CHAPTER VI

CONCLUSION & RECOMMENDATION

6.1 Overview

This chapter summarises the study based on the objectives of this research and provides recommendation or future work that can be carried out for further research.

6.2 Conclusion

Based on the experiment conducted in this research, it can be concluded that the objectives of this research have been achieved, which are as follows:

1. The randomness of Grain-128 has been evaluated using NIST Statistical Test Suite. With the reference of NIST statistical test results obtained, it can be concluded that the Grain-128 stream cipher algorithm was not random for 1%–5% significance level.
2. The MG-128 stream cipher algorithm has been constructed based on the NIST statistical test results obtained from Grain-128 stream cipher algorithm. The NIST statistical test has also been evaluated against MG-128 to determine whether the new algorithm was random or not random. Using the same methodology for Grain-128, the NIST statistical test

results showed that the MG-128 was random for 1%–5% significance level.

3. The NIST Statistical Test Suite results for both Grain-128 and MG-128 have been compared. The results obtained showed that the MG-128 stream cipher algorithm was better compared to Grain-128 stream cipher algorithm because the results obtained showed that the MG-128 was random for 1%–5% significance level. Therefore, the objective of this research to modify the original Grain-128 algorithm into new algorithm that is random for 1%–5% significance level has been achieved.
4. Generally, this research project has successfully achieved its objectives.

6.3 Future Work / Recommendation

There are a few recommendations to improve the MG-128 stream cipher algorithm:

1. Conduct cryptanalysis attacks to the MG-128 stream cipher algorithm to test the strength of this algorithm.
2. Conduct more samples on the keystream. The number of samples suggested is 10% of the all possible population of the bit key used. For example, in MG-128, the number of possible keys is 2^{128}, which is equal to 3.4×10^{38} because the bit key used is 128 bits. If the number of possible keys to be performed is 10% out of 2^{128}, the total number of samples to be conducted is 3.4×10^{37}.
3. Conduct NIST Statistical Test Suite against the three main building block components consisting of Linear Feedback Shift Register, Non-Linear Feedback Shift Register, and Boolean Function.