CHAPTER V

RESULTS AND DISCUSSION OF MODIFIED GRAIN-128

5.1 Modification of Grain-128 Stream Cipher Algorithm

The modification has been done on Grain-128 stream cipher algorithm, and the new algorithm is known as Modified Grain-128 (MG-128) stream cipher algorithm. The structure and flow of MG-128 is still similar with Grain-128, with three main building blocks, i.e. Linear Feedback Shift Register, Non-Linear Feedback Shift Register, and Boolean Function. However, several functions have been changed to further strengthen the existing algorithm. The experimental setup for the MG-128 is also discussed in this chapter. Lastly, the results and analysis from the experiment conducted is presented in the last section of this chapter.

5.1.1 Linear Feedback Shift Register (LFSR)

MG-128 stream cipher algorithm uses five Linear Feedback Shift Registers (LFSRs), namely $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$, and $LFSR_5$, with the size of 37, 31, 16, 19, and 25, respectively. All the five LFSRs are primitive polynomial. Below are the lists of LFSRs used in MG-128.

- $LFSR_1 = f_1(x) = 1 + x^{25} + x^{27} + x^{35} + x^{37}$
- $LFSR_2 = f_2(x) = 1 + x^{24} + x^{31}$

- $LFSR_3 = f_3(x) = 1 + x^2 + x^4 + x^5 + x^8 + x^9 + x^{12} + x^{13} + x^{15} + x^{16}$
- $LFSR_4 = f_4(x) = 1 + x^9 + x^{14} + x^{15} + x^{17} + x^{19}$
- $LFSR_5 = f_5(x) = 1 + x^{21} + x^{22} + x^{25}$

All the five LFSRs were updated for each clock that is explained later in section key initialization process and keystream generation process.

5.1.2 Non-Linear Feedback Shift Register (NLFSR)

The MG-128 stream cipher algorithm uses the same NLFSR as in Grain-128 stream cipher algorithm. However, the NLFSR was updated for each clock with different setting that is explained later in section key initialization process and keystream generation process. The NLFSR used is as follows:

$$NLFSR = g(x) = 1 + x^{32} + x^{37} + x^{72} + x^{102} + x^{128} + x^{44}x^{60} + x^{61}x^{125} + x^{63}x^{67} + x^{69}x^{101} + x^{80}x^{88} + x^{110}x^{111} + x^{115}x^{117}$$

5.1.3 Boolean Function

The MG-128 stream cipher algorithm also uses the same Boolean Function as in Grain-128. However, the input function taken was different. Four (4) bits of inputs were taken from NLFSR and 1-bit input was taken from each of $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$, and $LFSR_5$, respectively. The function used is as follows:

$$h(x) = b_{i+12}s1_i + b_{i+13}s2_i + b_{i+95}s3_i + b_{i+60}s4_i + b_{i+12}b_{i+95}s5_i$$

where $b_{i+12}, b_{i+13}, b_{i+95}, b_{i+60}$ were taken from NLFSR and $s1_i, s2_i, s3_i, s4_i, s5_i$ were respectively taken from $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$, and $LFSR_5$.

5.1.4 Keystream

In order to generate the keystream of MG-128, the cipher must be firstly initialized with the key and IV. To construct all the five LFSRs, the first 37 bits of key were loaded for $LFSR_1$. For $LFSR_2$, the 38^{th} bit until 68^{th} bit of key were loaded, followed by $LFSR_3$ with the 69^{th} bit until 84^{th} bit of key were loaded. For $LFSR_4$, it was taken from 85^{th} bit until 103^{th} bit of key. Lastly, the rest bits of key were loaded for $LFSR_5$. To construct NLFSR, the first 96 bits of NLFSR were loaded with 96-bit IV. The last 32 bits of the NLFSR were filled with 1s.

The structure of MG-128 is illustrated in Figure 14 and Figure 15 below. Figure 14 shows the process of key initialization of MG-128 stream cipher algorithm, while Figure 15 shows the process of generating the keystream of MG-128 stream cipher algorithm.

Figure 14: Key initialization process of MG-128

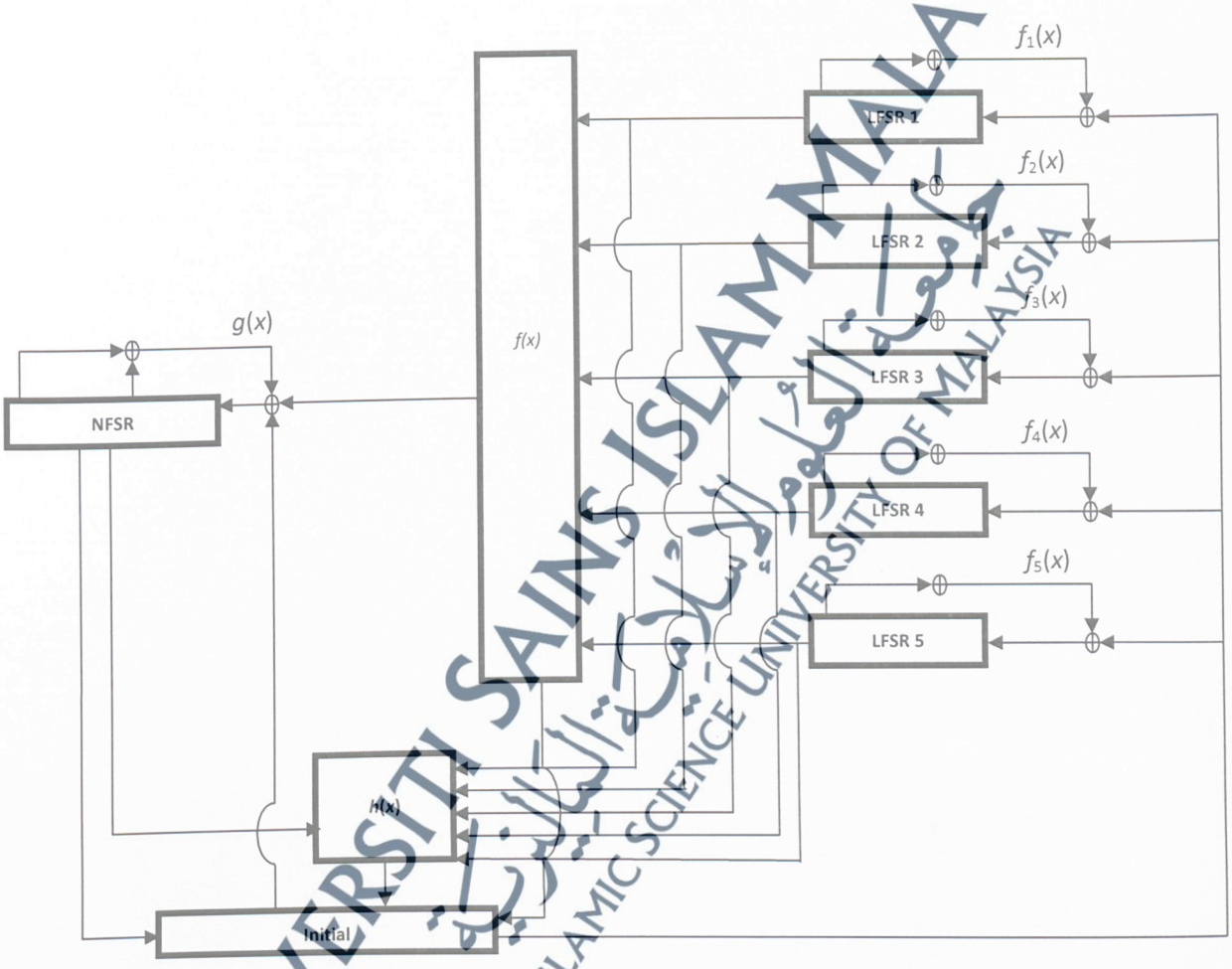
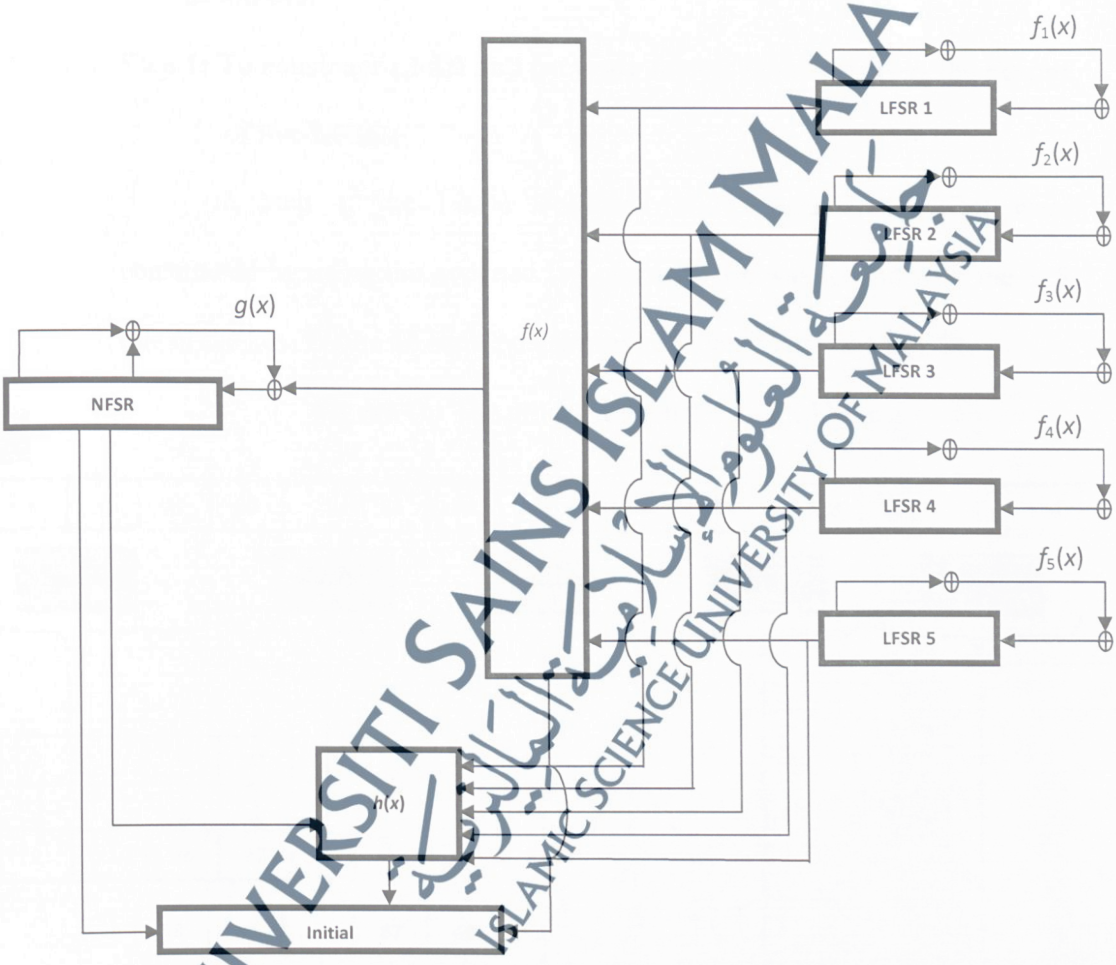


Figure 15: Keystream generation process of MG-128



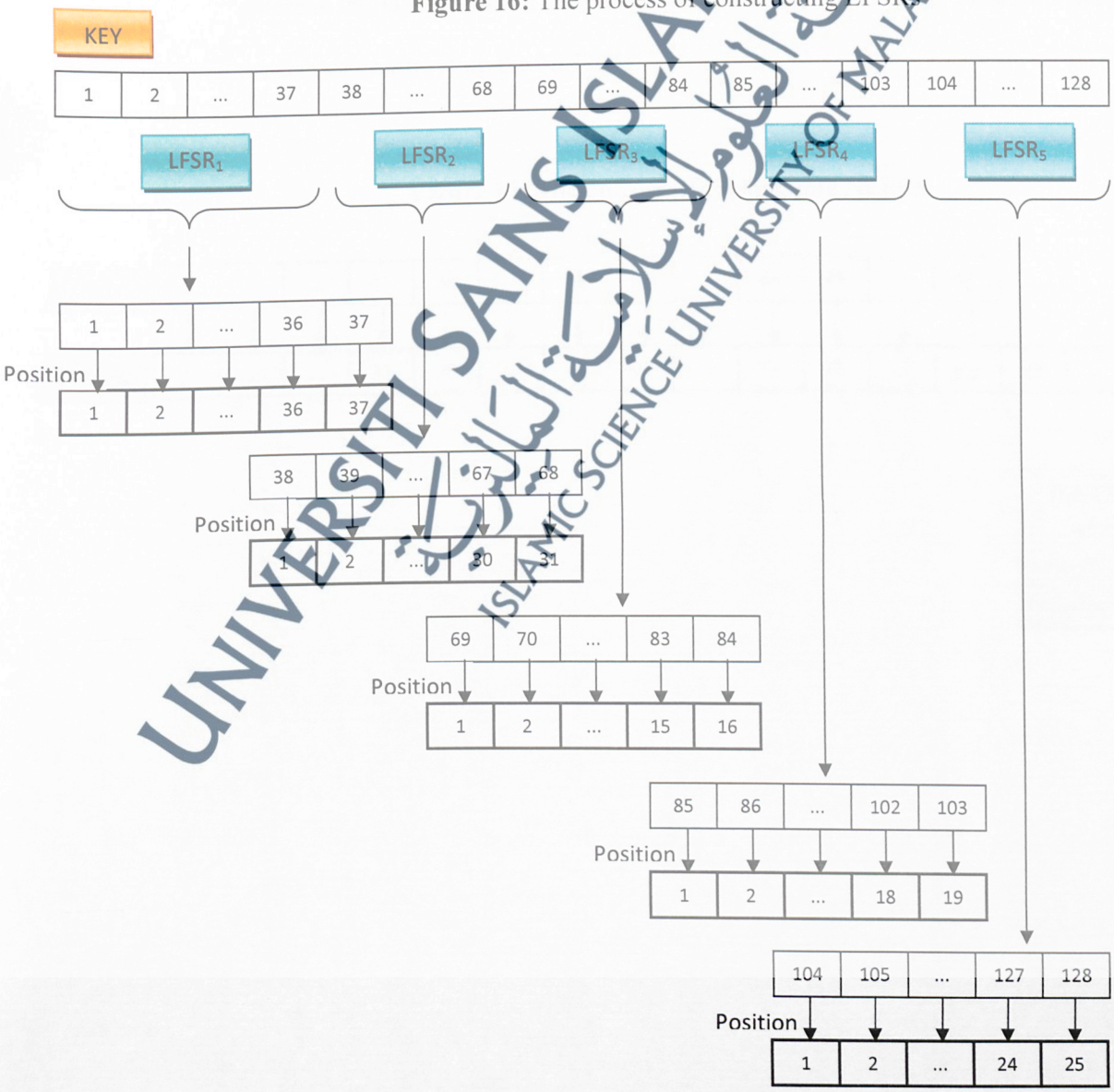
a. **Key Initialization of Modified Grain-128 Process**

In order to generate key initialization, the cipher must be firstly initialized with the key and the IV. The initialization of the key and the IV was done as follows:

Step 1: To construct LFSR and generate the bit sequence from the output of five LFSRs

In Step 1, the Linear Feedback Shift Registers (LFSRs) were constructed by using the assigned key. Each LFSR was loaded with the 128 bits of the key. Figure 16 shows the process of constructing the LFSRs.

Figure 16: The process of constructing LFSRs

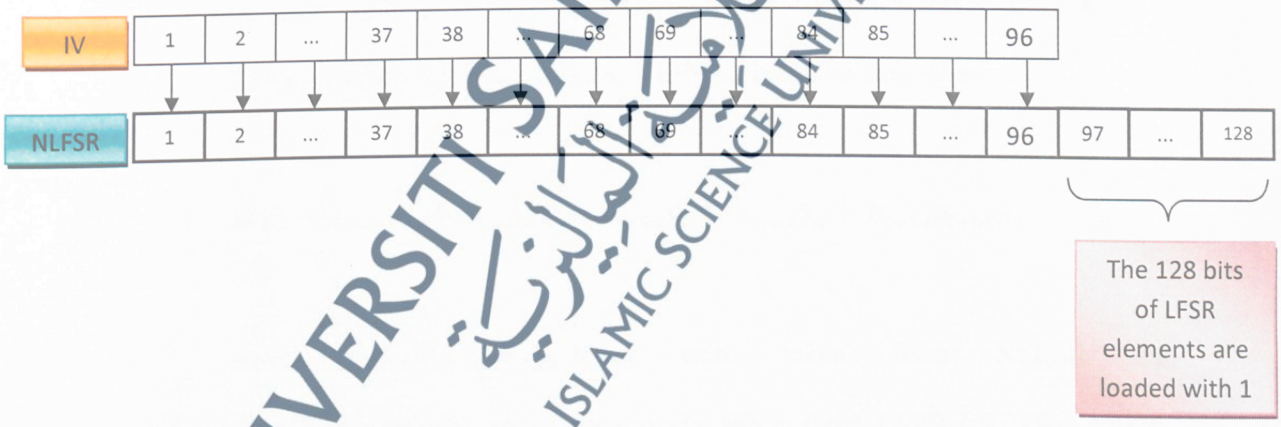


The bit sequences from the output of five independent LFSRs, namely $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$, and $LFSR_5$ were generated. For the configuration, the feedback tapping was based on the primitive polynomial used for each LFSR. Each LFSR produced bit sequence, namely S_1, S_2, S_3, S_4, and S_5, respectively.

Step 2: To construct NLFSR and generate the bit sequence from the output of NLFSR

In Step 2, the Non-Linear Feedback Shift Register (NLFSR) was constructed using the IV. The first 96 bits of NLFSR were loaded with IV bits, whereas the last 32 bits of NLFSR were filled with 1s. Figure 17 shows the process of constructing the NLFSR.

Figure 17: The process of constructing NLFSR



The NLFSR was updated for each clock by the following setting:

$$g(x)_{i+128} = f(x) + b_i + b_{i+26} + b_{i+56} + b_{i+91} + b_{i+96} + b_{i+3}b_{i+67} + b_{i+11}b_{i+13} + b_{i+17}b_{i+18} + b_{i+27}b_{i+59} + b_{i+40}b_{i+48} + b_{i+61}b_{i+65} + b_{i+68}b_{i+84}$$

Step 3: To obtain value of $f(x)$

In Step 3, to obtain the value of $f(x)$, each bit sequence of LFSR was XOR as the following:

$$f(x) = S_1 + S_2 + S_3 + S_4 + S_5$$

Step 4: To obtain value of Boolean function, $h(x)$

In Step 4, nine inputs were taken to obtain the value of $h(x)$. Four bits of input were taken from NLFSR and 1-bit input was taken from each of $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$ and $LFSR_5$. It can be defined as:

$$h(x) = b_{i+12}S_1 + b_{i+13}S_2 + b_{i+95}S_3 + b_{i+60}S_4 + b_{i+12}b_{i+95}S_5$$

where $b_{i+12}, b_{i+13}, b_{i+95}, b_{i+60}$ were taken from NLFSR and $s1_i, s2_i, s3_i, s4_i, s5_i$ were respectively taken from $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$, and $LFSR_5$.

Step 5: To obtain value of Initial

In Step 5, the initial value was obtained by applying XOR operation to the three bits of $f(x)$, $g(x)$, and $h(x)$, where the output function can be defined as:

$$\boldsymbol{initial} = \sum_{j \in A} b_{i+j} + h(x) + f(x)$$

where A = {2,15,36,45,64,73,89}

The initial was fed back and XOR with the input of NLFSR, $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$ and $LFSR_5$ respectively. The initial was clocked 256 times before producing the keystream.

b. Generating the Keystream of Modified Grain-128 (MG-128) Process

For Modified Grain-128, the process of producing keystream was similar with the key initialization process from step 1 until step 4. However, in step 5, there was a difference in order to obtain the output of keystream. The output of keystream was not fed back to the NLFSR, $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$, and $LFSR_5$.

5.2 Experimental Setup for Modified Grain-128 (MG-128) Stream Cipher Algorithm

The randomness testing activities were based on the application of the NIST Statistical Test Suite. Table 39 shows the requirement for parameter value(s) that must be considered in conducting the experiment for the Parameterized Test Selection.

The maximum number of rejection rate should be as shown in Table 40. For the Random Excursion Variant Test and the Random Excursion Test, the samples used for evaluation were only 67 samples, because only 67 samples had the number of cycles exceeding 500. For the other 33 samples, the number of cycles did not exceed 500. Therefore, the samples with the number of cycles not exceeding 500 were not evaluated.

Table 39: Parameter value(s) for Parameterized Tests Selection used for Modified Grain-128

Test	Requirement	Selection
Block Frequency Test	$N < 100$	$N = n/M$ $= 1{,}000{,}000/20{,}000$ $= 50$
	$n \geq 100$ and $n \geq MN$	$n = 1{,}000{,}000$ and $n \geq MN$ $= 20{,}000 \times 50$ $= 1{,}000{,}000$
	$M \geq 20$ $M \geq 0.01n$	$\boldsymbol{M = 20{,}000}$ **(Block Length)** $M \geq 0.01n$ $= 0.01 \times 1{,}000{,}000$ $= 10{,}000$
Non-Overlapping Test	$n \geq 1{,}000{,}000$	$n = 1{,}000{,}000$
	$M \geq 0.01n$ $= 0.01 \times 1{,}000{,}000$ $= 10{,}000$	$M = n/N$ $= 1{,}000{,}000/100$ $= 10{,}000$
	$N \leq 100$	$N = 8$ (fixed)
	NIST recommends to choose m = 9 or 10	$\boldsymbol{m = 10}$ **(Template Length)**
Overlapping Test	$N \leq 100$	$N = 8$ (fixed)
	$M \geq 0.01n$ $= 0.01 \times 1{,}000{,}000$ $= 10{,}000$	$M = n/N$ $= 1{,}000{,}000/100$ $= 10{,}000$
	n is not specific	$n = 1{,}000{,}000$
	NIST recommends to choose m = 9 or 10	$\boldsymbol{m = 10}$ **(Template Length)**
Maurer's Universal Test	$6 \leq L \leq 16$	$\boldsymbol{L = 7}$ **(Block Length)**
	$Q = 10 \times 2^L$	$\boldsymbol{Q = 10 \times 2^L = 10 \times 2^7 = 1{,}280}$ **(Number of Block)**
	$n \geq 904{,}960$	$n = 1{,}000{,}000$
Linear Complexity Test	$500 \leq M \leq 5{,}000$	$\boldsymbol{M = 2{,}000}$ **(Block Length)**
	$n \geq 1{,}000{,}000$	$n = 1{,}000{,}000$
	$N \geq 200$	$N = n/M$ $= 1{,}000{,}000/2{,}000$ $= 500$
Serial Test	$m < [\log_2 n] - 2$	$\boldsymbol{m = 2}$ **(Block Length)**
Approximate Entropy Test	$m < [\log_2 n] - 5$	$\boldsymbol{m = 2}$ **(Block Length)**

Table 40: Number of maximum rejection for keystream

Significance Level	Most of the NIST tests (based on 100 *p*-value)	Non-Overlapping (based on 14,800 *p*-value)	Random Excursion Variant (based on 1,206 *p*-value)	Random Excursion (based on 536 *p*-value)
0.01	3 samples	184 samples	22 samples	12 samples
0.02	6 samples	347 samples	38 samples	20 samples
0.03	8 samples	506 samples	53 samples	27 samples
0.04	9 samples	663 samples	68 samples	35 samples
0.05	11 samples	819 samples	83 samples	41 samples

5.3 Results and Analysis for Modified Grain-128 (MG-128) Stream Cipher Algorithm

Table 41 shows the NIST statistical tests results for keystream of MG-128 at 1% significance level. From the results, all the NIST statistical tests passed. Therefore, it can be concluded that all the 100 sequences of keystream for MG-128 have passed each of the 16 NIST statistical tests at 1% significance level.

Table 41: Results for keystream of MG-128 at 1% significance level

Statistical Test	Number of sequences at 1% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	100	0	Pass
2. Runs Test	100	0	Pass
3. Longest Runs of Ones Test	100	0	Pass
4. Spectral DFT Test	99	1	Pass
5. Lempel-Ziv Complexity Test	99	1	Pass
6. Cumulative Sums Test - Forward - Reverse	 100 100	 0 0	 Pass Pass
7. Random Excursion Variant Test (67 samples)	1444	8	Pass
8. Random Excursion Test (67 samples)	502	10	Pass
9. Binary Matrix Rank Test	100	0	Pass
Parameterized Test Selection			
1. Block Frequency Test	100	0	Pass
2. Non-Overlapping Test	14657	143	Pass
3. Overlapping Test	98	2	Pass
4. Maurer's Universal Test	100	0	Pass
5. Linear Complexity Test	99	1	Pass
6. Serial Test - P value 1 - P value 2	 100 100	 0 0	 Pass Pass
7. Approximate Entropy Test	100	0	Pass

Table 42 shows the NIST statistical tests results for keystream of MG-128 at 2% significance level. Referring to the results, all the NIST statistical tests results passed. Therefore, it can be concluded that all the 100 sequences of keystream for MG-128 have passed each of the 16 NIST statistical tests at 2% significance level.

Table 42: Results for keystream of MG-128 at 2% significance level

Statistical Test	Number of sequences at 2% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	100	0	Pass
2. Runs Test	100	0	Pass
3. Longest Runs of Ones Test	98	2	Pass
4. Spectral DFT Test	94	6	Pass
5. Lempel-Ziv Complexity Test	97	3	Pass
6. Cumulative Sums Test			
- Forward	100	0	Pass
- Reverse	99		Pass
7. Random Excursion Variant Test (67 samples)	1140	12	Pass
8. Random Excursion Test (67 samples)	490	13	Pass
9. Binary Matrix Rank Test	98	2	Pass
Parameterized Test Selection			
1. Block Frequency Test	99	1	Pass
2. Non-Overlapping Test	14497	303	Pass
3. Overlapping Test	97	3	Pass
4. Maurer's Universal Test	99	1	Pass
5. Linear Complexity Test	97	3	Pass
6. Serial Test			
- P value 1	100	0	Pass
- P value 2	100	0	Pass
7. Approximate Entropy Test	100	0	Pass

Table 43 below demonstrates the NIST statistical tests results for keystream of MG-128 at 3% significance level. Based on the results, all the NIST statistical tests passed. Therefore, it can be concluded that all the 100 sequences of keystream for MG-128 have passed each of the 16 NIST statistical tests at 3% significance level.

Table 43: Results for keystream of MG-128 at 3% significance level

Statistical Test	Number of sequences at 3% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	100	0	Pass
2. Runs Test	98	2	Pass
3. Longest Runs of Ones Test	96	4	Pass
4. Spectral DFT Test	94	6	Pass
5. Lempel-Ziv Complexity Test	95	5	Pass
6. Cumulative Sums Test - Forward - Reverse	 100 98	 0 2	 Pass Pass
7. Random Excursion Variant Test (67 samples)	1130	22	Pass
8. Random Excursion Test (67 samples)	490	22	Pass
9. Binary Matrix Rank Test	97	3	Pass
Parameterized Test Selection			
1. Block Frequency Test	99	1	Pass
2. Non-Overlapping Test	14329	471	Pass
3. Overlapping Test	96	4	Pass
4. Maurer's Universal Test	97	3	Pass
5. Linear Complexity Test	97	3	Pass
6. Serial Test - P value 1 - P value 2	 100 98	 0 2	 Pass Pass
7. Approximate Entropy Test	100	0	Pass

Table 44 below exhibits the NIST statistical tests results for keystream of MG-128 at 4% significance level. With reference to the results, all the NIST statistical tests results passed. Therefore, it can be concluded that all the 100 sequences of keystream for MG-128 have passed each of the 16 NIST statistical tests at 4% significance level.

Table 44: Results for keystream of MG-128 at 4% significance level

Statistical Test	Number of sequences at 4% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	97	3	Pass
2. Runs Test	96	4	Pass
3. Longest Runs of Ones Test	96	4	Pass
4. Spectral DFT Test	94	6	Pass
5. Lempel-Ziv Complexity Test	95	5	Pass
6. Cumulative Sums Test - Forward - Reverse	 98 98	 2 2	 Pass Pass
7. Random Excursion Variant Test (67 samples)	1119	33	Pass
8. Random Excursion Test (67 samples)	488	24	Pass
9. Binary Matrix Rank Test	97	3	Pass
Parameterized Test Selection			
1. Block Frequency Test	99	1	Pass
2. Non-Overlapping Test	14188	612	Pass
3. Overlapping Test	96	4	Pass
4. Maurer's Universal Test	96	4	Pass
5. Linear Complexity Test	95	5	Pass
6. Serial Test - P value 1 - P value 2	 100 96	 0 4	 Pass Pass
7. Approximate Entropy Test	99	1	Pass

Table 45 illustrates the NIST statistical tests results for keystream of MG-128 at 5% significance level. From the results, all the NIST statistical tests passed. Therefore, it can be concluded that all the 100 sequences of keystream for MG-128 have passed each of the 16 NIST statistical tests at 5% significance level.

Table 45: Results for keystream of MG-128 at 5% significance level

Statistical Test	Number of sequences at 5% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	96	4	Pass
2. Runs Test	94	6	Pass
3. Longest Runs of Ones Test	95	5	Pass
4. Spectral DFT Test	94	6	Pass
5. Lempel-Ziv Complexity Test	94	6	Pass
6. Cumulative Sums Test - Forward - Reverse	 98 97	 2 3	 Pass Pass
7. Random Excursion Variant Test (67 samples)	1112	40	Pass
8. Random Excursion Test (67 samples)	483	29	Pass
9. Binary Matrix Rank Test	95	5	Pass
Parameterized Test Selection			
1. Block Frequency Test	99	1	Pass
2. Non-Overlapping Test	14035	765	Pass
3. Overlapping Test	96	4	Pass
4. Maurer's Universal Test	93	7	Pass
5. Linear Complexity Test	94	6	Pass
6. Serial Test - P value 1 - P value 2	 100 94	 0 6	 Pass Pass
7. Approximate Entropy Test	98	2	Pass

In conclusion, based on the results obtained from the experiment conducted against the MG-128 stream cipher algorithm, it can be concluded that the keystream of MG-128 has passed all the tests in NIST Statistical Test Suite for all 1%–5%

significance level. Therefore, it can be concluded that the sequences tested for keystream of MG-128 were random for all significance level of 1%–5%.

5.4 Comparison between Grain-128 and MG-128 Stream Cipher Algorithms

This section explains the comparison between Grain-128 and MG-128 stream cipher algorithms. Each main building block used in both algorithms is discussed including Linear Feedback Shift Register (LFSR), Non-Linear Feedback Shift Register (NLFSR), and Boolean Function. In addition, the keystream for each algorithm is also discussed.

Furthermore, Table 51–55 show the comparison of NIST statistical test results for both Grain-128 and MG-128 stream cipher algorithms.

a. Linear Feedback Shift Register (LFSR)

Grain-128

Grain-128 used one (1) LFSR with 128 bits and it was primitive polynomial. The LFSR used can be defined as follows:

$$f(x) = 1 + x^{32} + x^{47} + x^{58} + x^{90} + x^{121} + x^{128}$$

Then, the LFSR was updated for each clock by setting

$$s_{i+128} = s_i + s_{i+7} + s_{i+38} + s_{i+70} + s_{i+81} + s_{i+96}$$

MG-128

MG-128 used five (5) LFSRs and each LFSR was primitive polynomial. The LFSRs are listed below:

- $LFSR_1 = f_1(x) = 1 + x^{25} + x^{27} + x^{35} + x^{37}$
- $LFSR_2 = f_2(x) = 1 + x^{24} + x^{31}$
- $LFSR_3 = f_3(x) = 1 + x^2 + x^4 + x^5 + x^8 + x^9 + x^{12} + x^{13} + x^{15} + x^{16}$
- $LFSR_4 = f_4(x) = 1 + x^9 + x^{14} + x^{15} + x^{17} + x^{19}$
- $LFSR_5 = f_5(x) = 1 + x^{21} + x^{22} + x^{25}$

Then, the LFSR was updated for each clock by setting

$$f(x)_{i+128} = s1_i + s2_i + s3_i + s4_i + s5_i$$

b. Non-Linear Feedback Shift Register (NLFSR)

Grain-128

For Non-Linear Feedback Shift Register, one (1) NLFSR with 128 bits was used in Grain-128. The NLFSR used was the sum of one linear and one bent function. The NLFSR used can be defined as follows:

$$g(x) = 1 + x^{32} + x^{37} + x^{72} + x^{102} + x^{128} + x^{44}x^{60} + x^{61}x^{125} + x^{63}x^{67} + x^{69}x^{101} + x^{80}x^{88} + x^{110}x^{111} + x^{115}x^{117}$$

Then, this NLFSR was updated for each clock by setting

$$b_{i+128} = s_i + b_i + b_{i+26} + b_{i+56} + b_{i+91} + b_{i+96} + b_{i+3}b_{i+67} + b_{i+11}b_{i+13} + b_{i+17}b_{i+18} + b_{i+27}b_{i+59} + b_{i+40}b_{i+48} + b_{i+61}b_{i+65} + b_{i+68}b_{i+84}$$

MG-128

For MG-128, the NLFSR used was similar as in Grain-128, which is as the following:

$$g(x) = 1 + x^{32} + x^{37} + x^{72} + x^{102} + x^{128} + x^{44}x^{60} + x^{61}x^{125} + x^{63}x^{67} + x^{69}x^{101} + x^{80}x^{88} + x^{110}x^{111} + x^{115}x^{117}$$

Then, this NLFSR was updated for each clock by setting

$$b_{i+128} = f(x) + b_i + b_{i+26} + b_{i+56} + b_{i+91} + b_{i+96} + b_{i+3}b_{i+67} + b_{i+11}b_{i+13} + b_{i+17}b_{i+18} + b_{i+27}b_{i+59} + b_{i+40}b_{i+48} + b_{i+61}b_{i+65} + b_{i+68}b_{i+84}$$

c. **Boolean Function**

Grain-128

For Grain-128, the Boolean Function used consisted of 9-input filter function taken from 7-bit input from LFSR and 2-bit input from NLFSR.

$$h(x) = h(x_0, x_1, \dots x_8) = x_0x_1 + x_2x_3 + x_4x_5 + x_6x_7 + x_0x_4x_8$$

MG-128

For MG-128, the Boolean Function used consisted of 9-input filter function taken from 4-bit input from NLFSR and 1-bit input from each of $LFSR_1$, $LFSR_2$, $LFSR_3$, $LFSR_4$, and $LFSR_5$.

$$h(x) = b_{i+12}S_1 + b_{i+13}S_2 + b_{i+95}S_3 + b_{i+60}S_4 + b_{i+12}b_{i+95}S_5$$

d. Keystream

Grain-128

For Grain-128, the formula used to obtain the keystream is as follows:

$$z_i = \sum_{j \in A} b_{i+j} + h(x) + s_{i+93}$$

Where A = {2,15,36,45,64,73,89}

MG-128

For MG-128, the formula used to get the keystream is as follows:

$$z_i = \sum_{j \in A} b_{i+j} + h(x) + f(x)$$

Where A = {2,15,36,45,64,73,89}

Table 46: Comparison of NIST Statistical Test results between Grain-128 and Modified Grain-128 for 1% significance level.

Statistical Test	Number of sequences at 1% significance level	
	Grain-128	MG-128
Non-Parameterized Test Selection		
1. Frequency Test	0	0
2. Runs Test	0	0
3. Longest Runs of Ones Test	1	0
4. Spectral DFT Test	0	1
5. Lempel-Ziv Complexity Test	5	1
6. Cumulative Sums Test - Forward - Reverse	 0 0	 0 0
7. Random Excursion Variant Test	5	8
8. Random Excursion Test	3	10
9. Binary Matrix Rank Test	1	0
Parameterized Test Selection		
1. Block Frequency Test	1	0
2. Non-Overlapping Test	147	143
3. Overlapping Test	1	2
4. Maurer's Universal Test	1	0
5. Linear Complexity Test	4	1
6. Serial Test - P value 1 - P value 2	 0 0	 0 0
7. Approximate Entropy Test	0	0

Table 46 shows the comparison of NIST statistical test results between Grain-128 and MG-128 stream cipher algorithms for 1% significance level. From the results, there were two (2) statistical tests failed for Grain-128 stream cipher, which were Lempel-Ziv Complexity Test and Linear Complexity Test. Both tests exceeded the maximum number of rejection for 1% significance level, with 5 and 4 rejections, respectively. Therefore, it can be concluded that the Grain-128 was non-random for 1% significance level.

On the other hand, for MG-128, it was shown that this algorithm has passed all the 16 NIST statistical tests. Therefore, it can be concluded that the MG-128 was random for 1% significance level.

Table 47: Comparison of NIST Statistical Test results between Grain-128 and Modified Grain-128 for 2% significance level.

Statistical Test	Number of sequences at 2% significance level	
	Grain-128	MG-128
Non-Parameterized Test Selection		
1. Frequency Test	3	0
2. Runs Test	1	0
3. Longest Runs of Ones Test	1	1
4. Spectral DFT Test	1	6
5. Lempel-Ziv Complexity Test	7	3
6. Cumulative Sums Test		
- Forward	3	0
- Reverse	3	1
7. Random Excursion Variant Test	15	12
8. Random Excursion Test	8	13
9. Binary Matrix Rank Test	1	2
Parameterized Test Selection		
1. Block Frequency Test	3	1
2. Non-Overlapping Test	278	303
3. Overlapping Test	2	3
4. Maurer's Universal Test	2	1
5. Linear Complexity Test	2	3
6. Serial Test		
- P value 1	1	0
- P value 2	1	0
7. Approximate Entropy Test	1	0

Table 47 shows the comparison of NIST statistical test results between Grain-128 and MG-128 for 2% significance level. Based on the results, the Lempel-Ziv Complexity test failed for Grain-128 with seven (7) rejections. Therefore, it can be concluded that Grain-128 was non-random for 2% significance level.

As for MG-128, it was shown that all the 16 NIST statistical tests passed with the number of rejection below the maximum number of rejection allowed. Therefore, it can be concluded that MG-128 was random for 2% significance level.

Table 48: Comparison of NIST Statistical Test results between Grain-128 and Modified Grain-128 for 3% significance level.

Statistical Test	Number of sequences at 3% significance level	
	Grain-128	MG-128
Non-Parameterized Test Selection		
1. Frequency Test	4	0
2. Runs Test	2	2
3. Longest Runs of Ones Test	1	4
4. Spectral DFT Test	1	6
5. Lempel-Ziv Complexity Test	9	5
6. Cumulative Sums Test		
- Forward	3	0
- Reverse	4	2
7. Random Excursion Variant Test	26	22
8. Random Excursion Test	15	22
9. Binary Matrix Rank Test	2	3
Parameterized Test Selection		
1. Block Frequency Test	5	1
2. Non-Overlapping Test	425	471
3. Overlapping Test	3	4
4. Maurer's Universal Test	4	3
5. Linear Complexity Test	2	3
6. Serial Test		
- P value 1	1	0
- P value 2	2	2
7. Approximate Entropy Test	1	0

Table 48 above shows the comparison of NIST statistical test results between Grain-128 and MG-128 for 3% significance level. With reference to the results, there was an NIST statistical test that failed for Grain-128, which was Lempel-Ziv Complexity test. The total number of rejection was nine (9), exceeding the maximum

number of rejection for 3% significance level, which was eight (8). Therefore, it can be concluded that the Grain-128 was non-random for 3% significance level.

As for MG-128, it was shown that this algorithm has passed all the 16 NIST statistical tests. Therefore, it can be concluded that the MG-128 was random for 3% significance level.

Table 49: Comparison of NIST Statistical Test results between Grain-128 and Modified Grain-128 for 4% significance level

Statistical Test	Number of sequences at 4% significance level	
	Grain-128	MG-128
Non-Parameterized Test Selection		
1. Frequency Test	10	3
2. Runs Test	3	4
3. Longest Runs of Ones Test	3	4
4. Spectral DFT Test	2	6
5. Lempel-Ziv Complexity Test	8	5
6. Cumulative Sums Test		
- Forward	5	2
- Reverse	5	2
7. Random Excursion Variant Test	30	33
8. Random Excursion Test	19	24
9. Binary Matrix Rank Test	2	3
Parameterized Test Selection		
1. Block Frequency Test	5	1
2. Non-Overlapping Test	576	612
3. Overlapping Test	3	4
4. Maurer's Universal Test	4	4
5. Linear Complexity Test	2	5
6. Serial Test		
- P value 1	2	0
- P value 2	3	4
7. Approximate Entropy Test	2	1

Table 49 above shows the comparison of NIST statistical test results between Grain-128 and MG-128 stream ciphers for 4% significance level. The results for Grain-128 showed that Frequency Test has exceeded the maximum number of

rejection for 4% significance level with 10 rejections. Therefore, it can be concluded that the Grain-128 was non-random for 4% significance level.

As for MG-128, it was shown that this algorithm has passed all the 16 NIST statistical tests. Therefore, it can be concluded that the MG-128 was random for 4% significance level.

Table 50: Comparison of NIST Statistical Test results between Grain-128 and Modified Grain-128 for 5% significance level.

Statistical Test	Number of sequences at 5% significance level	
	Grain-128	MG-128
Non-Parameterized Test Selection		
1. Frequency Test	12	4
2. Runs Test	3	6
3. Longest Runs of Ones Test	4	5
4. Spectral DFT Test	5	6
5. Lempel-Ziv Complexity Test	10	6
6. Cumulative Sums Test		
- Forward	6	2
- Reverse	6	3
7. Random Excursion Variant Test	37	40
8. Random Excursion Test	26	29
9. Binary Matrix Rank Test	2	5
Parameterized Test Selection		
1. Block Frequency Test	5	1
2. Non-Overlapping Test	719	765
3. Overlapping Test	3	4
4. Maurer's Universal Test	12	7
5. Linear Complexity Test	2	6
6. Serial Test		
- P value 1	5	0
- P value 2	3	6
7. Approximate Entropy Test	2	2

Table 50 above shows the comparison of NIST statistical test results between Grain-128 and MG-128 stream cipher algorithms for 5% significance level. From the result, there were two (2) statistical tests that failed for Grain-128 stream cipher, which

were Frequency Test and Maurer's Universal Test. Both tests exceeded the maximum number of rejection for 5% significance level, with 12 rejections, respectively. Therefore, it can be concluded that the Grain-128 was non-random for 5% significance level.

On the other hand, for MG-128, it was shown that this algorithm has passed all the 16 NIST statistical tests. Therefore, it can be concluded that the MG-128 was random for 5% significance level.

5.5 Conclusion

Based on the results obtained from the experiment conducted against the MG-128 stream cipher algorithm, the keystream of MG-128 has passed all tests in the NIST Statistical Test Suite for all 1%–5% significance level used. Therefore, it can be concluded that the sequences tested for keystream of MG-128 were random for all significance level of 1%–5%.

In contrast with Grain-128, this algorithm showed that it was non-random for all 1%–5% significance level.

In conclusion, from the analysis obtained, the MG-128 stream cipher algorithm showed sufficient results of statistical analysis compared with Grain-128 stream cipher algorithm. In the future, this algorithm can be applied for the application with little computational resources such as for cell phone or other small embedded devices.