CHAPTER 5

TESTING AND RESULTS

5.1 Introduction

This chapter discusses the testing techniques used to verify the cryptographic properties of the block cipher are discussed. The testing results are then presented and a summarized.

5.2 Testing

In this section, the implementations of the tests for the cryptographic properties of the proposed cipher are described. Testing is very important to verify that the proposed cipher fulfils the design goal. The design strategy separates the round transformation of the proposed block cipher into components which has their own functionalities and properties. Testing was performed on these properties and an evaluation was made based on the testing results.

5.2.1 Testing Differential Characteristics

Hypothesis: The S-Boxes of the proposed block cipher have good differential characteristics. An attacker can use the differential characteristic of an S-Box to launch differential cryptanalysis. To test the differential characteristics of the S-Boxes, a difference distribution table was generated for each S-Box. Let us denote X' as the difference between a pair of inputs and Y' as the output difference. The difference distribution table contains the distribution of the pairs of (X', Y') of all the possible inputs X. The differential characteristic of the S-Box can be determined by the maximum entry of the difference distribution table.

To generate a difference distribution table, each entry of the difference distribution table is initialised to the empty set. Then the following steps are executed.

```
For each X1 in $\{0, 1\}^n$
    For each X2 in $\{0, 1\}^n$
        $X' = X1 \oplus X2$
        $Y' = S(X1) \oplus S(X2)$
        $T[X', Y'] = T[X', Y'] + 1$
    End for
End for
```

Using the notation of Matsui [37], we define

$$DP_{max}(\gamma) = \max_{a \neq 0, b} \; \underset{X}{P_r}[\gamma(X \oplus X') \oplus \gamma(X) = Y']$$

$DP_{max}(\gamma)$ can be obtained by dividing the maximum differential table entry by the total possible entries in the table. A low value for $DP_{max}(\gamma)$ implies that the S-Box has good differential characteristics.

5.2.2 Testing Cyclic Properties

Hypothesis: The S-Boxes of the proposed block cipher have no fixed point and inverse fixed point. There are two cyclic properties to be determined for an S-Box, i.e. the number of fixed points, the number of opposite fixed points and the number of cycles. The number of fixed points and opposite fixed points can be determined by counting the X in $\{0, 1\}^n$ for which S(X) = X and S(X) = X', where X' is the bitwise complement of X.

5.2.3 Testing Nonlinearity

Hypothesis: The S-Boxes of the proposed block cipher has high nonlinearity. All operations in block cipher are linear except the S-Boxes. The linear relations between input bits and output bits of the S-Boxes can be derived by choosing a subset of the input bits and a subset of the output bits, calculating the parity of these bits for each of the possible inputs of the S box, and counting the number of inputs whose subset's parity is zero. If the S box is linear in the bits of the subset, all the inputs must have a zero parity of the subset. If the S box is affine in the bits of the subset, all the inputs must have parity 1. A subset will have many inputs with parity 0 and many inputs with parity 1. As the number of zeroes is closer to the number of ones, the subset is more nonlinear. The least linear subset under this definition is one that has the same number of inputs with parity zero and parity 1.

For the testing of nonlinearity, a linear approximation table was derived. Assume X is an input of an S-Box and Y is the output of the S-Box: $Y = \gamma(X)$. X' and Y' represent subsets of the bits of X and Y. Let XX' be the scalar product of the vectors X and X' and similarly for YY'. Let's look at the distribution of the parity XX'

$\oplus$ *YY'* for all the possible values *X*, *Y* given fixed choices of *X'*, *Y'*. For any given value of X', Y', the linear approximation table of an S-Box counts, half of the difference between the number of values X, Y for which XX' $\oplus$ YY' = 0, and those with XX' $\oplus$ YY' = 1. The entries with value 0 mean that the parities are balanced. In other word, the S-Box with more zero entries has higher nonlinearity. The steps to generate linear approximation table for an S-Box are summarized as follows:

```
For each X in $\{0, 1\}^n$
    For each X' in $\{0, 1\}^n$
        P = $XX' \oplus YY'$
        If P = 0
            $L[X', Y'] = L[X', Y'] + 0.5$
        Else
            $L[X', Y'] = L[X', Y'] - 0.5$
        End If
    End For
End For
```

Another way to measure nonlinearity of an S-Box is the probability of an entry in the linear approximation table. The probability of an entry in the linear approximation table is defined as the fraction of inputs *X* whose parity $XX' \oplus YY' = 0$.

Lets denote

$l_{X'Y'}$: the value of entry X', Y' in the linear approximation table

N_{odd} : number of entries with odd parity.

For an n x n S-Box,

$N_{even} = 2lX'Y' + 2^n - N_{even}$

$N_{even} = (2lX'Y' + 2^n)/2 = lX'Y' + 2^n\text{-}1$

$\Pr[(XX' \oplus YY') = 0] = N_{even}/2^n = l_{X'Y'}/2^n + ½$

Using the notation of Matsui [37], we define

$$LP_{max}(\gamma) = \max_{a,b\neq 0} \; (2 \underset{X}{\Pr}[X{\cdot}X' = \gamma(X){\cdot}Y'] - 1)^2$$

$$LP_{max}(\gamma) = \max_{X',Y'\neq 0} \; (2 \underset{X}{\Pr}[X{\cdot}X' \oplus YY' = 0]\text{-}1)^2 = \max_{X',Y'} \; (l_{X'Y'}/2^{n-1})^2$$

This means that $LP_{max}(\gamma)$ is the value of the maximum entries in the linear approximation table divided by half the number of possible inputs in the table.

5.2.4 Involution

Hypothesis: The proposed cipher is self-inverse. One of the characteristics of the proposed cipher is involution. Testing was performed by using a plaintext as input to obtain the ciphertext. The involution property was verified by reversing the process, i.e. took the ciphertext as input to obtain the output. If the output data match the plaintext, the cipher is self-reverse. The process was repeated for different plaintexts.

5.2.5 Avalanche Criterion and Completeness

Hypothesis: The proposed cipher satisfies good avalanche criterion and completeness property. To test the avalanche effect of the proposed cipher, some testing data were used as inputs. Then the data for one input was changed and the changes on the output were observed. This step is repeated for every other input. The cipher satisfies good avalanche criterion if any change in one input affects every output.

The same testing can also be applied to prove completeness. A cipher is said to be complete if every output is a function of all inputs. For a cipher which satisfies the avalanche criterion, any change in one input causes changes in all outputs. Since the cipher is self-inverse, any change in output is caused by changes in all inputs. Therefore, a self-inverse cipher that satisfies the avalanche criterion implies completeness.

5.3 Test Results

In the previous section, several testing methods for the important cryptographic properties were carried out. Those tests were performed on the two S-Boxes used in the proposed block cipher. We denote these S-Boxes as S0 and S1. The results of the tests are given in the following sections.

5.3.1 Differential Characteristics

Table 5.1 Maximum Differential Distribution Table Entry and DP_{max}

S-Box	Max Differential Distribution Table Entry	DP_{max}
S0	4	0.015625
S1	4	0.015625

Table 5.1 gives the testing results for the differential characteristics of the S-Boxes used in the proposed cipher based on the differential distribution tables for S0 and S1. The results show that both S-Boxes have good differential characteristics. Both S-Boxes have the same value for maximum differential distribution table entry of 4, which is a low value. The entries with value 4 means that for an input difference of X', the possibility that the corresponding output value is Y' is 0.015625. Differential cryptanalysis uses entries with large values, and in particular the 0 → 0 entry. The results supports the hypothesis made.

5.3.2 Cyclic Properties

Table 5.2 Cyclic Properties

S-Box	Number of Fixed Points	Number of Opposite Fixed Points
S0	0	0
S1	0	0

The test results shows that both S-Boxes have no fixed points and opposite fixed points. Thus, the results support the hypothesis made.

5.3.3 Nonlinearity

Table 5.3 Nonlinearity

S-Box	**LP_{max}**
S0	0.15625
S1	0.15625

Table 5.3 gives the testing results for nonlinearity of S-Boxes used in the proposed cipher. The results are based on the linear approximation tables for S0 and S1. The results show that both S0 and S1 has the same value for LP_{max}, i.e. 0.15625. This shows that both S-Boxes has high nonlinearity. Hence, the results supports the hypothesis made.

5.3.4 Involution

Test was performed by using a plaintext as input to obtain the ciphertext. The involution property was verified by reversing the process, i.e. took the ciphertext as input to obtain the output. The results show that the cipher satisfies the involution criteria since all outputs can be encrypted back into the input using the same key. Hence, the results supports the hypothesis made. Some of the results are shown below:

The key used for encryption and decryption is

01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 af ae ad ac ab aa a9 a8 a7 a6 a5 a4 a3 a2 a1 a0

Some test results:

```
Input   : 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f

Output : cc db 0e 58 20 91 79 c2 63 ff c1 a2 2f f7 cb 67


Input   : cc db 0e 58 20 91 79 c2 63 ff c1 a2 2f f7 cb 67

Output : 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f


Input   : 00 10 20 30 40 50 60 70 80 90 a0 b0 c0 d0 e0 f0

Output : 98 93 54 04 23 0c 8c f4 ca bc 89 72 52 6b 2e ea


Input   : 98 93 54 04 23 0c 8c f4 ca bc 89 72 52 6b 2e ea

Output : 00 10 20 30 40 50 60 70 80 90 a0 b0 c0 d0 e0 f0


Input   : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff

Output : 15 43 15 1b ae 9b 8c 5b 18 3e 6c 6e bd bb bd 37


Input   : 15 43 15 1b ae 9b 8c 5b 18 3e 6c 6e bd bb bd 37

Output : 00 11 22 33 44 55 66 77 88 99 aa bb cc dd ee ff
```

Input : 01 12 23 34 45 56 67 78 89 9a ab bc cd de ef f0

Output : 69 94 a5 ca 0d a9 84 42 66 48 c5 98 82 5b b6 12

Input : 69 94 a5 ca 0d a9 84 42 66 48 c5 98 82 5b b6 12

Output : 01 12 23 34 45 56 67 78 89 9a ab bc cd de ef f0

5.3.5 Avalanche Criterion and Completeness

Table 5.4 Avalanche Criterion and Completeness

	Min	**Standard Deviation**
Changes of output bits by change in one input plaintext bit	63.625	3.5860
Changes of output bits by change in one input key bit	64.25	5.2619

To test the avalanche effect of the proposed cipher, one input bit of the plaintext was changed and the changes on the output were observed. This step is repeated for every other input byte of the plaintext. Testing was performed over all 16 bytes of the plaintext. Then, the same test was repeated by changing one input bit of the cipher key. The average number of output bits changes for one input plaintext bit changes = 63.625 with a standard deviation of 3.5860 while the average number of output bits changes for one key bit change = 64.25 with a standard deviation of 5.2619.

The cipher satisfies good avalanche criterion if change in one input bit causes every output bit to change at a probability of one half. This means that half of the total output bits change. The results show that the cipher satisfies good avalanche criterion since the average number of output bits that change due to a one-bit change in either the plaintext or key approaches the ideal result of 64 bits. This implies that the cipher satisfies the completeness property. Thus, the result supports the hypothesis made.

5.4 Summary of Test Results

The test results for the standard cryptographic properties of the S-Box suggest that the S-Boxes used in the proposed cipher has good cryptographic properties. Fist of all, the differential characteristics test shows that the S-Boxes have the desired differential characteristics. The low value of the maximum differential distribution table entry and the low value for DP_{max} gives evidence that the S-Boxes used for the proposed cipher satisfied the design criterion (v) which specifies that the cipher should be resistant to differential cryptanalysis. Test results for cyclic properties shows that both S-Boxes have no fixed points nor opposite fixed points. This satisfies design criterion (iii). The results indicate that the S-Boxes possess good cryptographic properties since there is a strong correlation between cryptographic properties and the number of fixed points and opposite fixed points. For nonlinearity, the test results show that the S-Boxes has low LP_{max} value. An observation on the linear approximation table indicates that many entries have value 0, which implies high nonlinearity. This clearly proves that the S-Boxes satisfies design criterion (i).

The testing on the properties of the linear mixer proved that the linear mixer has highly desirable properties that satisfy the design criteria. The first test has proven that the linear mixer is self-inverse, which satisfies design criterion (iii) for linear transformation layer. This same testing implies that the linear mixer is injective, which satisfies design criterion (iv). For avalanche criterion, test results show that the linear mixer produce good avalanche effect. A small change in input causes changes in all outputs. This satisfies design criterion (v). The same testing implies design criterion (ii), i.e. completeness. Since the linear mixer is self-reverse, as proven in the first testing, the same result shows that the mixer has the completeness property, where each output is a function of every input. All these properties contribute to the overall diffusive level of the linear mixer. Hence, we can conclude that the linear mixer has uniform and good diffusion property, which satisfies design criterion (i).