International Journal of Cryptology Research 5(2): 28-44 (2015)

Statistical Analysis on Lightweight Block Cipher, SIMON

[1]Isma Norshahila Mohammad Shah, [2]Liyana Chew Nizam Chew, [3]Nor Azeala Mohd Yusof, [4]Nik Azura Nik Abdullah, [5]Norul Hidayah Lot@Ahmad Zawawi and [6]Hazlin Abdul Rani

Cyber Technology Research Department,
CyberSecurity Malaysia,
Kuala Lumpur, Malaysia

Email: [1]isma@cybersecurity.my, [2]liyana@cybersecurity.my,
[3]azeala@cybersecurity.my, [4]azura@cybersecurity.my,
[5]norul@cybersecurity.my, [6]hazlin@cybersecurity.my

ABSTRACT

In this paper, we present a statistical analysis on the members of the lightweight block cipher, SIMON. SIMON family of block ciphers was proposed by the National Security Agency (NSA) in June 2013. It consist variety of blocks and key sizes. Even though it is designed to be flexible on variety of platforms but it is tuned for optimal performance on hardware. In this paper, analysis was performed on SIMON64/96, SIMON96/96 and SIMON128/128 by using NIST Statistical Test Suite. These algorithms were tested using the output sequence generated from nine data categories. From the analysis conducted, it is conclude that the outputs from the sample tested on the algorithms are non-random.

Keywords: *lightweight block cipher, Statistical analysis, SIMON block cipher, significance level, NIST Statistical Test Suite, randomness analysis*

1. INTRODUCTION

Lightweight cryptography is being used in hardware with sensitive application such as RFID systems, sensor networks, the Internet of Things (IoT) and many more. The hardware used in these applications will likely be constrained in regards of computational power, battery, as well as memory. Lightweight cryptography is tailored for such constrained devices, with the goal of balancing the trade-offs between low resource requirements, performance, and cryptographic strength.

In June 2013, National Security Agency (NSA) released a new family of lightweight block cipher, SIMON (Ray B. *et al* (2013)). It comes in a variety of widths and key sizes. SIMON family can perform well in hardware and software but it is optimized for hardware platforms. There are several published research papers that discussed the attacks applied on Simon family since it was first published (A. Alkhzaimi and Lauridsen (2013), Biryukov *et al* (2015), F Abed *et al* (2015)).

One of the important criteria when evaluating an algorithm is to demonstrate its capability as a random number generator. The ciphertext generated from block cipher algorithm should be uniformly distributed when all of the plaintext or key blocks used during encryption are different. Statistical analysis can be used to determine whether the algorithm can fulfill this criterion. If a block cipher appears to be non-random, then it becames vulnerable to any type of attacks.

One of the techniques used to evaluate the randomness properties is by using the NIST Statistical Test Suite (Andrew R. *et. al* (2010)). For the evaluation of block ciphers presented for AES competition in 1997, Soto (2000) proposed nine different ways to generate large sequences of data from block ciphers and tested these streams using the NIST Statistical Test Suite.

This paper will illustrate the statistical analysis conducted on selected algorithms of SIMON family of lightweight block cipher. The analysis reported here focused on SIMON64/96, SIMON96/96 and SIMON128/128. Even though Simon has ten variety of sizes, we decided to only focus on three sizes of algorithm. Recent study shows that simplicity and security are the main goals when designing a lightweight block cipher. Therefore, 64 bits block size is great enough to be embedded on hardware and key size of around 80 bits is often enough. Beginning 2011, NIST recommended minimum security strength of 112 bits for algorithm used by Federal government (Barker E. and Roginsky A. (2011)). Therefore, SIMON128/128 is chosen due to the security provided by the key size of this algorithm. To the best of our knowledge, this is the first time that the statistical tests are performed on SIMON.

2. A BRIEF DESCRIPTION OF SIMON

SIMON algorithm, which was designed by NSA, aims to fill the need for secure, flexible, and analyzable lightweight block ciphers. SIMON was designed to be flexible on a variety of platforms but it is tuned for optimal performances in hardware (Ray B. *et al* (2013)). SIMON block cipher operates in classical Feistel scheme. SIMON supports block sizes of 32, 48, 64, 96 and 128 bits, with up to three key sizes to go along with each block size. In this paper, SIMON with 64-bit block and 96-bit key, they will be represented as SIMON64/96.

3. ROUND FUNCTION OF SIMON

SIMON utilizes a classical Feistel structure as shown in Figure 1. In general, each round of SIMON uses three operations; bitwise XOR (⊕), bitwise AND (&) and left circular shift (S^j) by j bits. It includes a non-linear and non-invertible function, F. Given X ϵ {0, 1}^{n}, F(X) is calculated as follows:

$$F(X) = (X <<< 2) \oplus ((X <<< 1) \,\&\, (X <<< 8))$$

SIMON operates on two n-bit halves in each round. The output of F is XORed with the right half and round key. Output of this XOR operation is swapped with the left half.

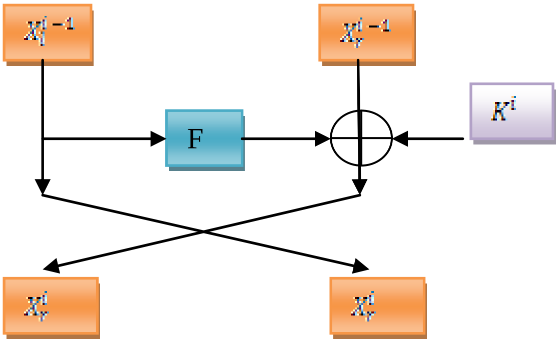

Figure 1: Round Function of SIMON

4. KEY SCHEDULE OF SIMON

Depending on the size of the algorithm, the key size varies. It operates on two and three n-bit words registers as shown in Table 1. It performs two rotation operations to the right by x >>> 3 and x >>>1. The rotation result is XORed with a fixed constant, c and a constant sequence, z which are dependent. Assuming that the number of word for key, K is m, the first subkeys are driven from K, i.e. $K^0 \ldots K^{m-1}$. The subkey for round i where $m \leq i \leq r\text{-}1$, is calculated as follows:

$$m{=}2;\ K^i = K^{i-2} \oplus (K^{i-1} >>> 3) \oplus (K^{i-1} >>> 4) \oplus \mathrm{c} \oplus (\mathrm{z})_{\mathrm{i-m}}$$
$$m{=}3;\ K^i = K^{i-3} \oplus (K^{i-1} >>> 3) \oplus (\mathrm{K}^{\mathrm{i-1}} >>> 4) \oplus \mathrm{c} \oplus (\mathrm{z})_{\mathrm{i-m}}$$

where $c = 2^{n-1} \oplus 3$;
$(z)_{i\text{-}m}$ denotes the i^{th} bit of z where $m \leq i \leq r\text{-}1$; $i\text{-}m$ is modulo by 62;

z = 10101111011100000011010010011000101000010001111110010110110011

Algorithm	**Block Size**	**Key Size**	**Number of Rounds**	**Input size of one word, *n***	**Number of word for key, *m***
SIMON64/96	64	96	42	32	3
SIMON96/96	96	96	52	48	2
SIMON128/128	128	128	68	64	2

Table 1: Details of variants in SIMON

5. RANDOMNESS TEST

Statistical tests for the output of the SIMON was analyzed under full round considerations, which are 42 rounds for SIMON64/96, 96 rounds for SIMON96/96 and 128 rounds for SIMON128/128.

This test was conducted using the NIST Statistical Test Suite (StsGui MFC Application) developed by the National Institute of Standards and Technology, USA (NIST). The tool was developed to evaluate the statements that the stream is generated by a truly random source. The NIST Statistical Test Suite (Ray B. *et al* (2013)) consists of 15 tests. Descriptions of each test are explained in Appendix A. These 15 tests are divided into two categories which are Parameterized Test Selection and Non-Parameterized Test Selection. Users need to identify parameter value for each test in Parameterized Test Selection.

The lists of tests for Parameterized Test Selection are Block Frequency Test, Overlapping Template Test, Non-overlapping Templates Test, Serial Test, Approximate Entropy Test, Linear Complexity Test and Maurer’s Universal Test. Whereas, the lists of tests for Non-Parameterized Test Selection are Cumulative Sums (Forward/Reverse) Test, Runs Test, Longest Runs of Ones Test, Binary Matrix Rank Test, Spectral Test, Random Excursion Test, Random Excursion Variants Test and Frequency Test.

Ten out of fifteen tests in the NIST Statistical Test Suite provided only one p-value, whereas two tests (Cumulative Sums and Serial) provided two p-values and the other three tests (Random Excursion, Random Excursion Variant and Non-Overlapping) provided eight, eighteen and 148 p-values respectively.

For each test, there is a recommended minimum bit length required as explained in Ray B. *et al* (2013). As stated earlier, Parameterized Test Selection requires some parameter inputs to run the statistical test. Table 2 shows the minimum required bit length for each test.

	Statistical Test	**Minimum bit length, n**
Non-Parameterized Test	Frequency Test	$n \geq 100$
	Runs	$n \geq 100$
	Longest Runs of Ones	$n \geq 128$
	Spectral Test	$n \geq 1000$
	Cumulative Sums	$n \geq 100$
	Random Excursion	$n \geq 10^6$
	Random Excursion Variants	$n \geq 10^6$
	Binary Matrix Rank	$n \geq 38\ 912$
Parameterized Test	Block Frequency Test	$n \geq 100$
	Overlapping Template Test	$n \geq 10^6$
	Non-Overlapping Templates Test	Not specific
	Serial Test	Not specific
	Approximate Entropy test	Not specific
	Linear Complexity Test	$n \geq 10^6$
	Universal Test	$n \geq 387{,}840$

Table 2: Minimum bit length for each test

Parameterized Test Selection requires some parameter input to run the statistical test. Table 3 shows the parameter(s) selection characteristics for each test in this category.

Statistical Test	Characteristics
Block Frequency Test	M, block length is selected such that i. $n \geq NM$ ii. $M \geq 20$ iii. $M \geq 0.01n$
Overlapping Template Test	m, template length is recommended that m = 9 or m = 10.
Non-Overlapping Templates Test	NIST recommends to choose m, template length is recommended that m = 9 or m = 10 to obtain a meaningful results.
Serial Test	m = block length is chosen such that $m < [\log_2 n]-2$, where n = bit sequence
Approximate Entropy test	m = block length is chosen such that $m < [\log_2 n]-5$, where n = bit sequence
Linear Complexity Test	M = block length must be in the range of $500 \leq M \leq 5000$ and $N \geq 200$ where as n = bit sequence and N = Partition the input sequence, n/M
Universal Test	The value of L, block length and Q, number of block is chosen such that If $n \geq 387{,}840$; L = 6, Q = 640, while if $n \geq 904{,}960$; L = 7, Q = 1280 but if $n \geq 2{,}068{,}480$; L = 8, Q = 2560

Table 3: Characteristics of the Parameterized Test Selection

6. DATA DESCRIPTION

Algorithms being tested are SIMON64/96, SIMON96/96 and SIMON128/128. Nine different sets of data for each algorithm are generated and analyzed. The nine different sets of data are Strict Key Avalanche (SKA), Strict Plaintext Avalanche (SPA), Plaintext Ciphertext Correlation

(PCC), Cipher Block Chaining (CBC), Random Plaintext Random Key (RPRK), Low Density Keys (LDK), High Density Keys (HDK), Low Density Plaintext (LDP) and High Density Plaintext (HDP). Each data set was selected due to their specific function (Juan Soto *et al* (2000)). The process to generate the sample of each data type is defined by Juan Soto *et al* (2000). The description of the data types are as follows.

A. *Strict Key Avalanche (SKA) and Strict Plaintext Avalanche (SPA)*

To examine the Strict Key Avalanche and Strict Plaintext Avalanche data category, 1 000 samples are generated for each algorithm.

The samples for Strict Key Avalanche are constructed as follows: 163, 109 and 62 numbers of base-key blocks are used for SIMON64/96, SIMON96/96 and SIMON128/128 respectively. The base-key is encrypted with the all zero plaintext block to derive a block of base-ciphertext. Then, every bit of the base-key is flipped and encrypted with the respective length of all zero plaintext blocks to get the perturbed-ciphertext. Every block of perturbed-ciphertext is then XORed with the base-ciphertext and concatenated to produce a derived block at least 10^6 –bit output for each sample. In the case of Strict Plaintext Avalanche, The numbers of base-key blocks are 245, 109 and 62 for SIMON64/96, SIMON96/96 and SIMON128/128 respectively. Furthermore, substitute “base-key” for “base-plaintext” in the above description and “plaintext” for “key”.

B. *Plaintext Ciphertext Correlation (PCC)*

In order to study the correlation of plaintext/ciphertext pairs, 1 000 samples are generated for each algorithm. Each sequence consists of at least 10^6 –bits. 15 625, 10 417 and 7 813 blocks of random plaintext and keys for SIMON64/96, SIMON96/96 and SIMON128/18 respectively are used to produce the concatenated ciphertext block of 1 000 000, 1 000 032 and 1 000 064 bits of output sequences. The output sequences are constructed using XOR operation between the plaintext block and its corresponding ciphertext block which is computed in ECB mode.

D. *Cipher Block Chaining (CBC)*

In this data category, 1 000 samples are generated using 15 625, 10 417 and 7 813 blocks of random keys for SIMON64/96, SIMON96/96 and SIMON128/128 respectively for each sample. The derived block of 1 000 000, 1 000 032 and 1 000 064 bit for each respectively algorithm from this data categories are constructed using CBC mode. The first ciphertext block

(*CT1*) is defined by *CT1* = *Ek* (IV ⊕ *PT*). Subsequent ciphertext blocks were defined by *CTi*+1 = *Ek* (*CTi* ⊕ *PT*) for $1 \leq i \leq N$ (*N* is 15 625, 10 417 or 7 813 blocks of random keys). These derived blocks are then concatenated to produce an output of at least 10^6 bits.

E. *Random Plaintext/Random Key (RPRK)*

To study this data category, 1 000 samples are generated. Each sample is a result of the concatenation of 15 625, 10 417 and 7 813 blocks of ciphertext using 15 625, 10 417 and 7 813 blocks of random plaintexts and random keys for SIMON64/96, SIMON96/96 and SIMON128/128 algorithm respectively. Each of these algorithms will produce at least 10^6 bits of sequences.

F. *Low Density Keys (LDK) and High Density Keys (HDK)*

In Low Density Keys data category, three sets of data consisted 1 000 sequences are created according to the algorithm tested. For each key size, a random plaintext block is used. The first ciphertext block is obtained using a block of all zeroes key. The lengths of plaintext blocks in this test rely on the size of the algorithm. Ciphertext blocks 2-97/ 2-97/ 2-129 are obtained using block of keys with a single one in each of the possible bit positions. Then, ciphertext for block 98-4 657/ 98-4 657 / 130-8 257 are obtained using blocks of keys with two ones and 62/70/94/94/126 zeroes (the two ones appear in each combination of two bit position within the length of the key). The derived blocks of ciphertext are concatenated.

In the case of High Density Keys, substitute “zeroes” with “ones” in the above description and “ones” with “zeroes”.

H. *Low Density Plaintext (LDP) and High Density Plaintext (HDP)*

In Low Density Plaintext data category, a set of data consisted 1 000 sequences are created for each algorithm. For each block size, a random key block is used. The first ciphertext blocks are obtained using a block of all zeroes plaintext. The length of key blocks in this test relies on the size of the algorithm. Ciphertext blocks 2-65/ 2-97/ 2-129 are calculated using block of plaintext with a single one in each of the possible bit positions. Then, ciphertext for block 66-2 081/ 98-4 657 / 130-8 257 are obtained using blocks of plaintext with two ones and 94/94/126 zeroes (the two ones appear in each combination of two bit position within the length of the plaintext). The derived blocks of ciphertext are concatenated.

In the case of High Density Plaintext, substitute “zeroes” with “ones” in the above description and “ones” with “zeroes”.

Table 4 shows the length of each sample generated according to the algorithm and data category.

Data Categories	**SIMON64/96**	**SIMON96/96**	**SIMON128/128**
SKA	1 001 472	1 004 544	1 015 808
SPA	1 003 520	1 004 544	1 015 808
PCC	1 000 000	1 000 032	1 000 064
CBC	1 000 000	1 000 032	1 000 064
RPRK	1 000 000	1 000 032	1 000 064
LDK	298 048	447 072	1 056 896
HDK	298 048	447 072	1 056 896
LDP	133 184	447 072	1 056 896
HDP	133 184	447 072	1 056 896

Table 4: Length in bits of each sample generated according to the algorithm and data category

7. ANALYSIS FRAMEWORK

The randomness testing was performed to three variations of SIMON family, which are SIMON64/96, SIMON96/96 and SIMON128/128. The statistical analysis conducted was based on significance level of 0.1%. This is with accordance to NIST recommendation, where the value of significance level is to be at least 0.1%. A sample size is proportional to the significance level. Thus, for a level of 0.001, a sample of at least 1 000 sequences has to be generated.

Table 5 shows the list of parameter used for each test in the parameterized test selection.

Statistical Test	**Parameter(s)**
Block Frequency Test	20 000
Overlapping Templates Test	10

Non-Overlapping Templates Test	10
Serial Test	2
Approximate Entropy test	2
Linear Complexity Test	2 000
Universal Test	Depends on the length of the bit sequence of the sample

Table 5: Input for the Parameterized Test Selection

All tests except for the Cumulative Sums Test, Serial Test, Non-overlapping Templates Test, Random Excursion Test and Random Excursion Variants Test, produce one p-value for each sample. Cumulative Sums and Serial Test produce two p-values for each test. However, these two p-values are analyzed independently. Non-overlapping Template Test produces 148 000 p-values in total (148 p-values for each sample). Random Excursion tests and Random Excursion Variant tests produce 8 p-values and 18 p-values per sample respectively.

As for the Random Excursions and Random Excursion Variants Test, the p-value produced depends on the sample accepted. Only samples with number of cycle exceeding 500 were evaluated. Samples with insufficient number of cycles are not applicable. The total number of samples evaluated for Random Excursion and Random Excursion Variant are as shown in Table 6.

Note that all p-values are collected and analyzed. The randomness of the algorithm based on data categories is determined by this value. The sequence for each sample will be considered as random if the p-value is more or equal to 0.001. If the p-value of the sample is less than 0.001, the sample is observed.

Since this analysis used 1 000 samples and the significance level was fixed at 0.001, the rejection rate for most of the test in all data categories for all algorithms should not exceed 3 samples. The formula used to compute the maximum number of rejections is as follows:

$$s\left(\alpha + 3\sqrt{\frac{\alpha(1-\alpha)}{s}}\right)$$

where s is the sample size and α is the significance level (Juan Soto Jr. (2000)). For example, Non-overlapping Template Test produces 148 000 p-values for each data categories in all algorithms. Therefore, the rejection rate for this test should not exceed 184 sequences.

The p-values produced in Random Excursion Test and Random Excursion Variants Test varied as it depended on the sample accepted. The rejection rates for these tests are different according to data categories and algorithm.

The rejection rate for Random Excursion Test for all algorithms in all data categories is 11 except for SKA data category in SIMON64/96. The rejection rate for this data is 12. Meanwhile, the rejection rate for Random Excursion Variants test for all algorithms in all data categories is 21 except in SKA and SPA data category of SIMON64/96 and CBC and RPRK data category of SIMON96/96. The rejection rate for SIMON64/96 in SKA is 22 and SPA is 20. Meanwhile, the rejection rate for SIMON96/96 in CBC and RPRK data category is 20 as well.

	SKA	**SPA**	**PCC**	**CBC**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
SIMON64/96	670	589	619	635	617	604	604	617	617
SIMON96/96	620	646	629	627	612	604	604	604	604
SIMON128/128	632	638	630	626	630	617	621	616	625

Table 6: Total number of samples evaluated for Random Excursion and Random Excursion Variants for each algorithm

8. ANALYSIS RESULT

This statistical test was conducted under nine data categories with each having 1 000 samples. A total of 27 000 binary sequences were evaluated. Each of the sample size in SIMON128/128 has bit length of at least at 10^6 bit. Due to this reason, the algorithm was evaluated using all 15 NIST tests under all data categories. Five data categories for two algorithms which are SIMON64/96 and SIMON96/96 having a sample size of at least 10^6 are SKA, SPA, PCC, CBC and RPRK. Therefore, sample from these data categories were evaluated using all 15 NIST tests for these two algorithms.

Table 7 shows that SIMON64/96 with 82 831 p-values are constructed altogether for one sample. Therefore, 82 831 000 p-values are analyzed for this algorithm. Meanwhile for Simon96/96, 82 935 000 p-values are constructed altogether for 1 000 sample. For SIMON128/128, a total of 147 977 000 p-values are analyzed. Note that, the p-values for SIMON128/128 are bigger that other because the sample was evaluated using all 15 NIST tests under all data categories.

Algorithms	Total P-values per sample	Total P-values
SIMON64/96	82 831	82 831 000
SIMON96/96	82 935	82 935 000
SIMON128/128	147 977	147 977 000

Table 7: Total of p-values Analyze

Table 8, Table 9 and Table 10 are described according to algorithm. In these tables, only the tests that exceeded the maximum number of rejection rate are discussed.

Data Categories	Statistical Test	Number of rejection
SIMON64/96		
Strict Key Avalanche	Linear Complexity	5
Random Plaintext Random Keys	Runs	5
	Serial (p-value 2)	5
Low Density Keys	Longest Runs of Ones	4
High Density Keys	Longest Runs of Ones	4
High Density Plaintext	Longest Runs of Ones	4
SIMON 96/96		
Cipher Block Chaining	Linear Complexity	5
SIMON128/128		
Cipher Block Chaining	Overlapping	4
Random Plaintext Random Keys	Overlapping	4
Low Density Keys	Longest Runs of Ones	4
	Maurer's Universal	4
Low Density Plaintext	Low Density Plaintext	5

Table 8: Number of sample which exceeded the maximum number of rejection rate = 3

Data Categories	Number of rejection
SIMON64/96	
Strict Key Avalanche	188
High Density Keys	186
Low Density Plaintext	212
High Density Plaintext	219
SIMON96/96	
Strict Key Avalanche	210
SIMON128/128	
Strict Key Avalanche	223

Table 9: Number of sample which exceeded the maximum number of rejection rate = 184 for Non-Overlapping Template Test

Data Categories	Number of rejection	Maximum number of rejection Rate
SIMON96/96		
Plaintext Ciphertext Correlation	26	11
SIMON128/128		
Low Density Keys	26	11

Table 10: Number of sample which exceeded the maximum number of rejection rate as in Table for Random Excursion Variants Test

CONCLUSION

In this research paper, we have examined the randomness of selected algorithms of SIMON Lightweight Block Cipher, namely SIMON64/96, SIMON96/96 and SIMON128/128. This analysis was conducted on 1 000 samples under nine data categories based on a significance level fixed to 0.001. From the analysis, we have found that each algorithm failed at least one of the NIST Statistical Tests. At least one statistical test exceed the rejection rate for each algorithm, where it is evident that the sequence of the sample tests is non-random Therefore, it is concluded that based on the sample tested on the algorithms, these algorithms are non-random at 0.1% significance level.

REFERENCES

Abdullah, N.A.N., Zawawi, N.H.L.A. and Rani, H.A. 2011. *Analysis on Lightweight Block Cipher, KTANTAN.* Sourced from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6122793&queryText%3Dktantan

Abed F, List E, Lucks S and Wenzel J. *Differential Cryptanalysis of Round-Reduced SIMON and SPECK*. Sourced from http://link.springer.com/chapter/10.1007/978-3-662-46706-0_27

Biryukov A , Roy A and Velichkov V. *Differential Analysis of Block Ciphers SIMON and SPECK*. Sourced from http://link.springer.com/chapter/10.1007/978-3-662-46706-0_28

Alkhzaimi HA and Lauridsen MM. *Cryptanalysis of the SIMON Family of Block Ciphers*. Sourced from https://eprint.iacr.org/2013/543.pdf

Andrew R., Juan S., James N., Miles S., Elaine B., Stefan L., Mark L., Mark V., David B., Alan H., James D. and San V. 2010. A *Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications.* Sourced from http://csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22rev1a.pdf

Barker E. and Roginsky A. *NIST Special Publication 800-131A.* Sourced from http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf

Juan S. 2000. *Randomness Testing of the AES Candidate Algorithms*. Sourced from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.39.231

Juan S. and Lawrence B. 2000. *Randomness Testing of the Advanced Encryption Standard Finalist Candidates.* Sourced from http://csrc.nist.gov/publications/nistir/ir6483.pdf

Ju Kim, Umeno K and Hasagawa A. *Corrections of the NIST Statistical Test Suite for Randomness*. Sourced from https://eprint.iacr.org/2004/018.pdf

Leander G. 2011. *Lightweight Block Cipher Design*. Sourced from https://www.cosic.esat.kuleuven.be/ecrypt/courses/albena11/slides/gregor_leander_lightweight.pdf

Liyana C.N.C, Isma N.M.S., Nik A.N.A., Norul H.A.Z., Hazlin A.R., Abdul A.Z. *Randomness Analysis on Speck Family of Lightweight Block Cipher*. Sourced from http://www.mscr.org.my/V5(1)/IJCR%205(1)%2044-60.pdf

Lot, N.H, Abdullah, N.A.N. and Rani, H.A. 2011. *Statistical Analysis on KATAN Block Cipher.* Sourced from http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=6125698&queryText%3Dkatan

Norul H. L., Kamaruzzaman S. and Nurzi J. M. Z. 2013. *Randomness analysis on Grain-128 Stream Cipher.* Sourced from http://scitation.aip.org/content/aip/proceeding/aipcp/10.1063/1.4823866

Ray B., Douglas S., Jason S., Stefan T., Bryan W., and Louis W. 2013. *The SIMON and SPECK Families of Lightweight Block Ciphers*. Sourced from http://eprint.iacr.org/2013/404.pdf