Security of PRESENT S-box

[1]Sufyan Salim Mahmood AlDabbagh, [2]Imad Fakhri Taha Al Shaikhli
[1]Department of information systems , [2]Department of computer science
IIUM
kuala lumpur, Malaysia
[1]sufyansalim_77@yahoo.com , [2]imadf@iium.edu.my

***Abstract*—Resource efficient cryptographic primitives become fundamental for realizing both security and efficiency in embedded systems like RFID (Radio-Frequency IDentification) tags and sensor nodes. Among those primitives, lightweight block cipher plays a major role to secure RFID's tag. One of the common lightweight block ciphers is PRESENT. In this paper, we attended both conditions of PRESENT substitution box S-box and those conditions of 4-bit S-box. They were studied and analyzed thoroughly in relation with linear and differential cryptanalysis. The results show that there is conflict in one of the conditions of PRESENT S-box.**

Keywords: S-box, PRESENT lightweight block cipher, linear cryptanalysis and differential cryptanalysis.

I. INTRODUCTION

Although the AES is an excellent and preferred choice for almost all block cipher applications, it is not suitable for extremely constrained environments such as RFID tags and sensor networks. The Advanced Encryption Standard (AES) was specified in 2001 by the National Institute of Standards and Technology. The purpose is to provide a standard algorithm for encryption, strong enough to keep U.S. government documents secure for at least the next 20 years. Since Rijndael was identified as the AES, it has been a hot spot study. S box of AES is the only nonlinear components in Rijndael algorithm directly affecting its security. Many block ciphers use S-box. The AES also uses S-box with name SubBytes transformation and it has a single simple function applied over and over again to each byte during stages of the encryption. There are `256` possible byte values and each of them is transformed to another byte value with the `SubBytes` transformation which is a full permutation. This means that every element gets changed and all `256` possible elements are represented as the result of a change. As a result, no two different bytes are changed to the same byte [1].

Lightweight block ciphers are new branch of cryptography and several new block cipher algorithms are classified as lightweight block ciphers. All of them are commonly referred to as algorithms with a very low implementation complexity especially in hardware [2]. In designing secure lightweight cryptographic modules, lightweight block cipher has become very vital and of a strong demand. Moreover, Lightweight block cipher is an important branch of cryptography and S-box is the essential part of many lightweight block ciphers. Meanwhile, the S-box will create confusion in the plaintext during the process of encryption.

Consequently, we can say that the strength of the lightweight block cipher mainly depends on S-box that is why many researchers have draw attention to improve the quality of S-box and develop some analysis to determine the confusion capability of S-box [3]. Generally, there are two types of S-boxes: 4-bit and 8-bit.

AES used 8-bit S-box as a 16*16 table and it is used with heavy applications [4][5]. Most of lightweight block ciphers are using 4-bit S-box like PRESENT, mCrypton, KLEIN, LBLOCK and HUMMING [6].

II. PRESENT S-BOX

First of all, we describe the PRESENT lightweight algorithm and then focus on PRESENT S-box. PRESENT is lightweight block cipher that contain 31 rounds, 64-bit plaintext and 64-bit ciphertext. For the key, there are two key lengths 80-bit and 128-bit but the recommended is 80-bit. Each of the 31 rounds consists of XOR operation to introduce a round key K_i for $1 \leq i \leq 32$, where K_{32} is used for post-whitening, a linear bitwise permutation and a non-linear substitution layer [7]. The high level PRESENT algorithm is described in Fig (1).

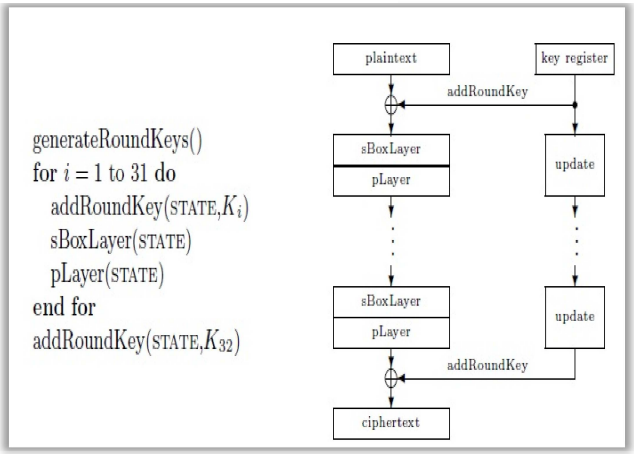

Figure 1. A high-level algorithmic description of PRESENT [7]

The non-linear layer uses a single 4-bit S-box S which is applied 16 times in parallel in each round. So, the only non linear part in the PRESENT is S-box and it called sBoxlayer. The PRESENT S-box has 4-bit input and 4-bit output and its values are in hexadecimal notation as in TableI. The PRESENT P-box (permutation box) is shown as in table II [7].

978-0-7695-4959-0/13 $25.00 © 2013 IEEE
DOI 10.1109/ACSAT.2012.23

TABLE I PRESENT S-box [7]

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

While the generation of the key is done in each round using the following steps:

- Rotate left the key bits by 61 bit position.
- Pass the left most four bit of the key to PRESENT S-box.
- XOR between right least significant bits of round counter with five bits of key [7].

Besides security and efficient implementation, the major goal for designing PRESENT was simplicity. The reason of designing lightweight block cipher to be suitable for extremely constrained environment and it is not necessarily suitable for wide-spread use because we already have the AES for that issue. Instead, we are targeting some very specific applications for which the AES is unsuitable [7].

The encryption and decryption of PRESENT are approximately the same in terms of physical requirements. Moreover, the encryption and decryption in a lightweight block cipher are still smaller than AES encryption-only. So, PRESENT encryption-only is called ultra-lightweight algorithm and the encryption subkeys can be computed on-the-fly [6].

For PRESENT, area requirements of approximately 1600 gate equivalences, it can be implement in hardware and encryption of one 64-bit plaintext block requires 32 clock cycles. It is possible to realize the cipher with as few as approximately 1000 gate equivalences, where the encryption of one 64-bit plaintext requires 547 clock cycles. A fully pipelined implementation of PRESENT with 31 encryption stages achieves a throughput of 64 bit per clock cycle, which can be translated into encryption throughputs of more than 50 G bit/s [8].

For the security of PRESENT S-box, there are four conditions for the S-box of PRESENT. According to [7], if the S-box fulfils the following conditions, where Fourier coefficient of S denoted by equation (1), then S-box will be resistant to linear and differential cryptanalysis.

$$S_b^w(a) = \sum_{x \in F_2^4} (-1)^{<b,S(x)>+<a,x>} \quad (1)$$

a. For any fixed non-zero input difference $\Delta_I \in F_2^4$ and any fixed non-zero output difference $\Delta o \in F_2^4$ the following equation must satisfied :

$$\#\{x \in F_2^4 | S(x) + S(x + \Delta_I) = \Delta o\} \leq 4 \quad (2)$$

b. For any fixed non-zero input difference $\Delta_I \in F_2^4$ and any fixed output difference $\Delta o \in F_2^4$ such that wt (Δ_I) =wt (Δo) =1. Wt() returns the humming weight of input and the following equation must satisfied :

$$\{x \in F_2^4 | S(x) + S(x + \Delta_I) = \Delta o\} = \quad (3)$$

c. For all non-zero $a \in F_2^4$ and for all non-zero $b \in F_4$ it hold that $|S_b^w(a)| \leq 8$.

d. For all $a \in F_2^4$ and all non-zero $b \in F_4$ such that wt (Δ_I) =wt (Δo) =1 it hold that $S_b^w(a) = \pm 4$.[9]

TABLE II The bit permutation in the PRESENT [7]

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

III. SECURITY OF 4-BIT S-BOX

The S-boxes are major part for the security of most modern block ciphers. There are two fundamental design strategies for block ciphers: Feistel networks and substitution permutation networks while the S-boxes form is the only non-linear part of a block cipher. Consequently, to make the cipher resistant to all kinds of attacks, the S-boxes have to be chosen carefully. In particular there are well studied criteria that a good S-box has to fulfil these criteria to make the cipher resistant against differential and linear cryptanalysis [10].

Two ways of generating good S-boxes in general:

- Picking a random large S-box.
- Generating small S-boxes with good linear and differential properties.

The main drawback of picking large S-boxes is that these S-boxes are much more inefficient to implement, especially in hardware [10].

We will focus on 4 bit S-boxes. One of advantages is that the optimal values for S-boxes with respect to linear and differential cryptanalyses are known. However, the number of 4-bit permutations is still huge roughly 2^{44}. Furthermore, it is still difficult to classify good 4 bit S-boxes. However, it is well known that the resistance of S-boxes against most attacks remains unchanged when an invertible affine transformation is applied before and after the S-box. This fairly standard technique allows us to easily classify all optimal 4 bit S-boxes [10].

Linear and differential attacks are commonly used to check the vulnerability of S-box. There are three equations mentioned later to check if the S-box is resistant to linear and differential cryptanalysis or not [10][8]. Before describing the linear and differential cryptanalysis, we introduce the notions and definitions that are used later. Suppose f(.) denote a Boolean function from F_2^n to F_2, while suppose F(.) or S(.) denote a Boolean function from F_2^n to F_2^m such that m ≤ n. Suppose X denote a bitwise variable (x1,..., xn), where xi {0, 1}. The Hamming weight of a vector a is denoted by wt (a) where a F_2^n while ⊕ and # represents the bitwise exclusive-or (XOR) operator and the cardinality of a set respectively [8].

The equations to check the S-box as follows:

A. Linear cryptanalysis.

Walsh transform is a good tool for linear cryptanalysis and other cryptography criteria of Boolean functions [11]. Suppose f be a function from F_2^n ,F_2, w ∈ F_2^n, · denotes the inner product of two vectors then

$$S_f(w) = \sum_{x \in F_2^n} (-1)^{f(x) \oplus w \bullet x} \quad (4)$$

is called a Walsh transformation of f at w. $S_f(w)$ describes how close is the Boolean function f to a linear or an affine function. It ranges from -2^n to 2^n and when it is close to 2^n, there exists a linear function that is a good approximation for f. Otherwise if $S_f(w)$ is close to -2^n, an affine function can be a good approximation [8].

Given an S-box from F_2^n to F_2^m for any vector $b \in F_2^m$ the corresponding component function S_b is defined as

$$S_b: F_2^n \to F_2 \quad (5)$$

$$x \to b \cdot S(x) \quad (6)$$

For measuring the linearity of S-box we apply the following equations:

$$S_b^w(a) = \sum_{x \in F_2^4} (-1)^{b.S(x) \oplus a.x} \quad (7)$$

where a ∈ F_2^4 and b ∈ F_2^4.

Let S denote an S-box from F_2^n to F_2^m . The linearity of the S-box (Lin(S)) is defined as follows:

$$Lin(S) = \max_{a \in F_2^n, b \in F_2^m / \{0\}} |S_b^w(a)| \quad (8)$$

If Lin(S) without wt is equal =8 and if Lin(S) =4 with wt (a) =wt (b) =1 then S-box is resistant to linear cryptanalysis and also S-box is called optimal S-box [10][8].

B. Differential cryptanalysis.

Besides linear cryptanalysis, differential cryptanalysis is also a general form of cryptanalysis to block ciphers based on the study of how differences in an input can affect the resultant differences in the output. Biham and Shamir were the first to present the differential cryptanalysis to attack DES. Later, differential cryptanalysis becomes a powerful technique to analyze the security of many other block ciphers. It exploits the high probability of certain occurrences of input differences and output differences to discover the non-random behaviour and use these properties to recover the secret key [12]. Hence a good block cipher design should ensure that given any nonzero input differences, no fixed output differences occur with a high probability [8].

To check for differential cryptanalysis, the equation (9) measures the differential resistance of S-box Diff(S):

$$Diff(S) = \max_{x \in F_2^n} \#\{S(x) + S(x + \Delta_I) = \Delta o\} \quad (9)$$

where $\Delta_I \in F_2^n$ and $\Delta o \in F_2^m$.

If Diff(S) without wt is equal = 4 and if Diff(S) = 2 with wt (Δ_I) =wt (Δo) =1 then S-box is resistant to differential cryptanalysis and also S-box is called optimal S-box [10][8].

Finally, if the S-box is satisfying points (a and b) then the S-box is optimal and resistant to linear and differential cryptanalysis [8].

IV. ANALYSIS OF SECURITY OF PRESENT S-BOX

Based on the theoretical framework in section 2 and 3, we analyzed the security of the PRESENT S-box by applying four steps. The first step is to use (7) and (8) for linear cryptanalysis testing without wt. The second step is to use the same equations in first step for linear cryptanalysis testing with wt (a) and wt (b) are equal to 1. The third step is to use (9) for differential cryptanalysis testing without wt. While the fourth step is to use the same equation in third step for differential cryptanalysis testing with wt (a) and wt (b) are equal to 1.

The steps are:

a. Lin(S) means test for linear cryptanalysis without wt.
b. Lin(S) with wt means test for linear cryptanalysis when the hamming weight equal to 1.
c. Diff(S) means test for differential cryptanalysis.
d. Diff(S) with wt means test for differential cryptanalysis when the hamming weight equal to 1.

After the above steps were applied, the results are described by table III.

TABLE III Implementation results for present s-box

	PRESENT S-box	Evaluation
a. Lin(S)	8	Resistance
b. Lin(S) with wt	4	Resistance
c. Diff(S)	4	Resistance
d. Diff(S) with wt	0	Not Resistance

The input was the values of PRESENT S-box and the output was that if the S-box is resistant to linear and differential cryptanalysis or not.

From table III, the PRESENT S-box is resistance for three parts (a, b and c) while it is penetrable in part (d). The value of Diff(S) in part (d) is zero because the second condition of PRESENT S-box always equal to zero while the value must equal to two to be S-box resistance to differential cryptanalysis when the hamming weight equal to one. As a result, the PRESENT S-box is not optimal and penetrable for differential cryptanalysis with hamming weight equal to 1.

V. CONCLUSION AND FUTURE WORK

In this paper, we found that there is a conflict between the conditions of the PRESENT S-box and the requirement conditions for the S-box to be resistant to differential cryptanalysis. To be more specific, the second condition of PRESENT S-box and (6). The value in second condition of PRESENT S-box is always zero while the value must be two for the S-box to be resistance to differential cryptanalysis when the hamming weight is equal to one. Finally, the PRESENT S-box is penetrable to differential cryptanalysis when hamming weight is equal to one.

For future work, we will try to check the resistance of the S-boxes of other lightweight block ciphers to linear and differential cryptanalysis.

ACKNOWLEDGMENT

The authors would like to acknowledge Prof. Dr. Mohamed Ridza Wahiddin for supporting and reviewing this paper.

REFERENCE

[1] C. Tu, "Design of an Improved Method of Rijndael S-Box Innovative Computing and Information." vol. 231, M. Dai, Ed., ed: Springer Berlin Heidelberg, 2011, pp. 46-51.

[2] C. Paar and J. Pelzl, *Understanding cryptography : a textbook for students and practitioners*. Berlin; Heidelberg: Springer, 2010.

[3] Iqtadar Hussain, Tariq Shah, Hasan Mahmood, Muhammad Asif Gondal, and U. Y. Bhatti, "Some Analysis of S-box based on Residue of Prime Number," in *Pakistan Academy of Sciences*, Pakistan, 2011, pp. 111–115.

[4] J. Daemen and V. Rijmen, "The Design of Rijndael," *Springer-Verlag,* 2002.

[5] K. Nyberg, "Perfect nonlinear S-boxes Advances in Cryptology — EUROCRYPT '91." vol. 547, D. Davies, Ed., ed: Springer Berlin / Heidelberg, 1991, pp. 378-386.

[6] Lars R. Knudsen and M. J. B. Robshaw, *The Block Cipher Companion*. Berlin Heidelberg: Springer-Verlag, 2011.

[7] A. Bogdanov, L. Knudsen, G. Leander, C. Paar, A. Poschmann, M. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An Ultra-Lightweight Block Cipher Cryptographic Hardware and Embedded Systems - CHES 2007." vol. 4727, P. Paillier and I. Verbauwhede, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 450-466.

[8] B. Liu, Z. Gong, W. Qiu, and D. Zheng, "On the Security of 4-Bit Involutive S-Boxes for Lightweight Designs Information Security Practice and Experience." vol. 6672, F. Bao and J. Weng, Eds., ed: Springer Berlin / Heidelberg, 2011, pp. 247-256.

[9] H. Yap, K. Khoo, A. Poschmann, and M. Henricksen, "EPCBC - A Block Cipher Suitable for Electronic Product Code Encryption Cryptology and Network Security." vol. 7092, D. Lin*, et al.*, Eds., ed: Springer Berlin / Heidelberg, 2011, pp. 76-97.

[10] G. Leander and A. Poschmann, "On the Classification of 4 Bit S-Boxes Arithmetic of Finite Fields." vol. 4547, C. Carlet and B. Sunar, Eds., ed: Springer Berlin / Heidelberg, 2007, pp. 159-176.

[11] Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. (eds.) CRYPTO 1990. LNCS, vol. 537, Springer, Heidelberg, 1990, pp. 2–21.

[12] Biryukov, A., De Cannière, C., Braeken, A., Preneel, B.: A toolbox for cryptanalysis: Linear and affine equivalence algorithms. In: Biham, E. (ed.) Advances in Cryptology – EUROCRPYT 2003. LNCS, vol. 2656, Springer, Heidelberg, 2003, pp. 33–50.