International Journal of Cryptology Research 5(1): 61-77 (2015)

Randomness Analysis on Speck Family Of Lightweight Block Cipher

[1]Liyana Chew Nizam Chew [2]Isma Norshahila Mohammad Shah
[3]Nik Azura Nik Abdullah [4]Norul Hidayah Ahmad Zawawi
[5]Hazlin Abdul Rani [6]Abdul Alif Zakaria
Cryptography Development Department, Cyber Security Malaysia, Kuala Lumpur, Malaysia
Email: [1]liyana@cybersecurity.my, [2]isma@cybersecurity.my, [3]azura@cybersecurity.my, [4]norul@cybersecurity.my, [5]hazlin@cybersecurity.my [6]alif@cybersecurity.my

ABSTRACT

Speck family of lightweight block cipher was publicly released by National Security Agency (NSA), USA in June 2013. Speck has been designed with ten instances which provides excellent performance in both hardware and software. Speck is optimized for performance on microcontrollers. This paper will present the result of randomness testing using NIST statistical test suite for SPECK cipher family, which are Speck128/128, Speck128/192, and Speck128/256. Nine data categories are applied to generate the input sequence (either plaintext or key) for each algorithm. Randomness is important for cryptography module to ensure that the cipher is unpredictable before it becomes available. From the analysis conducted, some failures were identified in some data categories.

Keywords: *Speck block cipher, NIST Statistical Test Suite, lightweight cryptography, statistical randomness testing, significance level, data categories.*

1. INTRODUCTION

Lightweight cryptography is a new field that applied specifically for highly constrained devices. Among the important design considerations of lightweight cryptography are reduced power consumption, sufficient encryption speed and small chip size. In highly constrained environments, hardware and software efficiency is becoming more important thus making lightweight cryptography an essential ongoing research. The standard usage of block cipher such as AES was deeming to be not a right choice for extremely constrained environment.

Speck family of lightweight block ciphers is the algorithm that was introduced in June 2013 by National Security Agency (NSA). Speck family supports a total of ten instances of different block sizes and key sizes. There were several published research papers that discussed the attacks applied on

Speck family since it was published (Alkhzaimi and Lauridsen, 2013, Abed et. al. 2013). Differential cryptanalysis is one of the attacks that have been applied to Speck family.

This paper will illustrate the randomness test conducted on the output of Speck algorithms. One of the techniques to check the randomness of the algorithm is by using the NIST statistical analysis. Nowadays, random number generator and pseudorandom number generator is important since the cryptography sequence should not able to be guessed by unauthorized people any easier than a brute force. Therefore, it is necessary for an algorithm to be random and unpredictable.

Encryption is a cryptographic operation that is used to provide confidentiality for sensitive information. Several algorithms that were approved for encryption by the Federal government of USA and published in NIST publications are algorithms which have keys sizes larger than 112 bits (Barker and Roginsky, 2011). Therefore this paper will only discuss on Speck algorithms with a large key size. The analysis will focus on the following Speck family algorithm; Speck128/128, Speck128/192 and Speck128/256.

2. A BRIEF DESCRIPTION OF SPECK FAMILY OF BLOCK CIPHER

Speck Family consists of ten instances with difference block sizes and key sizes, each algorithms is applicable in various implementations. The algorithms provide excellent performance in hardware and software, and also optimized performance on microcontroller. Speck Family has a range of block and key sizes to match application requirement and security needs without sacrificing the performance.

Algorithm	Block size	Key size	Round
Speck128/128	128	128	68
Speck128/192	128	192	69
Speck128/256	128	256	72

Table 1: Block sizes, key sizes and Round of Speck algorithms.

3. ROUND FUNCTIONS OF BLOCK CIPHER

Speck cipher encryption is operated using Feistel network. Speck encryption make use of three operations; bitwise XOR (⊕), addition modulo 2^n (+), and left and right circular shifts (S^j and S^{-j}), respectively, by j bits. Left word L_i of the input is rotated by $\alpha = 8$ bits to the left and the output is added with the right word R_i before modulo $2^n = 128$. The left output will be XORed with round key K_i and becomes the left input for next round. The right word is then rotated to the right by $\beta = 3$ bits, then is XORed with left output and the output will become the right input for next round. The process of Speck's round function and key expansion is shown in Figure 1 and Figure 2.

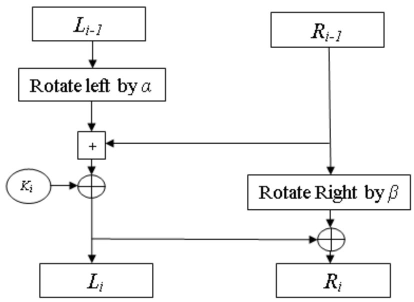


Figure 1: Round Function of SPECK; i steps of encryption.

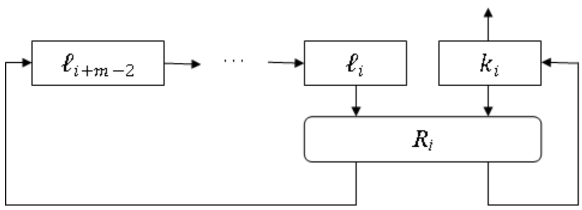


Figure 2: Key Expansion of SPECK.

4. KEY SCHEDULES OF BLOCK CIPHER

Round keys k_i are generated to be used in the round function of Speck. Round keys are written as $(K_0, \ell_0, \ldots, \ell_{m-2})$ for a value of m in $\{2, 3,4\}$. The round keys are defined by the following:

$$\ell_{i+m-1} = (k_i + S^{-\alpha}\ell_i) \oplus i$$

$$k_{i+1} = S^{\beta}k_i \oplus \ell_{i++m-1}$$

5. NIST STATISTICAL TEST SUITE

Binary output sequences of the algorithm can be applied on several statistical tests that attempts to compare and evaluate a random sequence. Although there has many statistical packages existed to determine the randomness of binary sequences, NIST statistical test suite is selected because it was used for the evaluation of AES candidates which covers a wide range of randomness characteristics. The properties of randomness of the sequence can be characterized and described in terms of probability (p-value).

Randomness test for the output of the Speck Family will be analyzed under full round considerations, which are 68 rounds for Speck128/128, 69 rounds for Speck128/192 and 72 rounds for Speck128/256. All the randomness testing was based on the application of the NIST Statistical Test Suite that consists of 15 tests. The tests aim to evaluate the randomness of binary sequences produced by either hardware or software based cryptographic random or pseudorandom number generators (Rukhin et. al. 2010). Each of these 15 tests is under different parameter input and number of p-values reported by each test listed in Table 2. Each p-value corresponds to an individual statistical test on one sample binary sequence. 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.

The tests differentiate into two categories, namely the Parameterized Test and the Non-Parameterized Test. To define the parameterized Test, it requires the parameter value(s) of block size, number of blocks and template length as stated in NIST Statistical Test Suite publication (Barker and Roginsky, 2011). The Non-Parameterized Test does not require any additional parameter in obtaining the p-values for each test. The tests are divided according to their categories as listed in Table 2. NIST has recommended a minimum number of bits required for each test. This is presented in Table 3.

Parameterized Test Selection	
Statistical Test	**No. of P-values**
Block Frequency Test	1

Non-Parameterized Test Selection	
Statistical Test	**No. of P-values**
Cumulative Sums (Forward/Reverse) Test	2

Overlapping Template Test	1	Runs Test	1
Non-Overlapping Templates Test	148	Longest Runs of Ones Test	1
Serial Test	2	Binary Matrix Rank Test	1
Approximate Entropy Test	1	Spectral (Discrete Fourier Transform) Test	1
Linear Complexity Test	1	Random Excursion Test	8
Maurer's Universal Test	1	Random Excursion Variant Test	18
		Frequency Test	1

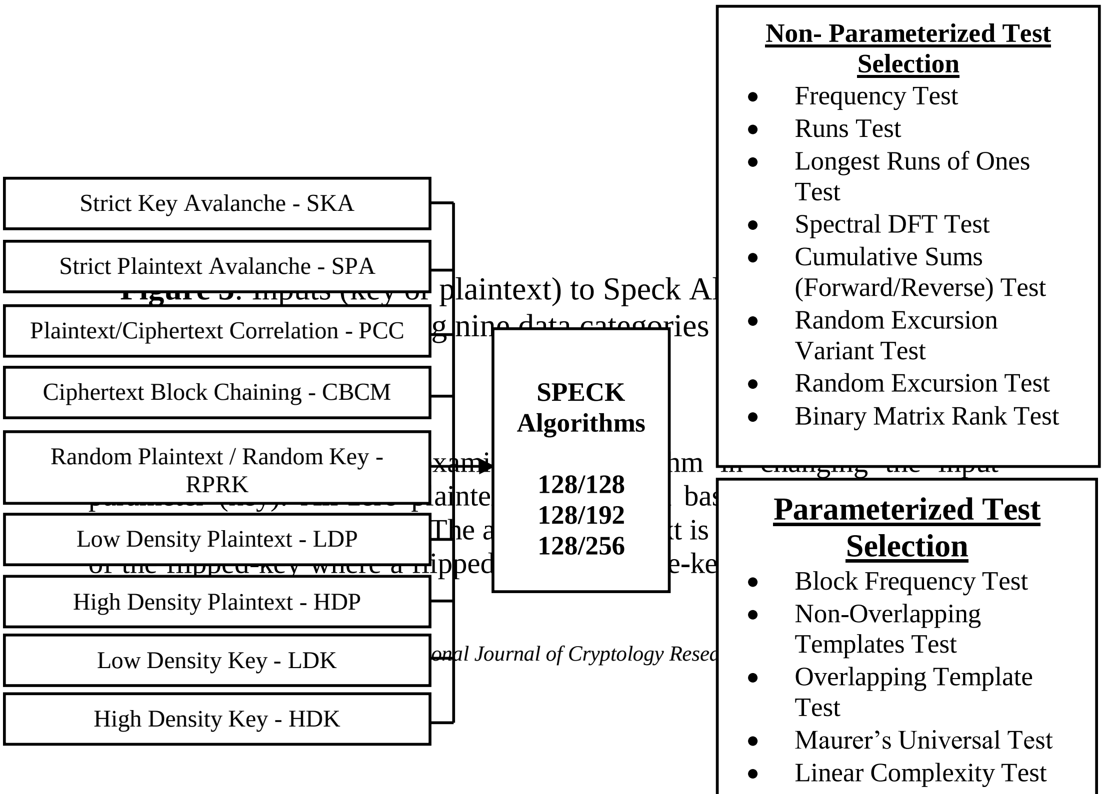
Table 2: Fifteen NIST tests and number of p-values generated by each test

	Statistical Test	Recommended bits
Non- Parameterized Test Selection	Frequency	$n \geq 100$
	Runs	$n \geq 100$
	Longest Runs of Ones	$n \geq 750{,}000$
	DFT	$n \geq 1{,}000$
	Cumulative Sums	$n \geq 100$
	Random Excursion Variant	$n \geq 10^6$
	Random Excursion	$n \geq 10^6$
	Binary Matrix Rank	$n \geq 38{,}912$
Parameterized Test Selection	Block Frequency	$n \geq 100$
	Non-Overlapping Templates	Not specified
	Overlapping Template	$n \geq 10^6$
	Maurer's Universal	Minimum $n \geq 387{,}480$
	Linear Complexity	$n \geq 10^6$
	Serial	Not specified
	Approximate Entropy	Not specified

Table 3: Minimum number of bits recommended by NIST for all 15 tests

6. DATA CATEGORIES

Inputs to Speck Algorithms are established by nine data categories (Soto, 1999, Abdullah *et al.*, 2011). Output of Speck Algorithms will be concatenated and tested using fifteen NIST statistical tests. This process is shown in Figure 3. These data categories have specific function in evaluating the randomness of the algorithm. Each of these data categories will produce 1000 input samples. Sequence length of each sample is depending on the key size or block size of tested algorithm.



i^{th} bit, for $1 \leq i \leq key\,size$. The ciphertext produce by flipped-key will then be XORed with initial ciphertext to produce a derived block. In order to produce at least 10^6–bit sequence for each sample, derived block will be concatenated by other selected random base-key. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

Strict Plaintext Avalanche

This data category is to examine the algorithm in changing the input parameter (Plaintext). This test is similar to Strict Key Avalanche but differs at using plaintext as changing parameter. All-zero key and random base-plaintext is encrypted as initial ciphertext for the test. For each base-plaintext, the all-zero key is encrypted with one of the flipped- plaintext where a flipped- plaintext is the base- plaintext with flipped bit at the i^{th} bit, for $1 \leq i \leq plaintext\,size$. The ciphertext produced by the flipped-plaintext will then be XORed with initial ciphertext to produce a derived block. In order to produce at least 10^6–bit sequence for each sample, derived block will be concatenated by other selected random base- plaintext. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

Plaintext/Ciphertext Correlation

This data category is to examine the correlation between plaintext/ciphertext pairs. For each sample, one random key and adequate block of random plaintext are chosen to produce at least 10^6-bit sequence. To generate a derived block, each plaintext block will be encrypted using the chosen random key and then the ciphertext will be XORed with each plaintext block. These derived blocks are computed in ECB mode and are then concatenated. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

Ciphertext Block Chaining Block

Given a random key, an initialization vector (IV) of all zeroes, and a plaintext of all-zero, a sequence of at least 10^6-bits was constructed in CBC mode. The first ciphertext block (CT_1) is defined by $CT_1 = E_k(IV \oplus PT_0)$. Subsequent ciphertext blocks are defined by $CT_i + 1 = EK(CT_i \oplus PT_i)$ for $1 \leq i \leq derived\,block$. All 1000 sequences were generated, each with a different random key. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

Random Plaintext / Random Key

This data category is to examine the randomness of ciphertext based on random plaintext and random key. For each sample, one random key and adequate blocks of random plaintext are chosen to produce at least 10^6-bit sequence using ECB mode. All 1000 sequences were generated, each with a different random key. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

Low Density Plaintext

This data type is formed based on low density plaintext blocks which consist of all zero plaintext block, plaintext blocks of all zero with a single bit of '1' and plaintext blocks of zeroes with two bits of '1' in each combination of two bit positions for all possible plaintext position, C_2^n, where n is plaintext size. These entire plaintext blocks are encrypted using ECB mode with one random key. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

High Density Plaintext

This data type is formed based on high density plaintext blocks which consist of all '1' plaintext block, plaintext blocks of all '1' with a single bit of zero and plaintext blocks of all '1' with two bits of zero in each combination of two bit positions for all possible plaintext position, C_2^n, where n is plaintext size. These entire plaintext blocks are encrypted using ECB mode with one random key. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

Low Density Keys

This data type is formed based on low density keys blocks which consist of all zero keys block, keys blocks of all zero with a single bit of '1' and keys blocks of zeroes with two bits of '1' in each combination of two bit positions for all possible keys position, C_2^n, where n is keys size. These entire plaintext blocks are encrypted using ECB mode with one random plaintext. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

High Density Keys

This data type is formed based on high density keys blocks which consist of all '1' keys block, keys blocks of all '1' with a single bit of zero and keys blocks of all '1' with two bits of zero in each combination of two bit positions for all possible keys position, C_2^n, where n is keys size. These entire plaintext blocks are encrypted using ECB mode with one random plaintext. The number of derived blocks and derived sequence length for each sample of Speck family are listed in Table 4.

	Speck128/128	**Speck128/192**	**Speck128/256**
	Strict Key Avalanche		
Number of Base-Key block	62	41	31
Derived blocks	7936	7872	7936
Sequence length	1015808	1007616	1015808
	Strict Plaintext Avalanche		
Number of Base-Plaintext block	62	62	62
Derived blocks	7936	7936	7936
Sequence length	1015808	1015808	1015808
	Plaintext/Ciphertext Correlation , Cipher Block Chaining Mode and Random Plaintext/Random Key		
Derived blocks	7813	7813	7813
Sequence length	1000064	1000064	1000064
	Low Density Plaintext and High Density Plaintext		
Derived blocks	8257	8257	8257
Sequence length	1056896	1056896	1056896
	Low Density Key and High Density Key		
Derived blocks	8257	18527	32897
Sequence length	1056896	2371712	4210816

Table 4: Number of Derived Blocks and Sequence Length for Three Speck Families Algorithm.

7. NIST Testing Experimental Setup

NIST test was performed using the following approach:

(a) Input parameters for 15 tests such as the sequence length, sample size, and significance level were fixed for each sample.

The sample size is corresponding to the choice of the significance level. The significance level was set to 0.001 and the sample size is 1000 sequence (Barker and Roginsky, 2011). Sample size is defined by inverse of significance level. For each binary sequence and each statistical test, p-value was reported. Parameters of Parameterized Test for Speck128/128, Speck128/192 and Speck128/256 are shown in Table 5.

(b) Inputs for all Speck algorithms are generated using nine different data categories. Each of these nine data categories will produce a sequence with 1000 input samples. During experimentation, a total of 27,000 ciphertexts (3 algorithms X 9 data categories X 1,000 samples) were evaluated. Sequence length of each data categories is depending on block size and key size of the algorithm to be tested. The sequence length for each data categories and algorithm are as shown in Table 4.

(c) The success or failure assessment on each p-value is based on whether or not it exceeded or fell below the selected significance level which is 0.001. For each statistical test and each sample, a sample was considered to have passed a statistical test if p-value for this sample is equal or greater than 0.001. If the p-value fell below 0.001, then the sample was flagged as failure.

(d) The maximum number of sequence that was expected to be rejected must be computed using the following formula (Soto, J. 1999). If the proportion of success-sequences falls outside of following acceptable interval, there is evidence that the data is non-random.

$$P' \pm 3\sqrt{\frac{P'(1-P')}{m}},$$

Where $\mathrm{P}' = 1 - \alpha$, m is the number of sequences and α represents the significance level used. This interval is determined the range of normal distribution which is an approximation of the binomial distribution under the assumption that each sequence is independent sample.

In order to explain the parameters that were used in the tests, the following abbreviation is used: block length (M or L), sequence length (n), non-overlapping blocks ($N = n/M$), template length (m), theoretical probabilities (π_i) and number of block in the initialization sequence (Q).

The requirements for Parameterized Test are as per describe as below:

- Block Frequency test: M is selected such that $n \geq MN$,$M \geq 20$,$M \geq 0.01n$ and $N < 100$.
- Non-Overlapping Template test: $N = 8$ has been specified, m is recommended that $m = 9$ or $m = 10$, $N \leq 100$ and $M > 0.01n$ and $N = \lfloor n/M \rfloor$.
- Overlapping Template test: m is recommended that $m = 9$ or $m = 10$, $n \geq MN$, $N(\min \pi_i) > 5$, $\lambda = (M - m + 1)/2m \approx 2$, $m \approx \log_2 M$ and $K \approx 2\lambda$.
- Linear Complexity test: the value of M must be in the range of $500 \leq M \leq 5000$ and $N \geq 200$.
- Serial tests: m and n chosen such that $m < [\log_2 n] - 2$.
- Approximate Entropy tests: m and n chosen such that $m < [\log_2 n] - 5$.

Based on the requirement stated, the NIST parameter input for Speck128/128, Speck128/192 and Speck128/256 for all nine data categories are as shown in Table 5. Speck128/128, Speck128/192 and Speck128/256 use the same input for parameterized test except for some data categories in block frequency test. Parameter input for Block Frequency Test of Speck128/128 is 20000 and this parameter value applied for all nine data categories for Speck 128/128. NIST parameter input of Block Frequency Test for Speck128/192 for Low Density Keys and High Density Keys is 30000, and parameter input for other data categories is 20000. NIST parameter input of Block Frequency Test for Speck128/256 for Low Density Keys and High Density Keys is 45000, and the remaining data categories use 20000 as parameter input for block frequency test.

Input for Parameterized Test			
Block Frequency Test	1	2	3
	20000	30000	45000
Overlapping Template Test	10		
Non-Overlapping Templates Test	10		
Serial Test	2		

Approximate Entropy Test	2
Linear Complexity Test	2000

Table 5: Input for Parameterized Test

8. RESULTS AND ANALYSIS

The three chosen Speck algorithms namely Speck128/128, Speck128/192 and Speck 128/256 are tested under nine data categories with each having 1000 samples. For each experiment, the significance level was fixed at 0.001. The acceptable interval is calculated using formula that has been discussed earlier in NIST testing experimental setup (section d). Note that Cumulative Sums and Serial tests produce two p-values. However, these two p-values are analyzed independently. Non-Overlapping Template test produces 148,000 p-values (148 p-values per sample) in total. Random Excursion (8 p-values) and Random Excursion Variant (18 p-values) tests did not make use of all 1,000 binary sequences because some of these sequences did not have sufficient number of cycles (500 cycles). The total number of samples evaluated for Random Excursion and Random Excursion Variant is as shown in Table 6.

	SKA	SPA	PCC	CBCM	RPRK	LDK	HDK	LDP	HDP
Speck128/128	739	618	619	642	636	646	625	630	618
Speck128/192	658	658	626	621	620	748	747	659	639
Speck128/256	620	635	622	633	607	828	812	624	637

Table 6: The total number of samples evaluated for Random Excursion and Random Excursion Variant for each algorithm.

The results and acceptable success rate for all tests are shown in Table 7, Table 9 and Table 11 for Speck128/128, Speck128/192 and Speck128/256 respectively. If an at least one success rate is out of the acceptable interval, then the test will be considered not passed. Acceptable success rate for Random Excursion Variant and Random Excursion tests will be presented separately in Table 8, Table, 10 and Table 12. The results of tests that out of acceptable success rate are highlighted in red ( ).

SPECK 128/128											
Non-parameterized Test Selection		**Acceptable Success Rate(%)**	**Data Categories**								
			SKA	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Frequency		99.6	100	100	100	99.9	99.8	100	99.9	99.9	99.8
Runs		99.6	100	99.9	100	99.9	99.7	99.9	99.9	99.5	99.8
Longest Runs of Ones		99.6	100	99.9	100	99.7	99.9	99.9	100	99.8	99.9
Spectral DFT		99.6	100	100	99.9	100	100	100	100	100	100
Cumulative Sums	Fwd	99.6	100	100	100	99.8	99.8	100	100	99.8	99.8
	Rvs	99.6	100	100	100	99.8	99.8	100	99.8	99.9	99.8
Random Excursion Variant		Refer table 8	99.97	99.89	99.83	99.88	99.91	99.86	99.9	99.86	99.96
Random Excursion		Refer table 8	99.9	99.82	99.96	99.94	99.96	99.88	99.92	99.9	99.82
Binary Matrix Rank		99.6	100	99.9	100	99.8	99.8	100	99.9	99.9	99.9
parameterized Test Selection		**Acceptable Success Rate(%)**	**Data Categories**								
			SKA	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Block Frequency		99.6	100	100	99.9	99.8	99.9	99.9	99.7	99.8	100
Non-Overlapping		99.88	99.91	99.89	99.89	99.89	99.89	99.90	99.9	99.91	99.9
Overlapping		99.6	99	99.8	99.8	100	99.8	99.7	99.8	100	99.9
Maurer's Universal		99.6	100	99.8	99.9	100	100	99.8	100	99.7	99.7
Linear Complexity		99.6	100	99.9	99.9	100	99.9	100	99.9	100	99.8
Serial	p-value1	99.6	100	100	100	99.9	99.6	100	99.9	99.7	99.8
	p-value2	99.6	100	99.9	100	99.9	99.8	99.9	99.9	99.6	99.9
Approximate Entropy		99.6	100	99.8	99.9	99.9	99.7	99.9	100	99.8	99.9

Table 7: Result for each statistical test for Speck 128/128

Speck128/128									
Data Categories	**SKA**	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Random	99.82	99.81	99.81	99.81	99.81	99.81	99.81	99.81	99.81

Excursion Variant									
Random Excursion	99.78	99.77	99.77	99.77	99.77	99.77	99.77	99.77	99.77

Table 8: Acceptable success rate of Speck128/128 for Random Excursion Variant and Random Excursion tests

SPECK 128/192											
Non-parameterized Test Selection		**Acceptable Success Rate(%)**	**Data Categories**								
			SKA	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Frequency		99.6	99.7	99.7	99.9	100	99.8	100	100	99.9	99.9
Runs		99.6	100	100	99.9	99.7	99.9	99.8	100	99.9	100
Longest Runs of Ones		99.6	100	100	99.9	99.7	99.9	99.8	99.8	99.8	99.6
Spectral DFT		99.6	100	100	100	100	100	100	100	100	100
Cumulative Sums	Fwd	99.6	99.7	99.7	99.8	100	99.7	100	100	100	100
	Rvs	99.6	99.8	99.8	99.9	100	99.8	100	99.9	99.9	99.8
Random Excursion Variant		Refer table 10	99.76	99.76	99.84	99.87	99.76	99.93	99.95	99.89	99.94
Random Excursion		Refer table 10	99.91	99.91	99.88	99.84	99.86	99.92	99.92	99.87	99.88
Binary Matrix Rank		99.6	100	100	99.7	100	100	100	99.9	99.9	99.8
parameterized Test Selection		**Acceptable Success Rate(%)**	**Data Categories**								
			SKA	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Block Frequency		99.6	99.8	99.8	100	100	100	99.8	100	99.9	99.9
Non-Overlapping		99.88	99.9	99.9	99.89	99.88	99.9	99.9	99.9	99.91	99.89
Overlapping		99.6	99.9	99.9	99.9	99.9	100	99.4	100	100	99.9
Maurer's Universal		99.6	99.8	99.8	100	99.8	99.9	100	99.7	99.9	99.9
Linear Complexity		99.6	99.8	99.8	99.9	99.6	99.9	100	99.7	99.8	99.9
Serial	p-value1	99.6	99.9	99.9	99.8	99.9	99.9	99.8	100	99.9	99.9
	p-value2	99.6	100	100	99.9	99.7	99.9	99.8	100	99.9	100
Approximate		99.6	99.9	99.9	99.9	99.8	99.9	99.8	99.8	99.6	99.9

Entropy										

Table 9: Result for each statistical test for Speck 128/192

Speck128/192									
Data Categories	**SKA**	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Random Excursion Variant	99.81	99.81	99.81	99.81	99.81	99.82	99.82	99.81	99.81
Random Excursion	99.77	99.77	99.77	99.77	99.77	99.78	99.78	99.77	99.77

Table 10: Acceptable success rate of Speck128/192 for Random Excursion Variant and Random Excursion tests

SPECK 128/256											
Non-parameterized Test Selection		**Acceptable Success Rate(%)**	**Data Categories**								
			SKA	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Frequency		99.6	100	100	99.7	100	100	100	100	100	100
Runs		99.6	100	99.9	99.8	99.8	99.9	99.7	100	99.8	100
Longest Runs of Ones		99.6	100	99.9	99.7	100	99.8	100	99.8	99.8	100
Spectral DFT		99.6	100	100	100	100	100	99.8	99	100	100
Cumulative Sums	Fwd	99.6	100	100	99.8	99.9	99.9	100	100	100	100
	Rvs	99.6	100	99.9	99.8	100	100	100	100	99.8	100
Random Excursion Variant		Refer table 12	99.8	99.91	99.89	99.85	99.9	99.89	99.92	99.82	99.84
Random Excursion		Refer table 12	99.82	99.82	99.74	99.84	99.88	99.86	99.88	99.96	99.96
Binary Matrix Rank		99.6	100	99.9	100	99.8	99.9	100	100	100	100
parameterized Test Selection		**Acceptable Success Rate(%)**	**Data Categories**								
			SKA	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Block Frequency		99.6	100	100	100	99.9	99.8	100	100	99.8	100

Non-Overlapping		99.88	99.92	99.89	99.89	99.90	99.89	99.90	99.89	99.86	99.86
Overlapping		99.6	100	99.8	100	99.9	99.7	99.9	99.8	100	99.8
Maurer's Universal		99.6	100	99.6	99.8	100	99.9	99.7	99.8	99.6	99.8
Linear Complexity		99.6	99.8	100	99.9	99.9	99.8	99.9	99.8	99.8	100
Serial	p-value1	99.6	100	100	99.8	99.8	100	99.8	100	100	99.8
	p-value2	99.6	100	99.9	99.8	99.8	99.9	99.7	100	99.8	100
Approximate Entropy		99.6	100	99.8	100	100	100	99.9	100	99.8	100

Table 11: Result for each statistical test for Speck 128/256

Speck128/256									
Data Categories	**SKA**	**SPA**	**PCC**	**CBCM**	**RPRK**	**LDK**	**HDK**	**LDP**	**HDP**
Random Excursion Variant	99.81	99.81	99.81	99.81	99.81	99.82	99.82	99.81	99.81
Random Excursion	99.77	99.77	99.77	99.77	99.76	99.78	99.78	99.77	99.77

Table 12: Acceptable success rate of Speck128/256 for Random Excursion Variant and Random Excursion tests

9. CONCLUSION

This paper has presented the statistical analysis on Speck Family algorithms which specifically focuses on Speck128/128, Speck128/192 and Speck128/256. The statistical analysis is using NIST Statistical Test Suite. During the analysis process, the significance level was set at 0.001 to determine whether the algorithm tested is random or non-random. At least one statistical test falls outside of acceptable success rate for each algorithm, where there is evidence that the sequence is non-random.

REFERENCES

Beaulieu, R, Shors, D, Smith, J, Treatman-Clark, S, Weeks, B and Wingers, L. 2013. *The SIMON and SPECK Families of*

Lightweight Block Ciphers. Cryptology ePrint Archive, Report 2013/404. Sourced from http://eprint.iacr.org/.

Rukhin, A, Soto, J, Nechvatal, J, Smid, M, Barker, E, Leigh, S, Levenson, M, Vangel, M, Banks, D, Heckert, A, Dray, J and Vo S. 2010. *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. NIST SpecialPublication 800-22.

Alkhzaimi, H.A and Lauridsen, M.M. 2013. *Cryptanalysis of the SIMON Family of Block Ciphers*. Cryptology ePrint Archive: Report 2013/543. Sourced from https://eprint.iacr.org/2013/543

Abed, F, Eik List, Lucks, S and Wenzel, J. 2013. *Cryptanalysis of the Speck Family of Block Ciphers*. Cryptology ePrint Archive: Report 2013/568. Sourced from http://eprint.iacr.org/2013/568

Soto, J. 1999. *Randomness Testing of the AES Candidate Algorithms*. Sourced from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.39.21

Barker, E and Roginsky, A. 2011.Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths. NIST Special Publication 800-131A.

Abdullah, N.A.N, Zawawi, N.H L.A. and Rani, H.A. 2011. Analysis on Lightweight Block Cipher, KTANTAN. Information Assurance and Security (IAS), 2011 7th International Conference. page 46-51. IEEE.

Zawawi, N.H L.A, Seman,K and Zaizi, N.J.M. 2013. *Randomness analysis on grain - 128 stream cipher*. AIP Conference Proceedings 1557, 15 (2013).

Abdullah, N.A.N., Seman K. and Norwawi N.M. *Statistical Analysis on LBlock Block Cipher.* International Conference on Mathematical Sciences and Statistics 2013 (Selected Papers). page 233 - 245.