Design 32-bit Lightweight Block Cipher Algorithm (DLBCA)

Sufyan Salim Mahmood AlDabbagh
Department of computer scienc
University of Mosul, Iraq

ABSTRACT

Lightweight block cipher algorithms are vital for constrained environment. There are many applications need secured lightweight block cipher algorithm like credit card, E-passport and etc. This paper will propose 32-bit lightweight block cipher algorithm. It will apply two attacks differential and boomerang attack. The results will show that the proposed algorithm is resistance to these attacks.

Keywords

Lightweight block cipher, Substitution, Permutation Network, Differential cryptanalysis and Boomerang cryptanalysis.

1. INTRODUCTION

No doubt that the life is changing tremendously especially in information technology and the needs of Security system to protect data is becoming crucial [1].

Generally, it is difficult to suggest a cryptographic algorithm that can suit to all types of target devices. However, it is unsuitable to use common cryptographic algorithms in specific devices with extremely constrained resources [2].

The fundamental principles and trends to design algorithms were proposed for implementation in the devices with extremely low resources and some different extent in the design aspect of the common cryptographic algorithms. Therefore, it is necessary to support a modern cryptographic lightweight algorithm [2].

A designer of the lightweight cryptography must be aware the importance of the balancing three factors which are the security, the cost (Gate Equivalent GE), and the performance.

Many lightweight block cipher algorithms[16] are proposed like PRINCE [3], PRINT [4], PRESENT [5], mCrypton [6], KLEIN [7], Lblock [8], TWINE [9] and LED [10].

But this paper are going to design small lightweight block cipher algorithm called DLBCA. Also, it will apply two attacks: differential and boomerang attacks on the proposed algorithm.

2. PROPOSED ALGORITHM DLBCA

DLBCA is 32-bit plaintext and key size 80-bit. The structure of DLBCA algorithm looks like the structure of feistel with some modifications [11]. There are 15 rounds and in each round, there are operations like: Substitution box, Bit permutation, XOR, Rotation and key update. Moreover, there is XOR between the cipher text and key in the last round. The DLBCA have four layers as following:

- First Layer: in this layer, the 32-bit plaintext is XOR with the 32-bit key. The plaintext divides into two parts. Each part is 16-bit and the results after XOR of each part will be as inputs to the second layer (Substitution box).
- Second Layer: this layer is the most important layer. It produces the confusion property and it gives the nonlinearity to the algorithm. It has 8 4-bit S-boxes and divides them into two parts, each part 4 S-boxes. The output of this layer will be as inputs to the third layer (bit permutation). Also, this layer uses one S-box and repeats it 8 times. The characteristics of the S-box are the same with good S-box. The values of S-box as shown in table (1).

Table 1 S-box values

X	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
S(X)	F	C	2	7	9	0	5	A	1	B	E	8	6	D	3	4

- Third Layer: This layer produces the diffusion which is also important part for any strong encryption algorithm. This method of bit permutation applies on two sides and each side is 16-bit.
- Fourth Layer: this layer applies the rotation and XOR operations on both sides. First of all, rotate the left 16-bit and then XOR with right 16-bit. The result will keep in left 16-bit. The next step is to rotate the right 16-bit and XOR with new left 16-bit and the result will keep in right 16-bit.

The last important part in any encryption algorithm is key schedule. The MASTER key size as mentioned before is 80-bit K_0, K_1, K_2, K_3, $K_{4,}$,….K_{79}.The key update or key schedule is operate as follows:

- $[K_3\ K_2\ K_1\ K_0] = S\ [K_3\ K_2\ K_1\ K_0]$
- Rotate left the MASTER key by P-bit and the initial value for P =13
- MASTER key = MASTER key << 13.
- The value of P for next round will increment by 2.

The master key is 80-bits while the encryption algorithm uses 32-bits only. The encryption algorithm takes the most right 32-bits of MASTER key. The figure (1) shows all layers of **DLBCA** in details.

3. COST DISCUSSION

The second important factor is the cost. According to [8] [9], it can calculate the cost of DLBCA algorithm. The details of calculating the cost of **DLBCA** algorithm as follows:

- The cost of saving 1bits is 6 GE. In **DLBCA** algorithm, we have 32bits for plaintext and 80bits for key. The total cost for plaintext and key as follows:
  Plaintext = 32 * 6 = 192 GE.
  Key = 80 *6 = 480 GE
- The cost for each S-box is approximately 22GE. In the proposed algorithm, we have 8 S-boxes. The total cost of four S-boxes is 8 * 22 = 176 GE.
- The cost of 16bit XOR is 43.5GE approximately. In **DLBCA**, there are four 16bits XOR. The total cost for XOR is 4 * 43.5 = 174 GE.

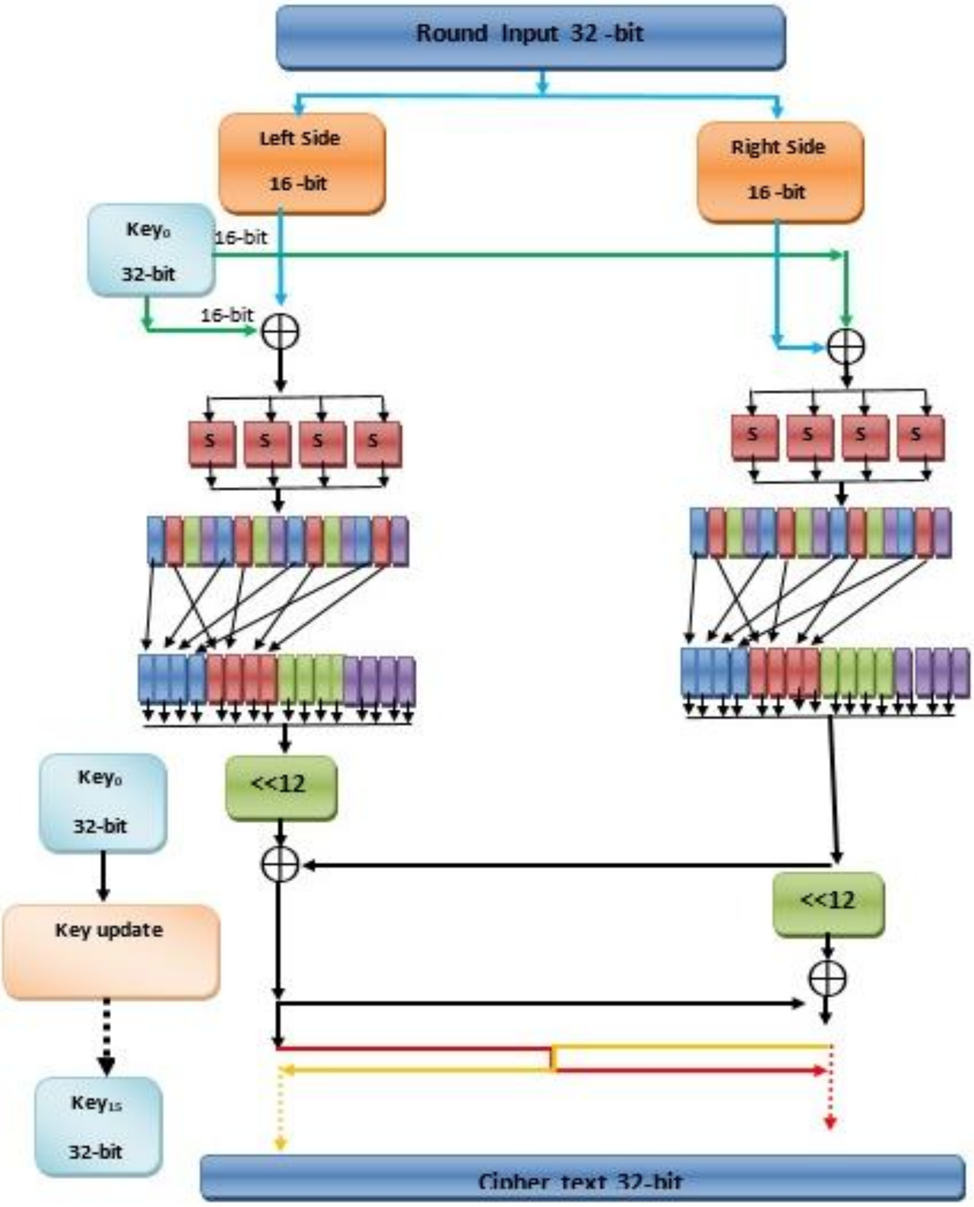

Fig. 1: All layers of DLBCA together in details

There is 50 GE as additional cost. The total cost for the encryption part of **DLBCA** algorithm is:

Plaintext 192 + Key 480 + 8 S-boxes 176 + 4-16bits XOR 174 + additional cost 50 = 1072GE. The cost of key update is:

1S-box 22 + addition 8 bit 2.76 * 8 = 22 + 22.08 = 44.08 GE. The total cost of whole **DLBCA** algorithm is 1072 + 44.08 = 1116.08 GE. The table (2) shows the comparison between the cost of DLBCA algorithm and others algorithms.

Table 2 Cost for DLBCA and other algorithms

Algorithm	**Plaintext**	**Key**	**S-box**	**Cost**
Lblock [9]	64	80	8	1320 GE
TWINE [10]	64	80	8	1503GE
PRESENT [6]	64	80	16	1570 GE
KLIEN [8]	64	80	16	2097 GE
DLBCA	32	80	8	1116 GE

From table (2), it can conclude that the cost of **DLBCA** algorithm is the smallest because it uses 8 s-boxes and 32-bit plaintext.

4. SECURITY DISCUSSION

The cryptanalysis is the important factor to test the security of the algorithm. To measure the security of any algorithm, this is done by using the cryptanalysis. This paper applied two attacks: differential attack and boomerang attack.

4.1 Differential Cryptanalysis

The most powerful way to gauge the resistance of any encryption algorithm against to differential cryptanalysis is count the minimum active S-box [12] [13] [14]. The table (3) shows the number of active S-box for the **DLBCA** algorithm and some others algorithms.

Table 3 Number of Active S-box for DLBCA and other algorithms

Algorithms	**Min number of active S-box for each round category**			
	4	**8**	**12**	**16**
TWINE [10]	3	11	24	-
Lblock [9]	3	11	24	35
PRESENT [6]	8	16	24	32
KLEIN [8]	15	30	45	60
DLBCA	13	31	48	65

From table (3), it can conclude that the **DLBCA** has the highest number of active S-boxes regardless there are two algorithms have 16 s-boxes. This means that the **DLBCA** is the most secure than other existing algorithm in term of differential cryptanalysis.

4.2 Boomerang Attack

The first step to mount this attack, it need to know the number of active S-boxes in each round. The second step is use the following equation (1) to calculate the probability of distinguisher of this attack[15]. The equation is:

$$p^2 . q^2 = (((2^{-2})^{NAS})^2 \times (((2^{-2})^{NAS})^2 \qquad (1)$$

Where $p^2 . q^2$is the probability of distinguisher and NAS is the number of active S-boxes. When the probability of distinguisher is less than the plaintext size base, it can say the attack can't go forward [18]. The following table (4) shows the number of active S-box for the first three rounds of **DLBCA** algorithm.

Table 4: Number of active S-box of DLBCA for three rounds

No.	**Round**	**Active S-box**
1.	1	1
2.	2	6
3.	3	8

Regarding to the **DLBCA** algorithm and depending on table (4), this attack can reach round 3 with maximal probability 2^{-28}. The following points will explain that:

- In round 2 there are 6 active S-boxes and in round 1 there is one active S-box.
- To find the probability, we need to apply the equation (1).
- The final probability is$(((2^{-2})^6)^2) \times (((2^{-2})^1)^2) = 2^{-24} \times 2^{-4} = 2^{-28}$.
- This attack can reach 3 rounds only with probability2^{-28}.

The **DLBCA** have 15 rounds which mean it is resistant to the boomerang attack. Moreover, it calculated the distinguisher probability of boomerang for PRESENT [6], Lblock [9], KLEIN [8] and TWINE [5] as following:

- PRESENT: The boomerang attack can reach round 7 with probability2^{-56}.
- Lblock : The boomerang attack can reach round 11 with probability2^{-60}.
- TWINE: The boomerang attack can reach round 11 with probability2^{-60}.
- KLIEN: The boomerang attack can reach round 4 with probability2^{-60}.

The table (5) shows the results of boomerang attack for the **DLBCA** algorithm and others algorithms.

Table 5: Maximum round of boomerang attack for DLBCA and other existing algorithms

No.	**Algorithms**	**Maximum round**	**Probability**
1.	KLEIN	4	2^{-60}
2.	PRESENT	7	2^{-56}
3.	Lblock	11	2^{-56}
4.	TWINE	11	2^{-56}
5.	DLBCA	3	2^{-28}

From table (5), the **DLBCA** algorithm is the most secure than other algorithms in the term of boomerang attack.

5. CONCLUSION

This paper proposed new lightweight block cipher algorithm (DLBCA). Also, it calculated the cost of DLBCA in GE and it compared it with others lightweight algorithms. Moreover, it presented the analysis of DLBCA against differential and boomerang attacks. The analysis showed that DLBCA is the most secure than other algorithms considered in this paper in the terms of differential and boomerang attacks. In spite of DLBCA used 8 S-boxes and there are two algorithms considered in this paper used 16 S-boxes, DLBCA has the highest security.

6. REFERENCES

[1] Panasenko, S., & Smagin, S., "Lightweight Cryptography: Underlying Principles and Approaches", International Journal of Computer Theory and Engineering, Vol 3 No.4, (2011).

[2] S. Salim and I. Taha, "Lightweight block ciphers: comparative study," Journal of Advanced Computer Science and Technology Research (JACSTR), vol. 2, pp. 159-165, 2012.

[3] J. Borghoff, et al., "PRINCE – A Low-Latency Block Cipher for Pervasive Computing Applications," in Advances in Cryptology – ASIACRYPT 2012. vol. 7658, Springer Berlin Heidelberg, 2012, pp. 208-225.

[4] L. Knudsen, et al., "PRINTcipher: A Block Cipher for IC-Printing," in Cryptographic Hardware and Embedded Systems, CHES 2010. vol. 6225, Springer Berlin Heidelberg, 2010, pp. 16-32.

[5] 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, Springer Berlin / Heidelberg, 2007, pp. 450-466.

[6] C. Lim and T. Korkishko, "mCrypton – A Lightweight Block Cipher for Security of Low-Cost RFID Tags and

Sensors Information Security Applications." Vol. 3786, Springer Berlin / Heidelberg, 2006, pp. 243-258.

[7] Z. Gong, S. Nikova, and Y. Law, "KLEIN: A New Family of Lightweight Block Ciphers RFID. Security and Privacy." Vol. 7055, Springer Berlin / Heidelberg, 2012, pp. 1-18.

[8] W. Wu and L. Zhang, "LBlock: A Lightweight Block Cipher Applied Cryptography and Network Security." Vol. 6715, Springer Berlin / Heidelberg, 2011, pp. 327-344.

[9] T. Suzaki, et al., "TWINE: A Lightweight Block Cipher for Multiple Platforms," in Selected Areas in Cryptography. vol. 7707, Springer Berlin Heidelberg, 2013, pp. 339-354.

[10] J. Guo, T. Peyrin, A. Poschmann, and M. Robshaw, "The LED Block Cipher Cryptographic Hardware and Embedded Systems – CHES 2011." Vol. 6917, Springer Berlin / Heidelberg, 2011, pp. 326-341.

[11] S. Panasenko and S. Smagin, "Lightweight cryptography: Underlying principles and approaches," International Journal of Computer Theory and Engineering, vol. 3, pp. 516-520, 2011.

[12] E. Biham and A. Shamir, "Differential Cryptanalysis of DES Variants," in Differential Cryptanalysis of the Data Encryption Standard, ed: Springer, 1993, pp. 33-77.

[13] J.-S. Kang, et al., "Practical and provable security against differential and linear cryptanalysis for substitution-permutation networks," ETRI journal, vol. 23, pp. 158-167, 2001.

[14] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," Journal of CRYPTOLOGY, vol. 4, pp. 3-72, 1991.

[15] D. Wagner, "The boomerang attack," in Fast Software Encryption, 1999, pp. 156-170.

[16] S. S. M. Aldabbagh, et al., " Lightweight Block Cipher Algorithms: Review Paper" in International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463, Vol. 5 Issue 5, May-2016.