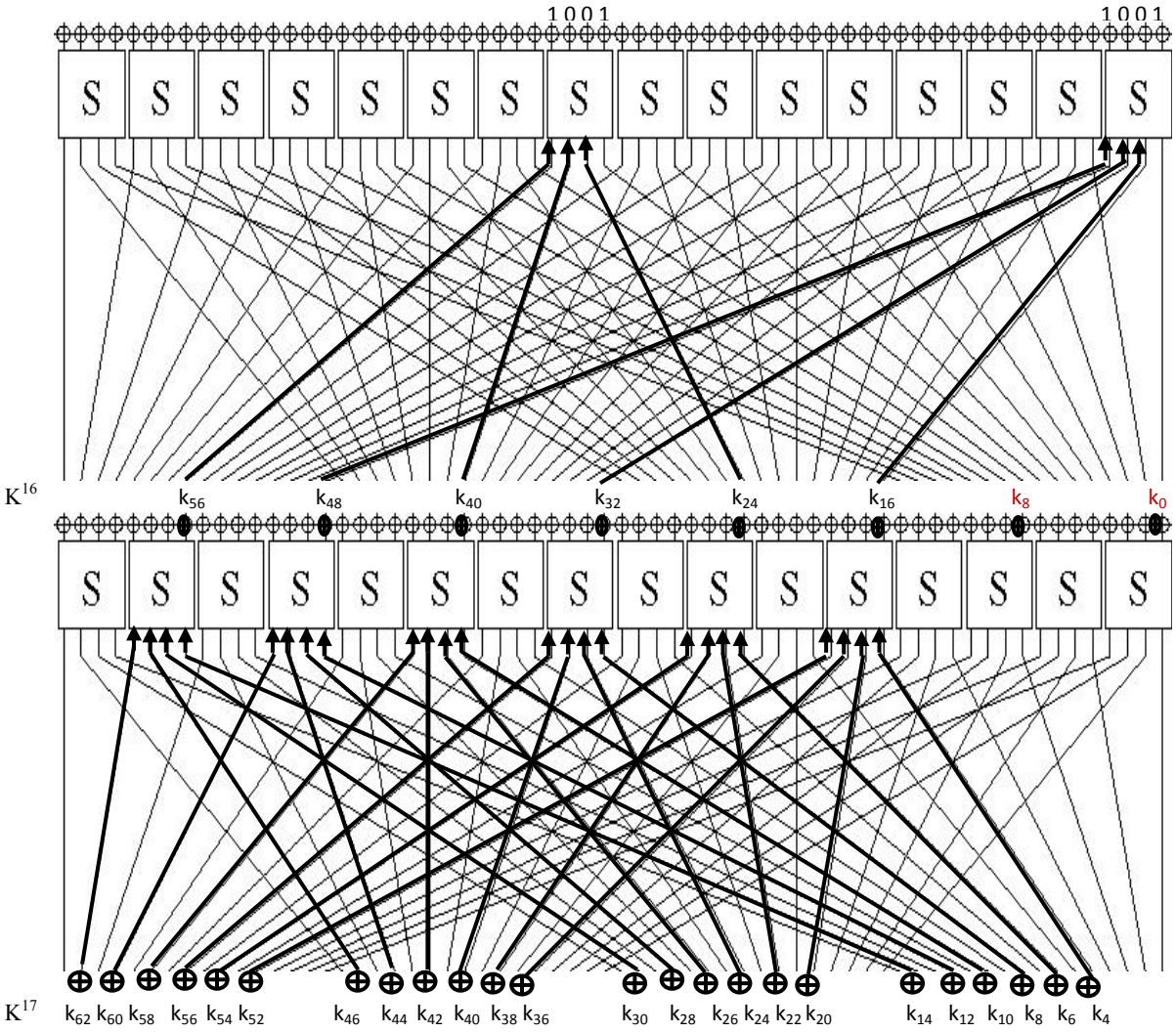
After applying inverse pLayer, the intermediate 24 ciphertext bits are namely $C_{16},C_{17},C_{18},C_{19}$, $C_{24},C_{25},C_{26},C_{27}$, $C_{32},C_{33},C_{34},C_{35}$, $C_{40},C_{41},C_{42},C_{43}$, $C_{48},C_{49},C_{50},C_{51}$, C_{56},C_{57}, C_{58},C_{59}, which will be passed through inverse S-box .

In round 15, we can extract at the most 6 intermediate ciphertext bits corresponding to 6 bits of round subkey K_{16} after getting 24 intermediate ciphertext bits from previous round. Extract the 6 ciphertext bits and x-or these with all possible values of 6 bits of round subkey K_{16} and apply inverse pLayer.

After applying inverse pLayer, only 6 intermediate ciphertext bits namely C'_1, C'_2, C'_3, C'_{33}, C'_{34}, C'_{35} are available to be passed through inverse S-box. But in practice, we need 4 bits to pass through one S-box because PRESENT uses one 4 bit to 4 bit S-box 16 times in parallel, which take 4 bits as input and produces 4 bits as output. These 6 bits can not be grouped together to pass through inverse S-box.

We need bits at position C'_0 and C'_{36} to complete the 4 bits set to pass through inverse S-box. For getting these two bits, we need to decrypt additional 8 bits from 16^{th} round. But this is not possible due to output of S-box in 15^{th} round; the possible outputs of 15^{th} round for input difference 1001 are all even with at the most 6 non zero bits, which leads to only 6 active S-boxes in 16^{th} round in place of our requirement of 8 active S-boxes in 16^{th} round. This is shown graphically in figure 3.

Figure 3: Flaws in differential attack on 16 reduced round PRESENT (Computational Graph)



4.2 Recovering 30 Subkey bits

For recovering 30 subkey bits, decrypt from round 16 to round 14 as follows:
Extract 24 bits of ciphertext corresponding to 24 bits of round subkey K^{17} namely $k_{17,4}$, $k_{17,20}$, $k_{17,36}$, $k_{17,52}$, $k_{17,6}$, $k_{17,22}$, $k_{17,38}$, $k_{17,54}$, $k_{17,8}$, $k_{17,24}$, $k_{17,40}$, $k_{17,56}$, $k_{17,10}$, $k_{17,26}$, $k_{17,42}$, $k_{17,58}$, $k_{17,12}$, $k_{17,28}$, $k_{17,44}$, $k_{17,60}$, $k_{17,14}$, $k_{17,30}$, $k_{17,46}$, $k_{17,62}$ and xor these with all possible values of 24 subkey bits, and then apply inverse permutation layer and inverse S-box. After that extract 6 intermediate ciphertext bits corresponding to 6 bits of round subkey K^{16} namely $k_{16,16}$, $k_{16,24}$, $k_{16,32}$, $k_{16,40}$, $k_{16,48}$, $k_{16,56}$ and xor these with all possible values of 6 subkey bits and then apply inverse permutation layer. Now for each intermediate ciphertext pair assume the values of additional two bits as 00 and 11 one by one, to complete set of 4 bits to be passed through inverse S-box. After that apply inverse S-box and find out xor of the two decrypted pairs then check whether it is the same xor as suggested by the characteristics. If it is the same xor value then increase the counter of the corresponding key value by 1 and the key giving the desired xor value maximum number of times will be our correct value of the 30 subkey bits.

4.3 Computational Complexity

As given in [4], 2^{40} structures of 2^{24}chosen plaintext each are required in this attack. 2^{40} possible values can be taken as inputs to 10 non-active S-boxes in each structure and the inputs to any two active S-boxes in each structure characteristic among the six S-boxes have 2^{24} possible values. The number of pairs for each possible characteristic is $2^{40}*2^{16}*2^{7}=2^{63}$. The number of pairs satisfying 24 characteristics is $2^{63}*20 = 2^{67.32}$. Since each characteristic has the same probability 2^{-62}, so there are $2^{63}*2^{-62}*24 = 48$ right pairs satisfying any one characteristic. For each structure, there is $(2^{24})^2/2 = 2^{47}$ possible pairs, thus we have to consider total $2^{47}.2^{40}=2^{87}$ pairs of plaintext.

For each structure, each pair should have 10 non-active S-boxes in round 16 satisfying each characteristic. After discarding wrong pairs, $2^{47}*2^{-40}=2^{7}$ candidates for right pair remain for each structure.

Among 16 S-boxes in round 16, 10 S-boxes must be non-active. Among the remaining 6 S-boxes in round 16, we will consider 6 cases according to the output of the S-box in round 15. As input to round 15 S-box is 9, so the possible outputs will be 2, 4, 6, 8, C, E according to S-box difference distribution table.

- If output is 2, the active S-boxes in round 16 will be x_4 and x_6.
- If output is 4, so the active S-boxes in round 16 will be x_8 and x_{10}.
- If output is 8, so the active S-boxes in round 16 will be x_{12} and x_{14}.
- If output is 6, so the active S-boxes in round 16 will be x_4, x_6, x_8 and x_{10}.
- If output is C, so the active S-boxes in round 16 will be x_8, x_{10}, x_{12} and x_{14}.
- If output is E, so the active S-boxes in round 16 will be x_4, x_6, x_8, x_{10}, x_{12} and x_{14}.

In first three cases, there are 2 active S-boxes and 4 non-active S-boxes. In next two cases, there are 4 active S-boxes and 2 non-active S-boxes and in last case all 6 S-boxes are active. If an S-box is active, the input difference to this S-box should be 1 and output

difference will be 3, 7, 9 or 13 and if S-box is non-active then input and output differences will be 0. Using this filter, discard any pair with a wrong output difference. So the numbers of remaining pairs for each structure are about:

$$2^7*\{3*(4/16)^2(1/16)^4 +2*(4/16)^4\ (1/16)^2+ (4/16)^6\} = 2^7*2^{-11.81} = 2^{-4.81}$$

For each structure, it is checked that if the remaining pair satisfy one of the 24 possible plaintext differences corresponding to 24 characteristic. Number of remaining pairs is a fraction of about $2^{-24}*20 = 2^{-19.68}$ out of the 2^{24} possible plaintext differences. So the expected number of remaining pairs in all 2^{40} structures is $2^{40}*2^{-4.81}*2^{-19.68} = 2^{15.5}$.

We guess the 24 bits of round subkey K^{17} and 6 bits of round subkey K^{16} and decrypt the remaining ciphertext pairs from round 16 to round 14. There are at most 4 pairs of occurrences for the input difference and output difference, according to the difference distribution table of PRESENT. Average count per counted pair of the subkey is 4, corresponding to one active S-box. There can be 2, 4 or 6 active S-boxes in round 16. We denote number of active S-boxes in round 16 by t and consider 3 cases according to the value of t:

- If t = 2, the number of ciphertext pairs satisfying the condition of two active S-boxes is $2^{15.5}*2^{-16} = 2^{-0.5}$, so the total counted times of subkey for the remaining pairs are about $2^{-0.5}*4^4 = 2^{7.5}$
- If t = 4, the number of ciphertext pairs satisfying the condition of two active S-boxes is $2^{15.5}*(2^{-8}- 2^{-12}) = 2^{7.41}$, so the total counted times of subkey for the remaining pairs are about $2^{7.41}*4^6 = 2^{19.41}$
- If t = 6, the number of ciphertext pairs satisfying the condition of two active S-boxes is $2^{15.5}*(1-2^{-4}) = 2^{15.41}$, so the total counted times of subkey for the remaining pairs are about $2^{15.41}*4^8 = 2^{31.41}$

The total counted times of subkey are $2^{7.5} + 2^{19.41} + 2^{31.41} = 2^{31.4104}$, on average wrong subkey will hit about $2^{31.4104}/2^{30}= 2.66$ times, but the right key can be easily identified because it is counted for the right pairs about 48 times. We can retrieve 30 subkey bits using at most $2^{33.18}$ times 2-round PRESENT encryptions and 2^{30} 6-bit counters.

We can find out 80 bit master key by exhaustively searching the remaining 50 bits of master key and the time complexity in this step will be 2^{50} 16 round PRESENT encryptions.

In modified attack, the signal to noise ratio will be [1]

$$S/N = (p*2^k) / (a*b) = 2^{-62}*2^{30} / (2^{31.41\ -15.5}*2^{15.5-67.32}) = 15.03$$

For the number of right pairs $\mu = p\ N = 2^{-62}*2^{63}*24 = 48$ which can be obtained and k=30 subkey bits involved in decryption from round 16 to round 14, the success probability[1] is:

$$P_s = 0.999999904397237$$

We can obtain 30 subkey bits with the probability 0.999999904. Time complexity is almost same as in [4], except the time complexity of 2^{50} 16-round PRESENT encryptions in step 3 of the algorithm presented in [4].

5.Conclusion

In this paper, we have shown that practical implementation of differential cryptanalysis of reduced round PRESENT to recover 32 subkey bits of 80 bit master key, as claimed in[3][4] is not possible. We have also shown that we can recover at the most 30 subkey bits by the attack proposed in [4] after some modification in the key recovery algorithm given in [4].

Acknowledgments: Authors are grateful to **Dr. PK Saxena** for his valuable guidance and support. Authors are also thankful to **Ms. Noopur Shrotriya** for her support in implementation. Special thanks are due for **Mr. Dhananjoy Dey** for giving his valuable time in fruitful discussions and **Mr. N. Rajesh Pillai** for his valuable suggestions to improve the paper.

References

[1] A.A. Selcuk and A. Bicak, On Probability of Success in Linear and Differential Cryptanalysis, SCN 2002, LNCS2576, pp.174-185, Springer, 2003.

[2] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y.Seurin, C. Vikkelsoe, PRESENT: An Ultra-Lightweight Block Cipher, in the proceedings of CHES 2007, Lecture Notes in Computer Science, vol 4727, pp 450-466,Vienna, Austria, September 2007.

[3] M. Wang, Differential cryptanalysis of PRESENT, Cryptology ePrint Archive, Report 2007/408, 2007. http://eprint.iacr.org/2007/408.

[4] M. Wang, Differential Cryptanalysis of Reduced-Round PRESENT, in the proceedings of AFRICACRYPT 2008, Lecture Notes in Computer Science, vol. 5023, pp 40-49, Casablanca, Morocco, June 2008.

[5] M. Wang. Private communication: 24 differential characteristics for 14-round PRESENT we have found, 2009.