HISEC: A New Lightweight Block Cipher Algorithm

Sufyan Salim Mahmood AlDabbagh
Department of information systems
IIUM
Malaysia
University of Mosul Iraq
sufyansalim_77@yahoo.com

Imad Fakhri Taha Al Shaikhli
Department of computer science
IIUM
Malaysia
imadf@iium.edu.my

Mohammad A. Alahmad
Department of computer science
PAAET
Kuwait
Malahmads@yahoo.com

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. In this paper, we propose a new lightweight block cipher algorithm called HISEC. We applied three attacks differential, integral attacks and boomerang attack. The results showed that HISEC is better than some lightweight algorithms.

Categories and Subject Descriptors

E.3 [DATA ENCRYPTION]: *Code breaking, Standards (e.g., DES, PGP, RSA).*

General Terms

Algorithms, Security.

Keywords

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

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 all types of target devices. However, it is not suitable to use common cryptographic algorithms in specific devices with extremely constrained resources [2].

The fundamental principles and trends to design algorithms proposed for implementation in devices with extremely low resources are to some extent different from the design aspect of commonly used cryptographic algorithms. In this specific field is supported by a branch of the modern cryptography lightweight cryptography [2].

Every designer of lightweight cryptography must be aware of the important of balancing between security, cost (Gate Equivalent GE), and performance. However, it is generally easy to optimize any two of the three designs proposal security and cost, security and performance, or cost and performance. At the same time it is difficult to enhance all three designed goals at once.

Many lightweight block cipher algorithms are proposed [3] like PRINCE [4], PRINT [5], PRESENT [6], mCrypton [7], KLEIN [8], Lblock [9], TWINE [10] and LED [11].

In this paper, we propose a new lightweight block cipher algorithm (called **HISEC**) which is more secure than some other existing algorithms in the terms of differential, integral and boomerang attacks. This research focuses on the security factor without major effect on the cost factor.

2. PROPOSED LIGHTWEIGHT ALGORITHM (HISEC)

HISEC used the same characteristics of PRESENT but different method for bit permutation. The structure of HISEC algorithm looks like the structure of feistel with some modifications [20][12]. The HISEC is 64-bit plaintext and 80-bit key size. 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 HISEC have four layers as following:

- First Layer: in this layer, the 64-bit plaintext is XOR with the 64-bit key. The plaintext divides into two parts. Each part is 32-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 16 4-bit S-boxes and divides them into two parts, each part 8 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 16 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 32-bit.
- Fourth Layer: this layer applies the rotation and XOR operations on both sides. First of all, rotate the left 32-bit and then XOR with right 32-bit. The result will keep in left 32-bit. The next step is to rotate the right 32-bit and XOR with new left 32-bit and the result will keep in right 32-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:

SIN '14, September 09 - 11 2014, Glasgow, Scotland Uk
Copyright 2014 ACM 978-1-4503-3033-6/14/09…$15.00.
http://dx.doi.org/10.1145/2659651.2659662

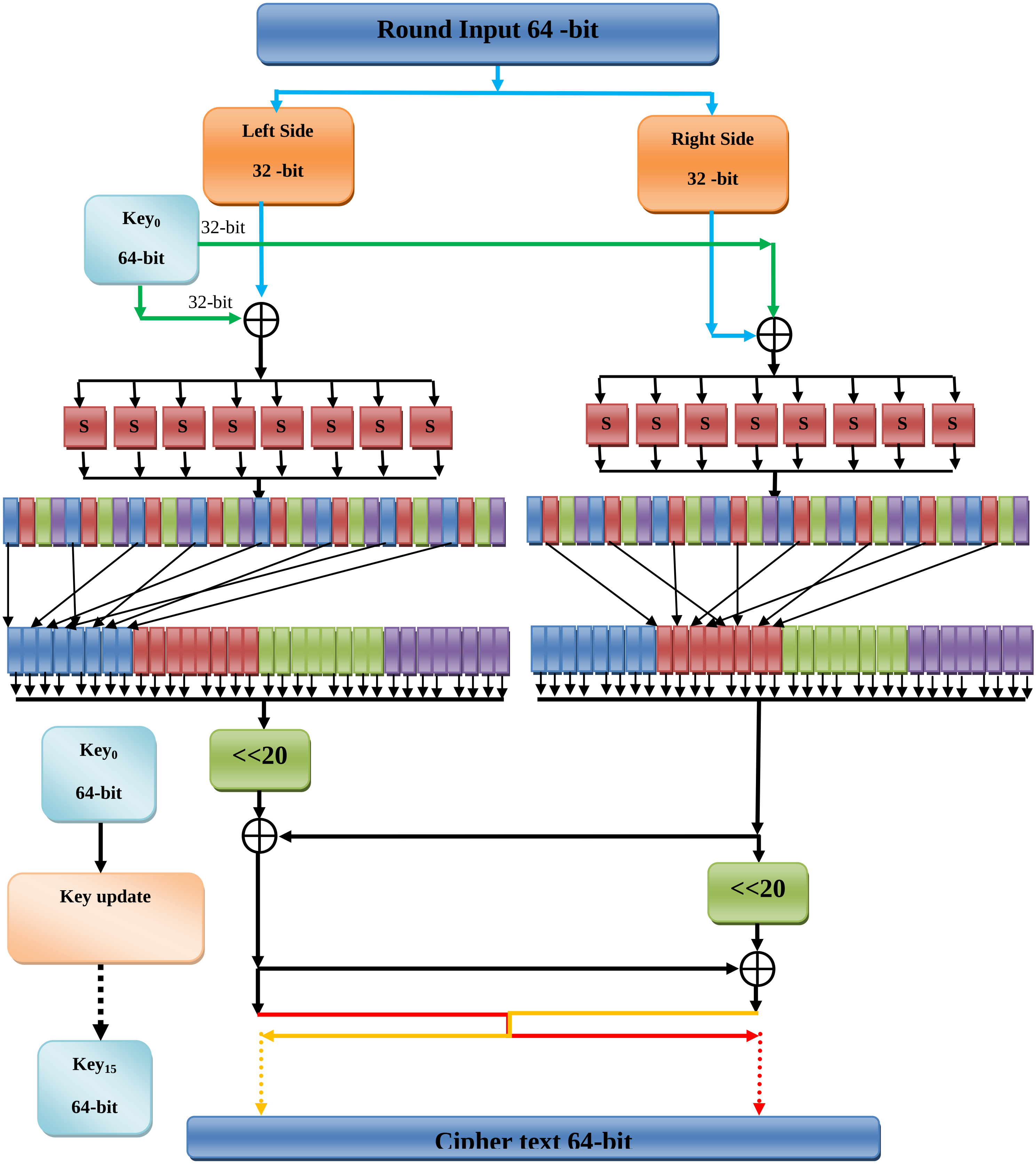

Figure (1): All layers together in details

- $[K_0\ K_1\ K_2\ K_3] = S\ [K_0\ K_1\ K_2\ K_3]$
- 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 64-bits only. The encryption algorithm takes the most right 64-bits of MASTER key. The figure (1) shows all layers of **HISEC** in details.

3. 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. We applied three attacks: differential attack, integral attacks and boomerang attack.

3.1Differential Cryptanalysis

The most powerful way to gauge the resistance of any encryption algorithm against to differential cryptanalysis is count the minimum active S-box [13] [14] [15]. The table (2) shows the number of active S-box for the **HISEC** algorithm and some others algorithms.

Table 2 Number of Active S-box for HISEC and other algorithms

Algorithms	**Min number of active S-box for each round category**							
	4	**8**	**12**	**16**	**20**	**24**	**28**	**32**
TWINE [10]	3	11	24	-	-	-	-	-
Lblock [9]	3	11	24	35	44			
PRESENT [6]	8	16	24	32	40	48	56	64
KLEIN [8]	15	30	45	60	75	90	105	120
HISEC	17	43	96	124	166	203	239	275

From table (1), we can conclude that the **HISEC** has the highest number of active S-boxes. This means that the **HISEC** is more secure than other existing algorithm in term of differential cryptanalysis.

3.2 Integral Cryptanalysis

It is one of the important attacks and every algorithm designer needs to apply this attack on his algorithm to check the resistance against this attack. We will start the analysis of the proposed algorithm by choosing one 4-bit all possible values, 16-bit all possible values and 32-bit all possible values while the others are constants. The important step for this attack is to build the distinguisher table and from this table we will know in which round this attack can reach [16].

3.2.1 One Nibble

In this case, there are 15 nibbles constants and one nibble takes all possible values. The table (3) illustrates in which round the integral attack can reach.

Table 3 Integral attack on one nibble for HISEC

No.	**Nibble Position**	**Round that the attack can reach**
1.	0 to 8	2
2.	9	3
3.	10-15	2

From table (3), we consider the position 9 to calculate the complexity of this attack. We start to do the key recovery. The integral attack can go until round four with complexity 2^{55} to recover 32-bits of key.

3.2.2 Four Nibbles

In this case, there are 12 nibbles constants and four nibbles take all possible values. The table (4) illustrates in which round the integral attack can reach.

Table 4 Integral attack on four nibbles for HISEC

No.	**Nibble Position**	**Round that the attack can reach**
1.	0 to 15	3
2.	1 to 4	3
3.	2 to 5	3
4.	3 to 6	3
5.	4 to 7	3
6.	5 to 8	3
7.	6 to 9	3
8.	7 to 10	3
9.	8 to 11	3
10.	9 to 12	3
11.	10 to 13	3
12.	11 to 14	3
13.	12 to 15	3

From the table (4), the distinguisher round is three and from this round we start to calculate the complexity of the attack. After that, we will use the same method in the previous section 1. The last round that the attacker can reach is 4 with complexity 2^{55} to recover 32 bits of key.

3.2.3Eight Nibbles

In this case, there are 8 nibbles constant and 8 nibbles take all possible values. The table (5) illustrates how the integral attack works in each round.

Table 5 Integral attack on eight nibbles for HISEC

No.	**Nibble Position**	**Round that the attack can reach**
1.	0 to 7	3
2.	1 to 8	3
3.	2 to 9	3
4.	3 to 10	3
5.	4 to 11	3
6.	5 to 12	3
7.	6 to 13	3
8.	7 to 14	3
9.	8 to 15	3

From the table (5), the distinguisher round is three and from this round we start to calculate the complexity of the attack. After that, we will use the same method in the previous section 1. The last round that the attacker can reach is 4 with complexity 2^{55} to recover 32 bits of key.

The table (6) shows the results of integral attack for the **HISEC** algorithm and others existing algorithms.

Table 6 Result of integral attack for HISEC and other algorithms

Algorithms	**Maximum round**
Lblock [18]	22
TWINE [10]	22
PRESENT [17]	9
KLEIN [8]	7
HISEC	4

From table (6), we can conclude that the integral attack can reach round four for **HISEC** which the least round when we compared with other existing algorithms. This means that **HISEC** is more secure than other algorithms in perspective of integral cryptanalysis.

3.3 Boomerang Attack

The first step to mount this attack, we 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. 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, we can say the attack can't go forward [18]. The following table (7) shows the number of active S-box for the first three rounds of **HISEC** algorithm.

Table 7: Number of active S-box of HISEC for three rounds

No.	**Round**	**Active S-box**
1.	1	1
2.	2	3
3.	3	9

Regarding to the **HISEC** algorithm and depending on table (7), this attack can reach round 5 with maximal probability 2^{-48}**.** The following points will explain that:

- In round 3 there are 9 active S-boxes and in round 2 there are 3 active S-boxes.
- To find the probability, we need to apply the equation (1).
- The final probability is$(((2^{-2})^{9})^{2}) \times (((2^{-2})^{3})^{2}) = 2^{-36} \times 2^{-12} = 2^{-48}$.
- This attack can reach 5 rounds only with probability2^{-48}.

The **HISEC** have 15 rounds which mean it is resistant to the boomerang attack.Moreover, we 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 (8) shows the results of boomerang attack for the **HISEC** algorithm and others algorithms.

Table 8: Maximum round of boomerang attack for HISEC and other existing algorithms

No.	Algorithms	Maximum round	Probability
1.	KLEIN	4	2^{-60}
2.	**HISEC**	5	2^{-48}
3.	PRESENT	7	2^{-56}
4.	Lblock	11	2^{-56}
5.	TWINE	11	2^{-56}

From table (8), the **HISEC** algorithm is more secure than other algorithms in the term of boomerang attack except KLIEN algorithm. The boomerang attack on KLIEN can reach to round 4 which is close to round 5 of **HISEC**.

4. COST DISCUSSION

The second important factor is the cost. According to [8] [9] [20], we can calculate the cost of **HISEC** algorithm. The details of calculating the cost of **HISEC** algorithm as follows:

- The cost of saving 1bits is 6 GE. In **HISEC** algorithm, we have 64bits for plaintext and 80bits for key. The total cost for plaintext and key as follows:
  Plaintext = 64 * 6 = 384 GE.
  Key = 80 *6 = 480 GE
- The cost for each S-box is approximately 22GE. In the proposed algorithm, we have 16 S-boxes. The total cost of four S-boxes is 16 * 22 = 352 GE.
- The cost of 32bit XOR is 87GE approximately. In **HISEC**, there are four 32bits XOR. The total cost for XOR is 4 * 87 = 384 GE.
- There is 50 GE as additional cost.

The total cost for the encryption part of **HISEC** algorithm is:

Plaintext 384 + Key 480 + 16 S-boxes 352 + 4-32bits XOR 384 + additional cost 50 = 1650GE. 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 **HISEC** algorithm is 1650 + 44.08 = 1694.08 GE. The table (9) shows the comparison between the cost of HISEC algorithm and others algorithms.

Table 9 Cost for HISEC 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
HISEC	64	80	16	1694.08GE
KLIEN [8]	64	80	16	2097 GE

From table (9), we can conclude that the cost of **HISEC** algorithm is reasonable and isn't the highest cost. Also, there are two algorithms used 8 S-boxes while **HISEC** used 16 S-boxes.

5. CONCLUSION

This paper proposed new lightweight block cipher algorithm (HISEC). Also, we presented the analysis of HISEC against differential, integral and boomerang attacks. The analysis showed that HISEC is more secure than other algorithms considered in this paper in the terms of differential and integral attacks. Regarding to the boomerang attack, the HISEC is better than other algorithms except KLEIN which the result is close to HISEC. Moreover, we calculated the cost of HISEC in GE and we compared it with others lightweight algorithms. The comparison showed that the cost of HISEC is reasonable which means the cost of HISEC between the least and highest costs of other algorithms.

6. REFERENCE

[1] F Alshaikhli, Imad, and Mohammad A AlAhmad. "Security Threats of Finger Print Biometric in Network System Environment." Journal of Advanced Computer Science and Technology Research 1.1 (2011).

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

[3] Sufyan Salim Mahmood AlDabbagh and Imad Al Shaikhli," Lightweight Block Ciphers: a Comparative Study", in Journal of Advanced Computer Science and Technology Research Vol.2 No.4, November 2012, 159-165.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

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

[10] 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.

[11] 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.

[12] A. Bogdanov and K. Shibutani, "Generalized Feistel networks revisited," Designs, Codes and Cryptography, vol. 66, pp. 75-97, 2013/01/01 2013.

[13] E. Biham and A. Shamir, "Differential Cryptanalysis of DES Variants," in Differential Cryptanalysis of the Data Encryption Standard, Springer New York, 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] Biham, E., Shamir, A.: Differential cryptanalysis of des-like cryptosystems. In: Menezes, A., Vanstone, S.A. CRYPTO 1990. LNCS, vol. 537, pp. 2–21. Springer, Heidelberg (1990).

[16] L. Knudsen and D. Wagner, "Integral Cryptanalysis," in Fast Software Encryption. vol. 2365, J. Daemen and V. Rijmen, Springer Berlin Heidelberg, 2002, pp. 112-127.

[17] W. Shengbao and W. Mingsheng, "Integral Attacks on Reduced-Round PRESENT," in Information and Communications Security. vol. 8233, Springer International Publishing, 2013, pp. 331-345.

[18] Y. Sasaki and L. Wang, "Comprehensive Study of Integral Analysis on 22-Round LBlock," in Information Security and Cryptology – ICISC 2012. vol. 7839, Springer Berlin Heidelberg, 2013, pp. 156-169.

[19] D. Wagner, "The Boomerang Attack," in Fast Software Encryption. vol. 1636, Springer Berlin Heidelberg, 1999, pp. 156-170.

[20] S. Panasenko and S. Smagin, "Lightweight Cryptography: Underlying Principles and Approaches," International Journal of Computer Theory and Engineering, vol. vol 3., 2011.