Cryptanalysis with Ternary Difference: Applied to Block Cipher PRESENT

Farzaneh Abazari*, Babak Sadeghian**
* Department of Computer Engineering and IT, Amirkabir University of Technology, f.abazari@aut.ac.ir
** Department of Computer Engineering and IT, Amirkabir University of Technology, basadegh@aut.ac.ir

Abstract: *Signed difference approach was first introduced by Wang for finding collision in MD5. In this paper we introduce ternary difference approach and present it in 3 symbols. To show its application we combine ternary difference approach with conventional differential cryptanalysis and apply that to cryptanalysis the reduced round PRESENT. We also use ant colony technique to obtain the best differential characteristic. To illustrate the privilege in the result of experiment, we calculate advantage of the attack.*

Keywords: ternary difference cryptanalysis; signed difference; lightweight block cipher PRESENT;

1. Introduction

Differential cryptanalysis was proposed by Biham and Shamir in [1]. It considered the relation between input and output differences for each S-box. Signed difference is first employed by Wang in [3] for finding collision in MD5. In contrast to XOR difference, signed difference is based on modular integer subtraction. In this paper we inspire from Wang's idea and introduce the concept of using ternary difference that is presented in three symbols 0, 1 and 2 and apply it for cryptanalysis of block cipher. To analyze the security of cryptosystems with our approach, we choose PRESENT as a light weight block cipher.

In this paper, we propose a new approach of cryptanalysis that helps us to analyze cryptosystems. In addition, we apply our method for the cryptanalysis of PRESENT as a lightweight block cipher.

Our proposed approach has a key-dependent characteristic. In the first round, the characteristic is affected by keys, so for the second round, there is key-dependent characteristic as an input. In [7], [9] characteristics of key-dependent S-boxes is introduced, and they have cryptanalyzed the block ciphers Twofish, IDEA. In all of them, they choose a specific characteristic to eliminate the effect of key dependency. In this paper, although we have a key-dependent characteristic but we overcome this problem by mapping ternary difference to xor difference.

The remainder of this paper is organized as follows. Section 2 introduces our ternary difference approach and its application. Section 3 describes the description of PRESENT block cipher. We propose our novel approach in Section 4. In addition, we combine the result of cryptanalysis for PRESENT reduced to 6, 7 and 8 rounds with our new approach in section 5. The signal to noise ratio is calculated in section 6. Section 7 concludes this paper.

2. Ternary Difference

Suppose a and a', are two variables, each of them is of n bits, and present in binary string:

$$a=(a_{n-1},a_{n-2},...,a_0), a'=(a'_{n-1},a'_{n-2},...,a'_0)$$

The conventional xor difference that is used in the differential cryptanalysis is:

$$\Delta_i^{\oplus} = a_i - a'_i \bmod 2^n = xor(a_i,a'_i)$$

The signed difference of a and a' according to [2] is defined to be:

$$\Delta^{\pm}=(r_{n-1},r_{n-2},...,r_0)$$

where $r_i \in \{-,0,+\}$ for $i \in \{0,...,n-1\}$ and

$$r_i=\begin{cases} + & if \;\; a_i=1,a'_i=0 \\ - & if \;\; a_i=0,a'_i=1 \\ 0 & if \;\; a_i=a'_i \end{cases}$$

Definition: Our ternary difference for two variables, each of them is of *n* bits, and present in binary string is defined to be:

$$a=(a_{n-1},a_{n-2},...,a_0), a'=(a'_{n-1},a'_{n-2},...,a'_0)$$

$$\Delta^{*}=(t_{n-1},t_{n-2},...,t_0)$$

where $t_i \in \{0,1,2\}$ for $i \in \{0,...,n-1\}$ and

$$t_i=\begin{cases} 0 \;\; if \;\; a_i=0,a'_i=0 \\ 1 \;\; if \;\; a_i=1,a'_i=1 \\ 2 \;\; if \;\; a_i=0,a'_i=1 \;\; or \;\; a_i=1,a'_i=0 \end{cases}$$

The differences which are defined above are shown in below table:

Input \ Difference		$\Delta^{\oplus}$ Conventional Xor Differential	$\Delta^{\pm}$ Signed Difference	Δ^{*} Ternary Difference
0	0	0	0	0
0	1	1	-	2
1	0	1	+	2
1	1	0	0	1

We form new profile for PRESENT's S-box that are 4×4 and call it ternary difference profile. It contains $3^4 \times 3^4$ cells (3 values contain 0, 1, 2) that each one demonstrates the probability of $\Delta^{*}_{in} \rightarrow \Delta^{*}_{out}$. The ternary difference profile seems to be better than conventional difference profile from an attacker point of view, due to the number of cells with probability 1 and 0.
Number of cells with Prob= 1 are 48.
Number of cells with Prob= 0 are 6352.

Theorem: The minimum number of cells with probability one in ternary difference profile for each S-box with 4 input bits is 48.

Proof: Cells with probability one divide in 2 groups:
1) Differences which contain digits with value 0 or 1 have only one output difference. They are 2*2*2*2=16 cells.
2) Differences which contain one digit with value 2 have only one output difference too. They are 4*8=32 cells. So, the minimum number of cells with probability one in ternary difference profile is 16+32=48.□

The below tables show part of ternary difference profile for PRESENT's S-box. They demonstrate three lines of ternary difference profile with 1, 2 and 3 digits of 2 for their input.

TABLE 1. TERNARY DIFFERENCE WITH 3 DIGITS OF 2

In \ Out	...	0211	**0212**	...	**1021**	...	**1102**	...	2221	**2222**
0222	0	0	**0.25**	0	**0.25**	0	**0.25**	0	0	**0.25**

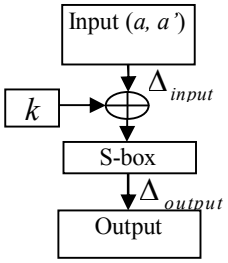
TABLE 2. TERNARY DIFFERENCE WITH 2 DIGITS OF 2

In \ Out	.....	2021	**2022**	....	**2101**	2102	.....
0221	0	0	**0.5**	0	**0.5**	0	0

TABLE 3. TERNARY DIFFERENCE WITH 1 DIGIT OF 2

In \ Out	.....	2211	**2212**	2220	.....
0012	0	0	**1**	0	0

According to the above tables, for those differential inputs with one digit of 2, probability of passing S-box is one. In contrast, the conventional xor profile has only one cell with probability equal to one. Let's illustrate the point with an example:



Suppose the above diagram:

1) In Differential Cryptanalysis:

$$\left.\begin{array}{l} a = 0010 \\ a' = 1010 \end{array}\right\} \Delta^{\oplus}_{input} = 1000$$

$$\Delta^{\oplus}_{output} = (0011, 0111, 1001, 1011, 1101, 1111)$$

2) In Ternary Differential Cryptanalysis:

$$\left.\begin{array}{l} a = 0010 \\ a' = 1010 \end{array}\right\} \Delta^{*}_{input} = 2010$$

Guess the key (Just for those input's digit with value 0 or 1): X000

$$\Delta^{*}_{input} = 2010 \xrightarrow{guessed\ key\ k = X000}$$

$$\Delta^{*}_{output} = 2112$$

Ternary difference can be transferred to a conventional one by changing bits with value 2 to 1 and 0, 1 to 0. In other words, ternary difference conveys more information than conventional difference.

As we are going to apply our new method for the cryptanalysis of PRESENT, in the following section we briefly describe it.

3. Description of PRESENT [4]

3.1 The Encryption Process

PRESENT is a 31-round Ultra-Lightweight block cipher. The block length is 64 bits. PRESENT uses only one 4-bit S-box 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

$$b_j \rightarrow b_j \oplus k^i_j$$

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

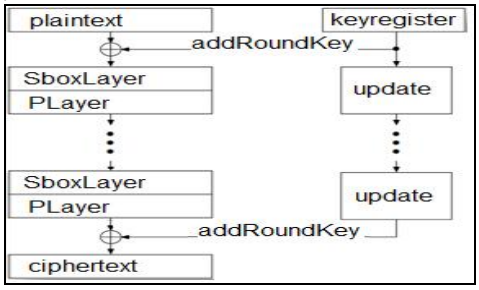


Figure 1. PRESENT

The second stage is sBoxLayer which consists of 16 parallel 4 bits to 4 bits S-boxes, which is given in table 5.

The third stage is the bit permutation pLayer, which is given by table 6. From pLayer, bit position i is moved to bit position $P(i)$.

TABLE 4. SBOXLAYER

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

TABLE 5. 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

In [11], [12], [13], [14] and [15] attacks on PRESENT are presented. Following results are the best characteristics in differential cryptanalysis from [11].

TABLE 6. PROBABILITY OF THE BEST CHARACTERISTICS[11]

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

3.2 The Key Schedule

PRESENT's key schedule can take key sizes as 80 bits or 128 bits. We will cryptanalyze 128 bits version. Although considering key schedule may help to have better result but we assume that subkeys are independent.

4. Cryptanalysis with Ternary Difference

In our approach we take advantage of the ternary difference and the conventional xor-difference. One of the main differences between ternary difference cryptanalysis and differential cryptanalysis is the target subkey. In differential cryptanalysis, most of the time the last round's subkey is targeted, while, in ternary difference cryptanalysis the first round's subkey is targeted. The procedure of the ternary differential cryptanalysis is as follows:

Step1) Obtaining the first round ternary input difference that preserves some conditions, describe in section 4.1.

Step 2) Obtaining the best differential characteristics for r-1 last rounds as describe in section 4.2.

Step 3) Developing a similarity algorithm according to the output characteristics from step 2 that assigns a number to each input difference proposed in step 1. Each input difference suggests different subkey for the first round, which are sorted and ranked according to the similarity algorithm output.

4.1 Step 1

We begin by obtaining a suitable ternary difference for the first round and a suitable xor-difference for the remaining rounds. Our goals are:

A) To have more probable characteristics for the r-1 last rounds of block cipher, we should have more S-boxes with $\Delta^{\oplus} = 0$ input to the second round.

B) To have input difference with more ternary difference digits of 2, for requiring less number of key bits in the first round subkey to guess.

To achieve the goal A, most ternary difference digits of input to the first round must be 0 or 1, while, to achieve the goal B, most ternary difference digits of input to the first round must be 2. The best trade-off is achieved based on a experimental observation on the ternary difference profile. In PRESENT when a ternary input difference has two digits of 2 and two digits of 0 or 1, the best trade-off happens. Thus, after the permutation, there are more S-boxes with $\Delta^{\oplus} = 0$ as an input to the second round, also less key bits to guess in the first round. The position of bits with value 2 that causes the best result is obtained based on the PRESENT's TDP. The most likely difference happens when $\Delta^{*}_{s-box(in)} = 1022$ and Δ^{*}_{out} is either 1112 or 2022 for each S-box. Hence, the ternary input difference for the first round of the block cipher, which causes $\Delta^{*}_{s-box(out)} = 1112$ as the output difference of the first round's S-boxes, must be founded. In other words, the first round characteristic must be founded. Actually, the correct input difference will be found by searching exhaustively through input pairs that have the same first two bits and different last two bits, e.g. 0110 and 0101, which have $\Delta^{*} = 0122$. There are 16 S-boxes; the first two bits in each S-box produce 4 different input differences (4^{16}) and the last two bits parity produce 2 different input differences (2^{16}). Hence, the cryptanalysis needs $2^{32}*2^{16}=2^{48}$ plaintexts.

If the above condition is hold true, then the input difference to the second round would be:

TABLE 7. INPUT TO ROUND 2

Sbox No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Input Diff R=2	15	15	15	15	0	0	0	0	0	0	0	0	0	0	0	0

4.2 Step2

In this step the best characteristics for r-1 last rounds with constant input difference must be obtained. In [6] a model for finding suitable differential characteristics with applying intelligent techniques was introduced. Ant-colony optimization (ACO) technique is a random optimization technique where a colony of artificial ants cooperates in finding good solutions to difficult discrete optimization problems. Cooperation is a key design component of ACO algorithms: The choice is to allocate the computational resources to a set of relatively simple agents that communicate indirectly. Good solutions are an emergent property of the agent's cooperative interaction. We use that technique to find characteristics for r-1 last rounds of PRESENT.

4.3 Step3

By applying the method of [6], the most probable characteristic with fixed input difference (Table 4) can be founded. The last round's input characteristics are

analyzed and the probable output characteristics are obtained. The similarity algorithm is according to the probable characteristics. Then, in this step the similarity between the output of the probable characteristic and the output of the specific ternary input difference must be calculated. In this part we propose the similarity algorithm that depends on the number of rounds which are attacked. The inputs of the similarity algorithm are:

1) The output differences for each ternary input difference

2) The probable outputs

The output of the similarity algorithm is a criteria number for each output difference of the ternary input difference. So the ternary input difference can be sorted by the criteria number. Each ternary input difference suggests first two key bits and parity of last two key bits in each four bits of the key.

5. Experiment

Let's introduce some notations from [5]. If an attack on *m* bit key gets the correct value ranked among the top '*r*' out of 2^m possible candidates, it is said that the attack obtained *a* bits "advantage" over exhaustive search, where $a=m - log\ r$. '*N*' is the number of chosen plaintext and '*a*' is the advantage of an attack.

In the following sections cryptanalysis of 6, 7 and 8 rounds of PRESENT are explained.

5.1 Cryptanalysis of 6 rounds of PRESENT

As it is mentioned in 4.2, it is considered to have a differential characteristics for r-1 last rounds. The ant colony algorithm run and probable characteristics are obtained. The result of the cryptanalysis 6 rounds PRESENT is shown in the below:

- Number of rounds = r-1 = 6-1=5
- Number of ants =100000

Result of the ant colony algorithm

The best characteristic has:

- Total Active S-box = 12
- Total Cost = $2^{(-24)}$

The probable last round differential characteristics are as follow:

InMask	1	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0
OutMask	3	3	0	0	0	3	0	0	0	0	0	0	3	0	0	0

InMask	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0
OutMask	7	13	0	0	0	0	0	0	13	9	0	0	0	0	0	0

InMask	4	0	0	4	0	0	0	0	0	0	0	0	4	0	0	4
OutMask	5	0	0	5	0	0	0	0	0	0	0	0	5	0	0	5

From the above probable characteristics, we consider 4 and 1 in the input to the last round. The xor profile for the differences 1 and 4 of PRESENT's S-box are as follow:

TABLE 8. XOR PROFILE FOR PRESENT(INPUT DIFF.=1 & 4)

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	0	0	0	¼	0	0	0	¼	0	¼	0	0	0	¼	0	0
4	0	0	0	0	0	¼	⅛	⅛	0	⅛	⅛	0	⅛	0	⅛	0

The above table shows that output difference with values 3, 5, 7, 9, D have probabilities=¼ or more and output differences with values 6, A, C, E have less probability. Therefore, the similarity algorithm that is a ranking procedure is as follow. This algorithm assigns a criteria number to each input difference and as a consequence to each possible key. MaskOut is a hexadecimal output value for each S-box.

```
for(Sbox(0) to Sbox(15)){
//more probable (criteria = c)
if(maskOut==D || maskOut==9 || maskOut==3 || maskOut==7||
maskOut==5)
        c=c+30;
//less probable
else if(maskOut==6 || maskOut==A || maskOut==C ||
maskOut==E)
        c=c+20;
// dispensable probability
else
        c=c-10;}
```

Similarity algorithm for 6 rounds

Parts of the algorithm's result for 2^{48} plaintexts are shown below:

```
maskIn: 0022002200220022002200220022002200220022002200220022002201220122
maskOut:1101110111111110110101010011001101011010101000000100110101011 1
criteria:290
maskIn: 0022002200220022002200220022002200220022002200220022002201221122
maskOut:1100100000001111100000000011111000110101100001011111101111001101
criteria 280
maskIn: 0022002200220022002200220022002200220022002200220022002211221022
maskOut:0001100001011011110000000011000100011000000000001111110010100 10
criteria 270
maskIn: 0022002200220022002200220022002200220022002200220022002211221122
maskOut:0010100101010010010110011011000011100111001111001001101001110 0
criteria 310
```

The ranking procedure is applied to 2^{48} pair and the correct pair is ranked in top $0.0123 * 2^{48}$ pairs. So this experiment according to formula $a=m - log\ r$ has 7 bits advantage than exhaustive search.

The correct key has criteria equal to 240.

Experimental Result:

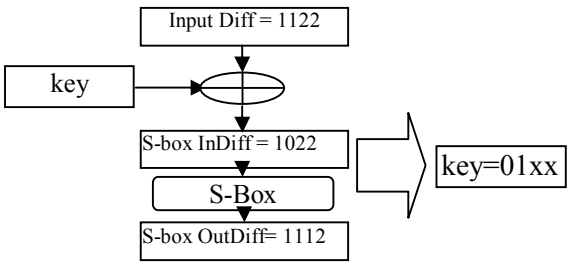
$N = 2^{48}$ (calculate in 4.1)

m = 48 (key bits= 32(first two bits)+16(parity of last two bits))

$rank = 0.0123 * 2^{47}$

$a=m - log\ r \approx 7$ bits

After obtaining the ternary input difference, the key bits for one S-box are calculated as follow: The S-box input difference is equal to 1022 according to section 4.1. The input pair is 1101 and 1110, so the parity of the last two bits of the key is 0.



5.2 Cryptanalysis of 7 rounds PRESENT

The result of the cryptanalysis 7 rounds PRESENT is shown in the below:

- Number of rounds = r-1 = 7-1=6
- Number of ants =100000

Result of the ant colony algorithm

The best characteristic has:

- Total Active S-box = 14
- Total Cost = $2^{(-28)}$

The probable last round differential characteristics are as follow:

InMask 3 0 3 0 0 0 0 0 3 0 3 0 0 0 0 0
OutMask 6 0 6 0 0 0 0 0 6 0 6 0 0 0 0 0

InMask 9 0 9 0 0 0 9 0 0 0 0 0 9 0 0 0
OutMask 14 0 14 0 0 0 14 0 0 0 0 0 14 0 0 0

InMask 9 0 9 0 0 0 0 0 9 0 9 0 0 0 0 0
OutMask 6 0 14 0 0 0 0 0 4 0 4 0 0 0 0 0

From the above probable characteristics, 3 and 9 are considered for the input of the last round. The xor profile for differences 3 and 9 of PRESENT's S-box are as follow:

TABLE 9. XOR PROFILE FOR PRESENT

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
9	0	0	⅛	0	¼	0	⅛	0	⅛	0	0	0	⅛	0	¼	0
3	0	⅛	0	⅛	⅛	0	¼	⅛	0	0	⅛	⅛	0	0	0	0

The above table shows that the output differences with value 4, 6, E has higher probability and the output differences with value 1,2,3,7,8 have less probability. Also 9 is more probable than 3 as an input to last round, so those bits with less probability in 9 are considered for evaluating. Therefore, the similarity algorithm that is a ranking procedure is as follow.

```
for(Sbox(0) to Sbox(15)){
//more probable (criteria = c)
if(maskOut==4 || maskOut==6 || maskOut==E)
        c=c+30;
//less probable
else if(maskOut==2 || maskOut==8|| maskOut==C )
        c=c+20;
// dispensable probability
else
        c=c-10 ;}
```

Similarity algorithm for 7 rounds

The correct key has criteria equal to 300.
Experimental Result:
$N = 2^{48}$
$m = 48$
$rank = 0.041 * 2^{47}$
$a \approx 6$ bits

5.3 Cryptanalysis of 8 rounds of PRESENT

The result of cryptanalysis 8 rounds PRESENT is shown in the below:

- Number of rounds = r-1 = 8-1=7
- Number of ants =100000

The result of ant colony algorithm
Best characteristic has:

- Total Active S-box = 16
- Total Cost = $2^{(-32)}$

The probable last round differential characteristics are as follow:

InMask 0 0 0 0 0 3 0 0 3 0 3 0 0 0 0 0
OutMask 0 0 0 0 0 10 0 0 11 0 4 0 0 0 0 0

InMask 0 0 0 0 0 0 0 0 5 0 5 0 0 0 0 0
OutMask 0 0 0 0 0 0 0 0 12 0 12 0 0 0 0 0

InMask 0 0 0 0 0 0 0 0 3 0 3 0 0 0 0 0
OutMask 0 0 0 0 0 0 0 0 6 0 6 0 0 0 0 0

From the above probable characteristics, we consider 3 and 5 in the input of the last round. The xor profile for differences 3 and 5 of PRESENT's S-box are as follow:

TABLE 10. XOR PROFILE FOR PRESENT

X	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
3	0	⅛	0	⅛	⅛	0	¼	⅛	0	0	⅛	⅛	0	0	0	0
5	0	⅛	0	0	⅛	0	0	0	0	⅛	⅛	⅛	¼	⅛	0	0

The above table shows that the output differences with value 1, 4, 6, A, B, C have probabilities=¼ and others have less probability. Therefore, the similarity algorithm that is a ranking procedure is as follow.

```
for(Sbox(0) to Sbox(15)){
//more probable (criteria = c)
if(maskOut==1 || maskOut==4 || maskOut==6 || maskOut==A||
maskOut==B||maskOut==C)
        c=c+30;
// dispensable probability
else
        c=c-10 ;}
```

Similarity algorithm for 8 rounds

The correct key has criteria equal to 280.
Experiment Result:
$N = 2^{48}$
$m = 48$
$rank = 0.0398 * 2^{47}$
$a \approx 5$ bits

6. Complexity

In our approach, each pair with ternary input and output difference suggests less possible key bits than conventional difference. This helps to have a better signal to noise ratio as we calculate it in follow.

The signal to noise ratio is defined as the proportion of the probability of the correct key being suggested by a correct pair to the probability of a random key being suggested by a random pair with the initial difference. According to [10], the signal to noise ratio can be computed by the following formula:

$$S/N = \frac{2^k \times p}{\alpha \times \beta}$$

Where k is the number of guessed key bits, p is the probability of the differential characteristic, α is the average number of keys suggested by a counted pair, and β is the ratio of the counted pairs to all pairs (both counted and discarded).

$$6\ Round \rightarrow S/N = \frac{2^k \times p}{\alpha \times \beta} = \frac{2^{48} \times 2^{-24}}{1 \times \frac{2^{40}}{2^{47}}} = \frac{2^{24}}{2^{-7}} = 2^{31}$$

$$7\ Round \rightarrow S/N = \frac{2^k \times p}{\alpha \times \beta} = \frac{2^{48} \times 2^{-28}}{1 \times \frac{2^{41}}{2^{47}}} = \frac{2^{20}}{2^{-6}} = 2^{26}$$

$$8\ Round \rightarrow S/N = \frac{2^k \times p}{\alpha \times \beta} = \frac{2^{48} \times 2^{-32}}{1 \times \frac{2^{42}}{2^{47}}} = \frac{2^{16}}{2^{-5}} = 2^{21}$$

The results show the correctness of our approach.

7. Conclusion

We propose a new cryptanalytic technique combining differential cryptanalysis and ternary difference approach. We show that this technique can be effectively used to attack block ciphers. Ternary difference may offer some advantages when compared to differential cryptanalysis. In conventional differential cryptanalysis, bits with value 0 don't have useful information for recovering the key. In the other hand, in ternary differential cryptanalysis, digits with value 0 and 1 contain key bit value.

Although there have been several important cryptanalytical results for PRESENT, but our goal is introducing a novel approach and apply it to cryptanalyze a block cipher. As an illustration, we applied it against reduced round of PRESENT.

By investigating other cipher's S-box that didn't include in this paper, we conclude that our method is applicable to other block ciphers and also they may have better result than PRESENT.

Our result provides the starting point for the further research on ternary differential cryptanalysis.

References

[1] E. Biham, A. Shamir, "Differential cryptanalysis of the data encryption standard," Springer-Verlag, New York, 1993.

[2] M. Daum, "Cryptanalysis of hash functions of the MD4-Family," PhD thesis, Ruhr University at Bochum, 2005.

[3] X. Wang and Hongbo Yu,"How to break MD5 and other hash functions", Eurocrypt, pp. 19-35, 2005.

[4] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar , A. Poschm ann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT : An ultra-light weight block cipher", CHES, vol. 4727, pp. 450-466, 2007.

[5] A. A. Selcuk, "On probability of success in linear and differential cryptanalysis," Journal of Cryptology, vol. 21, pp. 131-147, January 2008.

[6] A.G. Bafghi, B. Sadeghiyan, "Finding suitable differential characteristics for block ciphers with Ant colony technique," iscc, vol. 1, pp.418-423, 2004.

[7] S. Murphy, M. Robshaw,"Key-dependent S-boxes, differential cryptanalysis, and Twofish",2002.

[8] L. J. O'Connor, "On the distribution of characteristics in composite permutation,". Advances in Cryptology, Proc. of CRYPTO '93, Springer-Verlag, 1993.

[9] M. Macchetti, "Characteristics of key-dependent S-boxes: the case of twofish,". 2005.

[10] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," . Journal of Cryptology, Vol.4, No.1, pp. 3-72, 1991.

[11] Wang, M.,"Differential Cryptanalysis of Reduced-Round PRESENT,". AFRICACRYPT 2008. LNCS, vol. 5023, pp. 40–49. Springer, Heidelberg, 2008.

[12] B. Collard and F. Standaert, "A statistical saturation attack against the block cipher PRESENT", CT-RSA, Lecture Notes in Computer Science, vol. 5473, Springer, 2009, pp. 195–210.

[13] K. Ohkuma, Weak keys of reduced-round PRESENT for linear cryptanalysis, in preproceeding of SAC 2009, 2009.

[14] Onur Ozen, Kerem Varc, Cihangir Tezcan, Celebi Kocair, "Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT", Australasian Conference on Information Security and Privacy (ACISP), Australia, 2009.

[15] Jorge Nakahara, Pouyan Sepehrdad, Bingsheng Zhang, Meiqin Wang, "Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT" CANS 2009, pp. 58-75, 2009.