Cryptanalysis with Ternary Difference: Applied to Block Cipher PRESENT

Farzaneh Abazari and Babak Sadeghiyan

***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.**

***Index Terms*—Lightweight block cipher PRESENT, signed difference, ternary difference cryptanalysis.**

I. Introduction

Differential cryptanalysis or DC 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 [2] 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 [3], [4] 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. The signal to noise ratio is calculated in section 5. Section 6 concludes this paper.

Manuscript received February 27, 2012; revised April 29, 2012.

This paper has been supported by Research Center of ICT – ITRC.

The authors are with the Department of Computer Engineering and IT in Amirkabir University of Technology, Tehran, Iran (e-mail: f.abazari@aut.ac.ir;basadegh@aut.ac.ir).

II. Ternary Difference

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

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

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 [5] is defined to be:

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

where $r_i \in \{-, 0, +\}$ for $i \in \{0, \ldots, n-1\}$ 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:

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

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

where $t_i \in \{0, 1, 2\}$ for $i \in \{0, \ldots, n-1\}$ 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:

TABLE I: Type of Difference

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 or TDP. 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 TDP for PRESENT's S-box. They demonstrate three lines of TDP with 1, 2 and 3 digits of 2 for their input.

TABLE II: TERNARY DIFFERENCE WITH 3 DIGITS OF 2

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

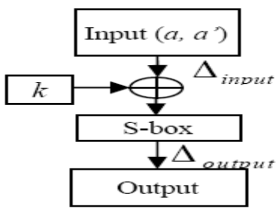
TABLE III: TERNARY DIFFERENCE WITH 2 DIGITS OF 2

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

TABLE IV: TERNARY DIFFERENCE WITH 1 DIGIT OF 2

Out / In	.....	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) ***Differential Cryptanalysis:***

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

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

2) ***Ternary Differential Cryptanalysis:***

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

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

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

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

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.

III. DESCRIPTION OF PRESENT [6]

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.

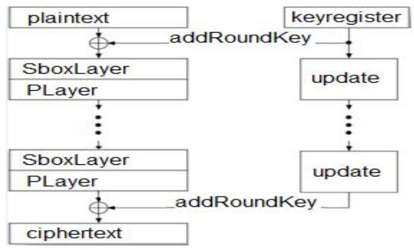


Fig. 1. PRESENT

In [7], [8], [9], [10] and [11] attacks on PRESENT are presented. Following results are the best characteristics in differential cryptanalysis from [7].

TABLE V: PROBABILITY OF THE BEST CHARACTERISTICS[7]

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

IV. CRYPTANALYSIS WITH TERNARY DIFFERENCE

Our new approach is a combination of ternary difference and conventional xor-difference. One of the main differences between TDC and DC is the target subkey. In DC, most of the time the last round's subkey is targeted, while, in TDC the first round's subkey is compromised. The procedure of the ternary differential cryptanalysis is as follows:

Step1) Obtaining first round ternary input difference that preserves some conditions such as constant input xor difference to second round.

Step 2) Obtaining the best differential characteristics for r-1 last rounds and considering the last round characteristic.

Step 3) Developing a similarity algorithm according to output characteristics from step 2 that assigning a number to each input difference in step 1. Each input difference suggests one subkey for the first round.

A. Step 1

For cryptanalysis, we begin by obtaining the ternary difference for the first round and xor-difference for the remaining rounds. Our goals are:

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

B) More ternary difference digits with value 2 in the input difference require less number of key bits in the first round subkey to guess.

To preserve the goal A, most ternary difference digits of input to first round must be 0 or 1, while, to preserve the goal B, most ternary difference digits of input to first round must be 2. The best trade-off happens when a ternary input difference has two digits with value 2 and two digits with value 0 or 1. 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 TDP. The most likely difference happens when $\Delta^{*}_{s-box(in)} = 1022$ for each S-box, then Δ^{*}_{out} is either 1112 or 2022. So 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, first round characteristic must be founded. Actually, correct input difference will be found by searching exhaustively through pairs that have the same first two bits and different last two bits, such as 0110 and 0101 which have $\Delta^{*} = 0122$. Each pair suggests two bits of the key, also parity of last two bits. The cryptanalysis needs $2^{32+16}=2^{48}$ plaintext.

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

TABLE VI: 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

B. Step2

In this step the best characteristics for r-1 last rounds with constant input difference must be obtained. In [12] 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 the second step of our analysis in PRESENT.

C. Step3

So by applying the method of [12], the most probable characteristic can be founded. Last round inputs are analyzed and the probable output characteristics are obtained. The similarity algorithm is according to probable characteristics. Then, in this step the similarity between output of probable characteristic and output of specific ternary input difference must be calculated. In this part we propose the similarity algorithm that depends on the number of rounds which is attacked. The inputs of the similarity algorithm are output difference for each ternary input difference and probable outputs. The output of the similarity algorithm is a criteria number for each output difference of ternary input difference. So the ternary input difference can be sorted. Each ternary input difference suggests first two bits and parity of last two bits in each four bits.

V. EXPERIMENT

Let's introduce some notations from [13]. 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.

A. 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 ant colony algorithm

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 of the last round. The xor profile for differences 1 and 4 of PRESENT's S-box are as follow:

TABLE VII: XOR PROFILE FOR PRESENT

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

```
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

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

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

```
maskIn:  0022002200220022002200220022002200220022002200220022002201220122
maskOut:1101110111111101101010100100110010101101010100000010011010101111
criteria:290
maskIn:  0022002200220022002200220022002200220022002200220022002201221122
maskOut:1100100000001111100000000011111000110101100001011111101111001101
criteria 280
maskIn:  0022002200220022002200220022002200220022002200220022002211221022
maskOut:0001100001011011110000000011000100011000000000011111001010010
criteria 270
maskIn:  0022002200220022002200220022002200220022002200220022002211221122
maskOut:0010100101010010010101100110110000111001110011110010011010011100
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)

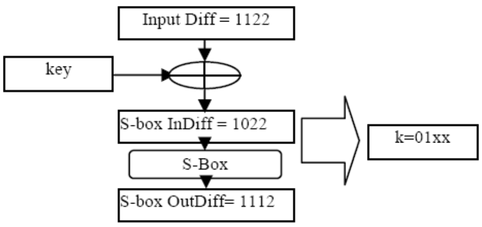
$m = 48$

(32 first two bits in each 4 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:



B. Cryptanalysis of 7 Rounds PRESENT

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

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

Result of ant colony algorithm

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, we consider 3 and 9 in the input of the last round. The xor profile for differences 3 and 9 of PRESENT's S-box are as follow:

TABLE VIII: 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

Above table shows that output difference with value 4, 6, E has higher probability and output difference 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, similarity algorithm that is 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

C. 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

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 IX: 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

Above table shows that output difference with value 1, 4, 6, A, B, C have probabilities=¼ and others have less probability. Therefore, similarity algorithm that is 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

VI. 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 [14], 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.

VII. 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.

References

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

[2] X. Wang and Hongbo Yu, "How to break MD5 and other hash functions," *Euro crypt*, pp. 19-35, 2005.

[3] S. Murphy and M. R. haw, "Key-dependent S-boxes, differential cryptanalysis, and Two fish," 2002.

[4] M. Macchetti, "Characteristics of key-dependent S-boxes: the case of two fish," 2005.

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

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

[7] M. Wang, "Differential Cryptanalysis of Reduced-Round PRESENT," *AFRICACRYPT8*. LNCS, vol. 5023, pp. 40–49. Springer, Heidelberg, 2008.

[8] 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.

[9] K. Ohkuma, "Weak keys of reduced-round PRESENT for linear cryptanalysis," *SAC*, 2009.

[10] O. Ozen, K. Varc, C. Tezcan, and C. Kocair, "Lightweight Block Ciphers Revisited: Cryptanalysis of Reduced Round PRESENT and HIGHT," *Australasian Conference on Information Security and Privacy (ACISP)*, Australia, 2009.

[11] J. Nakahara, P. Sepehrdad, B. Zhang, and M. Wang, "Linear (Hull) and Algebraic Cryptanalysis of the Block Cipher PRESENT" *CANS*, pp. 58-75, 2009.

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

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

[14] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," . *Journal of Cryptology*, vol.4, no.1, pp. 3-72, 1991.

Farzaneh Abazari was borned in Tehran, Iran in 1986. She received her B.Sc. in 2008 in Software Engineering and M.Sc. in 2011 in Information Technology from Amirkabir University of Technology, Tehran, Iran.

She is currently Ph.D. student in Computer Architecture in Iran University of Science and Technology.

Her research area of interest includes Cryptology, Network Security, and Social Networks;

Babak Sadeghiyan, Ph.D., was born in 1961. He received his B.Sc. in 1985 in Electrical (Electronics) Engineering from Isfahan University of Technology, and his M.Sc. in 1989 in Electronics Engineering from Amirkabir University of Technology, Tehran, Iran.

He received his Ph.D. in 1993, in Computer Science from University College, University of New South Wales, Australia, on the design of secure hash functions. Then he joined the Computer Engineering and IT Department of Amirkabir University of Technology in 1993, where he is still continuing his academic activities, and is currently an associate professor of the department.

His research area of interest includes all aspects of Cryptology and Information Security, more specifically; he has contributed on the design and analysis cryptographic algorithms, cryptographic protocols, hardware implementation and cryptanalysis of cipher systems, network security and intrusion detection systems.

He has pioneered the academic study of intrusion detection systems in Iranian universities since 1996. He is an author to one book, 14 research journal papers and to more than 100 conference papers.