CHAPTER 1

THE PROBLEM

This chapter presents the background of this project. It includes : the rationale, theoretical framework, conceptual paradigm, statement of the problem, hypothesis, assumption, scope, delimitation, and importance of the study.

1.1 Rationale

Recently the use of RFID System significantly increases. Several systems in Indonesia use RFID technology for authentication such as : Fuel Subsidy Controlling Systems by PERTAMINA, RFID Access Control by various companies, and in national scale, Indonesian Government has been applied electronic - Kartu Tanda Penduduk (e-KTP) or e-Identification. Almost all of those cases apply RFID technology to authenticate the owner of RFID tag.

Several companies have implemented RFID technology such as in NXP Semiconductor. One of the products is called as Mifare Classic. In 2009, more than one billion cards is sold and Mifare classic covered more than 70% of the contactless smartcard market [11]. Mifare Classic tags provide three pass mutual authentication and encryption algorithm called Crypto-1. This is a stream cipher which uses forty eight bits of secret key. Crypto-1 is NXP Semiconductor's proprietary and the algorithm design is kept secret [10].

In the last few years, several of the studies discuss the problem of data security on Mifare Classic. In 2008, Garcia *et al.* discuss several security vulnerabilities on Mifare classic namely authentication protocol, symmetric cipher and initialization mechanism. Based on this study, it can be concluded that the secret key from one or two authentications from those three mutual authentication can be recovered from the reader without accessing the tag in less than one second. That attack uses public hardware without any pre computation. Besides, communication between tag and reader can be retrieved and decrypted even there are many authentications on it [10]. In 2009, Garcia *et al.* could even retrieve secret key only through wireless access to the tag because its weaknesses on cryptography and protocol stack. Furthermore, the secret key can be used to clone RFID tag [11].

In 2008, NXP semiconductor produced a new product called Mifare Plus to replace Mifare Classic. It has four security levels to overcome any weaknesses of Mifare classic with main cryptography addition based on AES-128 bits [13]. Mifare Plus still uses Crypto-1 Authentication in second and third security level. The higher security level, the more safety offered but with decreased performance. Since the performance is getting low, it is necessary to find a way to maintain the performance while maintaining security.

In 2008, Karsten Nohl [17] stated that both Crypto-1 on Mifare Classic and Mifare Plus can be attacked by Algebraic vulnerability. Algebraic attack recovers secret key by solving a large system of polynomial equation. The large system consists of several small steps which are converted into low degree of algebraic equation [6]. There are several methods to solve that equation but SAT Solver is the efficient one [6]. It solves the equation by first converting polynomial equation into CNF SAT Problem and then guessing each variable using SAT Solver algorithm. [2].

1.2 Theoretical Framework

Nowadays, some research studies about lightweight cryptography which is applied on constrained devices. Most of them use symmetric cipher which the cryptography cost is cheaper than the asymmetric ones. The simple implementation of symmetric cipher which can be implemented on embedded hardware with low cost is Stream Cipher. It is suitable for fast telecommunication application because they operate on a small data unit, bit or few bits [3]. The first method is Linear Feedback Shift Register(LFSR), and its improvement called Non Linear Feedback Shift Register(NLFSR). There are two kinds of Feedback Shift Register such as combination (combine several LFSRs) and non linear boolean function (filter) pseudorandom generator [3]. It means that boolean function plays important role in this cryptosystem.

The resistance of the cryptosystem leads to some fundamental characteristics of boolean function such as algebraic degree, nonlinearity, balancedness, and algebraic immunity [3]. There is another characteristic for combination generator called resiliency. Those characteristics work based on how the boolean function react to the incoming input. The more difficult it predicts, the better boolean function of cryptosystem is used.

1.3 Conceptual Framework/Paradigm

Crypto-1 cipher uses LFSR stream cipher which has forty eight bits of secret key and save it on the tag. It has two main boolean functions called feedback and filter to produce the keystream [10]. The feedback function is used to randomize the input bit and the filter function uses the output of the feedback function to produce the keystream. After that, keystream is XOR-ed with the messages and the output is called the ciphertext. The ciphertext is sent to the RFID reader. Crypto-1 feedback function is a linear meant that it only has one algebraic degree with eighteen input variables. On the other hand, the function of the filter is a nonlinear which has twelve algebraic degree from twenty input variables [10]. Both of that function have high differences regard to their cryptography properties.

1.4 Statement of the Problem

Since 2008 several research [6] [10] [16] [18] [11] about the weaknesses of Crypto-1 have been conducted. **The output and the process of Crypto-1 algorithm can be converted into polynomial equation. Therefore, it can be attacked algebraicly by solving its equation.** There are several ways to solve that equation such as: Linearization and Grobner bases or XL (eXtended Linearization) algorithm[5]. In 2007, Bard *et al.* have studied another way to solve multivariate equation on the sparse system using SAT [2]. It claims that this method is the fastest way. **The security of Crypto-1 cipher is very weak [6], because the secret key can be recovered just in two hundred seconds with one known Tag Nonce and fifty output bits which come from a single encryption [6].** Furthermore the new SAT Solver called cryptominiSAT can reduce attacking time down to forty seconds [18]. One of the weakness is its regular LFSR taps so that it can be attacked using SAT Solver [7]. Algebraic attack is a passive attack so it does not need to interact with the reader or tag. Besides, the feedback function in Crypto-1 cryptosystem has low complexity. Its boolean function is linear so that it is easy for SAT Solver in guessing each variable on the equation.

1.5 Hypothesis

RFID Technology users definitely want to store the data in the tag safely. In contrast, RFIDs environment computing power is limited. The higher security level is chosen, the higher time and computation process is needed, but the performance is decreased. **This study proposes to modify encryption algorithm on Crypto-1 by analyzing three aspect of LFSR such as : chosen register tap as the input both of that function, feedback and filter boolean function.** Based on Soos *et al.* [18] research, Crypto-1 is weak because it lacks complex feedback function. Crypto-1 feedback function modification is proposed to increase the time and complexity for attacking Crypto-1 using SAT solver.

1.6 Assumption

Algebraic attack uses 'known plaintext attack' and known cipher. So that the variables, including ciphertext, can be used to build a polynomial equation.

This research improves LFSR stream cipher algorithm which is used specifically on RFID Tag. The case study on this research is the RFID Tag which is used as an e-identification in Indonesia called e-Ktp, student ID card in Telkom University and Indonesian Driving License (still not implement RFID tag in the card).

1.7 Scope and Delimitation

This research focuses on software implementation by strengthening Crypto-1 algorithm against algebraic attack using CryptominiSAT Solver.

1.8 Importance of the Study

The contribution of this study in lightweight cryptography of RFID is strengthening the cipher to face SAT Solver attack while it has limitation in power and computation. Furthermore, this study reduces logic gate on its construction implementation so that computation resources can be lowered.