CHAPTER I

INTRODUCTION

Nowadays, random number generator and pseudorandom number generator are needed for many purposes such as for cryptographic, modelling, and simulation applications. For example, in cryptographic field, all cryptosystems use keys and other cryptographic algorithm parameters must be generated in random pattern. Therefore, it is necessary for an algorithm to be random, but it is not sufficient for the algorithm to be considered as a strong algorithm.

One of the techniques to verify the randomness of the algorithm is by using statistical analysis. Statistical analysis is used to determine the randomness of the output sequence produced by the algorithms to be tested (Soto & Bassham, 2000). There are quite a number of statistical analysis tests available to evaluate the output sequence to verify whether the output sequence is random or not random, including National Institute of Standards and Technology (NIST) statistical test suite, Diehard suite of statistical test,

and Crypt-XS, as stated by Juan Soto in his article titled "Statistical Testing of Random Number Generator" published in 1999 (Soto, 1999).

Grain-128 is one of the stream cipher algorithms. It was introduced in 2006 by Hell, Johansson, Maximov, and Meier. The algorithm supports 128-bit key and 96-bit initial value (IV). There are 3 main building blocks in Grain-128, which are Linear Feedback Shift Register (LFSR), Non-Linear Feedback Shift Register (NLFSR), and an output of Boolean function (Hell et al., 2006). There were several cryptanalysis attacks performed on Grain-128 between 2008 and 2011, such as linear approximation (Hell et al., 2006; 2008), algebraic attack (Hell et al., 2006; 2008; Afzal & Masood, 2008; Berbain et al., 2009), time-memory-data trade off attack (Hell et al., 2006; 2008), fault attack (Hell et al., 2006; 2008; Berzati et al., 2009; Karmakar & Roy Chandhury, 2011), distinguishing attack (Maximov, 2006; Knellwolf et al., 2010), key-recovery attack (Maximov, 2006), chosen-IV attack (Hell et al., 2008), slide attack (De Cannière et al., 2008), differential attack (De Cannière et al., 2008), related-key chosen attack (Lee et al., 2008), correlation attack (Berbain et al., 2009), self-sliding attack (Zhang & Wang, 2009), cube attack (Dinur et al., 2011), and dynamic cube attack (Dinur & Shamir, 2011).

1.1 Background of Problem

Stream cipher algorithm is still a choice to be used either in software or hardware, because the stream cipher algorithm can be designed to allow faster keystream generation in software and it can also be designed to be smaller in hardware. Therefore, the stream cipher can be interesting in the aspect of being faster in software or smaller in hardware (Hell et al., 2006).

One of the important criteria in evaluating a stream cipher algorithm is the suitability of the algorithm to act as a random number generator (Federal Register, 18 December 2011). Hence, statistical analysis using randomness test can determine whether the stream cipher to be tested satisfies this requirement (Rukhin et al., 2010).

Grain-128 is one of the stream cipher algorithms that is very well suited for hardware and it aims environments with limited resources such as in gate count, power consumption, and chip area (Hell et al., 2006; 2008). According to Hell et al. (2006), there is no other 128-bit cipher offering the same security as Grain-128 stream cipher algorithm. However, several attacks had been applied against Grain-128, between 2006 and 2011 and the results showed that this algorithm still has weaknesses.

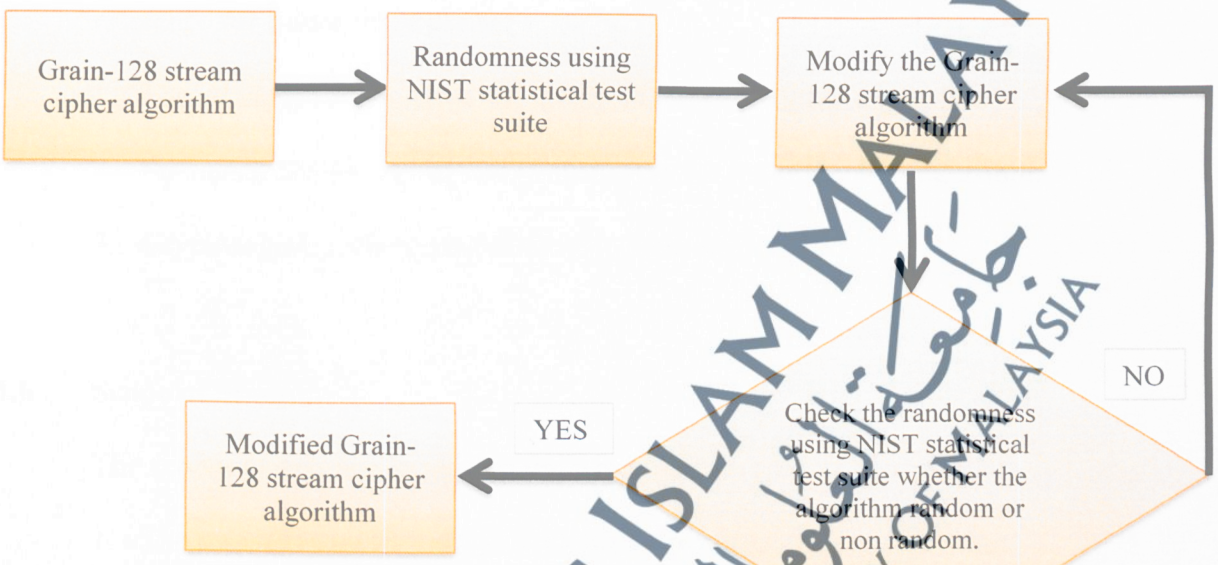
1.2 Problem Statement

The most important property of stream cipher algorithm is the resistance against different attacks. Based on the previous works done in the area of cryptology, it showed that Grain-128 stream cipher algorithm is not considered secure. There is a number of cryptanalysis attacks performed on this algorithm. Thus, it is important to develop algorithm that provide acceptable security level when subjected to attacks and mathematical analysis. Therefore, research on modification of Grain-128 stream cipher algorithm was done in this study.

1.3 Conceptual Framework

The conceptual framework of this research is illustrated in Figure 1 below.

Figure 1: The conceptual framework



1.4 Objective of Research

The objectives of conducting this research are as follows:

1. To identify the randomness of Grain-128 stream cipher algorithm.
2. To modify the algorithm, which was later named Modified Grain-128 (MG-128) stream cipher algorithm.
3. To conduct the randomness test on Modified Grain-128 stream cipher algorithm.

1.5 Significance of Study

In completion of this research, the enhancement of Grain-128 stream cipher algorithm is expected. This study may become a reference for future analysis of the encryption algorithm. Besides that, this study may become a reference for future research on:

1. The strength and weakness of Grain-128 stream cipher algorithm.
2. Statistical analysis using randomness test for stream cipher algorithm.
3. Cryptanalysis techniques for stream cipher algorithm.

1.6 Scope of Study

The scopes of this research are as follows:

1. The research mainly focused on Grain-128 stream cipher algorithm.
2. The randomness of the Grain-128 and Modified Grain-128 stream cipher algorithms was evaluated using NIST statistical test suite.
3. The significance levels used to determine the randomness of the algorithms were 1%-5%.
4. This research used 100 samples for both Grain-128 and Modified Grain-128 stream cipher algorithms due to infeasible system and time constraint.

1.7 Outline of Thesis

This thesis is divided into six chapters, including the current chapter which contains an introduction of the project performed. The rest of this thesis is outlined as follows.

Chapter 2 presents the literature review that was done at the earlier stage of the research. It consists of stream cipher design, Grain-128 stream cipher algorithm, randomness testing using statistical test, and NIST statistical test suite.

Chapter 3 explains the research methodology used in this research. The aims of conducting this research were to analyse the Grain-128 stream cipher algorithm and to produce a new Grain-128 stream cipher algorithm known as Modified Grain-128 (MG-128) stream cipher algorithm. The subtopics covered in this chapter are research design, population and sample, research tools, and experimental setup.

Chapter 4 presents the analysis results for Grain-128 stream cipher algorithm that was obtained from conducting the experiment and observation. It consists of experimental setup for Grain-128, results and analysis, and conclusion from the results obtained.

Chapter 5 presents the analysis results for Modified Grain-128 (MG-128) stream cipher algorithm. It consists of modification of Grain-128, experimental setup for Modified Grain-128 (MG-128), results and analysis, comparison between Grain-128 and Modified Grain-128 (MG-128), and conclusion based on the results obtained.

Chapter 6 consists of the overview of this research, the conclusion of works conducted in this study, and the future work or recommendation that can be extended from this research.