ISSN 2278-3091
Volume 9, No.1.3, 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse3991.32020.pdf
https://doi.org/10.30534/ijatcse/2020/3991.32020

Modified Round Function of SIMECK 32/64 Block Cipher

Philipcris C. Encarnacion[1], Bobby D. Gerardo[2], Alexander A. Hernandez[3]
[1] Technological Institute of the Philippines Quezon City, Philippines, qpencarnacion@tip.edu.ph
[2] Technological Institute of the Philippines Quezon City, Philippines, bobby.gerardo@gmail.com
[3] Technological Institute of the Philippines Manila, Philippines, alexander.hernandez@tip.edu.ph

ABSTRACT

Lightweight Block Cipher's (LBC) various algorithms need to meet the security requirements for all resource-constrained devices and Internet of Things (IoT) technologies. Various LBC addressed such concerns as the SIMON and SPECK block ciphers, which are known for security and performance. SIMECK, a combination of SIMON and SPECK, shows better performance. However, the SIMECK round function remains a concern. This paper aims to present a modification on the SIMECK round function method simulated on its circular and ARX structure. It took at least seven attempts to reach the appropriate structure. The seventh modification had a circular parameter of (3,5) and a change of right-shift on the structure. The results show that the modified round function achieves 54.58% average on the avalanche effect, the runtime performance of 1.3945ms with a randomness p-value of 0.46931 compared with p-value 0.51512 of the original algorithm. The study explores the ARX structure of LBC, which leads to a good venue to implement with other block ciphers. It is recommended that further evaluation of the modified algorithm will be conducted to test its efficiency, like to verify its vulnerability through different attacks.

Key words: SIMECK, ARX Operations, Avalanche Effect, Randomness Test, Runtime Performance, SIMON, SPECK.

1. INTRODUCTION

Security, cost, and performance are the three significant parts of the lightweight cryptographic architecture. These aim to further lightweight algorithms for Internet of Things (IoT) to have a more secure data with the least memory and power utilization [1]. Over the years, several evaluations and reviews of the different features of Lightweight Block Ciphers (LBC), particularly on security, performances, memory, speeds, and frequency using different cryptanalysis and testing. These procedures are utilizing different platforms, hardware, and software [2], [3], [4], [5].

As the IoTs have gained tremendous use, such as the application of wireless network sensors (WNS) and radio frequency identification (RFID), these are still vulnerable to security threats as devices go smaller in the future with its drawback in shorter processing cycles and lower power supplies [6].

It is important in all LBCs enhancement in recent studies to meet the basic security principles; the need of authenticity and integrity of the information. Such modification may be done in various complex security mechanism; substitution and transposition techniques [7], [8], [9]. The Modified S-DES [7] with the basic operations of bits splits, use of XOR operations and bit shifts influence this study to look for the ARX designs such as the SIMON, SPECK and SIMECK block ciphers.

The release of SIMON and SPECK brought attention to cryptographers in the field of LBC [10]. SIMON is tuned for optimal performance in hardware while SPECK is for optimal performance in software. SIMECK inherits SIMON and SPECK block ciphers' algorithm [11], which is more compact and efficient, providing the same level of information security and properties.

The design of these LBCs made simple using the ARX operation structures where the implementation of the two left-shift operations from the left side to the right side of the plaintext [11]. It also uses a bitwise-AND and three XOR operators in the entire round function. With the reduced rounds [12], all SIMECK variants can be attacked with integral cryptanalysis. The result of the comparison with SIMON and SIMECK [13] leads to an open question on whether better differentials exist on both ciphers with surprisingly higher probability in differential attack for SIMECK32 as observed. In the security evaluation of the SIMECK family, SIMECK32 has the best result in zero linear correlation cryptanalysis on 20-round. Further, SIMECK is an open study on the security level against other cryptanalytic methods [14].

This study attempts to establish a better security performance of the enhanced round function method of the SIMECK 32/64 variant using the primitive arithmetic operators. Moreover, the study is to identify the appropriate ARX structure of the round function through different simulations.

2. RELATED LITERATURE

The study is inspired by the two LBC designed to have optimal performance, both hardware and software, in a resource constraint environment.

2.1 SIMON and SPECK Block Cipher

SIMON is intended for constrained devices to optimize hardware performance and implementations on a low-cost design and to address the security in its simplicity [10], [15]. For its flexible algorithm, SIMON is suitable for WSNs and RFID systems. Its round function is designed, shown in Figure 1. [5] for SIMON represents its simplicity using a combination of the ARX Operations with its different variants in the form of SIMON 2n/mn; 2n-bit block and m-word (mn-bit) key. Table 1 shows the different variants of SIMON and SPECK [16]. As a classic Feistel Network structure, SIMON follows the operations on n-bit words on its round functions [5],

$$f(x)=((x\lll 1) \wedge (x\lll 8)) \oplus (x\lll 2) \quad (1)$$

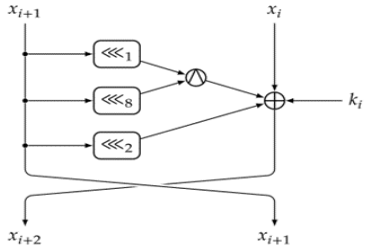


Figure 1: SIMON Round Function

Table 1: SIMON and SPECK Block Ciphers' Parameters

SIMON and SPECK Family Block Cipher (2n/mn)	
Block Size	**Key Sizes**
32	64
48	72, 96
64	96, 128
96	96, 144
128	128, 192, 256

More recently, SIMON is evaluated [17] for its algebraic differential fault analysis on its bit-flip model. As SIMON and SIMECK are of the same structure of parameters (a, b, c) [18], both parameters are not optimal concerning differential characteristics. The design rationale of the SIMON block cipher was clarified that rotation constants (1, 8,2) were not chosen to optimize resistance against integral and impossible differential attacks.

SPECK shows notable performance in software implementation in terms of code size and memory consumption. Moreover, it uses modular addition as nonlinearity [19], likewise the ARX Operations. SPECK round function constructed in a simple method, as shown in Figure 2. [5], has a strong key schedule.

The round function is expressed as:

$$(x,y) \rightarrow (((x \ggg \alpha) + y) \oplus k,\ (y \lll \beta) \oplus ((x \ggg \alpha) + y) \oplus k) \quad (2)$$

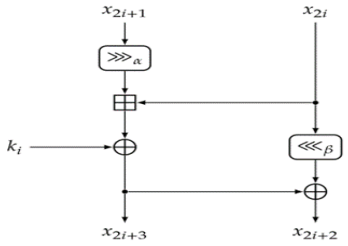


Figure 2: SPECK Round Function

Recently, a study on cryptanalysis of the SPECK round function shows that the SPECK32 with parameter (8,3) is better than SPECK32 with the original (7,2) [19]. Being ARX structure, SPECK was evaluated [20] by formulating SAT/SMT model for Rotational-XOR cryptanalysis. Prior studies relate to its enhancement on the randomness of key-schedule for more secured block cipher and perform faster encryption in software implementation [21].

2.2 SIMECK Family Lightweight Block Cipher

As a Feistel structure, the round function of SIMECK is influenced by both SIMON and SPECK, which performs well in both software and hardware implementations, particularly in the IoT [11], [13], [22]. SIMECK was designed based on the ARX operations such as the AND, XOR, left shift, and rotation from the same structure of SIMON[23].

In Yang [11] design, as shown in Figure 3. denotes SIMECK 2n/mn, where n is the plaintext size, and n should be 16, 24, or 32. 2n is the block size, and mn is the key size. Therefore, SIMECK had the following variants; SIMECK 32/64, SIMECK 48/96, and SIMECK 64/128. The round function is expressed as:

$$R_{Ki}(l_i, r_i) = (r_i \oplus f(l_i) \oplus k_i, l_i);$$
$$f(x) = (x \odot (x \lll 5)) \oplus (x \lll 1). \quad (3)$$

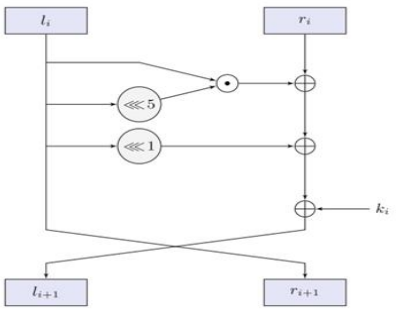


Figure 3: SIMECK Round Function

Years after SIMECK was introduced, a brief comparison with SIMON was conducted to analyze the impact of the design on the compared upper bounds probability of differential and linear cryptanalysis [13]. It provides new differentials for SIMECK, which covered more rounds than the previous SIMON's results, which can cover more rounds compared to previous results. More studies also conducted with SIMECK to further understand its challenges [14], [23], [24], [25], [26], [27]. Another comparative work on reduced-round SIMON-32/64 and SIMECK-32/64 on correlated sequence attack with a record of best attack in 16% security margin [28].

2.3 ARX Operations and Structure

ARX is short for Addition, Rotation, XOR, which is a broad class of symmetric-key cryptographic algorithms is designed by combining a small set of simple operations. Different algorithms had adopted this type of design, including block ciphers, hash functions, and stream ciphers. Prior studies show different ciphers implementing such ARX structures [29], [30], [31]. Advantages with the design include getting rid of the table look-ups, minimizes the total number of operations during encryption, and programming codes are minimal in terms of memory use.

SIMECK as an ARX structure, perform and operate quickly on software with different file sizes, and demonstrates swift encryption times as evaluated as the demand for the IoT structures increases, implementations. Evaluation of ARX-based LBC continues, such as to the following [29], [32].

2.4 Avalanche Effect

This technique is used for the cryptographic algorithm to evaluate its desirable percentage, or a significant number of bits changed from the plain text to ciphertext. One way to get the number of changed bits in ciphertext is through the Hamming Distance [33]. This technique is express as the following:

$$AE(\%) = \frac{\#\ of\ changed\ bits\ in\ ciphertext}{total\ \#\ of\ bits\ in\ ciphertext} x\ 100 \quad (4)$$

The result of the avalanche effect should satisfy the probability of more than 50%. Such technique is also used in subsequent studies in LBC [34], [35], [36].

3. PROPOSED METHOD

This paper modifies the round function method of SIMECK 32/64 variant block cipher to test the security with the use of avalanche effect and randomness test on the output ciphertext and its performance. Figure 4. shows the diagram of the SIMECK 32/64 round function with the proposed modification implemented only the encryption process.

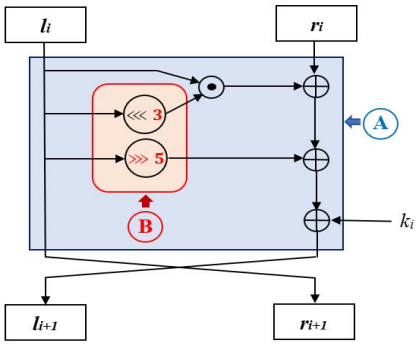


Figure 4: Modification of SIMECK Round Function

This study performed different modifications and its simulations on the identified area A in Figure 4. Different structural parameters of the round function were evaluated from circular and ARX operations to determine the appropriate parameters for SIMECK 32/64.

Figure 4. area B shows the final modification of SIMECK 32/64 round function, particularly the ARX constant values of 3 and 5 on the shift operators, and the use of right-shift instead of left-shift, respectively. The other operators remain the same with the key schedule algorithm, which has a substantial security issue that inherits from SPECK block cipher [37]. The modified SIMECK 32/64 is now expressed as:

$$R_{Ki}(l_i, r_i) = (r_i \oplus f(l_i) \oplus k_i, l_i);$$
$$f(x) = (x \odot (x \lll 3)) \oplus (x \ggg 5). \quad (5)$$

```
SIMECK Encryption Process:
{
   Input: 32-bit plaintext(P)
   Key: 64 bits (k)
   Output: ciphertext (C)

   Split P into L1 and R2                  //Left and Right plain text
   Split km into t0, t1, t2, and k0        //km- master key

   For i ← 1 to roundNumber {
      (Li, Ri) ←Ri XOR (Li AND leftshift(Li, 3)) XOR
                  rightshift(Li, 5) XOR Ki, Li)
      KeyExpansion(t0, t1, t2, k0)
   }
   C ← Li || Ri
}
```

This study used C programming language adopted the designed algorithm [12] and implemented, compiled, and run with Dev-C++ 5.11 in Windows 10 environment. The system platform used for the experiment has the specifications; Processor: Intel (R) Core (TM) i7 – 8565U CPU @ 1.80GHz 1.99 GHz; RAM: 8:00 GB; System Type: 64 – bit Operating System, x64-based processor.

For the simulation of the avalanche effect and on the other variables for this study, test data of 15 sets of plaintexts in a hexadecimal value served as the input data. These plaintexts already set as the left-value and right-value, as depicted in Table 2—this test data utilized in processing the computation of the randomness test and its runtime performance. Different simulations were illustrated below to present the performance of the algorithm. Table 3 shows the binary value of Table 2.

Table 2: Test Data: The Plaintexts in Hexadecimal Value

SN	PlainText_32 (Hexadecimal Value)							
	Left				Right			
1	6	8	7	7	6	5	6	5
2	3	8	5	3	9	7	4	3
3	7	5	2	9	5	8	3	6
4	8	7	5	2	3	9	4	9
5	3	9	7	2	9	0	4	1
6	4	9	2	2	4	0	7	3
7	5	0	3	0	6	4	0	2
8	7	4	0	1	2	8	0	5
9	5	6	8	8	7	9	4	4
10	4	5	5	2	6	2	7	7
11	1	0	0	2	1	2	7	5
12	4	3	1	2	2	0	2	0
13	0	2	1	2	7	9	4	5
14	8	8	2	5	6	6	1	0
15	3	0	1	6	2	1	0	9

Table 3: Plaintexts in Binary Value

SN	Plain Text_32 (Binary Value)							
	Left Value				Right Value			
1	0110	1000	0111	0111	0110	0101	0110	0101
2	0011	1000	0101	0011	1001	0111	0100	0011
3	0111	0101	0010	1001	0101	1000	0011	0110
4	1000	0111	0101	0010	0011	1001	0100	1001
5	0011	1001	0111	0010	1001	0000	0100	0001
6	0100	1001	0010	0010	0100	0000	0111	0011
7	0101	0000	0011	0000	0110	0100	0000	0010
8	0111	0100	0000	0001	0010	1000	0000	0101
9	0101	0110	1000	1000	0111	1001	0100	0100
10	0100	0101	0101	0010	0110	0010	0111	0111
11	0001	0000	0000	0010	0001	0010	0111	0101
12	0100	0011	0001	0010	0010	0000	0010	0000
13	0000	0010	0001	0010	0111	1001	0100	0101
14	1000	1000	0010	0101	0110	0110	0001	0000
15	0011	0000	0001	0110	0010	0001	0000	1001

4. RESULT AND DISCUSSION

This study tried to look for the appropriate circular shift constant values with its equivalent bitwise-AND and XOR operators. Below are the different simulations of the SIMECK 32/64 round function.

A. SIMECK 32/64 Block Cipher Round Function - Original

This section speaks on the Avalanche Effect simulations on different modifications of the round function method of SIMECK 32/64 block cipher. Table 4 presents the ciphertexts produced using the original algorithm of the SIMECK 32/64 round function. The encryption process produced an average of 48.33% in several bits changed in the given test data and a median value of 50.00 for an avalanche effect.

B. Modification on SIMECK 32/64 Round Function

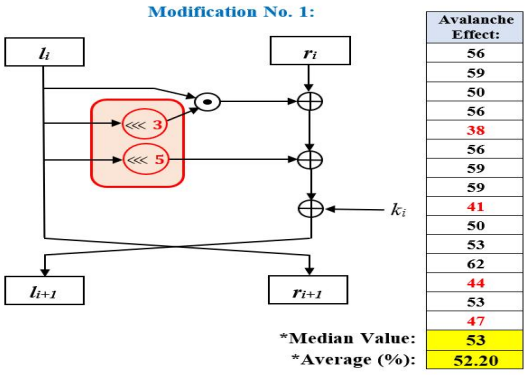
To illustrate the different trials on the experiments and evaluation conducted in this study before coming up with the appropriate modification, below are the strategies:

The first simulation presents the modification of the constant values of the left-shifts (Figure 5). It provided a good result of 52.20% average number of bits changed and a median value of 53 for an avalanche effect on 15 sets of data. Simulation 2 depicts in Figure 6, this time, presents the modified XOR operator into bitwise-AND, which provides an average of 51.13% of the total number of bits changed and a median value of 53 as the encryption process being performed.

This strategy only modifies the left-shift into a right-shift with the same condition in Figure 6. and Figure 7. illustrates the 3rd simulation, which provides an average of 48.40% of the total number of bits changed and a median value of 53 of the avalanche effects on the given test data.

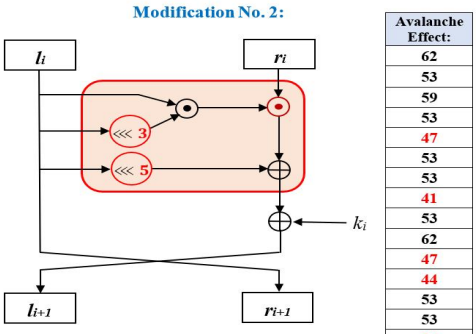
Table 4: Ciphertext Output of the Original Round Function - SIMECK 32/64

Ciphertext Output of the Original Algorithm of SIMECK 32/64			
SN	Ciphertext (Hexa-decimal Value)	Ciphertext_32 (output) (Binary Value)	Avalanche Effect:
1	770d2c76	01110111000011010010110001110110	50.00
2	5e480e4b	01011110010010000000111001001011	40.63
3	89953cd5	10001001100101010011110011010101	59.38
4	d9c5fddd	11011001110001011111110111011101	50.00
5	b653633d	10110110010100110110000100111101	56.25
6	de52892a	11011110010100101000100100101010	50.00
7	113ae86a	00010001001110101110100001101010	31.25
8	f1ead6c3	11110001110101011010111000011	62.50
9	feda30d5	11111110110110100011000011010101	37.50
10	ebc17cb2	11101011110000010111110010110010	53.13
11	47b4d80d	01000111101101001101100000001101	50.00
12	9ed3f964	10011110110100111111100101100100	31.25
13	73379551	01110011001101111001010101010001	62.50
14	b9fd8411	10111001111111011000010000010001	37.50
15	ff84e9f3	11111111100001001110100111110011	53.13
		* The Median Value:	50.00
		*The Average (%):	48.33



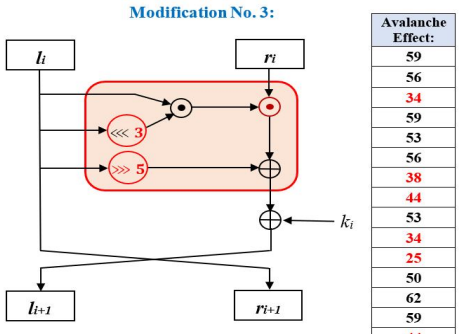
Avalanche Effect:
56
59
50
56
38
56
59
59
41
50
53
62
44
53
47
*Median Value: 53
*Average (%): 52.20

Figure 5: Modification No. 01 - SIMECK 32/64 Round Function



Avalanche Effect:
62
53
59
53
47
53
53
41
53
62
47
44
53
53
34
*Median Value: 53
*Average (%): 51.13

Figure 6: Modification No. 02 - SIMECK 32/64 Round Function

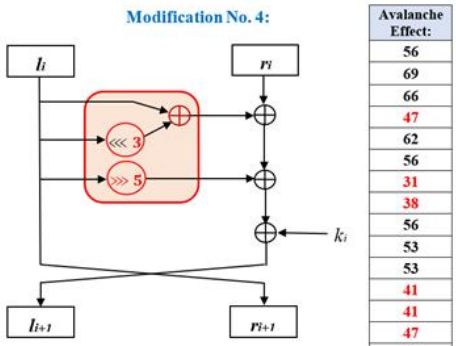


Avalanche Effect:
59
56
34
59
53
56
38
44
53
34
25
50
62
59
44
*Median Value: 53
*Average (%): 48.40

Figure 7: Modification No. 03 - SIMECK 32/64 Round Function

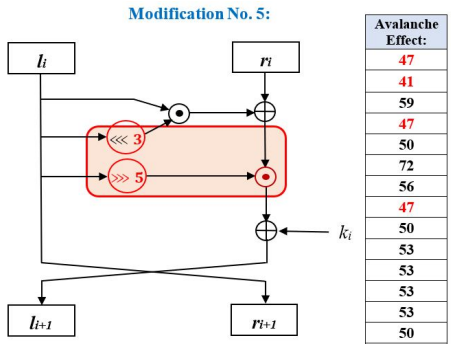
Figure 8. shows the same concepts of Figure 7., but it changes the bitwise-AND into XOR operator. With this, the average avalanche effect gives us 51.47% of the total number of bits changed with a median value of 53.

Another two simulations are shown in Figure 9. and Figure 10. It demonstrates that changing the middle XOR operator at the right side in Figure 9, resulted in an avalanche effect of 51.47% of the total number of bits changed with a median of 50. It also observed that ciphertext values of 2555bb98 and fbd5ce68 repeatedly 6 and 4 times, respectively.



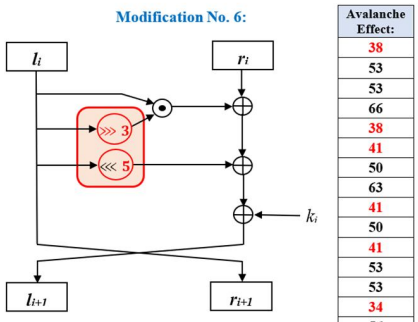
Avalanche Effect:
56
69
66
47
62
56
31
38
56
53
53
41
41
47
56
*Median Value: 53
*Average (%): 51.47

Figure 8: Modification No. 04 - SIMECK 32/64 Round Function



Avalanche Effect:
47
41
59
47
50
72
56
47
50
53
53
53
53
50
41
*Median Value: 50
*Average (%): 51.47

Figure 9: Modification No. 05 - SIMECK 32/64 Round Function



Avalanche Effect:
38
53
53
66
38
41
50
63
41
50
41
53
53
34
56
*Median Value: 50
*Average (%): 48.67

Figure 10: Modification No. 06 - SIMECK 32/64 Round Function

After doing the above six modifications and simulations, it is observed that the seventh modification reached the highest avalanche effect. The study appropriately selects the circular shift with its constant values of 3 and 5, respectively, as expressed in Figure 11. This modification turned the left-shift into the right-shirt on the last circular moved. It shows the highest avalanche effect of 54.67% of the total number of bits changed with a median value of 56. As a summary, Table 5 provides the details.

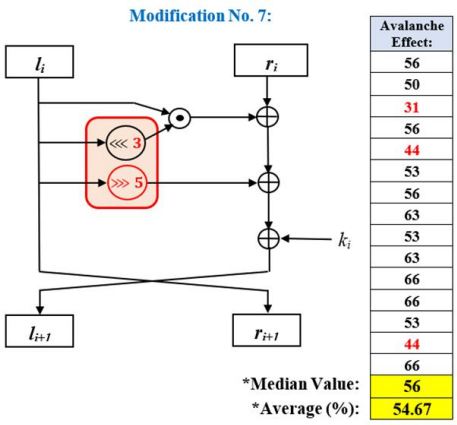


Figure 11: Modification No. 07 - SIMECK 32/64 Round Function (Final)

Table 5 depicts that only three ciphertexts under the required percentage of an avalanche effect. Numbers 3, 5, and 14 represent the data with red color, which means failed to meet the required percentage of a strong avalanche effect. Therefore, it shows that Figure 11., with its modified algorithm, is more secured than the original algorithm (Table 4). More so, Table 6 depicts that it is more advantageous in terms of security with the modified round function of the SIMECK 32/64 variant.

Table 5: Ciphertext Output of the Modified Round Function - SIMECK 32/64 (Final)

Ciphertext Output of the Modified 07 of SIMECK 32/64			
SN	**Ciphertext (Hexadecimal Value)**	**Ciphertext_32 (output) (Binary Value)**	**Avalanche Effect:**
1	a52cb4d4	10100101001011001011010011010100	56
2	51fea8c3	01010001111111101010100011000011	50
3	f4082820	11110100000010000010100000100000	31
4	f83ebd3a	11111000001111101011110100111010	56
5	83f15a4b	10000011111000101011010010011011	44
6	5e56afb3	01011110010101101010111110110011	53
7	33130b55	00110011000100110000101101010101	56
8	99d7bd79	10011001110101111011110101111001	63
9	70ba06d2	01110000101110100000011011010010	53
10	eb7a990c	11101011011101010011001000011100	63
11	27bfef1d	00100111101111111111011100011101	66
12	328dff2f	00110010100011011111111100101111	66
13	2fdde1ad	00101111101110111110000110101101	53
14	91938e98	10010001100100111000111010011000	44
15	97e1f0fb	10010111111000011111000011111011	66
		*** The Median Value:**	**56**
		***The Average (%):**	**54.67**

Table 6: Comparative Summary of SIMECK 32/64 - Avalanche Effect

Method	SIMECK 32/64 (Original)	SIMECK 32/64 **(Modified)**
Avalanche Effect (Average - %)	48.33	**54.58**

C. Runtime Performance Test

The original and modified algorithms of the round function of SIMECK 32/64 were evaluated in terms of runtime performance. Table 7 shows the comparative runtime performance of the two algorithms, which ended in favor of the modified algorithm with the shortest time of 1.3945ms. An average of the 15 sets of samples, while the original algorithms have an average time of 2.4423ms.

D. Randomness Tests

The randomness test for SIMECK 32/64 resulted in an average of 0.46931, which identified that the original algorithm has the best result over the modified algorithm. Tables 8 and 9 show the comparative randomness test of the two algorithms. It also shows that under the modified algorithm, the first value tested does not meet the acceptable p-value of 0.0010. Instead, it only achieves a p-value of 0.00421. Out of 15 test data evaluated, only 1 data failed, which in Table 9. Unlike on the original algorithm, all test data achieves the required p-value.

Table 7: Comparative Runtime Performance Evaluation of SIMECK 32/64

Runtime Performance Evaluation of SIMECK 32/4				
SN	**Original Algorithm**		**Modified Algorithm**	
	Ciphertext (Hexadecimal Value)	Runtime (ms)	Ciphertext (Hexadecimal Value)	Runtime (ms)
1	770d2c76	0.5719	a52cb4d4	1.0210
2	5e480e4b	1.0520	51fea8c3	1.1860
3	89953cd5	1.0050	f4082820	1.1490
4	d9c5fddd	1.6850	f83ebd3a	0.9525
5	b653633d	1.2020	83f15a4b	0.9641
6	de52892a	0.7822	5e56afb3	1.2250
7	113ae86a	0.7711	33130b55	2.8640
8	f1ead6c3	1.6760	99d7bd79	0.8521
9	feda30d5	3.4130	70ba06d2	0.8518
10	ebc17cb2	5.0320	eb7a990c	5.0390
11	47b4d80d	2.7920	27bfef1d	0.9599
12	9ed3f964	1.5210	328dff2f	0.7875
13	73379551	5.0510	2fdde1ad	0.9275
14	b9fd8411	5.0430	91938e98	1.3710
15	ff84e9f3	5.0380	97e1f0fb	0.7666
***Median Value:**		**1.6760**		**0.9641**
***Average Value:**		**2.4423**		**1.3945**

Table 8: Randomness Test for Original SIMECK 32/64

SN	Original Algorithm - Randomness Test			
	Ciphertext (Hexadecimal Value)	**Frequency (Monobit) Test**	**Frequency Block Test**	**Runs Test**
1	770d2c76	0.72367	0.72367	0.70608
2	5e480e4b	0.47950	0.47950	0.92845
3	89953cd5	1.00000	1.00000	0.07710
4	d9c5fddd	0.03389	0.03389	1.00000
5	b653633d	0.47950	0.47950	0.24309
6	de52892a	0.72367	0.72367	0.03141
7	113ae86a	0.47950	0.47950	0.24309
8	f1ead6c3	0.28884	0.28884	0.56695
9	feda30d5	0.28884	0.28884	0.56695
10	ebc17cb2	0.47950	0.47950	0.92845
11	47b4d80d	0.72367	0.72367	0.98230
12	9ed3f964	0.28884	0.28884	0.83670
13	73379551	0.72367	0.72367	0.14932
14	b9fd8411	1.00000	1.00000	0.28884
15	ff84e9f3	0.07710	0.07710	0.17802
			***Median Value:**	**0.56695**
			***Average Value:**	**0.51512**

Table 9: Randomness Test for Modified 07 SIMECK 32/64

SN	Modified Algorithm - Randomness Test			
	Ciphertext (Hexadecimal Value)	**Frequency (Monobit) Test**	**Frequency Block Test**	**Runs Test**
1	a52cb4d4	0.72367	0.72367	0.00421
2	51fea8c3	0.72367	0.72367	0.98230
3	f4082820	0.01333	0.01333	0.49829
4	f83ebd3a	0.15730	0.15730	0.70608
5	83f15a4b	1.00000	1.00000	0.72367
6	5e56afb3	0.15730	0.15730	0.05935
7	33130b55	0.47950	0.47950	0.12690
8	99d7bd79	0.07710	0.07710	0.31536
9	70ba06d2	0.47950	0.47950	0.65346
10	eb7a990c	0.72367	0.72367	0.46413
11	27bfef1d	0.03389	0.03389	0.03389
12	328dff2f	0.15730	0.15730	0.70608
13	2fdde1ad	0.15730	0.15730	0.70608
14	91938e98	0.47950	0.47950	0.92845
15	97e1f0fb	0.15730	0.15730	0.13143
			***Median Value:**	**0.49829**
			***Average Value:**	**0.46931**

5. CONCLUSION

This paper attempts to evaluate the proposed modified round function of SIMECK 32/64, through some modification on the circular and ARX operations. There were 15 sets of data utilized for the avalanche effect in all simulations. The modified SIMECK 32/64 variant has a comparative advantage, with an average of 54.67% on the total number of bits changed over the original SIMECK 32/64. It is tested in terms of its run time performance, which resulted in 1.3945ms shortest time than the other. This study found that the modified algorithm of SIMECK 32/64 is more reliable in terms of security and performance than the original algorithm. Furthermore, on the evaluation for the randomness of the bits, it shows that the original algorithm of SIMECK 32/64 has a better average p-value of 0.51512 than the modified algorithm of 0.4693.

Modification of the round function, particularly in ARX structure by substitution, enhance the security and performance of a block cipher. It can be implemented both hardware and software in the field of IoT. This proposed enhancement would help more learners to explore the ARX structure in cryptography.

For future research, a challenge to look over on the manipulation of what appropriate circular structures and ARX operations be applied to meet the best evaluation for SIMECK 32/64. For better security, it might be useful also to modify the key expansion method. It is recommended that further evaluation of the modified algorithm will be conducted to test its efficiency like to test its vulnerability through different attacks.

ACKNOWLEDGEMENT

The authors are grateful to the anonymous reviewers for providing constructive comments and suggestions to improve the quality of the paper. Also, the authors acknowledge the support of the Commission on Higher Education in providing financial support in the study.

REFERENCES

1. A. Shah and M. Engineer, “A Survey of Lightweight Cryptographic Algorithms for IoT-Based Applications,” in *Smart Innovations in Communication and Computational Sciences, Advances in Intelligent Systems and Computing*, 2019, pp. 283–293. https://doi.org/10.1007/978-981-13-2414-7_27
2. D. Sehrawat and N. S. Gill, “Lightweight Block Ciphers for IoT based applications: A Review,” *Int. J. Appl. Eng. Res. ISSN 0973-4562*, vol. 13, no. 5, pp. 2258–2270, 2018.
3. B. S. Rao and P. Premchand, “A Review on Combined Attacks on Security Systems,” *Int. J. Appl. Eng. Res. ISSN 0973-4562*, vol. 13, no. 23, pp. 16252–16278, 2018.
4. G. Hatzivasilis, K. Fysarakis, I. Papaefstathiou, and C. Manifavas, “A review of lightweight block ciphers,” *J. Cryptogr. Eng.*, vol. 8, no. 2, pp. 141–184, 2018.
5. R. Avanzi, “A Salad of Block Ciphers.,” *IACR Cryptol. ePrint Arch. ISSN 19853505*, vol. 2016, no. 3, p. 1171, 2016.
6. N. Khan, N. Sakib, I. Jerin, S. Quader, and A.

Chakrabarty, "Performance analysis of security algorithms for IoT devices," *5th IEEE Reg. 10 Humanit. Technol. Conf. 2017, R10-HTC 2017*, vol. 2018-Janua, pp. 130–133, 2018.

7. A. Maqsood and W. Haider, "Towards Security Enhancement using Block Cipher Algorithm with Transposition Techniques," *Int. J. Multidiscip. Cryptol. Inf. Secur. ISSN 2320 -2610*, vol. 6, no. 3, pp. 1–6, 2017.
8. M. G. Z. Fernando, A. M. Sison, and R. P. Medina, "Secured Private Key Handling using Transposition Cipher Technique," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1, pp. 85–89, 2020.
9. N. Sharma, H. Meghwal, M. Mehta, and T. Kumar, "A Review on Playfair Substitution Cipher and Frequency Analysis Attack on Playfair," *2018 2nd Int. Conf. Trends Electron. Informatics (ICOEI), Tirunelveli*, pp. 1–9, 2018. https://doi.org/10.1109/ICOEI.2018.8553837
10. R. Beaulieu *et al.*, "The SIMON and SPECK lightweight block cIPhers," *Proc. - Des. Autom. Conf.*, vol. 2015-July, pp. 1–6, 2015.
11. G. Yang, B. Zhu, V. Suder, M. D. Aagaard, and G. Gong, "The Simeck Family of Lightweight Block Ciphers," *Int. Assoc. Cryptologic Res. CHES 2015*, vol. LNCS 9293, pp. 307–329, 2015.
12. K. Zhang, J. Guan, B. Hu, and D. Lin, "Integral cryptanalysis on Simeck," in *6th International Conference on Information Science and Technology, ICIST 2016*, 2016, pp. 216–222. https://doi.org/10.1109/ICIST.2016.7483413
13. S. Kölbl and A. Roy, "A brief comparison of Simon and Simeck," *A. Bogdanov Light. 2016*, vol. 10098 LNCS, pp. 69–88, 2017.
14. K. Zhang, J. Guan, B. Hu, and D. Lin, "Security evaluation on Simeck against zero-correlation linear cryptanalysis," *IET Inf. Secur.*, vol. 12, no. 1, pp. 1–11, 2018.
15. S. Abed, R. Jaffal, B. J. Mohd, and M. Alshayeji, "FPGA modeling and optimization of a SIMON lightweight block cipher," *Sensors (MDPI, Basel, Switzerland)*, vol. 19, no. 4, 2019.
16. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, "Simon and Speck: Block Ciphers for the Internet of Things," *Proc. 52nd Annu. Des. Autom. Conf. - DAC '15*, 2015.
17. D. P. Le, S. L. Yeo, and K. Khoo, "Algebraic Differential Fault Analysis on SIMON Block Cipher," *IEEE Trans. Comput.*, vol. 68, no. 11, pp. 1561–1572, 2019.
18. K. Kondo, Y. Sasaki, Y. Todo, and T. Iwata, "On the Design Rationale of Simon Block Cipher: Integral Attacks and Impossible Differential Attacks against Simon Variants," *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, vol. E101A, no. 1, pp. 88–98, 2018.
19. J. Ren and S. Chen, "Cryptanalysis of Reduced-Round SPECK," *IEEE Access*, vol. 7, pp. 63045–63056, 2019.
20. Y. Liu, G. De Witte, A. Ranea, and T. Ashur, "Rotational-XOR Cryptanalysis of Reduced-round SPECK," *IACR Trans. Symmetric Cryptol. ISSN 2519-173X*, vol. 2017, no. 3, pp. 24–36, 2017.
21. R. A. F. Lustro, A. M. Sison, and R. P. Medina, "Performance Analysis of Enhanced SPECK Algorithm," in *ICIBE' 18, October 24–26, 2018, Macau, Macao*, 2019, pp. 256–264. https://doi.org/10.1145/3288155.3288196
22. H. Li, J. Ren, and S. Chen, "Improved Integral Attack on Reduced-Round Simeck," *IEEE Access*, vol. 7, pp. 118806–118814, 2019.
23. S. Sadeghi and N. Bagheri, "Security analysis of SIMECK block cipher against related-key impossible differential," *Inf. Process. Lett.*, vol. 147, no. July 2019, pp. 14–21, 2019.
24. Y. S. Sofu Risqi and S. Windarta, "Statistical test on lightweight block cipher-based PRNG," *Proceeding 2017 11th Int. Conf. Telecommun. Syst. Serv. Appl. TSSA 2017*, vol. 2018-Janua, pp. 1–4, 2018.
25. T. A. Darumaya and B. H. Susanti, "Forgery Attack on LightMAC Hash Function Scheme using SIMECK 32/64 Lightweight Block Cipher," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 453, no. 1, 2018.
26. M. Zaheri and B. Sadeghiyan, "SMT-based Cube Attack on Simeck32/64," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 130, 2018.
27. P. Bhoyar, S. B. Dhok, and R. B. Deshmukh, "Hardware implementation of secure and lightweight Simeck32/64 cipher for IEEE 802.15.4 transceiver," *AEU - Int. J. Electron. Commun.*, vol. 90, no. December 2017, pp. 147–154, 2018. https://doi.org/10.1016/j.aeue.2018.04.002
28. R. Rohit and G. Gong, "Correlated Sequence Attack on Reduced-Round Simon-32/64 and Simeck-32/64," *IACR Cryptol. ePrint Arch. Math. Comput. Sci.*, pp. 1–19, 2018.
29. B. Seok and C. Lee, "Fast implementations of ARX-based lightweight block ciphers (SPARX, CHAM) on 32-bit processor," *Int. J. Distrib. Sens. Networks*, vol. 15, no. 9, pp. 1–9, 2019.
30. A. D. Dwivedi and P. Morawiecki, "Di□erential cryptanalysis in ARX ciphers, Application to SPECK (Dwivedi, 2016).pdf," *IACR Cryptol. ePrint, 2018 Comput. Sci.*, p. 899, 2018.
31. D. Dinu, L. Perrin, A. Udovenko, V. Velichkov, J. Großschädl, and A. Biryukov, "Design strategies for ARX with provable bounds: SPARX and LAX," in *IACR Cryptology ePrint Archive 2016*, 2016, p. 984. https://doi.org/10.1007/978-3-662-53887-6_18
32. M. Qasaimeh, R. S. Al-Qassas, and S. Tedmori, "Software randomness analysis and evaluation of lightweight ciphers: the prospective for IoT

security," *Multimed. Tools Appl.*, vol. 77, pp. 18415–18449, 2018.

33. M. O. Espina, A. C. Fajardo, B. D. Gerardo, and R. P. Medina, "Multiple level information security using image steganography and authentication," *Int. J. Adv. Trends Comput. Sci. Eng. ISSN 2278-3091*, vol. 8, no. 6, pp. 3297–3303, 2019. https://doi.org/10.30534/ijatcse/2019/100862019
34. R. J. Rasras, Z. Alqadi, M. R. A. Sara, and B. Zahran, "Developing new Multilevel security algorithm for data encryption-decryption (MLS_ED)," *Int. J. Adv. Trends Comput. Sci. Eng. ISSN 2278-3091*, vol. 8, no. 3, pp. 3228–3235, 2019. https://doi.org/10.30534/ijatcse/2019/90862019
35. R. M. Marzan, A. M. Sison, and R. P. Medina, "Randomness analysis on enhanced key security of Playfair cipher algorithm," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 8, no. 4, pp. 1248–1253, 2019. https://doi.org/10.30534/ijatcse/2019/34842019
36. R. B. Antonio, A. M. Sison, and R. P. Medina, "A modified generation of S-box for advanced encryption standards," *ACM Int. Conf. Proceeding Ser.*, vol. Part F1483, pp. 280–283, 2019.
37. R. Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, and B. Weeks, "Notes on the design and analysis of Simon and Speck," *IACR Cryptol. ePrint Arch.*, p. 560, 2017.