

## Improving the Cost Factor of DLBCA Lightweight Block Cipher Algorithm

Sufyan Salim Mahmood Al-Dabbagh<sup>\*1</sup>, Alyaa Ghanim Sulaiman<sup>2</sup>, Imad Fakhri Taha Al Shaikhli<sup>3</sup>,  
Khalid Abdulkareem Al-Enezi<sup>4</sup>, Abdulrahman Yousef Alenezi<sup>5</sup>

<sup>1</sup>Department of Computer Science, University of Mosul, Iraq

<sup>2</sup>Department of Software Engineering, University of Mosul, Iraq

<sup>3</sup>Department of Computer Science, International Islamic University, Malaysia

<sup>4</sup>Central Agency for Information Technology, Kuwait

<sup>5</sup>Technology & Infrastructure Department, Zain Kuwait Telecom Company, Kuwait

---

### Article Info

#### Article history:

Received Nov 19, 2017

Revised Jan 21, 2018

Accepted Feb 24, 2018

#### Keywords:

Cost factor

Cryptanalysis

Lightweight algorithms

---

### ABSTRACT

The need to secure information in restricted environments is very important so that lightweight block cipher algorithm is suitable for these environments. This paper improved DLBCA algorithm by decreasing the cost factor through using the less number of S-boxes. Also, differential and boomerang attacks have been applied in this paper. Finally, all the results have been presented.

Copyright © 2018 Institute of Advanced Engineering and Science.  
All rights reserved.

---

### Corresponding Author:

Sufyan Salim Mahmood Al-Dabbagh  
Computer Science Dept.,  
College of computer science and mathematics,  
Mosul University, Mosul, Iraq.  
Email: sufyansalim\_77@yahoo.com

---

## 1. INTRODUCTION

Information technology is changing tremendously, and the security system is needed to protect data [1]. Generally, it is not easy to suggest a cryptographic algorithm for all kinds of target devices [2]. There are three factors cost, security and performance. The designer must be aware how to use these factors [2]. There are many proposed lightweight algorithms like TWINE [9], PRINT [4], KLEIN [7], PRESENT [5], LBLOCK [8], mCrypton [6], PRINCE [3] and LED [10].

This research paper, will enhance the cost element of DLBCA algorithm by reducing the number of S-box without major change on other elements. Also, two attacks differential and boomerang have been applied on the suggested algorithm.

## 2. DLBCA LIGHTWIGH ALGORITHM

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 32 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 left 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 four 4-bit 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 left side which 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 K0, K1, K2, K3, K4,.....K79. The key update or key schedule is operate as in [17].

**3. PROPOSED LIGHTWEIGHT ALGORITHM**

This paper enhances the cost factor of DLBCA by reducing the S-box numbers. The suggested algorithm utilizes four S-box instead of eight S-box. However, it has xoring 32bit of plaintext with first 32bit of key. The round number of suggested algorithm is similar as DLBCA. The suggested algorithm layers are shown in Figure (2).

**4. THE DISCUSSION OF COST**

The cost element is one of essential factors that the designer must be consider it when he designs any algorithm. This paper calculated the cost of suggested algorithm according to [12]. The cost calculating details as follows:

- The saving value of 1bits is 6 GE while cost value of one S-box is 22 GE.
- The cost of 16-bit XOR is 43.5GE.
- For additional cost, there is 50GE.

The costs of the algorithms are presented in table (2).

Table 2: Cost Comparison between Proposed Algorithm and Others 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 [ 19]	32	80	8	1116 GE
Proposed algorithm	32	80	4	1028 GE

The cost of the suggested algorithm is the lowest comparing with the other algorithms as shown in table (2)

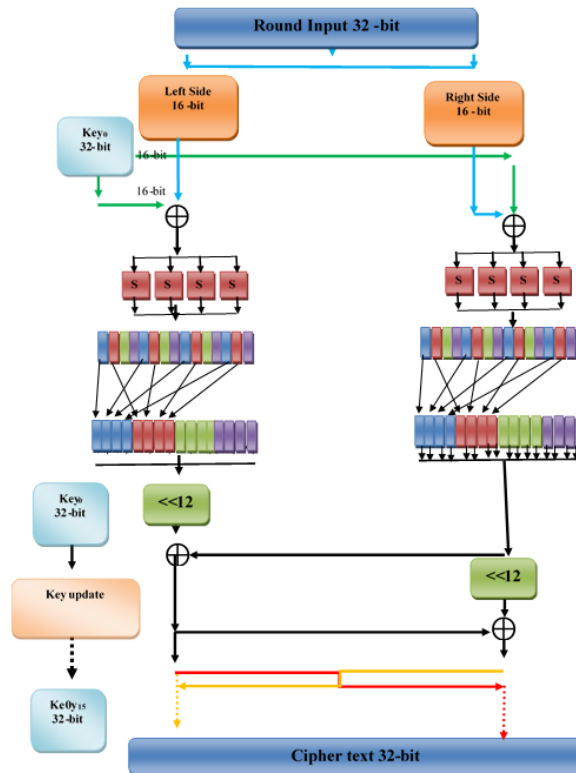


Figure 1. DLBCA Algorithm Layers in Details [17]

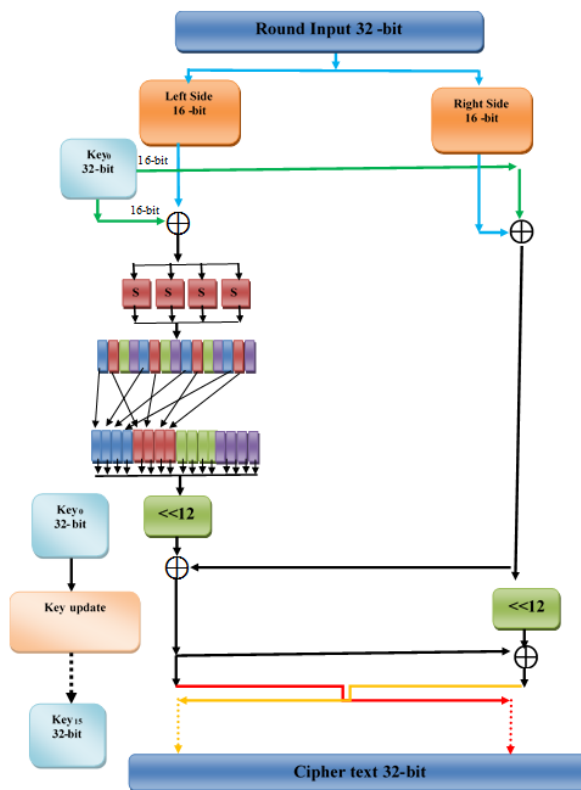


Figure 2. Suggested Algorithm Layers in Details

**5. THE DISCUSSION OF SECURITY**

The cryptanalysis is essential tool that it can scale the security of whatever algorithm. Differential and boomerang attacks are applied in this paper.

**5.1. Differential Cryptanalysis**

The minimum active S-box is the most powerful way to measure the resistance of block cipher algorithm against differential algorithm [13]-[15]. The results of this attack are presented in table (3).

Table 3. Active S-box Numbers for Suggested Algorithm and Other Algorithms

No.	Algorithm	Min number of active S-box			
		4	8	12	16
1.	TWINE [10]	3	11	24	-
2.	Lblock [9]	3	11	24	35
3.	PRESENT [6]	8	16	24	32
4.	KLEIN [8]	15	30	45	60
5.	DLBCA [17]	13	31	48	65
6.	Proposed algorithm	8	16	24	32

The Table (3) shows that the number of active S-boxes of LBLOCK, PRESENT and TWINE is closer to suggested algorithm while the number of active S-box of DLBCA and KLEIN are better than our suggested algorithm. On the other hand, the cost of both of them are higher compared with this suggested algorithm.

**5.2. Boomerang Cryptanalysis**

Knowing the active S-box numbers in each step is the first step to amount this attack while the second step is calculating the distinguisher probability for this attack. The Equation is:

$$p^2 \cdot q^2 = (((2^{-2})^{NAS})^2 \times ((2^{-2})^{NAS}))^2 \tag{1}$$

Which  $p^2 \cdot q^2$  is the distinguisher probability and NAS is the active S-box. When the probability of distinguisher is less than  $2^{-plaintext\ size}$ , we can say the attack can't go forward [16].

Regarding to the proposed algorithm and depending on equation (1), this attack can reach round 3 with maximal probability  $2^{-28}$ . The following points will explain that:

- a. In round 2 there are 4 active S-boxes and in round 1 there is two active S-box.
- b. To find the probability, we need to apply the equation (1).
- The final probability is  $((2^{-2})^4)^2 \times ((2^{-2})^2)^2 = 2^{-16} \times 2^{-8} = 2^{-24}$ .
- c. This attack can reach 3 rounds only with probability  $2^{-24}$ .

The proposed algorithm has 32 rounds meaning that it is resistant to the boomerang attack. The results of this attack are presented in table (4).

Table 4: Boomerang Attack Results for Suggested Algorithm and Other Algorithms

No.	Algorithm	Maximum Round
1	LBLOCK [9]	11
2	TWINE [5]	11
3	PRESENT [6]	7
4	KLEIN [8]	4
5	DLBCA [17]	3
6	Proposed	3

The Table (4) shows that boomerang cryptanalysis can reach to round 11 with TWINE and LBLOCK algorithms but it can reach to round 7 and round 4 with PRESENT and KLEIN respectively.

While the boomerang cryptanalysis can reach round 3 with DLBCA and suggested algorithm. This is mean that the suggested algorithm still has the same number of rounds which is equal with DLBCA after reducing the cost factor. Also, the suggested algorithm is better than other algorithms regarding of boomerang cryptanalysis.





## 6. CONCLUSION

This paper has improved the cost factor of DLBCA by reducing the number of S-box. Also, the comparisons for cost and security between suggested algorithm and others are shown. To sum up results, the cost of suggested algorithm is the lowest cost. Regarding to security side, the suggested algorithm has similar number of active S-box when compared with algorithms (TWINE, LBLOCK and PRESENT). According to the boomerang attack, the suggested algorithm has the same number of rounds with DLBCA algorithm and it is the best from other algorithms.

## 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. S. M. Aldabbagh and I. F. T. A. Shaikhli, "OLBCA: A New Lightweight Block Cipher Algorithm," in *Advanced Computer Science Applications and Technologies (ACSAT)*, 2014 3rd International Conference on, 2014, pp. 15-20.
- [12] S. Panasenko and S. Smagin, "Lightweight cryptography: Underlying principles and approaches," *International Journal of Computer Theory and Engineering*, vol. 3, pp. 516-520, 2011.
- [13] E. Biham and A. Shamir, "Differential Cryptanalysis of DES Variants," in *Differential Cryptanalysis of the Data Encryption Standard*, ed: Springer, 1993, pp. 33-77.
- [14] 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.
- [15] E. Biham and A. Shamir, "Differential cryptanalysis of DES-like cryptosystems," *Journal of CRYPTOLOGY*, vol. 4, pp. 3-72, 1991.
- [16] D. Wagner, "The boomerang attack," in *Fast Software Encryption*, 1999, pp. 156-170.
- [17] S. S. M. Aldabbagh, "Design 32-bit Lightweight Block Cipher Algorithm (DLBCA)" *International Journal of Computer Applications* vol. 166, pp. 17-20, 2017.

**BIOGRAPHIES OF AUTHORS**

	<p>Sufyan Salim Mahmood Al-Dabbagh received his bachelor degree and master degree in computer science from Mosul university in 1999 and 2003 respectively. He received his PhD degree in information technology from International Islamic University Malaysia (IIUM) in 2015. He is working at Mosul university as deputy dean of computer science and mathematics college. His research interests include security, cryptography and LTE/4G. He is expert in block cipher in general and in lightweight block cipher in more specific</p>
	<p>Alyaa Ghanim Sulaiman received her bachelor degree in computer science from Mosul university in 2002. She received her master degree in information technology from International Islamic University Malaysia (IIUM) in 2014. She is working at Mosul university as assistant lecturer. Her research interests include security, cryptography and LTE/4G. She is expert in LTE/4G security algorithms</p>
	<p>Professor Imad Fakhri Taha is an IEEE senior member, obtained his BSc (Hon) in Mathematics, MSc in Computer Science from Iraq, and PhD degree from Pune University, India, 2000. In 2003 he was appointed as the head of department of computer information systems at Alrafidain University College until 2005. Then he joined Gulf university- Bahrain January 2006 and appointed as the founding Dean of the college of computer engineering and sciences, during this period he introduced the CCNA certificate to be part of the curriculum which had a strong impact on the students career. In November 2010 he joined IIUM at the Dept. of Computer Science/ kulliyah of Information and Communication Technology. He received the best teacher award in 2011. He is the editor in chief of JACSTR (international Journal on Advanced Computer Science and Technology Research) since 2011 till now and IJPCC international journal since 2015, and the general chair of the international conference on Advanced Computer Science Applications and Technologies) since 2012 till now. He obtained a US patent for his work with his PhD student on smart traffic light with accident detection system on 2nd Dec 2014 . Prof. Imad has published more than 200 articles, conference papers, and book chapters in addition to three books. In addition, he secured more than 10 research grants. Presently Prof. Dr Imad is a Professor at the Department of Computer Science and Head of Research at the Kulliyah of Information and Communications Technology, the International Islamic University Malaysia (IIUM) since 1st November 2013.</p>
	<p>Khaled Abdulkareem Alenzi received his bachelor degree from Kuwait University in applied statistics in 1987 and master degree in management system from Gulf University – Bahrain in 2010. He received his PhD degree in computer science from International Islamic University Malaysia (IIUM) in 2016. He is working at Central Agency for Information Technology - Kuwait. His research interests include security, and he is expert in government sector security.</p>