CHAPTER 7

CRYPTANALYSIS OF LAO-3D LIGHTWEIGHT BLOCK CIPHER

7.1 Introduction

This chapter highlights the cryptanalysis conducted for the evaluation of LAO-3D lightweight block cipher. In order to examine the security characteristics of LAO-3D algorithm, three avalanche effects experiments were carried out including correlation coefficient, bit error, and key sensitivity tests. In addition, randomness analysis was executed to evaluate the randomness characteristics of the cipher output. For verification of the security strength against cryptanalytic attacks, differential cryptanalysis and linear cryptanalysis were executed on LAO-3D. The evaluation methodologies implemented in this research are significant to differentiate the strength of block ciphers.

7.2 Avalanche Effect Tests

Avalanche effect measures and analyses the non-linearity characteristics of a lightweight block cipher. The non-linear transformation can offer confusion property to the algorithm (Dobraunig et al., 2020). This security feature is dependent on each output produced from the cipher input. The correlation coefficient, bit error rate, and key sensitivity tests were conducted to observe the avalanche effect of LAO-3D lightweight block cipher using the source code provided in APPENDIX I. All of the 64 bits plaintexts and 128 bits keys were generated using a pseudo-random bit generator and converted to ciphertext through the encryption process. Avalanche effect, E (Astuti et al., 2019) is defined in equation (6).

$$E = \frac{1}{s}\sum_{i=1}^{s}|c_i - p_i| \quad (6)$$

where s is the length of plaintext/ciphertext while c_i and p_i are the i^{th} bit of ciphertext and plaintext.

7.2.1 Correlation Coefficient Test

Correlation coefficient test aims to analyse the non-linear association between plaintext and ciphertext (Sallam et al., 2017). The correlation coefficient, r_{pc} can distinguish the confusion effect of a lightweight block cipher. The coefficient takes values from +1 to -1 where the accepted ranges of the results are listed in Table 7.1 (Kanjo et al., 2017).

Table 7.1: Correlation Coefficient Test Results Indication

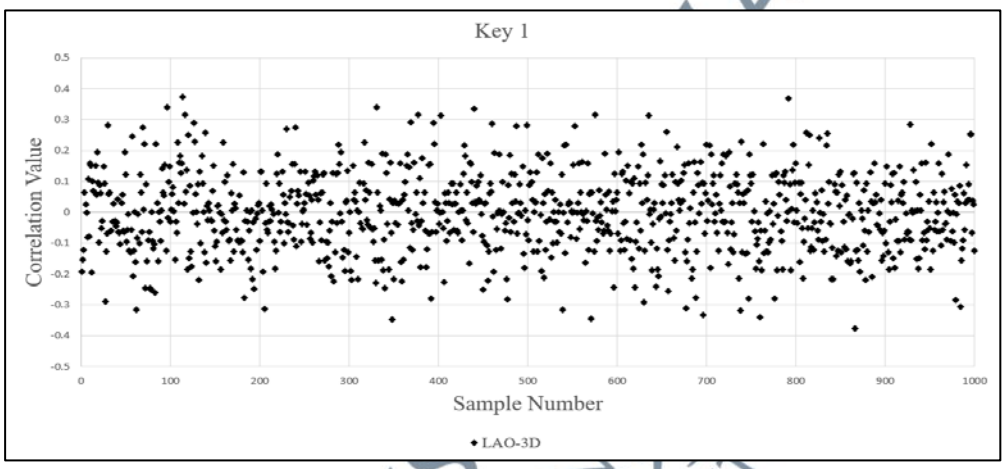
Condition	Result
$r_{pc} = 0$	Non-linear relationship
$0 < r_{pc} \leq 0.3$ or $-0.3 \leq r_{pc} < 0$	Weak positive/negative linear relationship
$0.3 < r_{pc} < 0.7$ or $-0.7 < r_{pc} < -0.3$	Moderate positive/negative linear relationship
$0.7 \leq r_{pc} < 1$ or $-1 < r_{pc} \leq -0.7$	Strong positive/negative linear relationship
$r_{pc} = 1$ or $r_{pc} = -1$	Perfect positive/negative linear relationship

The correlation coefficient is given by equation (7).

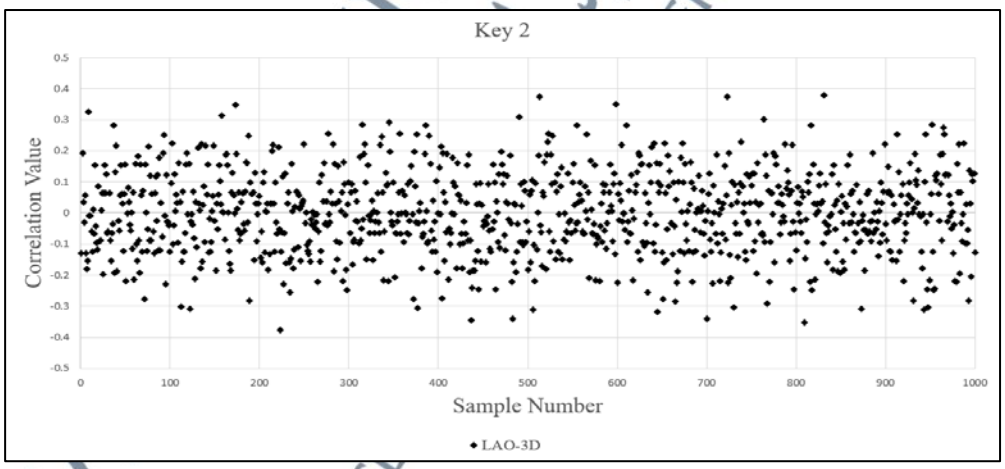
$$r_{pc} = \frac{\sum_{i=1}^{s}(p_i - E)(c_i - E)}{\sqrt{\sum_{i=1}^{s}(p_i - E)^2}\sqrt{\sum_{i=1}^{s}(c_i - E)^2}} \quad (7)$$

where E is the avalanche effect, p_i is the i^{th} plaintext bit, and c_i is the i^{th} ciphertext bit.

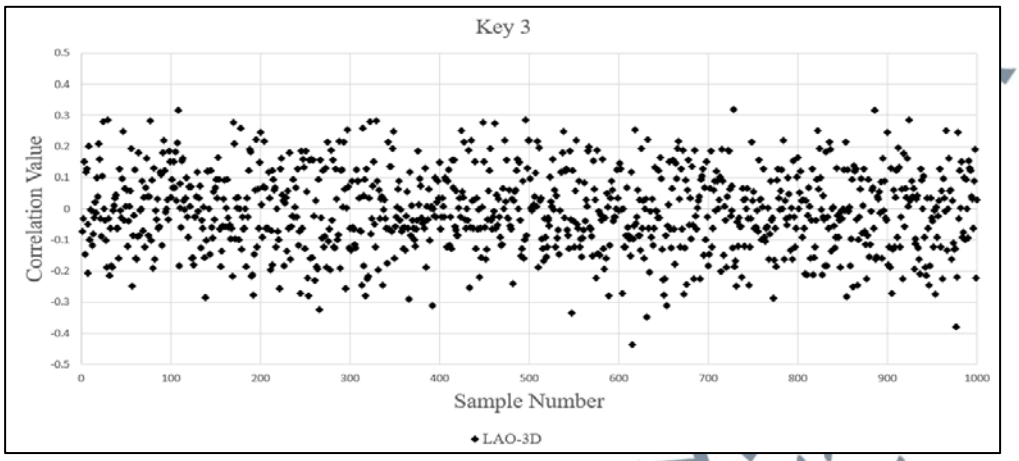
The analysis was carried out in which the correlation values between the plaintext and ciphertext were recorded. Scatter charts of the correlation coefficient results are presented in Figure 7.1 where five random keys and 1,000 random plaintext samples were tested on LAO-3D block cipher. The values in the scatter charts were plotted according to the computed correlation coefficient based on the key and plaintext inputs.



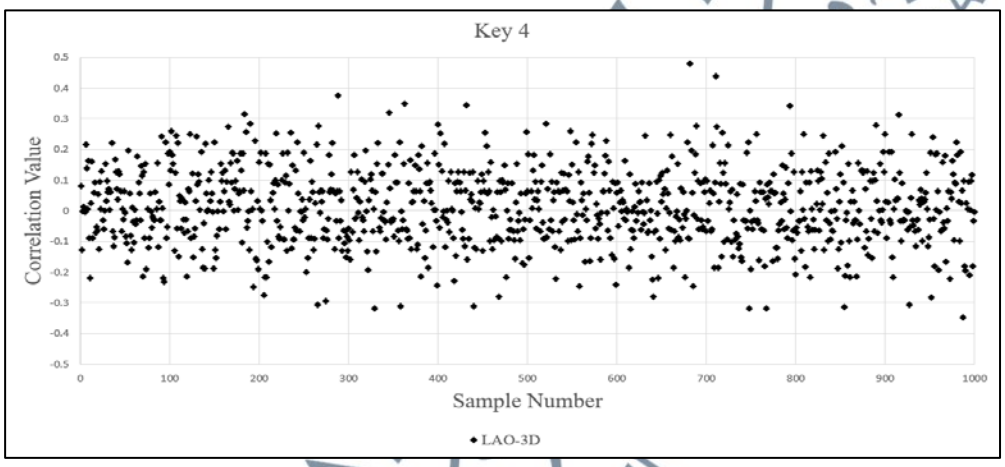
(i) Key 1



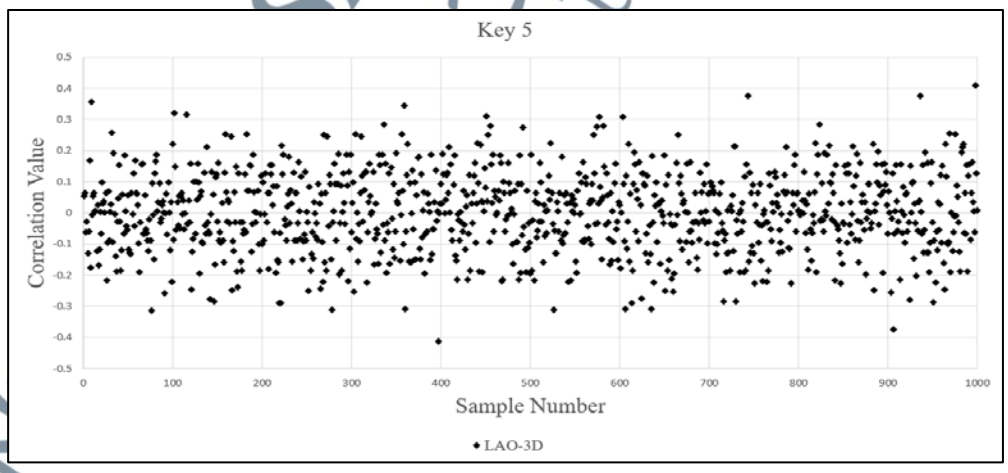
(ii) Key 2



(iii) Key 3



(iv) Key 4



(v) Key 5

Figure 7.1: Scatter Charts of Correlation Coefficient Results

The correlation coefficient results are summarized in Table 7.2. Results produced by all of the five keys indicate that the majority of the correlation coefficients, r_{pc} of LAO-3D are located in the $0 < r_{pc} \leq 0.3$ and $-0.3 \leq r_{pc} < 0$ ranges which indicate a weak linear relationship between the input and output. Overall, LAO-3D recorded 98.20% correlation value between 0 to 0.3 (and -0.3 to 0), and 1.80% between 0.3 to 0.7 (and -0.7 to -0.3).

Table 7.2: Correlation Coefficient Results of LAO-3D

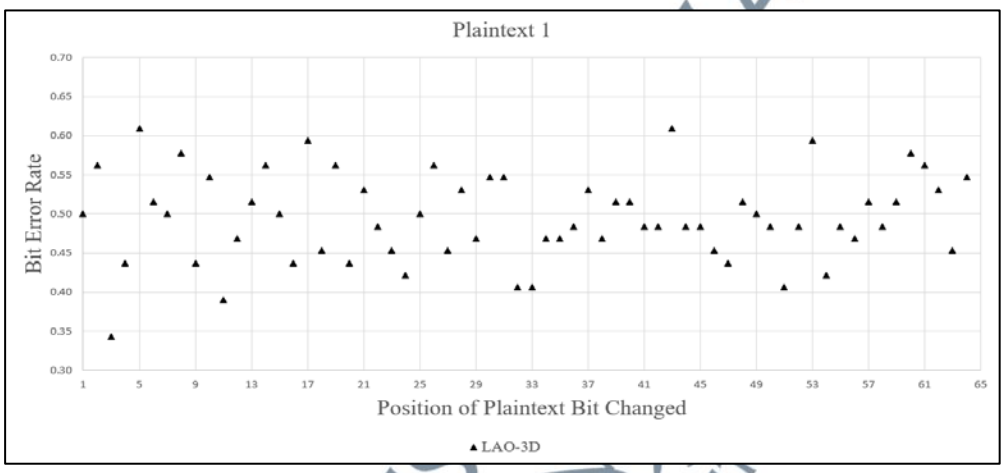
Input	r_{pc} = -1, r_{pc} = 0, and r_{pc} = 1	$0 < r_{pc} \leq 0.3$ and $-0.3 \leq r_{pc} < 0$	$0.3 < r_{pc} < 0.7$ and $-0.7 < r_{pc} < -0.3$	$0.7 \leq r_{pc} < 1$ and $-1 < r_{pc} \leq -0.7$
Key 1	0	979	21	0
Key 2	0	977	23	0
Key 3	0	990	10	0
Key 4	0	982	18	0
Key 5	0	982	18	0

7.2.2 Bit Error Rate Test

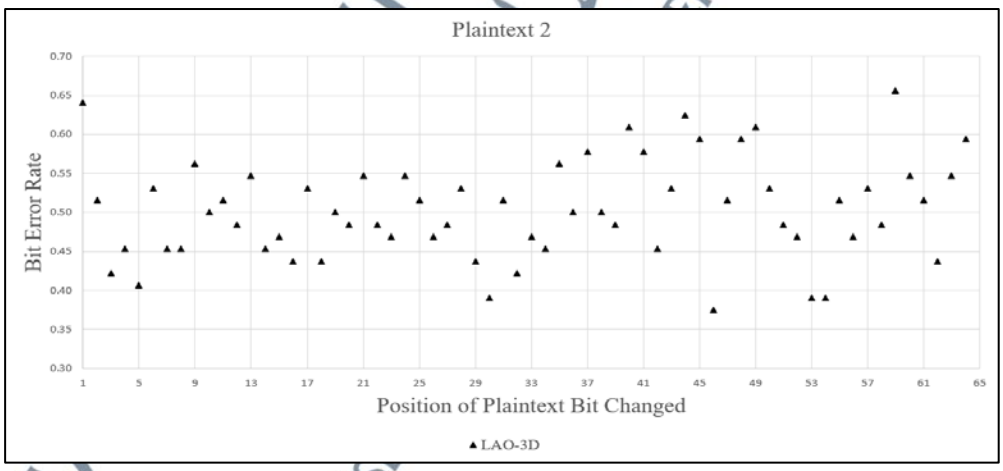
Bit error rate measures the differences of ciphertext caused by a change in its associated plaintext. The number of ciphertext bits changed upon modification of one plaintext bit is called bit error rate. An optimum bit error rate result should be 0.5 or 50.00% modification of the total plaintext bits (Zhu et al., 2015). Bit error rate, *BER* (Salam et al., 2019) defines the total bit differences divided by the cumulative ciphertext bit as shown in equation (8).

$$BER = \frac{\text{Number of ciphertext bit difference}}{\text{Total number of ciphertext bit}} \quad (8)$$

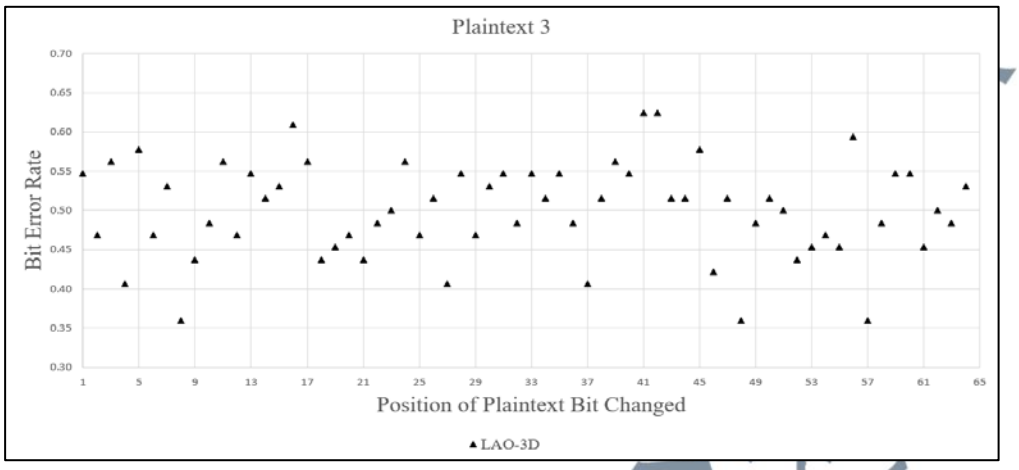
The bit error rate test aims to measure the plaintext and ciphertext relationship. Scatter charts of the bit error rate results are depicted in Figure 7.2 where a random key and five random plaintext samples were tested on LAO-3D block cipher. The data plots in each scatter chart display the bit error values that represent the changes of ciphertext upon plaintext modifications.



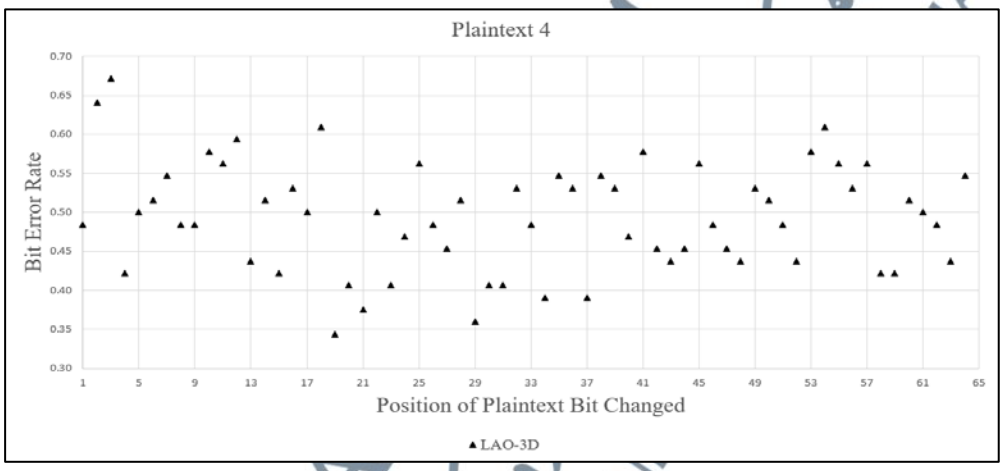
(i) Plaintext 1



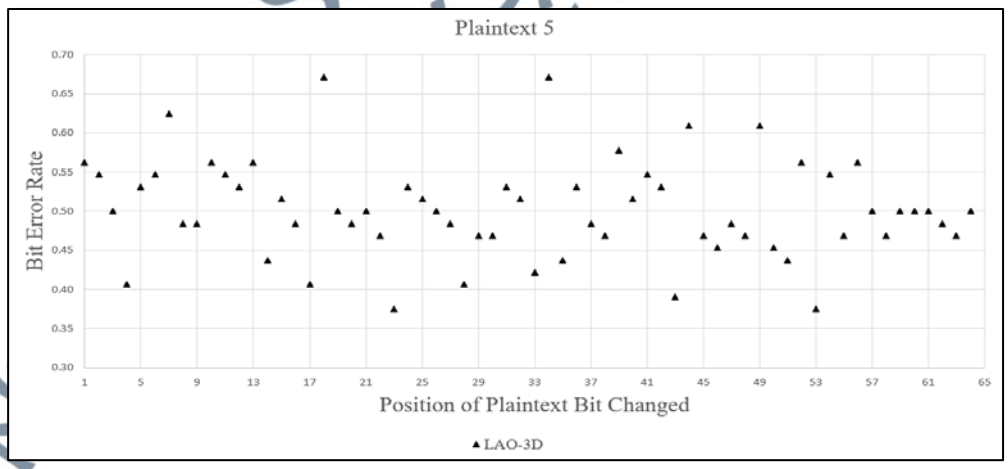
(ii) Plaintext 2



(iii) Plaintext 3



(iv) Plaintext 4



(v) Plaintext 5

Figure 7.2: Scatter Charts of Bit Error Rate Results

The comparison of bit error rate test results shown in Table 7.3 indicates that LAO-3D lightweight block cipher obtained an average of *BER* that is close to 0.5. The results generated by all five plaintexts indicate that LAO-3D algorithm achieved a 50.00% bit error rate which is the optimum test result. Results obtained from this experiment verified that the ciphertext is entirely modified with a single alteration in the plaintext bit of LAO-3D lightweight block cipher.

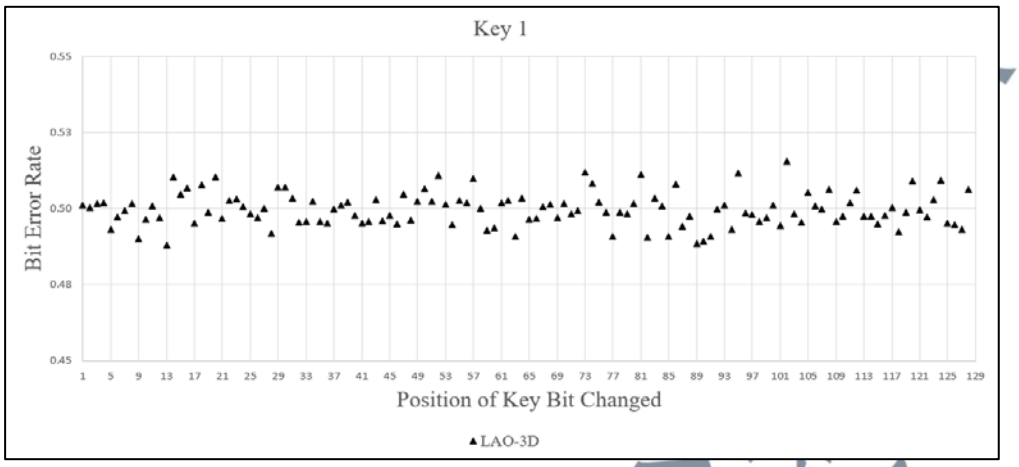
Table 7.3: Bit Error Rate Results of LAO-3D

Input	Average Different Bits	Average Bit Error Rate
Plaintext 1	31.703125	0.495361
Plaintext 2	32.203125	0.503174
Plaintext 3	32.046875	0.500732
Plaintext 4	32.046875	0.500732
Plaintext 5	32.156250	0.502441

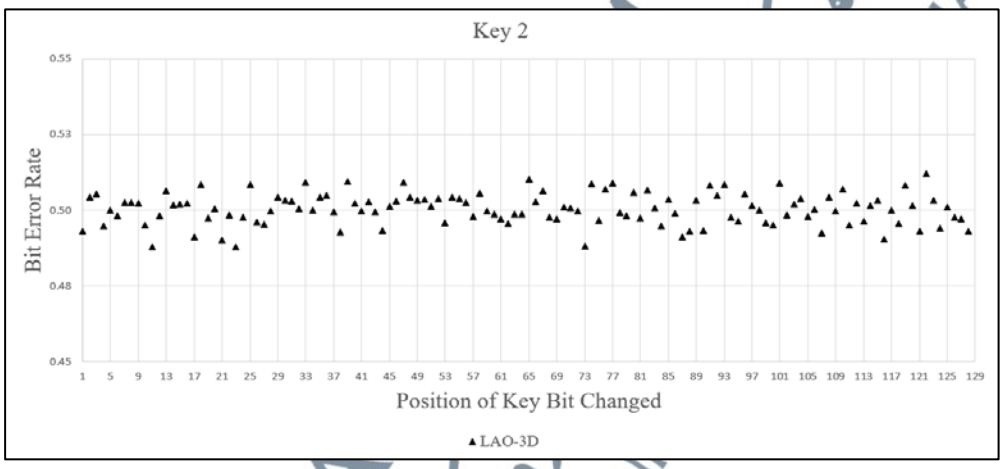
7.2.3 Key Sensitivity Test

Key sensitivity test observes the ciphertext affected by the modification of a secret key (Jallouli et al., 2016). A slight modification to the key would cause significant changes to a ciphertext. In the key sensitivity test, a small modification was made by replacing a single bit of the key from its first bit to the last bit position.

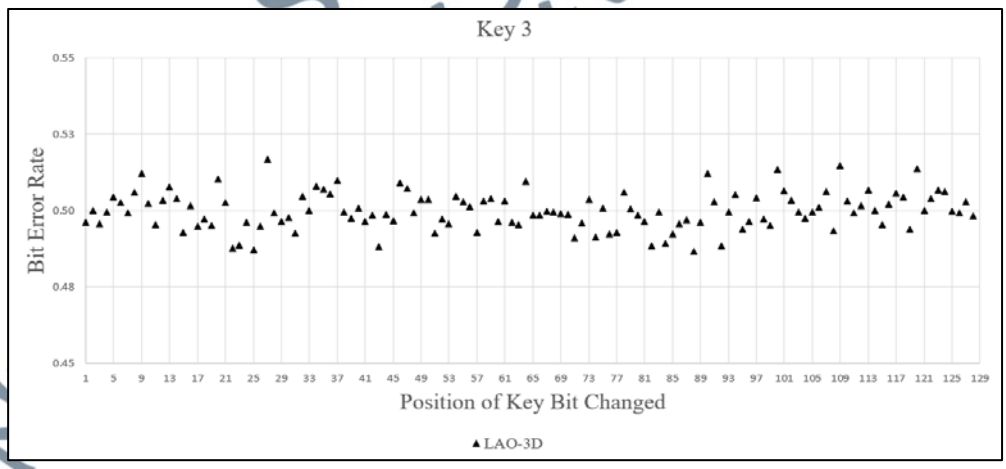
Results of the key sensitivity were calculated using the bit error rate equation. The results for a secure block cipher should be within the range of 0.5 or 50.00% modification of the ciphertext bits. Scatter charts of the key sensitivity test results are displayed in Figure 7.3, where five random keys and a random plaintext sample were tested on the LAO-3D block cipher.



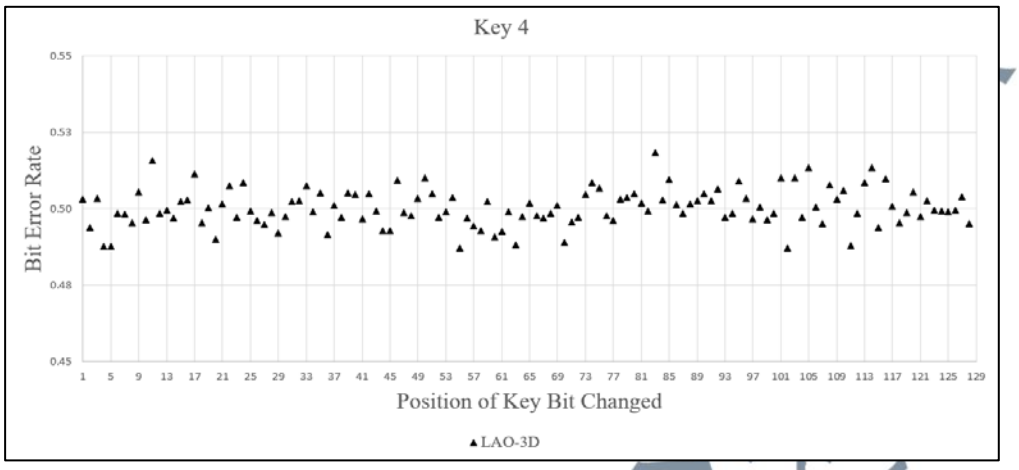
(i) Key 1



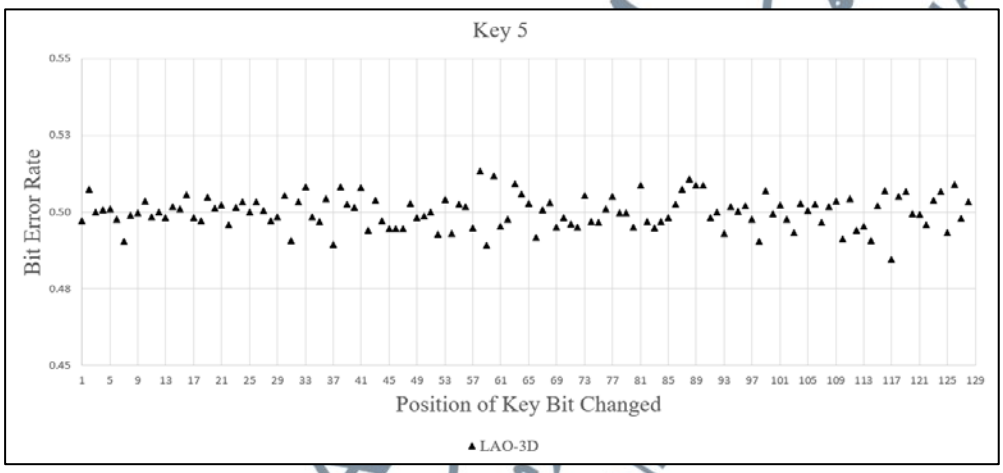
(ii) Key 2



(iii) Key 3



(iv) Key 4



(v) Key 5

Figure 7.3: Scatter Charts of Key Sensitivity Results

The comparison of key sensitivity test results shown in Table 7.4 indicates that LAO-3D recorded 50.00% bit error rate. The results indicate that LAO-3D has a non-linear relationship between the key and ciphertext which also represents a high sensitivity of the key to the ciphertext. The 50.00% key sensitivity result denotes that the entire key bits have an impact on every ciphertext bit of LAO-3D lightweight block cipher.

Table 7.4: Key Sensitivity Results of LAO-3D

Input	Average Different Bits	Average Bit Error Rate
Key 1	32.000122	0.500002
Key 2	32.028317	0.500442
Key 3	32.007694	0.500120
Key 4	31.948364	0.499193
Key 5	32.013795	0.500216

7.3 Randomness Tests

The randomness tests were performed by adopting 15 statistical tests from the NIST Special Publication 800-22 that provides its test application which is called the NIST Statistical Test Suite (Rukhin et al., 2010). The open-source randomness tests application focuses on various non-randomness characteristics of ciphertext produced from LAO-3D lightweight block cipher.

Eight tests including Binary Matrix Rank (1 *p*-value), Frequency (1 *p*-value), Runs (1 *p*-value), Spectral DFT (1 *p*-value), Longest Runs of Ones (1 *p*-value), Cumulative Sums (2 *p*-values), Random Excursion (8 *p*-values), and Random Excursion Variant (18 *p*-values) are categorized as non-parameterized tests which do not require parameter value to be included in the test suite.

The remaining seven tests including Linear Complexity (1 *p*-value), Approximate Entropy (1 *p*-value), Block Frequency (1 *p*-value), Overlapping Templates (1 *p*-value), Maurer's Universal (1 *p*-value), Serial (2 *p*-values), and Non-Overlapping (148 *p*-values) are classified as the parameterized tests that need parameter values to be inserted in the NIST Statistical Test Suite.

A significance level must be defined to evaluate the randomness of the ciphertext (Imdad et al., 2022). The significance level, α should be at the minimum of 0.1% (0.001) but not exceed 1% (0.01). Meanwhile, the number of samples is at least the inverse of the significance level (1 ÷ 0.01 = 100 samples). The ciphertext is considered random if the *p*-value ≥ α. Contrarily, the ciphertext is treated as non-random if the *p*-value < α.

For this experiment, the proportion of the test samples determines the randomness of a cryptographic algorithm as defined in equation (9) (Rukhin et al., 2010).

$$p_\alpha = (1-\alpha) - 3\sqrt{\frac{\alpha(1-\alpha)}{s}} \tag{9}$$

where α is the significance level which equals to 0.001 (and 0.01) with s representing the sample size of 1,000 ciphertexts. If the number of rejections falls beyond the proportion p_α, then the sample is non-random.

For LAO-3D lightweight block cipher, nine data categories were applied to produce the input data using the source code provided in APPENDIX F. Table 7.5 detailed the format of data categories input based on 64-bit plaintext and 128-bit key implemented by LAO-3D. Each data category generated a different set of 1,000 ciphertext samples where the block number obtained from every sample is determined by the size of the key and block (Baker & Nori, 2022). The derived blocks appended the ciphertext to construct large bit sequences for the randomness tests.

Table 7.5: Data Categories Input

Data Category	Key	Plaintext	Derived Blocks	Derived Bits
Strict Key Avalanche (SKA)	123 random 128-bit keys	All zero	15,744	1,007,616
Strict Plaintext Avalanche (SPA)	All zero	245 random 64-bit plaintext	15,680	1,003,520
Plaintext/Ciphertext Correlation (PCC)	One random 128-bit key	15,625 random 64-bit plaintext	15,625	1,000,000
Ciphertext Block Chaining Mode (CBCM)	One random 128-bit key	All zero	15,625	1,000,000
Random Plaintext/ Random Key (RPRK)	One random 128-bit key	15,625 random 64-bit plaintext	15,625	1,000,000
Low-Density Key (LDK)	3,241 specific 128-bit keys	8,257 random 64-bit plaintext	8,257	528,448
High-Density Key (HDK)	3,241 specific 128-bit keys	8,257 random 64-bit plaintext	8,257	528,448
Low-Density Plaintext (LDP)	2,081 specific 128-bit keys	2,081 random 64-bit plaintext	2,081	133,184
High-Density Plaintext (HDP)	2,081 specific 128-bit keys	2,081 random 64-bit plaintext	2,081	133,184

Every data category generated multiple ciphertext lengths based on the input data as described in Table 7.5. For LAO-3D, five data categories including CBC, RPRK, SKA, SPA, and PCC can be evaluated using all 15 statistical tests since they can produce at least 1,000,000 bits of data which automatically fulfil the bits requirements for NIST statistical tests as stated earlier in Table 2.13 from Chapter 2. On the other hand, only 11 tests can be examined for LDK and HDK, while ten tests for LDP and HDP are due to insufficient length of data. Table 7.6 and Table 7.7 display the randomness tests results for $\alpha = 0.1\%$. Meanwhile, Table 7.8 and Table 7.9 present the randomness tests results for $\alpha = 1\%$.

Table 7.6: Randomness Results for α = 0.1% (CBC, PCC, RPRK, SKA, and SPA)

No.	Statistical Test	Data Category				
		CBC	PCC	RPRK	SKA	SPA
		No. of Passed Samples (Range of Acceptance Rejection: [0, 4])				
1	Runs	997/1000	999/1000	999/1000	1000/1000	999/1000
2	Frequency	1000/1000	999/1000	998/1000	997/1000	1000/1000
3	Spectral DFT	999/1000	1000/1000	996/1000	1000/1000	1000/1000
4	Block Frequency	998/1000	999/1000	1000/1000	999/1000	1000/1000
5	Binary Matrix Rank	999/1000	997/1000	1000/1000	1000/1000	999/1000
6	Approximate Entropy	1000/1000	1000/1000	998/1000	997/1000	999/1000
7	Longest Runs of Ones	998/1000	999/1000	1000/1000	1000/1000	997/1000
8	Serial	999/1000	1000/1000	1000/1000	1000/1000	1000/1000
9	Cumulative Sums	1000/1000	999/1000	999/1000	997/1000	1000/1000
10	Non-Overlapping Templates	999/1000	999/1000	999/1000	999/1000	999/1000
11	Maurer's Universal	999/1000	998/1000	998/1000	999/1000	1000/1000
12	Linear Complexity	998/1000	998/1000	999/1000	1000/1000	999/1000
13	Overlapping Templates	999/1000	999/1000	999/1000	1000/1000	999/1000
		No. of Passed Samples (Range of Acceptance Rejection: [0, 3])				
14	Random Excursion	583/584	616/617	595/595	620/622	632/633
15	Random Excursion Variant	583/584	616/617	594/595	621/622	633/633

Table 7.7: Randomness Results for α = 0.1% (LDK, HDK, LDP, and HDP)

No.	Statistical Test	Data Category			
		LDK	HDK	LDP	HDP
		No. of Passed Samples (Range of Acceptance Rejection: [0, 4])			
1	Runs	999/1000	998/1000	1000/1000	1000/1000
2	Frequency	1000/1000	997/1000	999/1000	998/1000
3	Spectral DFT	998/1000	999/1000	997/1000	998/1000
4	Block Frequency	1000/1000	1000/1000	998/1000	1000/1000
5	Binary Matrix Rank	999/1000	998/1000	1000/1000	1000/1000
6	Approximate Entropy	999/1000	999/1000	999/1000	1000/1000
7	Longest Runs of Ones	1000/1000	999/1000	999/1000	999/1000
8	Serial	999/1000	999/1000	999/1000	999/1000
9	Cumulative Sums	1000/1000	997/1000	999/1000	997/1000
10	Non-Overlapping Templates	999/1000	999/1000	999/1000	999/1000
11	Maurer's Universal	1000/1000	999/1000	*	*
12	Linear Complexity	*	*	*	*
13	Overlapping Templates	*	*	*	*
		No. of Passed Samples (Range of Acceptance Rejection: Not Available)			
14	Random Excursion	*	*	*	*
15	Random Excursion Variant	*	*	*	*

* = no test executed due to insufficient data length

Table 7.8: Randomness Results for α = 1% (CBC, PCC, RPRK, SKA, and SPA)

No.	Statistical Test	Data Category				
		CBC	PCC	RPRK	SKA	SPA
		No. of Passed Samples (Range of Acceptance Rejection: [0, 20])				
1	Runs	992/1000	987/1000	990/1000	990/1000	988/1000
2	Frequency	989/1000	992/1000	993/1000	984/1000	989/1000
3	Spectral DFT	991/1000	996/1000	988/1000	990/1000	985/1000
4	Block Frequency	986/1000	986/1000	993/1000	994/1000	996/1000
5	Binary Matrix Rank	987/1000	985/1000	992/1000	995/1000	989/1000
6	Approximate Entropy	994/1000	995/1000	989/1000	988/1000	988/1000
7	Longest Runs of Ones	989/1000	991/1000	994/1000	997/1000	985/1000
8	Serial	992/1000	992/1000	990/1000	991/1000	990/1000
9	Cumulative Sums	991/1000	992/1000	989/1000	989/1000	991/1000
10	Non-Overlapping Templates	990/1000	990/1000	990/1000	990/1000	990/1000
11	Maurer's Universal	992/1000	989/1000	988/1000	983/1000	986/1000
12	Linear Complexity	986/1000	986/1000	992/1000	989/1000	991/1000
13	Overlapping Templates	983/1000	987/1000	992/1000	995/1000	987/1000
		No. of Passed Samples (Range of Acceptance Rejection: [0, 14])				
14	Random Excursion	577/584	609/617	590/595	613/622	627/633
15	Random Excursion Variant	578/584	611/617	590/595	616/622	627/633

Table 7.9: Randomness Results for α = 1% (LDK, HDK, LDP, and HDP)

No.	Statistical Test	Data Category			
		LDK	HDK	LDP	HDP
		No. of Passed Samples (Range of Acceptance Rejection: [0, 20])			
1	Runs	990/1000	986/1000	992/1000	992/1000
2	Frequency	987/1000	988/1000	992/1000	991/1000
3	Spectral DFT	988/1000	984/1000	986/1000	984/1000
4	Block Frequency	994/1000	991/1000	986/1000	990/1000
5	Binary Matrix Rank	990/1000	989/1000	993/1000	990/1000
6	Approximate Entropy	987/1000	992/1000	987/1000	989/1000
7	Longest Runs of Ones	995/1000	989/1000	987/1000	989/1000
8	Serial	992/1000	989/1000	986/1000	991/1000
9	Cumulative Sums	985/1000	987/1000	993/1000	986/1000
10	Non-Overlapping Templates	990/1000	990/1000	990/1000	989/1000
11	Maurer's Universal	989/1000	992/1000	*	*
12	Linear Complexity	*	*	*	*
13	Overlapping Templates	*	*	*	*
		No. of Passed Samples (Range of Acceptance Rejection: Not Available)			
14	Random Excursion	*	*	*	*
15	Random Excursion Variant	*	*	*	*

* = no test executed due to insufficient data length

Findings from the randomness analysis show that LAO-3D lightweight block cipher passed all of the data categories and statistical tests. Comparison of randomness tests results of LAO-3D using two different significance levels is summarized in Table 7.10.

Table 7.10: Comparison of Randomness Results

Significance Level	Results	Data Category	Statistical Test
0.1%	Pass	9	15
	Fail	0	0
1%	Pass	9	15
	Fail	0	0

In addition, the *p*-values produced by the block cipher from the NIST Statistical Test Suite are uniformly distributed since the values are larger than 0.0001 for $\alpha = 0.1\%$ and $\alpha = 1\%$ as shown in Table 7.11 andTable 7.12. The 100% passing rate achieved in the randomness and uniformity test results verified the randomness characteristics of LAO-3D cipher output.

Table 7.11: Uniformity Results (CBC, PCC, RPRK, SKA, and SPA)

No.	Statistical Test	Data Category				
		CBC	PCC	RPRK	SKA	SPA
		***p*-values**				
1	Runs	0.870856	0.691081	0.061260	0.069430	0.402962
2	Frequency	0.336111	0.530120	0.626709	0.641284	0.731886
3	Spectral DFT	0.771469	0.765632	0.651693	0.225998	0.277082
4	Block Frequency	0.092041	0.711601	0.116746	0.552383	0.719747
5	Binary Matrix Rank	0.377007	0.122325	0.682823	0.944274	0.264901
6	Approximate Entropy	0.431754	0.331408	0.881662	0.128874	0.739918
7	Longest Runs of Ones	0.070737	0.302657	0.591409	0.771469	0.334538
8	Serial	0.366038	0.391685	0.089581	0.624739	0.560316
9	Cumulative Sums	0.741256	0.712763	0.082836	0.687575	0.379922
10	Non-Overlapping Templates	0.540168	0.477106	0.538421	0.501121	0.500920
11	Maurer's Universal	0.814724	0.164425	0.245490	0.277082	0.689019
12	Linear Complexity	0.120207	0.471146	0.668321	0.298282	0.463512
13	Overlapping Templates	0.102526	0.199045	0.554420	0.743915	0.228367
14	Random Excursion	0.533205	0.399313	0.592636	0.556975	0.585012
15	Random Excursion Variant	0.474550	0.414868	0.472390	0.577133	0.547103

Table 7.12: Uniformity Results (LDK, HDK, LDP, and HDP)

No.	Statistical Test	Data Category			
		LDK	HDK	LDP	HDP
		p-values			
1	Runs	0.291091	0.177628	0.239266	0.496351
2	Frequency	0.114712	0.566688	0.773405	0.639202
3	Spectral DFT	0.274341	0.914025	0.684890	0.943242
4.	Block Frequency	0.500279	0.769527	0.361938	0.118812
5	Binary Matrix Rank	0.370262	0.711601	0.001953	0.118120
6	Approximate Entropy	0.889118	0.316052	0.072066	0.009535
7	Longest Runs of Ones	0.757790	0.301194	0.749884	0.821937
8	Serial	0.226422	0.576050	0.262395	0.804706
9	Cumulative Sums	0.141130	0.181735	0.660295	0.418857
10	Non-Overlapping Templates	0.503304	0.539874	0.425798	0.418952
11	Maurer's Universal	0.570792	0.471146	*	*
12	Linear Complexity	*	*	*	*
13	Overlapping Templates	*	*	*	*
14	Random Excursion	*	*	*	*
15	Random Excursion Variant	*	*	*	*

* = no test executed due to insufficient data length

Overall, LAO-3D lightweight block cipher managed to pass all of the randomness tests. Combinations of substitution and permutation components in the LAO-3D have optimized the confusion and diffusion properties of the algorithm that contributed to the randomization of the ciphertext.

7.4 Cryptanalysis Attacks

Cryptanalysis attacks investigate the security of the lightweight block cipher against a variety of attacks. This method measures and analyses the combination of confusion and diffusion function implemented in LAO-3D algorithm. In this research, the two most popular cryptanalysis attacks were implemented which include differential cryptanalysis and linear cryptanalysis. The analyses were conducted to ensure that confidentiality is robustly provided by LAO-3D lightweight block cipher.

7.4.1 Differential Cryptanalysis

Differential cryptanalysis (DC) is a chosen plaintext attack that exploits the existence of a linear relationship between the encryption of two plaintexts using the same secret key (Biham & Shamir, 1993). A difference propagation is composed of a set of differential trails, where its probability is the sum of the probabilities of all differential trails that have the specified input difference and output difference (Daemen & Rijmen, 2013).

The tool used to calculate the probability of this attack is the Difference Distribution Table (DDT) for a $m \times n$ S-box as shown in Table 7.13. Let Δ_α and Δ_β denote the input and output differences of an S-box, respectively. The DDT contains 2^m rows that denote all possible input differences Δ_α and 2^n columns that denote all possible output differences Δ_β. An entry in the DDT represents the number of times that an input difference Δ_α causes an output difference Δ_β to occur. This event is denoted by $\Delta_\alpha \xrightarrow{S_{16}^1} \Delta_\beta$ where the probability of the occurrence of this event can be calculated from the DDT as follows:

$$\hat{p} = \frac{\mathrm{DDT}[\Delta_\alpha][\Delta_\beta]}{2^m} \tag{10}$$

Table 7.13: Difference Distribution Table

Input Difference \ Output Difference	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	4	0	0	0	4	0	4	0	0	0	4	0	0
2	0	0	0	2	0	4	2	0	0	0	2	0	2	2	2	0
3	0	2	0	2	2	0	4	2	0	0	2	2	0	0	0	0
4	0	0	0	0	0	4	2	2	0	2	2	0	2	0	2	0
5	0	2	0	0	2	0	0	0	0	2	2	2	4	2	0	0
6	0	0	2	0	0	0	2	0	2	0	0	4	2	0	0	4
7	0	4	2	0	0	0	2	0	2	0	0	0	2	0	0	4
8	0	0	0	2	0	0	0	2	0	2	0	4	0	2	0	4
9	0	0	2	0	4	0	2	0	2	0	0	0	2	0	4	0
A	0	0	2	2	0	4	0	0	2	0	2	0	0	2	2	0
B	0	2	0	0	2	0	0	0	4	2	2	2	0	2	0	0
C	0	0	2	0	0	4	0	2	2	2	2	0	0	0	2	0
D	0	2	4	2	2	0	0	2	0	0	2	2	0	0	0	0
E	0	0	2	2	0	0	2	2	2	2	0	0	2	2	0	0
F	0	4	0	0	4	0	0	0	0	0	0	0	0	0	4	4

To attack an *n*-bit block cipher using differential cryptanalysis, there must be a predictable difference propagation overall but a few rounds with a probability significantly larger than 2^{1-n}. For LAO-3D block cipher to be resistant against differential cryptanalysis, it is a necessary condition that there is no difference propagation with a probability higher than 2^{-63}.

In the distinguishing phase of the attack, an *r*-round differential characteristic was constructed by concatenating *R* 1-round characteristics. The 1-round characteristic was built by approximating the differences for selected S-boxes in the round. Let Δ_p denote the plaintext difference and Δ_x denote the output difference after *R* rounds. If this *R*-round characteristic involves m_d differentially active S-boxes, then the total probability for this *R*-round characteristic is defined as follows:

$$Prob = \prod_{i=1}^{m_d} \hat{p}_i \tag{11}$$

where $\hat{p}_i$ denotes the probability for the i^{th} S-box.

In order to obtain the best *R*-round differential characteristics for LAO-3D block cipher, the following four characteristics were implemented in the differential cryptanalysis using the source code provided in APPENDIX G.

i) Characteristic 1: The highest probability was selected and followed by the lowest number of active S-box.
ii) Characteristic 2: The highest probability was selected and followed by the highest number of active S-box.
iii) Characteristic 3: The lowest number of active S-box was selected and followed by the highest probability.
iv) Characteristic 4: The lowest number of active S-box was selected and followed by the lowest probability.

Table 7.14: Probability of Differential Characteristics

Rounds	Characteristic 1		Characteristic 2		Characteristic 3		Characteristic 4	
	Prob.	S-box	Prob.	S-box	Prob.	S-box	Prob.	S-box
1	2^{-2}	1	2^{-2}	1	2^{-2}	1	2^{-2}	1
2	2^{-6}	3	2^{-8}	4	2^{-8}	3	2^{-8}	3
3	2^{-16}	8	2^{-28}	14	2^{-15}	6	2^{-17}	6
4	2^{-32}	16	2^{-55}	27	2^{-27}	11	2^{-31}	11
5	2^{-52}	26	2^{-85}	42	2^{-44}	17	2^{-56}	20
6	2^{-83}	41	-	-	2^{-64}	25	2^{-90}	32

From Table 7.14, differential Characteristic 3 is the best among others as it achieved the highest probability (2^{-44}) at the highest attackable round (round 5). Moreover, differential Characteristic 3 utilized the smallest number of active S-boxes in every round. Figure 7.4 until Figure 7.9 show the best 6-round differential characteristics of LAO-3D algorithm and are described as follows:

i) Round 1

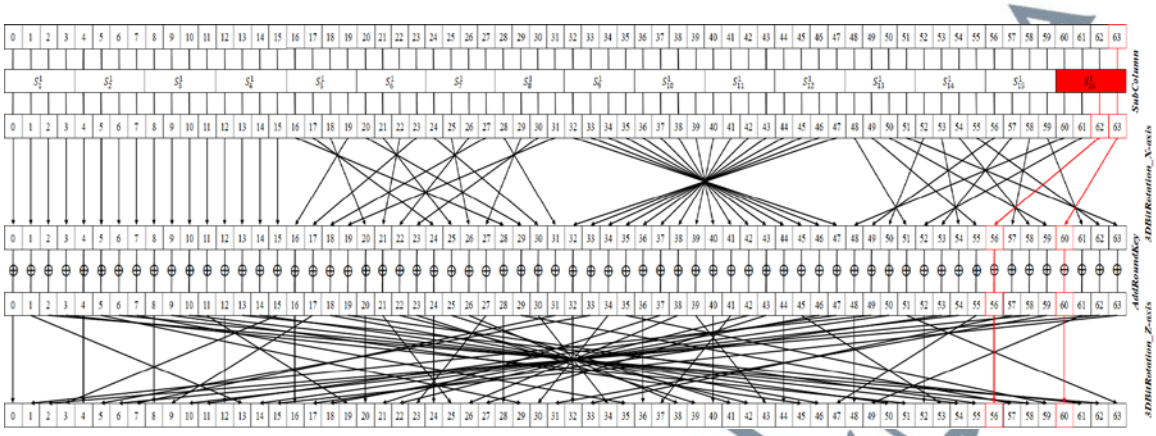


Figure 7.4: 1-Round Differential Characteristic for Round 1 of LAO-3D

$$\hat{p}\left(\Delta 1 \xrightarrow{S_{16}^{1}} \Delta 3\right) = \frac{4}{16} = 2^{-2}$$

$$Prob\ (0000\ 0000\ 0000\ 0001 \xrightarrow{F} 0000\ 0000\ 0000\ 0088) = 2^{-2}$$

$$Prob\ (R_1) = 2^{-2}$$

ii) Round 2

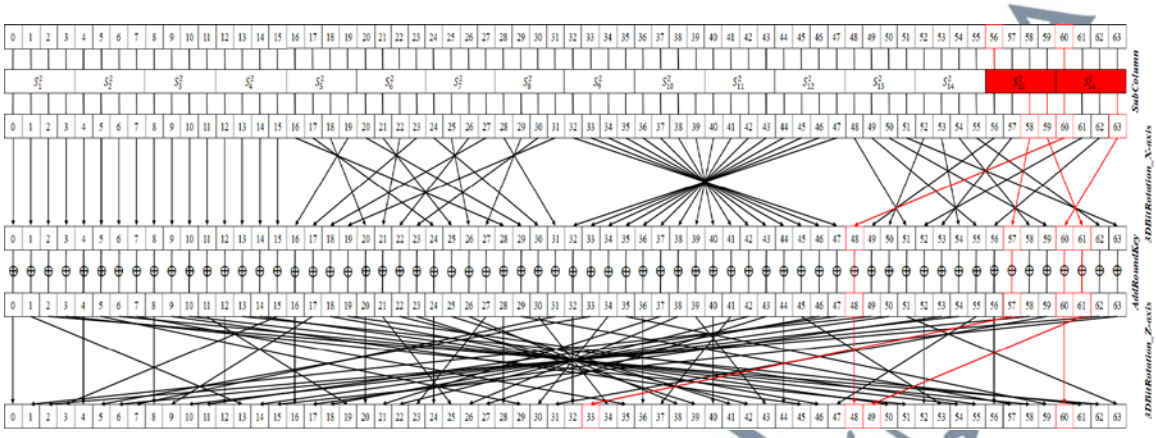


Figure 7.5: 1-Round Differential Characteristic for Round 2 of LAO-3D

$$\hat{p}\left(\Delta 8 \xrightarrow{S_{15}^2} \Delta 3\right) = \frac{2}{16} = 2^{-3} \qquad \hat{p}\left(\Delta 8 \xrightarrow{S_{16}^2} \Delta 9\right) = \frac{2}{16} = 2^{-3}$$

$$Prob\ (0000\ 0000\ 0000\ 0088 \xrightarrow{F} 0000\ 0000\ 4000\ C008) = (2^{-3})^2 = 2^{-6}$$

$$Prob\ (R_1 \rightarrow R_2) = (2^{-2})(2^{-6}) = 2^{-8}$$

iii) Round 3

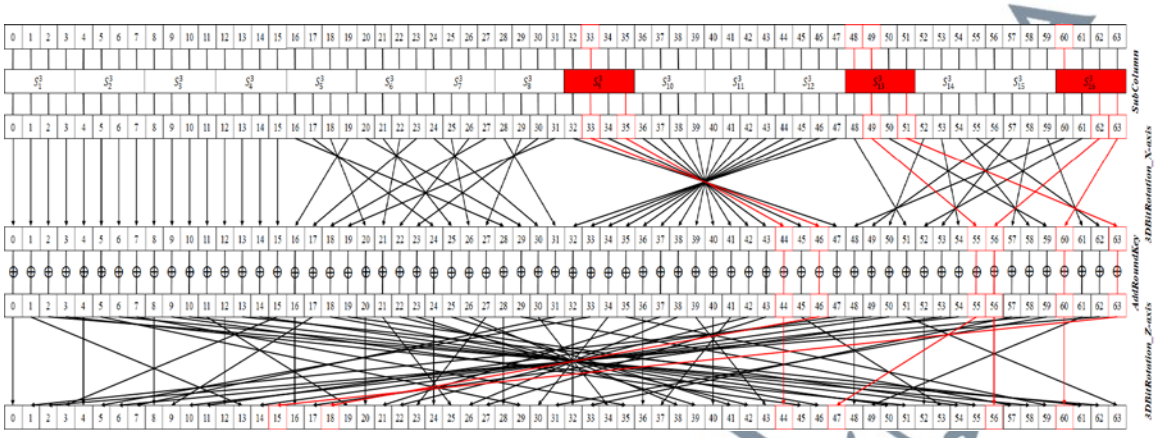


Figure 7.6: 1-Round Differential Characteristic for Round 3 of LAO-3D

$$\hat{p}\left(\Delta 4 \xrightarrow{S_9^3} \Delta 5\right) = \frac{4}{16} = 2^{-2} \qquad \hat{p}\left(\Delta C \xrightarrow{S_{13}^3} \Delta 5\right) = \frac{4}{16} = 2^{-2}$$

$$\hat{p}\left(\Delta 8 \xrightarrow{S_{16}^3} \Delta 3\right) = \frac{2}{16} = 2^{-3}$$

$$Prob\ (0000\ 0000\ 4000\ C008 \xrightarrow{F} 0001\ 2000\ 0009\ 0088) = (2^{-3})(2^{-2})^2 = 2^{-7}$$

$$Prob\ (R_1 \rightarrow R_3) = (2^{-8})(2^{-7}) = 2^{-15}$$

iv) Round 4

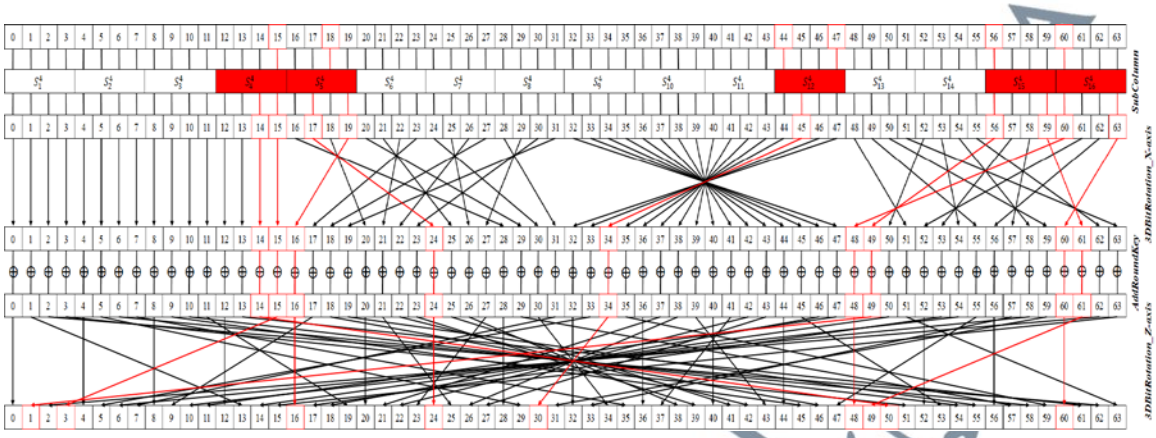


Figure 7.7: 1-Round Differential Characteristic for Round 4 of LAO-3D

$$\hat{p}\left(\Delta 1 \xrightarrow{S_4^4} \Delta 3\right) = \frac{4}{16} = 2^{-2} \qquad \hat{p}\left(\Delta 2 \xrightarrow{S_5^4} \Delta 5\right) = \frac{4}{16} = 2^{-2}$$

$$\hat{p}\left(\Delta 9 \xrightarrow{S_{12}^4} \Delta 4\right) = \frac{4}{16} = 2^{-2} \qquad \hat{p}\left(\Delta 8 \xrightarrow{S_{15}^4} \Delta 9\right) = \frac{2}{16} = 2^{-3}$$

$$\hat{p}\left(\Delta 8 \xrightarrow{S_{16}^4} \Delta 9\right) = \frac{2}{16} = 2^{-3}$$

$$Prob\ (0001\ 2000\ 0009\ 0088 \xrightarrow{F} 5000\ 8082\ 0000\ E008) = (2^{-2})^3(2^{-3})^2 = 2^{-12}$$

$$Prob\ (R_1 \rightarrow R_4) = (2^{-15})(2^{-12}) = 2^{-27}$$

v) Round 5

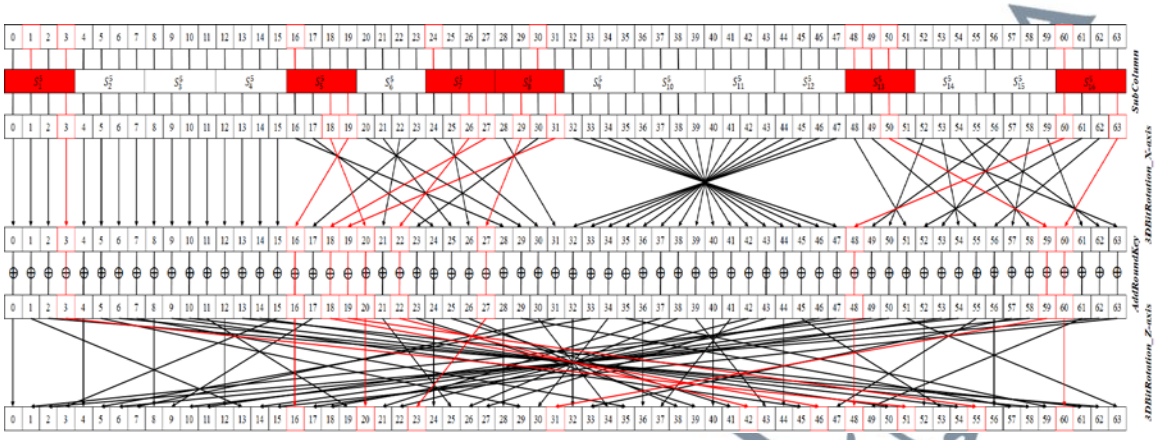


Figure 7.8: 1-Round Differential Characteristic for Round 5 of LAO-3D

$$\hat{p}\left(\Delta 5 \xrightarrow{S_1^5} \Delta 1\right) = \frac{2}{16} = 2^{-3} \qquad \hat{p}\left(\Delta 8 \xrightarrow{S_5^5} \Delta 3\right) = \frac{2}{16} = 2^{-3}$$

$$\hat{p}\left(\Delta 8 \xrightarrow{S_7^5} \Delta 3\right) = \frac{2}{16} = 2^{-3} \qquad \hat{p}\left(\Delta 2 \xrightarrow{S_8^5} \Delta 5\right) = \frac{4}{16} = 2^{-2}$$

$$\hat{p}\left(\Delta \mathrm{E} \xrightarrow{S_{13}^5} \Delta 2\right) = \frac{2}{16} = 2^{-3} \qquad \hat{p}\left(\Delta 8 \xrightarrow{S_{16}^5} \Delta 9\right) = \frac{2}{16} = 2^{-3}$$

$$Prob\ (5000\ 8082\ 0000\ \mathrm{E}008 \xrightarrow{F} 0000\ 8901\ 0022\ 9108\ ) = (2^{-2})(2^{-3})^5 = 2^{-17}$$

$$Prob\ (R_1 \rightarrow R_5) = (2^{-27})(2^{-17}) = 2^{-44}$$

vi) Round 6

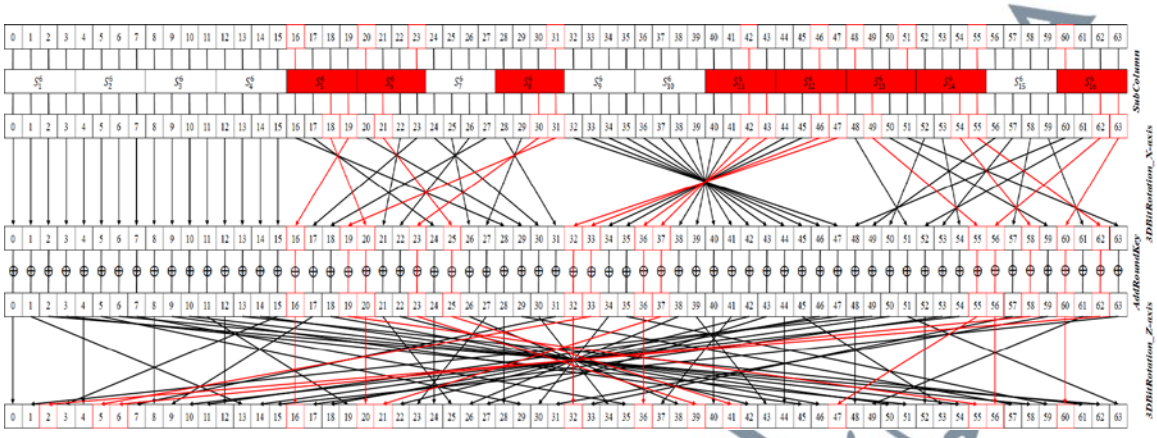


Figure 7.9: 1-Round Differential Characteristic for Round 6 of LAO-3D

$$\hat{p}\left(\Delta 8 \xrightarrow{S_5^6} \Delta 3\right) = \frac{2}{16} = 2^{-3} \qquad \hat{p}\left(\Delta 9 \xrightarrow{S_6^6} \Delta 4\right) = \frac{4}{16} = 2^{-2}$$

$$\hat{p}\left(\Delta 1 \xrightarrow{S_8^6} \Delta 3\right) = \frac{4}{16} = 2^{-2} \qquad \hat{p}\left(\Delta 2 \xrightarrow{S_{11}^6} \Delta 3\right) = \frac{2}{16} = 2^{-3}$$

$$\hat{p}\left(\Delta 2 \xrightarrow{S_{12}^6} \Delta 3\right) = \frac{2}{16} = 2^{-3} \qquad \hat{p}\left(\Delta 9 \xrightarrow{S_{13}^6} \Delta 4\right) = \frac{4}{16} = 2^{-2}$$

$$\hat{p}\left(\Delta 1 \xrightarrow{S_{14}^6} \Delta 3\right) = \frac{4}{16} = 2^{-2} \qquad \hat{p}\left(\Delta 8 \xrightarrow{S_{16}^6} \Delta 3\right) = \frac{2}{16} = 2^{-3}$$

$$Prob\ (0000\ 8901\ 0022\ 9108 \xrightarrow{F} 2600\ 8C00\ 8941\ 0188) = (2^{-2})^4 (2^{-3})^4$$

$$= 2^{-20}$$

$$Prob\ (R_1 \to R_6) = (2^{-44})(2^{-20}) = 2^{-64}$$

The highest probability of difference propagation found at the 6th round is 2^{-64} which is lower than 2^{-63}. Table 7.15 presents the 6-round differential iterative of LAO-3D block cipher that consists of the input, output, active S-box, and probability of the substitution and permutation layers in each round as depicted in Figure 7.4 until Figure 7.9. From these results, it is impossible to construct an effective differential distinguisher with more than five rounds for LAO-3D algorithm.

Table 7.15: 6-round Differential Iterative of LAO-3D

Rounds	Layer	Input	Output	S-box	Prob.
1	Substitution	0000 0000 0000 0001	0000 0000 0000 0003	1	2^{-2}
	Permutation	0000 0000 0000 0003	0000 0000 0000 0088	-	1
2	Substitution	0000 0000 0000 0088	0000 0000 0000 0039	2	2^{-6}
	Permutation	0000 0000 0000 0039	0000 0000 4000 C008	-	1
3	Substitution	0000 0000 4000 C008	0000 0000 5000 5003	3	2^{-7}
	Permutation	0000 0000 5000 5003	0001 2000 0009 0088	-	1
4	Substitution	0001 2000 0009 0088	0003 5000 0004 0099	5	2^{-12}
	Permutation	0003 5000 0004 0099	5000 8082 0000 E008	-	1
5	Substitution	5000 8082 0000 E008	1000 3035 0000 2009	6	2^{-17}
	Permutation	1000 3035 0000 2009	0000 8901 0022 9108	-	1
6	Substitution	0000 8901 0022 9108	0000 3403 0033 4303	8	2^{-20}
	Permutation	0000 3403 0033 4303	2600 8C00 8941 0188	-	1

* indicates no effective trail from the encryption round onwards

Differential cryptanalysis results of LAO-3D algorithm and the number of active S-boxes of the differential cryptanalysis is presented in Table 7.16. The results show that LAO-3D recorded the allowable probabilities of differential trails (2^{-44}) with 17 active S-boxes in the fifth round. Hence, 20-round LAO-3D is enough to resist differential cryptanalysis.

Table 7.16: Active S-Boxes and Probabilities of Differential Trails

Rounds	Active S-Boxes	Probability
1	1	2^{-2}
2	3	2^{-8}
3	6	2^{-15}
4	11	2^{-27}
5	17	2^{-44}
6	*25	$*2^{-64}$

* indicates no effective trail from the encryption round onwards

7.4.2 Linear Cryptanalysis

Linear cryptanalysis (LC) is a known-plaintext attack that exploits the high probability occurrences of linear expressions involving plaintext, ciphertext, and round key bits. A linear propagation is composed of a set of linear trails, where its amplitude is the sum of the correlation contributions of all linear trails that have the specified input and output selection patterns (Daemen & Rijmen, 2013). The correlation contributions of the linear trails are signed and their sign depends on the value of the round keys.

The tool used to show the biases in an $m \times n$ S-box is the Linear Approximation Table (LAT) as shown in Table 7.17. Let λ_α and λ_β denote the input and output masks of an S-box. The LAT contains 2^m rows that denote all possible input masks λ_α and 2^n columns that denote all possible output masks λ_β. An entry in the LAT represents the number of occurrences that an input parity masked by λ_α equals an output parity masked by λ_β, minus half the number of possible inputs. The bias for the corresponding event, denoted $\lambda_\alpha \rightarrow \lambda_\beta$, can be calculated from the LAT (Heys, 2002) as follows:

$$\hat{q} = \frac{\mathrm{LAT}[\lambda_\alpha][\lambda_\beta]}{2^m} \tag{12}$$

Meanwhile, the probability of linear approximation is defined as

$$Prob = \frac{1}{2} + q \tag{13}$$

Table 7.17: Linear Approximation Table

		Output Sum															
		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
Input Sum	**0**	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	-4	0	-4	0	0	0	0	0	-4	0	4
	2	0	0	2	2	-2	-2	0	0	2	-2	0	4	0	4	-2	2
	3	0	0	2	2	2	-2	-4	0	-2	2	-4	0	0	0	-2	-2
	4	0	0	-2	2	-2	-2	0	4	-2	-2	0	-4	0	0	-2	2
	5	0	0	-2	2	-2	2	0	0	2	2	-4	0	4	0	2	2
	6	0	0	0	-4	0	0	-4	0	0	-4	0	0	4	0	0	0
	7	0	0	0	4	4	0	0	0	0	-4	0	0	0	0	4	0
	8	0	0	2	-2	0	0	-2	2	-2	2	0	0	-2	2	4	4
	9	0	4	-2	-2	0	0	2	-2	-2	-2	-4	0	-2	2	0	0
	A	0	0	4	0	2	2	2	-2	0	0	0	-4	2	2	-2	2
	B	0	-4	0	0	-2	-2	2	-2	-4	0	0	0	2	2	2	-2
	C	0	0	0	0	-2	-2	-2	-2	4	0	0	-4	-2	2	2	-2
	D	0	4	4	0	-2	-2	2	2	0	0	0	0	2	-2	2	-2
	E	0	0	2	2	-4	4	-2	-2	-2	-2	0	0	-2	-2	0	0
	F	0	4	-2	2	0	0	-2	-2	-2	2	4	0	2	2	0	0

To attack an *n*-bit block cipher using linear cryptanalysis, there must be a predictable linear propagation overall but a few rounds with an amplitude significantly larger than $2^{-\frac{n}{2}}$ (Jithendra & Kassim, 2020). For LAO-3D block cipher, to be resistant against LC, it is a necessary condition that there is no linear propagation with an amplitude higher than 2^{-32}.

In the distinguishing phase of the attack, an *R*-round linear characteristic was constructed by concatenating *R* 1-round characteristics. The 1-round characteristic was built by approximating the parities for selected S-boxes in the round. If this *R*-round characteristic involves m_l linearly active S-boxes, then the total bias is estimated using the Piling-Up lemma (Matsui, 1993) as follows:

$$q = 2^{m_l - 1} \prod_{i=1}^{m_l} \hat{q}_i \quad (14)$$

where $\hat{q}_i$ denotes the bias for the i^{th} S-box.

To obtain the best linear characteristics for LAO-3D block cipher, the following four characteristics were implemented in the linear cryptanalysis using the source code provided in APPENDIX H.

i) Characteristic 1: The highest absolute probability was selected and followed by the lowest number of active S-box.

ii) Characteristic 2: The highest absolute probability was selected and followed by the highest number of active S-box.

iii) Characteristic 3: The lowest number of active S-box was selected and followed by the highest absolute probability.

iv) Characteristic 4: The lowest number of active S-box was selected and followed by the lowest absolute probability.

Table 7.18: Correlation Potentials of Linear Characteristics

Rounds	Characteristic 1			Characteristic 2			Characteristic 3			Characteristic 4		
	Corr.	S-box	Prob.	Corr.	S-box	Prob.	Corr.	S-box	Prob.	Corr.	S-box	Prob.
1	2^{-2}	1	0.250	2^{-2}	1	0.750	2^{-2}	1	0.250	2^{-2}	1	0.250
2	2^{-6}	3	0.437	2^{-10}	5	0.515	2^{-8}	3	0.484	2^{-8}	3	0.484
3	2^{-18}	9	0.499	2^{-34}	17	0.499	2^{-14}	5	0.499	2^{-14}	5	0.500
4	2^{-42}	21	0.500	2^{-64}	32	0.500	2^{-20}	7	0.500	2^{-20}	7	0.500
5	-	-	-	-	-	-	2^{-26}	9	0.500	2^{-26}	7	0.500
6	-	-	-	-	-	-	2^{-32}	11	0.500	2^{-32}	11	0.500
7	-	-	-	-	-	-	2^{-38}	13	0.500	2^{-38}	13	0.500

From Table 7.18, linear Characteristic 3 is the best among others as it achieved the highest probability (2^{-32}) at the highest attackable round (round 6). Moreover, differential Characteristic 3 utilized the smallest number of active S-boxes in every round. Figure 7.10 until Figure 7.16 show the best 7-round linear characteristics of LAO-3D algorithm and are described as follows:

i) Round 1

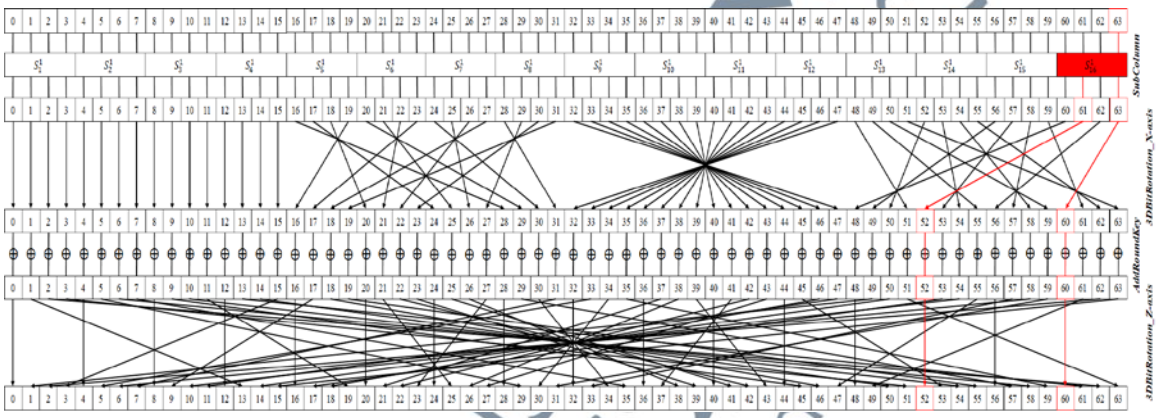


Figure 7.10: 1-Round Linear Characteristic for Round 1 of LAO-3D

$$\hat{q}\left(\Delta 1 \overset{S_{16}^{1}}{\rightarrow} \Delta 5\right) = -\frac{4}{16} = -2^{-2}$$

$$\hat{q}\,(0000\ 0000\ 0000\ 0001 \overset{F}{\rightarrow} 0000\ 0000\ 0000\ 0808) = -2^{-2}$$

$$q = 2^{0}(-2^{-2}) = -2^{-2}$$

$$Prob\,(R_1) = \frac{1}{2} - 2^{-2} = 0.25$$

Correlation Potentials $(R_1) = 2^{-2}$

ii) Round 2

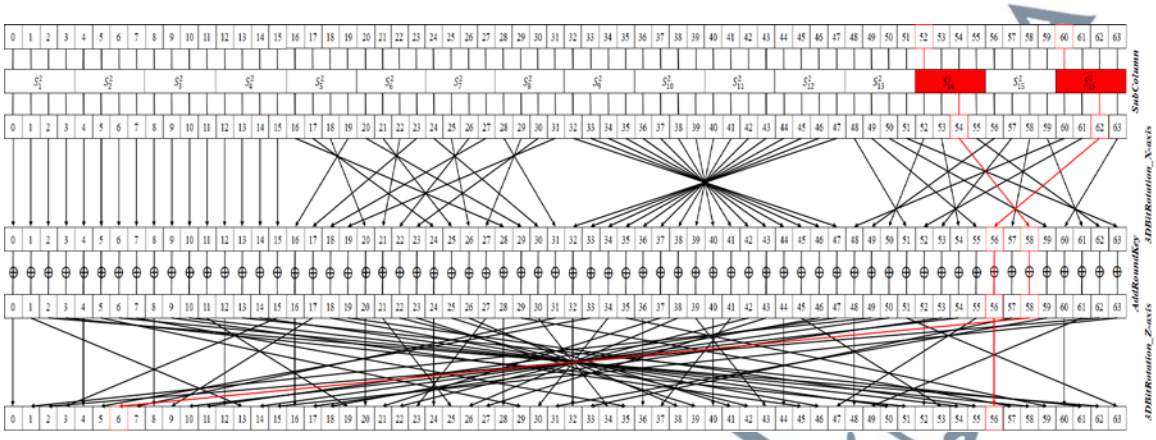


Figure 7.11: 1-Round Linear Characteristic for Round 2 of LAO-3D

$$\hat{q}\left(\Delta 8 \xrightarrow{S_{14}^2} \Delta 2\right) = \frac{2}{16} = 2^{-3} \qquad \hat{q}\left(\Delta 8 \xrightarrow{S_{16}^2} \Delta 2\right) = \frac{2}{16} = 2^{-3}$$

$$\hat{q}\,(0000\ 0000\ 0000\ 0808 \xrightarrow{F} 0200\ 0000\ 0000\ 0080) = (2^{-3})^2 = 2^{-6}$$

$$q = 2^2(-2^{-2})(2^{-6}) = -2^{-6}$$

$$Prob\ (R_1 \rightarrow R_2) = \frac{1}{2} - 2^{-6} = 0.484375$$

Correlation Potentials $(R_1 \rightarrow R_2) = (2^{-2})(2^{-6}) = 2^{-8}$

iii) Round 3

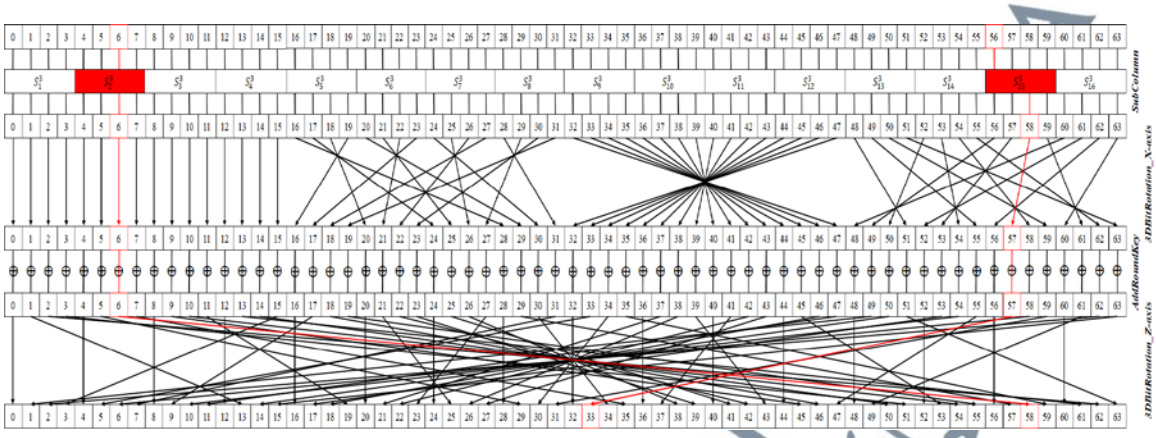


Figure 7.12: 1-Round Linear Characteristic for Round 3 of LAO-3D

$$\hat{q}\left(\Delta 2 \xrightarrow{S_2^3} \Delta 2\right) = \frac{2}{16} = 2^{-3} \qquad \hat{q}\left(\Delta 8 \xrightarrow{S_{15}^3} \Delta 2\right) = \frac{2}{16} = 2^{-3}$$

$$\hat{q}\,(0200\ 0000\ 0000\ 0080 \xrightarrow{F} 0000\ 0000\ 4000\ 0020) = (2^{-3})^2 = 2^{-6}$$

$$q = 2^4(-2^{-2})(2^{-6})(2^{-6}) = -2^{-10}$$

$$Prob\ (R_1 \rightarrow R_3) = \frac{1}{2} - 2^{-10} = 0.499023$$

Correlation Potentials $(R_1 \rightarrow R_3) = (2^{-8})(2^{-6}) = 2^{-14}$

iv) Round 4

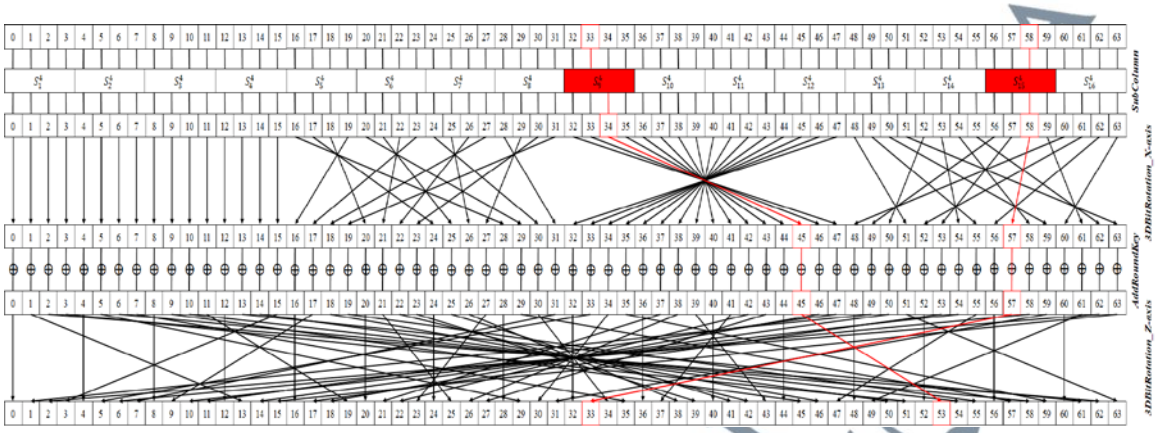


Figure 7.13: 1-Round Linear Characteristic for Round 4 of LAO-3D

$$\hat{q}\left(\Delta 4 \xrightarrow{S_9^4} \Delta 2\right) = -\frac{2}{16} = -2^{-3} \qquad \hat{q}\left(\Delta 2 \xrightarrow{S_{15}^4} \Delta 2\right) = \frac{2}{16} = 2^{-3}$$

$$\hat{q}\,(0000\ 0000\ 4000\ 0020 \xrightarrow{F} 0000\ 0000\ 4000\ 0400) = (-2^{-3})(2^{-3}) = -2^{-6}$$

$$q = 2^{6}(-2^{-2})(2^{-6})(2^{-6})(-2^{-6}) = 2^{-14}$$

$$Prob\ (R_1 \rightarrow R_4) = \frac{1}{2} + 2^{-14} = 0.500061$$

Correlation Potentials $(R_1 \rightarrow R_4) = (2^{-14})(2^{-6}) = 2^{-20}$

v) Round 5

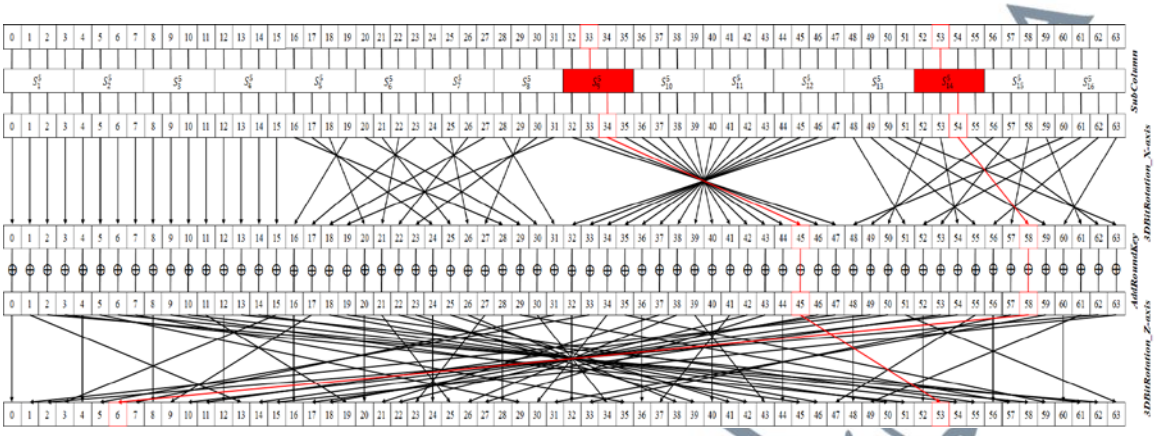


Figure 7.14: 1-Round Linear Characteristic for Round 5 of LAO-3D

$$\hat{q}\left(\Delta 4 \xrightarrow{S_9^5} \Delta 2\right) = \frac{2}{16} = 2^{-3} \qquad \hat{q}\left(\Delta 4 \xrightarrow{S_{14}^5} \Delta 2\right) = \frac{2}{16} = 2^{-3}$$

$$\hat{q}\,(0000\ 0000\ 4000\ 0400 \xrightarrow{F} 0200\ 0000\ 0000\ 0400) = (2^{-3})^2 = 2^{-6}$$

$$q = 2^8(-2^{-2})(2^{-6})(2^{-6})(-2^{-6})(2^{-6}) = 2^{-18}$$

$$Prob\ (R_1 \rightarrow R_5) = \frac{1}{2} + (2^{-18}) = 0.500004$$

Correlation Potentials $(R_1 \rightarrow R_5) = (2^{-20})(2^{-6}) = 2^{-26}$

vi) Round 6

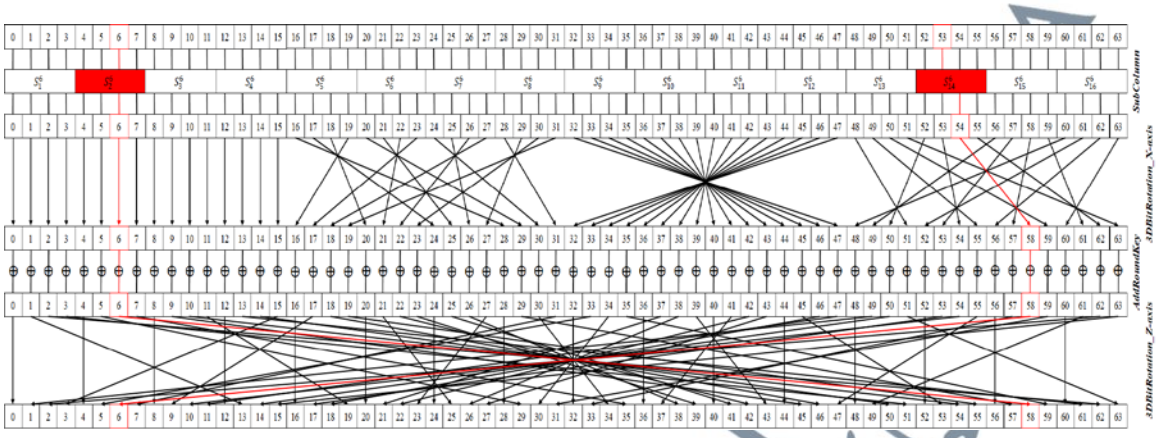


Figure 7.15: 1-Round Linear Characteristic for Round 6 of LAO-3D

$$\hat{q}\left(\Delta 2 \xrightarrow{S_2^6} \Delta 2\right) = \frac{2}{16} = 2^{-3} \qquad \hat{q}\left(\Delta 4 \xrightarrow{S_{14}^6} \Delta 2\right) = -\frac{2}{16} = -2^{-3}$$

$$\hat{q}\,(0200\ 0000\ 0000\ 0400 \xrightarrow{F} 0200\ 0000\ 0000\ 0020) = (-2^{-3})(2^{-3}) = -2^{-6}$$

$$q = 2^{10}(-2^{-2})(2^{-6})(2^{-6})(-2^{-6})(2^{-6})(-2^{-6}) = -2^{-22}$$

$$Prob\ (R_1 \rightarrow R_6) = \frac{1}{2} - 2^{-22} = 0.5$$

Correlation Potentials $(R_1 \rightarrow R_6) = (2^{-26})(2^{-6}) = 2^{-32}$

vii) Round 7

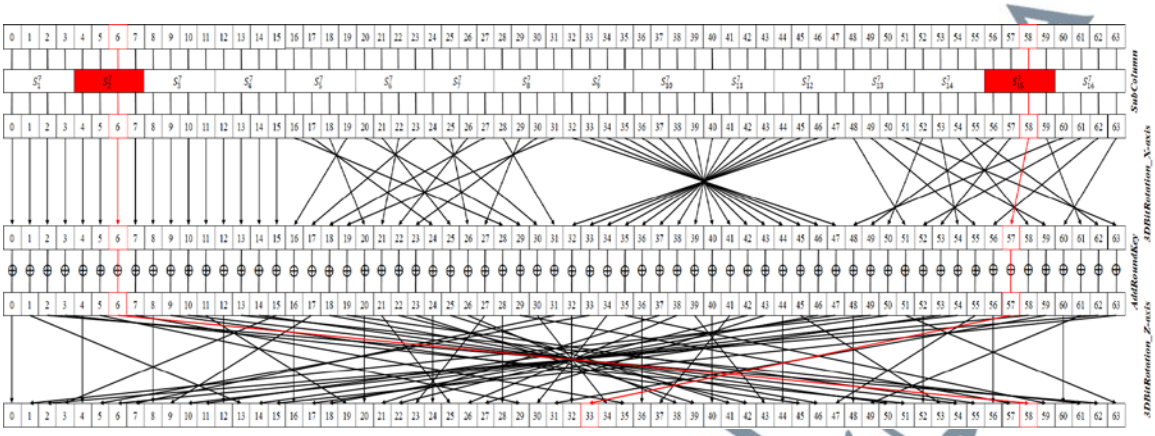


Figure 7.16: 1-Round Linear Characteristic for Round 7 of LAO-3D

$$\hat{q}\left(\Delta 2 \xrightarrow{S_2^7} \Delta 2\right) = \frac{2}{16} = 2^{-3} \qquad \hat{q}\left(\Delta 2 \xrightarrow{S_{15}^7} \Delta 2\right) = \frac{2}{16} = 2^{-3}$$

$$\hat{q}\,(0200\ 0000\ 0000\ 0020 \xrightarrow{F} 0000\ 0000\ 4000\ 0020) = (2^{-3})^2 = 2^{-6}$$

$$q = 2^{12}(-2^{-2})(2^{-6})(2^{-6})(-2^{-6})(2^{-6})(-2^{-6})(2^{-6}) = -2^{-26}$$

$$Prob\ (R_1 \rightarrow R_7) = \frac{1}{2} - 2^{-26} = 0.5$$

Correlation Potentials $(R_1 \rightarrow R_7) = (2^{-32})(2^{-6}) = 2^{-38}$

From the above results, the highest probability of linear propagation at the 7th round is 2^{-38} which is lower than 2^{-32}. Table 7.19 presents the 7-round linear iterative of LAO-3D block cipher that consists of the input, output, active S-box, and probability of the substitution and permutation layers in each round as depicted in Figure 7.10 until Figure 7.16. It can be seen that the clustering of linear trails of LAO-3D is limited, which cannot be used to construct an effective linear propagation with more than six rounds.

Table 7.19: 7-round Linear Iterative of LAO-3D

Rounds	Layer	Input	Output	S-box	Bias
1	Substitution	0000 0000 0000 0001	0000 0000 0000 0005	1	2^{-2}
	Permutation	0000 0000 0000 0005	0000 0000 0000 0808	-	1
2	Substitution	0000 0000 0000 0808	0000 0000 0000 0202	2	2^{-6}
	Permutation	0000 0000 0000 0202	0200 0000 0000 0080	-	1
3	Substitution	0200 0000 0000 0080	0200 0000 0000 0020	2	2^{-6}
	Permutation	0200 0000 0000 0020	0000 0000 4000 0020	-	1
4	Substitution	0000 0000 4000 0020	0000 0000 2000 0020	2	2^{-6}
	Permutation	0000 0000 2000 0020	0000 0000 4000 0400	-	1
5	Substitution	0000 0000 4000 0400	0000 0000 2000 0200	2	2^{-6}
	Permutation	0000 0000 2000 0200	0200 0000 0000 0400	-	1
6	Substitution	0200 0000 0000 0400	0200 0000 0000 0200	2	2^{-6}
	Permutation	0200 0000 0000 0200	0200 0000 0000 0020	-	1
7	Substitution	0200 0000 0000 0020	0200 0000 0000 0020	2	2^{-6}
	Permutation	0200 0000 0000 0020	0000 0000 4000 0020	-	1

The results of the linear cryptanalysis of LAO-3D algorithm and the number of active S-boxes of the linear cryptanalysis are presented in Table 7.20. The results show that LAO-3D achieved the allowable correlation potentials of linear trails (2^{-32}) at the sixth round with 11 active S-boxes. Hence, 20-round LAO-3D is enough to resist linear cryptanalysis.

Table 7.20: Active S-Boxes and Correlation Potentials of Linear Trails

Rounds	Active S-Boxes	Correlation Potential
1	1	2^{-2}
2	3	2^{-8}
3	5	2^{-14}
4	7	2^{-20}
5	9	2^{-26}
6	11	2^{-32}
7	*13	$*2^{-38}$

* indicates no effective trail from the encryption round onwards

7.5 Discussion

This section highlights the results and discusses the findings from the cryptanalysis of LAO-3D lightweight block cipher. As presented in the earlier sections, six cryptanalysis tests were conducted that include correlation coefficient test, bit error rate test, key sensitivity test, randomness tests, differential cryptanalysis, and linear cryptanalysis as shown in Table 7.21.

Table 7.21: A Summary of Cryptanalysis Results

Test	Result	Finding
Correlation Coefficient	Achieved 98.2% weak linear relationship	LAO-3D has high non-linearity characteristics
Bit Error Rate	Achieved 50% average avalanche effect	LAO-3D has high non-linearity characteristics
Key Sensitivity	Achieved 50% average avalanche effect	LAO-3D has high non-linearity characteristics
Randomness	Achieved 100% passing rate	LAO-3D has high randomization characteristics
Differential Cryptanalysis	Achieved the highest probability of difference propagation at the 6th rounds	LAO-3D is resistant to differential attack
Linear Cryptanalysis	Achieved the highest probability of linear propagation at the 7th rounds	LAO-3D is resistant to linear attack

Avalanche effect contains three types of tests that include the correlation coefficient, bit error rate, and key sensitivity. The avalanche effect tests are able to analyse the non-linearity characteristics of an algorithm. Non-linearity characteristics can be obtained from the substitution (*SubColumn*) function in LAO-3D algorithm. In the correlation coefficient test, LAO-3D achieved a 98.20% correlation coefficient value that falls in the range of weak linear relationship between the input and output. For the bit error rate test, LAO-3D recorded the optimum result with 50% average avalanche effect. Similar to the key sensitivity test, LAO-3D achieved the optimum result of 50% average avalanche effect.

Random ciphertext can be generated by a combination of effective substitution and permutation components in a cryptographic algorithm. In LAO-3D, the *SubColumn* and *Double3DRotation* were able to optimize the confusion and diffusion properties of the lightweight block cipher that contributed to the randomization of the produced ciphertext. Randomness tests conducted in this research included two different significance levels, 0.1% and 1%. The purpose of executing two experiments was to observe the impact of changing the parameter values on the randomness of the lightweight block cipher. The results showed that LAO-3D passed all of the randomness tests for both significance levels.

Cryptanalytic attacks implemented in this research are differential and linear cryptanalysis which are the common technique used to evaluate the security strength of a cryptographic algorithm. In differential cryptanalysis, LAO-3D achieved the highest probability of difference propagation at round six. Meanwhile, the algorithm recorded the highest probability of linear propagation at round seven. Similar to the randomness tests, the differential and linear cryptanalysis results of LAO-3D were influenced by the substitution and permutation components implemented in the algorithm. A combination of

the *SubColumn* and *Double3DRotation* function was able to obtain the highest number of active S-boxes in a lesser number of rounds to reduce the probability of attacks.

LAO-3D was developed based on the enhancements made to the RECTANGLE block cipher with the introductions of a strengthened key schedule algorithm and improved confusion and diffusion properties in the encryption algorithm. These enhancements have contributed to the cryptanalysis results which eventually enhanced the security of lightweight block cipher. Therefore, it is concluded that LAO-3D lightweight block cipher is a secure algorithm that can be implemented in security products such as mobile encryption applications.

7.6 Chapter Summary

Cryptanalysis was conducted in this chapter which is divided into avalanche effect, randomness tests, and cryptanalytic attacks. Firstly, LAO-3D recorded 98.20% correlation coefficient result shows a weak linear relationship between the plaintext and ciphertext, 50% result obtained from the bit error rate indicates that the ciphertext is completely changed whenever one plaintext bit is modified, and 50% result achieved in the key sensitivity test suggests that each bit of the ciphertext depends on the entire key bits.

Secondly, the 100% passing rate obtained in the randomness tests denotes the randomness characteristics of the ciphertext produced from LAO-3D algorithm. The results indicate that LAO-3D lightweight block cipher able to behave as a pseudorandom bit generator.

Thirdly, the maximum number of rounds that can be attacked using differential and linear cryptanalysis on LAO-3D are five and six rounds correspondingly. Overall, the experimental results concluded that LAO-3D block cipher has enhanced the confusion and diffusion properties thus increasing security.

In the following Chapter 8, the cryptanalysis results of LAO-3D are compared with the RECTANGLE block cipher. Apart from that, the cryptanalysis results of LAO-3D are also compared with other existing block ciphers to observe the security and performance of the proposed lightweight block cipher.