CHAPTER IV

RESULTS AND DISCUSSION OF GRAIN-128

4.1 Experimental Setup for Grain-128 Stream Cipher Algorithm

This chapter shows the results and analysis of Grain-128 stream cipher algorithm based on the experiment conducted. It consists of four data types that have been discussed in chapter 3. The four data types are keystream, output of LFSR, output of NLFSR, and output of Boolean function.

The randomness testing activities were based on the application of the NIST Statistical Test Suite. Table 10 shows the requirement for parameter(s) values considered in conducting the experiment for the Parameterized Test Selection.

For the maximum rejection rate, Table 11–14 show the number of maximum rejection rate for keystream, output of LFSR (fx), output of NLFSR (gx) and output of Boolean function (hx), respectively. All the tests had the same number of rejection rate for each data, except for the Random Excursion Variant Test and the Random Excursion Test, because both of the tests depended on the samples with the number of cycles exceeding 500. These two tests were not applicable for samples with insufficient number of cycles. The maximum number of rejection rate should be as shown in Table 16–19.

Table 10: Parameter value(s) for Parameterized Tests Selection used for 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 $n \geq MN$ $= 20{,}000 \times 50$ $= 1{,}000{,}000$
	$M \geq 20$ $M \geq 0.01n$	**$M = 20{,}000$ (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	**$m = 10$ (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	**$m = 10$ (Template Length)**
Maurer's Universal Test	$6 \leq L \leq 16$	**$L = 7$ (Block Length)**
	$Q = 10 \times 2^L$	**$Q = 10 \times 2^L = 10 \times 2^7 = 1{,}280$ (Number of Block)**
	$n \geq 904{,}960$	$n = 1{,}000{,}000$
Linear Complexity Test	$500 \leq M \leq 5{,}000$	**$M = 2{,}000$ (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	$m < [\log_2 n] - 2$	**$m = 2$ (Block Length)**
Approximate Entropy Test	$m < [\log_2 n] - 5$	**$m = 2$ (Block Length)**

Table 11: 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	Random Excursion
			Grain-128 (based on 1,152 *p*-value)	Grain-128 (based on 512 *p*-value)
0.01	3 samples	184 samples	21 samples	11 samples
0.02	6 samples	347 samples	37 samples	19 samples
0.03	8 samples	506 samples	51 samples	26 samples
0.04	9 samples	663 samples	66 samples	33 samples
0.05	11 samples	819 samples	79 samples	40 samples

Table 12: Number of maximum rejection for output of LFSR (*fx*)

Significance Level	Most of the NIST tests (based on 100 *p*-value)	Non-Overlapping (based on 14,800 *p*-value)	Random Excursion Variant	Random Excursion
			Grain-128 (based on 954 *p*-value)	Grain-128 (based on 424 *p*-value)
0.01	3 samples	184 samples	18 samples	10 samples
0.02	6 samples	347 samples	32 samples	17 samples
0.03	8 samples	506 samples	44 samples	23 samples
0.04	9 samples	663 samples	56 samples	29 samples
0.05	11 samples	819 samples	67 samples	34 samples

Table 13: Number of maximum rejection for output of NLFSR (*gx*)

Significance Level	Most of the NIST tests (based on 100 *p*-value)	Non-Overlapping (based on 14,800 *p*-value)	Random Excursion Variant	Random Excursion
			Grain-128 (based on 1,044 *p*-value)	Grain-128 (based on 464 *p*-value)
0.01	3 samples	184 samples	20 samples	11 samples
0.02	6 samples	347 samples	34 samples	18 samples
0.03	8 samples	506 samples	47 samples	24 samples
0.04	9 samples	663 samples	60 samples	31 samples
0.05	11 samples	819 samples	73 samples	37 samples

Table 14: Number of maximum rejection for output of Boolean Function (hx)

Significance Level	Most of the NIST tests (based on 100 p-value)	Non-Overlapping (based on 14,800 p-value)	Random Excursion Variant	Random Excursion
			Grain-128 (based on 882 p-value)	Grain-128 (based on 384 p-value)
0.01	3 samples	184 samples	17 samples	9 samples
0.02	6 samples	347 samples	30 samples	15 samples
0.03	8 samples	506 samples	41 samples	21 samples
0.04	9 samples	663 samples	52 samples	26 samples
0.05	11 samples	819 samples	63 samples	32 samples

4.2 Result and Analysis for Grain-128 Stream Cipher Algorithm

4.2.1 NIST Statistical Test Suite Result for Keystream

Table 15 shows the NIST statistical tests results for keystream at 1% significance level. From the results, with five (5) failures, the Lempel-Ziv Complexity Test exceeded the maximum number of rejected rate. The Linear Complexity Test also exceeded the maximum number of rejected with four (4) failures. Other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 15: Results for keystream 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	99	1	Pass
4. Spectral DFT Test	100	0	Pass
5. Lempel-Ziv Complexity Test	95	5	Failure
6. Cumulative Sums Test			
- Forward	100	0	Pass
- Reverse	100	0	Pass
7. Random Excursion Variant Test (64 samples)	1,147	5	Pass
8. Random Excursion Test (64 samples)	509	3	Pass
9. Binary Matrix Rank Test	99	1	Pass
Parameterized Test Selection			
1. Block Frequency Test	99	1	Pass
2. Non-Overlapping Test	14,653	147	Pass
3. Overlapping Test	99	1	Pass
4. Maurer's Universal Test	99	1	Pass
5. Linear Complexity Test	96	4	Failure
6. Serial Test			
- P value 1	100	0	Pass
- P value 2	100	0	Pass
7. Approximate Entropy Test	100	0	Pass

Table 16 shows the NIST statistical tests results for keystream at 2% significance level. From the results, the Lempel-Ziv Complexity Test exceeded the maximum number of rejected with seven (7) failures. Other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 16: Results for keystream at 2% significance level

Statistical Test	Number of sequences at 2% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	97	3	Pass
2. Runs Test	99	1	Pass
3. Longest Runs of Ones Test	99	1	Pass
4. Spectral DFT Test	99	1	Pass
5. Lempel-Ziv Complexity Test	93	7	Failure
6. Cumulative Sums Test			
- Forward	97	3	Pass
- Reverse	97	3	Pass
7. Random Excursion Variant Test (64 samples)	1,137	15	Pass
8. Random Excursion Test (64 samples)	504	8	Pass
9. Binary Matrix Rank Test	99	1	Pass
Parameterized Test Selection			
1. Block Frequency Test	97	3	Pass
2. Non-Overlapping Test	14,522	278	Pass
3. Overlapping Test	98	2	Pass
4. Maurer's Universal Test	98	2	Pass
5. Linear Complexity Test	98	2	Pass
6. Serial Test			
- P value 1	99	1	Pass
- P value 2	99	1	Pass
7. Approximate Entropy Test	99	1	Pass

Table 17 shows the NIST statistical tests results for keystream at 3% significance level. From the results, the Lempel-Ziv Complexity Test exceeded the maximum number of rejected with nine (9) failures. Other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 17: Results for keystream at 3% significance level

Statistical Test	Number of sequences at 3% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	96	4	Pass
2. Runs Test	98	2	Pass
3. Longest Runs of Ones Test	99	1	Pass
4. Spectral DFT Test	99	1	Pass
5. Lempel-Ziv Complexity Test	91	9	Failure
6. Cumulative Sums Test - Forward - Reverse	 97 96	 3 4	 Pass Pass
7. Random Excursion Variant Test (64 samples)	1,126	26	Pass
8. Random Excursion Test (64 samples)	497	15	Pass
9. Binary Matrix Rank Test	98	2	Pass
Parameterized Test Selection			
1. Block Frequency Test	95	5	Pass
2. Non-Overlapping Test	14,375	425	Pass
3. Overlapping Test	97	3	Pass
4. Maurer's Universal Test	96	4	Pass
5. Linear Complexity Test	98	2	Pass
6. Serial Test - P value 1 - P value 2	 99 98	 1 2	 Pass Pass
7. Approximate Entropy Test	99	1	Pass

Table 18 shows the NIST statistical tests results for keystream at 4% significance level. From the results, the Frequency Test exceeded the maximum number of rejected with 10 failures. Other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 18: Results for keystream at 4% significance level

Statistical Test	Number of sequences at 4% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	90	10	Failure
2. Runs Test	97	3	Pass
3. Longest Runs of Ones Test	97	3	Pass
4. Spectral DFT Test	98	2	Pass
5. Lempel-Ziv Complexity Test	92	8	Pass
6. Cumulative Sums Test			
- Forward	95	5	Pass
- Reverse	95	5	Pass
7. Random Excursion Variant Test (64 samples)	1,122	30	Pass
8. Random Excursion Test (64 samples)	493	19	Pass
9. Binary Matrix Rank Test	98	2	Pass
Parameterized Test Selection			
1. Block Frequency Test	95	5	Pass
2. Non-Overlapping Test	14,224	576	Pass
3. Overlapping Test	97	3	Pass
4. Maurer's Universal Test	96	4	Pass
5. Linear Complexity Test	98	2	Pass
6. Serial Test			
- P value 1	98	2	Pass
- P value 2	97	3	Pass
7. Approximate Entropy Test	98	2	Pass

Table 19 shows the NIST statistical tests results for keystream at 5% significance level. From the results, two NIST statistical tests failed, which were the Frequency Test and the Maurer's Universal Test, because they exceeded the maximum number of rejection rate. The number of rejected for both tests were 12, respectively. Other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 19: Results for keystream at 5% significance level

Statistical Test	Number of sequences at 5% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	82	12	Failure
2. Runs Test	97	3	Pass
3. Longest Runs of Ones Test	96	4	Pass
4. Spectral DFT Test	95	5	Pass
5. Lempel-Ziv Complexity Test	90	10	Pass
6. Cumulative Sums Test - Forward - Reverse	 94 94	 6 6	 Pass Pass
7. Random Excursion Variant Test (64 samples)	1,115	37	Pass
8. Random Excursion Test (64 samples)	486	26	Pass
9. Binary Matrix Rank Test	98	2	Pass
Parameterized Test Selection			
1. Block Frequency Test	95	5	Pass
2. Non-Overlapping Test	14,081	719	Pass
3. Overlapping Test	97	3	Pass
4. Maurer's Universal Test	88	12	Failure
5. Linear Complexity Test	98	2	Pass
6. Serial Test - P value 1 - P value 2	 95 97	 5 3	 Pass Pass
7. Approximate Entropy Test	98	2	Pass

4.2.2 NIST Statistical Test Suite Result for Output of LFSR (*fx*)

Table 20 below shows the NIST statistical tests results of the output of LFSR, (*fx*) at 1% significance level. The result showed that the Longest Runs of Ones Test and the Linear Complexity Test exceeded the maximum number of rejection rate. For the Longest Runs of Ones Test, the number of rejected was four (4). For the Linear Complexity Test, all the 100 sequences of the output of LFSR, (*fx*) failed this test. The other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection.

Table 20: Results for LFSR (*fx*) at 1% significance level

Statistical Test	Number of sequences at 1% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	98	2	Pass
2. Runs Test	98	2	Pass
3. Longest Runs of Ones Test	96	4	Failure
4. Spectral DFT Test	100	0	Pass
5. Lempel-Ziv Complexity Test	100	0	Pass
6. Cumulative Sums Test			
- Forward	98	2	Pass
- Reverse	98	2	Pass
7. Random Excursion Variant Test (53 samples)	944	10	Pass
8. Random Excursion Test (53 samples)	416	8	Pass
9. Binary Matrix Rank Test	100	0	Pass
Parameterized Test Selection			
1. Block Frequency Test	100	0	Pass
2. Non-Overlapping Test	14,639	161	Pass
3. Overlapping Test	98	2	Pass
4. Maurer's Universal Test	100	0	Pass
5. Linear Complexity Test	0	100	Failure
6. Serial Test			
- P value 1	100	0	Pass
- P value 2	98	2	Pass
7. Approximate Entropy Test	98	2	Pass

Table 21 below demonstrates the results of the NIST statistical tests for output of LFSR, (fx) at 2% significance level. The result showed that the Linear Complexity Test failed for all the 100 sequences of the output of LFSR, (fx). Other NIST statistical tests results showed that the number of rejected were still under the maximum number of rejection rate.

Table 21: Results for LFSR (fx) at 2% significance level

Statistical Test	Number of sequences at 2% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	98	2	Pass
2. Runs Test	96	4	Pass
3. Longest Runs of Ones Test	95	5	Pass
4. Spectral DFT Test	99	1	Pass
5. Lempel-Ziv Complexity Test	98	2	Pass
6. Cumulative Sums Test - Forward - Reverse	 97 97	 3 3	 Pass Pass
7. Random Excursion Variant Test (53 samples)	927	27	Pass
8. Random Excursion Test (53 samples)	411	13	Pass
9. Binary Matrix Rank Test	99	1	Pass
Parameterized Test Selection			
1. Block Frequency Test	100	0	Pass
2. Non-Overlapping Test	14,516	284	Pass
3. Overlapping Test	98	2	Pass
4. Maurer's Universal Test	98	2	Pass
5. Linear Complexity Test	0	100	Failure
6. Serial Test - P value 1 - P value 2	 98 96	 2 4	 Pass Pass
7. Approximate Entropy Test	97	3	Pass

Table 22 below demonstrates the results of the NIST statistical tests for output of LFSR, (fx) at 3% significance level. The result showed that the Linear Complexity test also failed for all the 100 sequences of the output of LFSR, (fx). Other NIST statistical tests results showed that the number of rejected were under the range of the maximum number of rejection rate.

Table 22: Results for LFSR (fx) at 3% significance level

Statistical Test	Number of sequences at 3% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	98	2	Pass
2. Runs Test	96	4	Pass
3. Longest Runs of Ones Test	95	5	Pass
4. Spectral DFT Test	98	2	Pass
5. Lempel-Ziv Complexity Test	97	3	Pass
6. Cumulative Sums Test			
- Forward	97	3	Pass
- Reverse	97	3	Pass
7. Random Excursion Variant Test (53 samples)	915	89	Pass
8. Random Excursion Test (53 samples)	408	16	Pass
9. Binary Matrix Rank Test	95	5	Pass
Parameterized Test Selection			
1. Block Frequency Test	98	2	Pass
2. Non-Overlapping Test	14,353	447	Pass
3. Overlapping Test	97	3	Pass
4. Maurer's Universal Test	96	4	Pass
5. Linear Complexity Test	0	100	Failure
6. Serial Test			
- P value 1	94	6	Pass
- P value 2	96	4	Pass
7. Approximate Entropy Test	96	4	Pass

Table 23 below demonstrates the results of the NIST statistical tests for output of LFSR, (fx) at 4% significance level. The result showed that the Linear Complexity test also failed for all the 100 sequences of the output of LFSR, (fx) at 4% significance level. However, the other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 23: Results for LFSR (fx) 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	95	5	Pass
3. Longest Runs of Ones Test	91	9	Pass
4. Spectral DFT Test	98	2	Pass
5. Lempel-Ziv Complexity Test	95	5	Pass
6. Cumulative Sums Test - Forward - Reverse	 97 96	 3 4	 Pass Pass
7. Random Excursion Variant Test (53 samples)	905	49	Pass
8. Random Excursion Test (53 samples)	401	23	Pass
9. Binary Matrix Rank Test	93	7	Pass
Parameterized Test Selection			
1. Block Frequency Test	96	4	Pass
2. Non-Overlapping Test	14,211	589	Pass
3. Overlapping Test	96	4	Pass
4. Maurer's Universal Test	95	5	Pass
5. Linear Complexity Test	0	100	Failure
6. Serial Test - P value 1 - P value 2	 94 95	 6 5	 Pass Pass
7. Approximate Entropy Test	96	4	Pass

Table 24 below demonstrates the results of the NIST statistical tests for output of LFSR, (*fx*) at 5% significance level. The result showed that the Linear Complexity test also failed for all the 100 sequences of the output of LFSR, (*fx*) at 5% significance level. However, the other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 24: Results for LFSR (*fx*) at 5% significance level

Statistical Test	Number of sequences at 5% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	95	5	Pass
2. Runs Test	95	5	Pass
3. Longest Runs of Ones Test	89	11	Pass
4. Spectral DFT Test	98	2	Pass
5. Lempel-Ziv Complexity Test	94	6	Pass
6. Cumulative Sums Test			
- Forward	96	4	Pass
- Reverse	96	4	Pass
7. Random Excursion Variant Test (53 samples)	894	60	Pass
8. Random Excursion Test (53 samples)	397	27	Pass
9. Binary Matrix Rank Test	93	7	Pass
Parameterized Test Selection			
1. Block Frequency Test	95	5	Pass
2. Non-Overlapping Test	14,058	742	Pass
3. Overlapping Test	95	5	Pass
4. Maurer's Universal Test	95	5	Pass
5. Linear Complexity Test	0	100	Failure
6. Serial Test			
- P value 1	94	6	Pass
- P value 2	95	5	Pass
7. Approximate Entropy Test	94	6	Pass

4.2.3 NIST Statistical Test Suite Result for Output of NLFSR (gx)

Table 25 shows the NIST statistical tests results for output of NLFSR, (gx) at 1% significance level. Referring to the results, two NIST statistical tests failed, which are the Frequency Test and the Maurer's Universal Test. Both tests exceeded the maximum number of rejected with four (4) failures, respectively. Other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 25: Results for NLFSR (gx) at 1% significance level

Statistical Test	Number of sequences at 1% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	96	4	Failure
2. Runs Test	100	0	Pass
3. Longest Runs of Ones Test	98	2	Pass
4. Spectral DFT Test	100	0	Pass
5. Lempel-Ziv Complexity Test	99	1	Pass
6. Cumulative Sums Test			
- Forward	97	3	Pass
- Reverse	97	3	Pass
7. Random Excursion Variant Test (58 samples)	1,042	2	Pass
8. Random Excursion Test (58 samples)	459	5	Pass
9. Binary Matrix Rank Test	98	2	Pass
Parameterized Test Selection			
1. Block Frequency Test	99	1	Pass
2. Non-Overlapping Test	14,643	157	Pass
3. Overlapping Test	100	0	Pass
4. Maurer's Universal Test	96	4	Failure
5. Linear Complexity Test	100	0	Pass
6. Serial Test			
- P value 1	97	3	Pass
- P value 2	100	0	Pass
7. Approximate Entropy Test	98	2	Pass

Table 26 shows the NIST statistical tests results for output of NLFSR, (gx) at 2% significance level. Referring to the results, only the Non-Overlapping Test exceeded the maximum number of rejection rate with 350 failures. Other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 26: Results for NLFSR (gx) at 2% significance level

Statistical Test	Number of sequences at 2% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	96	4	Pass
2. Runs Test	99	1	Pass
3. Longest Runs of Ones Test	98	2	Pass
4. Spectral DFT Test	100	0	Pass
5. Lempel-Ziv Complexity Test	98	2	Pass
6. Cumulative Sums Test			
- Forward	97	3	Pass
- Reverse	97	3	Pass
7. Random Excursion Variant Test (58 samples)	1,039	5	Pass
8. Random Excursion Test (58 samples)	454	10	Pass
9. Binary Matrix Rank Test	97	3	Pass
Parameterized Test Selection			
1. Block Frequency Test	98	2	Pass
2. Non-Overlapping Test	14,450	350	Failure
3. Overlapping Test	99	1	Pass
4. Maurer's Universal Test	96	4	Pass
5. Linear Complexity Test	99	1	Pass
6. Serial Test			
- P value 1	96	4	Pass
- P value 2	99	1	Pass
7. Approximate Entropy Test	97	3	Pass

Table 27 shows the NIST statistical tests results for output of NLFSR, (gx) at 3% significance level. Referring to the results, all the NIST statistical tests passed. Therefore, it can be concluded that all the 100 sequences of output of NLFSR, (gx) have passed each of the 16 NIST statistical tests at 3% significance level.

Table 27: Results for NLFSR (gx) at 3% significance level

Statistical Test	Number of sequences at 3% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	96	4	Pass
2. Runs Test	97	3	Pass
3. Longest Runs of Ones Test	95	5	Pass
4. Spectral DFT Test	99	1	Pass
5. Lempel-Ziv Complexity Test	98	2	Pass
6. Cumulative Sums Test - Forward - Reverse	 97 95	 3 5	 Pass Pass
7. Random Excursion Variant Test (58 samples)	1,036	8	Pass
8. Random Excursion Test (58 samples)	452	12	Pass
9. Binary Matrix Rank Test	96	4	Pass
Parameterized Test Selection			
1. Block Frequency Test	96	4	Pass
2. Non-Overlapping Test	14,358	442	Pass
3. Overlapping Test	99	1	Pass
4. Maurer's Universal Test	95	5	Pass
5. Linear Complexity Test	99	1	Pass
6. Serial Test - P value 1 - P value 2	 95 97	 5 3	 Pass Pass
7. Approximate Entropy Test	96	4	Pass

Table 28 shows the NIST statistical tests results for output of NLFSR, (gx) at 4% significance level. Referring to the results, only Longest Runs of Ones Test exceeded the maximum number of rejection rate with 10 failures. Other NIST statistical tests results showed that the number of rejected were still under the range of the maximum number of rejection rate.

Table 28: Results for NLFSR (gx) at 4% significance level

Statistical Test	Number of sequences at 4% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	96	4	Pass
2. Runs Test	97	3	Pass
3. Longest Runs of Ones Test	90	10	Failure
4. Spectral DFT Test	99	1	Pass
5. Lempel-Ziv Complexity Test	98	2	Pass
6. Cumulative Sums Test			
- Forward	96	4	Pass
- Reverse	93	7	Pass
7. Random Excursion Variant Test (58 samples)	1,033	11	Pass
8. Random Excursion Test (58 samples)	449	15	Pass
9. Binary Matrix Rank Test	96	4	Pass
Parameterized Test Selection			
1. Block Frequency Test	96	4	Pass
2. Non-Overlapping Test	14,207	593	Pass
3. Overlapping Test	98	2	Pass
4. Maurer's Universal Test	94	6	Pass
5. Linear Complexity Test	98	2	Pass
6. Serial Test			
- P value 1	95	5	Pass
- P value 2	97	3	Pass
7. Approximate Entropy Test	94	6	Pass

Table 29 shows the NIST statistical tests results for output of NLFSR, (gx) at 5% significance level. Referring to the results, all the NIST statistical tests passed. Therefore, it can be concluded that all the 100 sequences of output of NLFSR, (gx) have passed each of the 16 NIST statistical tests at 5% significance level.

Table 29: Results for NLFSR (gx) 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	97	3	Pass
3. Longest Runs of Ones Test	90	10	Pass
4. Spectral DFT Test	97	3	Pass
5. Lempel-Ziv Complexity Test	95	5	Pass
6. Cumulative Sums Test - Forward - Reverse	 96 93	 4 7	 Pass Pass
7. Random Excursion Variant Test (58 samples)	1,029	15	Pass
8. Random Excursion Test (58 samples)	443	21	Pass
9. Binary Matrix Rank Test	94	6	Pass
Parameterized Test Selection			
1. Block Frequency Test	95	5	Pass
2. Non-Overlapping Test	14,046	754	Pass
3. Overlapping Test	97	3	Pass
4. Maurer's Universal Test	94	6	Pass
5. Linear Complexity Test	98	2	Pass
6. Serial Test - P value 1 - P value 2	 95 97	 5 3	 Pass Pass
7. Approximate Entropy Test	94	6	Pass

4.2.4 NIST Statistical Test Suite Result for Output of Boolean Function (*hx*)

Table 30 exhibits the results of the NIST statistical tests for output of Boolean function, (*hx*) at 1% significance level. With reference to the results, all the NIST statistical tests results failed, exceeding the maximum number of rejected, except for the Binary Matrix Rank Test and the Linear Complexity Test. Both of these tests passed with the number of rejected 2 and 0, respectively.

Table 30: Results for Output of Boolean Function (*hx*) at 1% significance level

Statistical Test	Number of sequences at 1% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	0	100	Failure
2. Runs Test	0	100	Failure
3. Longest Runs of Ones Test	0	100	Failure
4. Spectral DFT Test	55	45	Failure
5. Lempel-Ziv Complexity Test	0	100	Failure
6. Cumulative Sums Test - Forward - Reverse	 0 0	 100 100	 Failure Failure
7. Random Excursion Variant Test (49 samples)	0	882	Failure
8. Random Excursion Test (49 samples)	0	392	Failure
9. Binary Matrix Rank Test	98	2	Pass
Parameterized Test Selection			
1. Block Frequency Test	0	100	Failure
2. Non-Overlapping Test	6,458	8,342	Failure
3. Overlapping Test	0	100	Failure
4. Maurer's Universal Test	0	100	Failure
5. Linear Complexity Test	100	0	Pass
6. Serial Test - P value 1 - P value 2	 0 10	 100 90	 Failure Failure
7. Approximate Entropy Test	0	100	Failure

Table 31 exhibits the results of the NIST statistical tests for output of Boolean function, (hx) at 2% significance level. With reference to the results, all the NIST statistical tests results failed, exceeding the maximum number of rejected, except for the Binary Matrix Rank Test and the Linear Complexity Test. Both of these tests passed with the number of rejected 2 and 0, respectively.

Table 31: Results for Output of Boolean Function (hx) at 2% significance level

Statistical Test	Number of sequences at 2% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	0	100	Failure
2. Runs Test	0	100	Failure
3. Longest Runs of Ones Test	0	100	Failure
4. Spectral DFT Test	38	62	Failure
5. Lempel-Ziv Complexity Test	0	100	Failure
6. Cumulative Sums Test - Forward - Reverse	 0 0	 100 100	 Failure Failure
7. Random Excursion Variant Test (49 samples)	0	882	Failure
8. Random Excursion Test (49 samples)	0	392	Failure
9. Binary Matrix Rank Test	98	2	Pass
Parameterized Test Selection			
1. Block Frequency Test	0	100	Failure
2. Non-Overlapping Test	5,898	8,902	Failure
3. Overlapping Test	0	100	Failure
4. Maurer's Universal Test	0	100	Failure
5. Linear Complexity Test	100	0	Pass
6. Serial Test - P value 1 - P value 2	 0 8	 100 92	 Failure Failure
7. Approximate Entropy Test	0	100	Failure

Table 32 exhibits the results of the NIST statistical tests for output of Boolean function, (hx) at 3% significance level. With reference to the results, all the NIST statistical tests results failed, exceeding the maximum number of rejected, except for the Binary Matrix Rank Test and the Linear Complexity Test. Both of these tests passed with the number of rejected 5 and 1, respectively.

Table 32: Results for Output of Boolean Function (hx) at 3% of significance level

Statistical Test	Number of sequences at 3% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	0	100	Failure
2. Runs Test	0	100	Failure
3. Longest Runs of Ones Test	0	100	Failure
4. Spectral DFT Test	33	67	Failure
5. Lempel-Ziv Complexity Test	0	100	Failure
6. Cumulative Sums Test - Forward - Reverse	 0 0	 100 100	 Failure Failure
7. Random Excursion Variant Test (49 samples)	0	882	Failure
8. Random Excursion Test (49 samples)	0	392	Failure
9. Binary Matrix Rank Test	95	5	Pass
Parameterized Test Selection			
1. Block Frequency Test	0	100	Failure
2. Non-Overlapping Test	5,534	9,266	Failure
3. Overlapping Test	0	100	Failure
4. Maurer's Universal Test	0	100	Failure
5. Linear Complexity Test	99	1	Pass
6. Serial Test - P value 1 - P value 2	 0 6	 100 94	 Failure Failure
7. Approximate Entropy Test	0	100	Failure

Table 33 exhibits the results of the NIST statistical tests for output of Boolean function, (hx) at 4% significance level. With reference to the results, all the NIST statistical tests results failed, exceeding the maximum number of rejected, except for the Binary Matrix Rank Test and the Linear Complexity Test. Both of these tests passed with the number of rejected 7 and 1, respectively.

Table 33: Results for Output of Boolean Function (hx) at 4% significance level

Statistical Test	Number of sequences at 4% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	0	100	Failure
2. Runs Test	0	100	Failure
3. Longest Runs of Ones Test	0	100	Failure
4. Spectral DFT Test	29	71	Failure
5. Lempel-Ziv Complexity Test	0	100	Failure
6. Cumulative Sums Test - Forward - Reverse	 0 0	 100 100	 Failure Failure
7. Random Excursion Variant Test (49 samples)	0	882	Failure
8. Random Excursion Test (49 samples)	0	392	Failure
9. Binary Matrix Rank Test	93	7	Pass
Parameterized Test Selection			
1. Block Frequency Test	0	100	Failure
2. Non-Overlapping Test	5,297	9,503	Failure
3. Overlapping Test	0	100	Failure
4. Maurer's Universal Test	0	100	Failure
5. Linear Complexity Test	99	1	Pass
6. Serial Test - P value 1 - P value 2	 0 5	 100 95	 Failure Failure
7. Approximate Entropy Test	0	100	Failure

Table 34 exhibits the results of the NIST statistical tests for output of Boolean function, (hx) at 5% significance level. With reference to the results, all the NIST statistical tests results failed, exceeding the maximum number of rejected, except for the Binary Matrix Rank Test and the Linear Complexity Test. Both of these tests have passed with the number of rejected 7 and 1, respectively.

Table 34: Results for Output of Boolean Function (hx) at 5% significance level

Statistical Test	Number of sequences at 5% significance level		
	Pass	Fail	Pass/Failure
Non-Parameterized Test Selection			
1. Frequency Test	0	100	Failure
2. Runs Test	0	100	Failure
3. Longest Runs of Ones Test	0	100	Failure
4. Spectral DFT Test	25	75	Failure
5. Lempel-Ziv Complexity Test	0	100	Failure
6. Cumulative Sums Test - Forward - Reverse	 0 0	 100 100	 Failure Failure
7. Random Excursion Variant Test (49 samples)	0	882	Failure
8. Random Excursion Test (49 samples)	0	392	Failure
9. Binary Matrix Rank Test	93	7	Pass
Parameterized Test Selection			
1. Block Frequency Test	0	100	Failure
2. Non-Overlapping Test	5,069	9,731	Failure
3. Overlapping Test	0	100	Failure
4. Maurer's Universal Test	0	100	Failure
5. Linear Complexity Test	99	1	Pass
6. Serial Test - P value 1 - P value 2	 0 5	 100 95	 Failure Failure
7. Approximate Entropy Test	0	100	Failure

4.3 Conclusion

4.3.1 Keystream of Grain-128 stream cipher algorithm

The keystream of Grain-128 stream cipher algorithm mostly passed all the 16 NIST statistical tests at 1%–5% significance level. However, there were four (4) tests that failed, consist of the Frequency Test for significance level of 4%–5%, the Lempel-Ziv Complexity Test for significance level of 1%–3%, the Maurer's Universal Test for significance level of 5%, and the Linear Complexity Test at 1% significance level. Therefore, it can be concluded that the sequences tested for the keystream of Grain-128 stream cipher algorithm were not random for all significance level of 1%–5%. Table 35 below shows the list of tests that failed.

Table 35: Number of rejected result for keystream

Non-Parameterized Test Selection		
	Number of rejected	Significance Level
Frequency Test	10	4%
	12	5%
Lempel-Ziv Complexity Test	5	1%
	7	2%
	9	3%
Parameterized Test Selection		
Maurer's Universal Test	12	5%
Linear Complexity Test	4	1%

4.3.2 Output of LFSR (fx) of Grain-128 stream cipher algorithm

The output of LFSR, (fx) of Grain-128 mostly passed all the 16 NIST statistical tests at 1%–5% significance level, except for the Longest Runs of Ones Test for significance level of 1% and the Linear Complexity Test for significance level of 1%–5%. Therefore, it can be concluded that the sequences tested for output of LFSR, (fx) of Grain-128 stream cipher

algorithm were not random for all significance level of 1%–5%. Table 36 below shows the list of tests that failed.

Table 36: Number of rejected result for output of LFSR (*fx*)

Non-Parameterized Test Selection		
	Number of rejected	**Significance Level**
Longest Runs of Ones Test	4	1%
Linear Complexity Test	100	1%–5%

4.3.3 Output of NLFSR (*gx*) of Grain-128 stream cipher algorithm

The output of NLFSR, (*gx*) mostly passed all the 16 NIST statistical tests for significance level of 1%–5% except for several tests, as listed in Table 37 below. The tests that failed the NIST Statistical Test Suite were the Frequency Test for 1% of significance level, the Longest Runs of Ones Test for 4% of significance level, the Maurer's Universal Test for 1% of significance level, and the Non-Overlapping Test for 2% of significance level. Therefore, it can be concluded that the sequences tested for output of NLFSR, (*gx*) were not random for 1%, 2%, and 4% of significance level. On the other hand, these sequences have passed for the significance level of 1% and 3%.

Table 37: Number of rejected result for output of NLFSR (gx)

Non-Parameterized Test Selection		
	Number of rejected	**Significance Level**
Frequency Test	4	1%
Longest Runs of Ones Test	10	4%
Parameterized Test Selection		
Maurer's Universal Test	4	1%
Non-Overlapping Test	350	2%

4.3.4 Output of Boolean Function (hx) of Grain-128 stream cipher algorithm

The output of Boolean function, (hx) failed for all the 16 NIST statistical tests at 1%–5% significance level, except for Binary Matrix Rank Test for significance level of 1%–5% and Linear Complexity Test for significance level of 1%–5%. Therefore, it can be summarised that the sequences tested for Boolean function, (hx) were not random for significance level of 1%–5%. Table 38 below shows the list of tests that failed.

Table 38: Number of rejected result for output of Boolean Function (hx)

Non-Parameterized Test Selection		
	Number of rejected	**Significance Level**
Frequency Test	100	1%–5%
Runs Test	100	1%–5%
Longest Runs of Ones Test	100	1%–5%
Spectral DFT Test	45	1%
	62	2%
	67	3%
	71	4%
	75	5%
Lempel-Ziv Complexity Test	100	1%–5%
Cumulative Sums - Forward - Reverse	 100 100	 1%–5% 1%–5%
Random Excursion Variant Test	882	1%–5%
Random Excursion Test	392	1%–5%
Parameterized Test Selection		
Block Frequency	100	1%–5%
Non-Overlapping Test	8,342	1%
	8,902	2%
	9,266	3%
	9,503	4%
	9,731	5%
Overlapping Test	100	1%–5%
Maurer's Universal Test	100	1%–5%
Serial Test - P value 1 - P value 2	 100 90 92 94 95 95	 1%–5% 1% 2% 3% 4% 5%
Approximate Entropy Test	100	1%–5%