Modified A5/1 Based Stream Cipher For Secured GSM Communication

Nur Hafiza Zakaria[1], Kamaruzzaman Seman[2] and Ismail Abdullah[3]

Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan, Malaysia

Abstract.

A5/1 is the stream cipher algorithm used in GSM communication in order to provide over the air communication privacy. The objective of this paper is to modify the algorithm of the existing A5/1 stream cipher in order to improve the security of GSM communication. Several statistical tests such as frequency test, serial test, runs test, long runs of ones test, and linear complexity test were used to test the strength of the algorithm. Two proposed modified A5/1 algorithms successfully passed all the basic statistical tests.

Keywords

component; stream cipher, keystream generator, linear feedback shift register (LFSR), non-linear feedback shift register (NLFSR), clocking, least significant bit (LSB), cryptanalysis.

1. Introduction

The GSM standard specifies algorithms for data encryption and authentication. A5/1 and A5/2 are the two encryption algorithms stipulated by this standard, where the stream cipher A5/1 is used within Europe and most countries [1]. The purpose of cryptography is to hide the contents of messages by encrypting them to make them unrecognizable except by someone who has been given a special decryption key. The purpose of cryptanalysis is then to defeat this by finding ways to decrypt messages without being given the key. In this paper, we propose a modified version of A5 stream cipher with more complexity structure of A5 stream cipher and by changing the tapping mechanism. Besides, this paper also presents results for the analysis of two modified A5/1 stream cipher based on several statistical analysis such as frequency test, serial test, runs test, long runs of ones test, and linear complexity test. The algorithms are considered strong if they pass the five basic statistical tests. The purpose of this study is to modify the A5/1 stream cipher algorithm.

Figure 1 shows the design of original A5/1 Stream Cipher. There are three LFSRs used in A5/1 stream cipher with 19 bits, 22 bits, and 23 bits respectively [2]. Each LFSR, there are different tapping bits.

Manuscript received February 5, 2011
Manuscript revised February 20, 2011

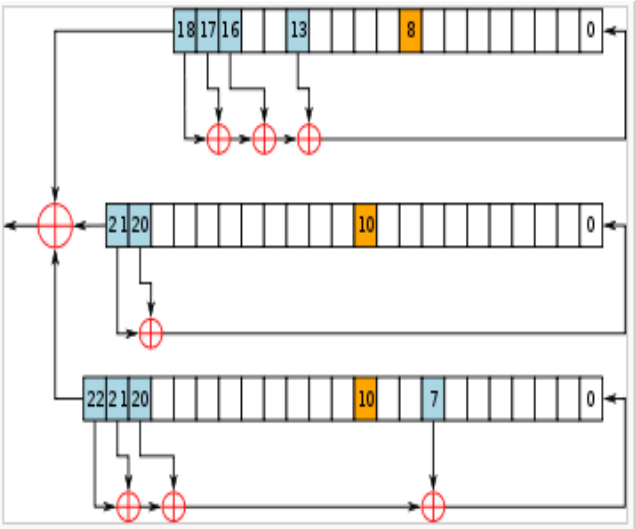

Figure 1 : The A5/1 Stream Cipher

The taps of LFSR1 are at bit positions 13, 16, 17, and 18, the taps of LFSR2 are at bit positions 20 and 21, and the taps of LFSR3 are at bit positions 7, 20, 21, and 22. Each LFSR has single clocking tap in bit 8 for LFSR 1, bit 10 for LFSR 2 and bit 10 for LFSR 3. At each cycle, the clocking bits of all the three registers are examined and the majority bit is determined. A register is clocked if the clocking bit agrees with majority bit. The Table 1 shows the polynomials of A5/1 stream cipher.

Table 1: Polynomials of A5/1 Algorithm

LFSR 1	x19 + x18 + x17 + x14 + 1
LFSR 2	x22 + x21 + 1
LFSR 3	x23 + x22 + x21 + x8 + 1

The arrangement of taps for feedback in an LFSR can be expressed in finite field arithmetic as a polynomial mod 2. This means that the coefficients of the polynomial must be

1's or 0's. This is called the feedback polynomial or characteristic polynomial. The 'one' in the polynomial does not correspond to a tap — it corresponds to the input to the first bit (i.e. x0, which is equivalent to 1). The powers of the terms represent the tapped bits, counting from the left. The first and last bits are always connected as an input and tap respectively [3]. However, based on number of attacks, several weaknesses on A5/1 have been published. There are several attacks on GSM encryption. The first is an active attack. GSM phones can be convinced to use the much weaker A5/2 cipher briefly. A5/2 can be broken easily, and the phone uses the same key as for the strongest A5/1 algorithm. Besides, there are also attacks on A5/1 due to its poor clocking mechanism. To overcome the above problems, we have offer a new clocking mechanism in the existing A5/1 stream cipher.

2. The Proposed Modified A5/1 Algorithms

This part discusses the proposed modified A5/1 algorithm. Figure 2 shows the first proposed A5/1 stream cipher. It has also three LFSRs, but in this design we proposed different tapping bits.

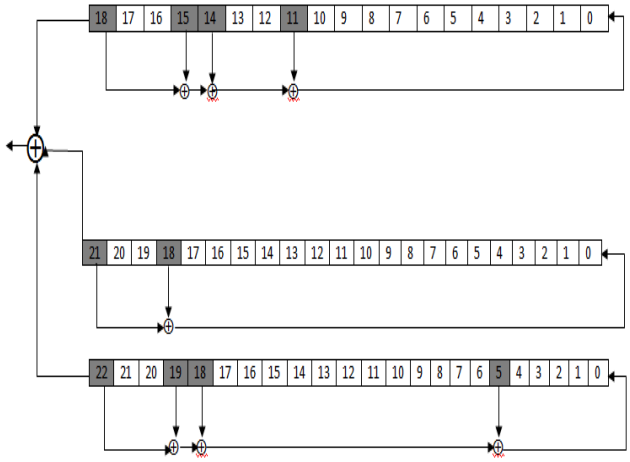

Figure 2: The First Proposed A5/1 Stream Cipher

The output sequence is represented by :

$$z(n) = s_0(n) \oplus s_1(n) \oplus s_2(n)$$

Where $s_0(n), s_1(n), s_2(n)$ represent the outputs of LFSR1, LFSR2, and LFSR3. The LFSR used are defined by polynomials as shown in Equation (1), (2), and (3) :

$$f(x) = 1 + x^{12} + x^{15} + x^{16} + x^{19} \quad (1)$$

$$f(x) = 1 + x^{19} + x^{22} \quad (2)$$

$$f(x) = 1 + x^{6} + x^{19} + x^{20} + x^{23} \quad (3)$$

The output of the generator is generated by x-or the most significant bits of LFSR1, LFSR2, and LFSR3.

Figure 3 shows the second proposed A5/1 stream cipher. Compared to first proposed A5/1 stream cipher, we added two more LFSRs in this design.

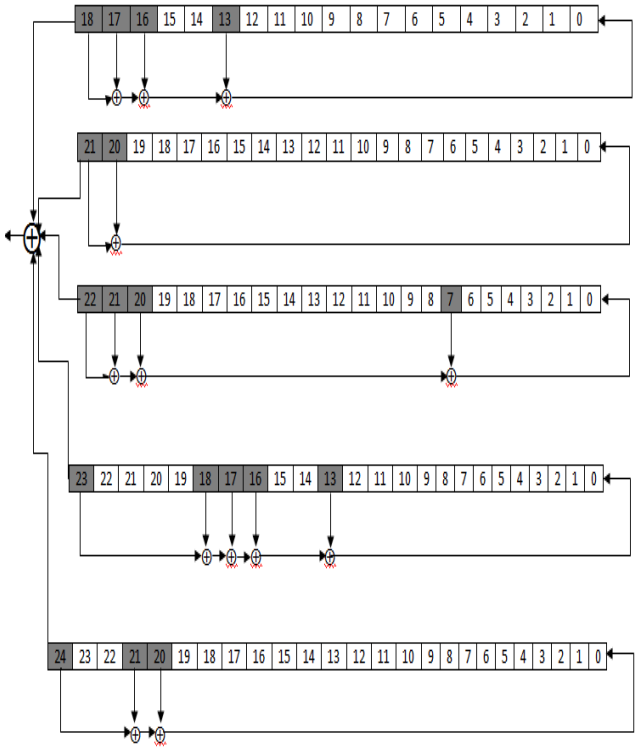

Figure 3: The Second Proposed Stream Cipher

The output sequence is given by :

$$z(n) = s_0(n) \oplus s_1(n) \oplus s_2(n) \oplus s_3(n) \oplus 4(n)$$

Where $s_0(n), s_1(n), s_2(n), s_3(n), s_4(n)$ represent the outputs of LFSR1, LFSR2, LFSR3, LFSR4 and LFSR5. The LFSR used are defined by polynomials as shown in Equation (4), (5), (6), (7) and (8)

$$f(x) = 1 + x^{14} + x^{17} + x^{18} + x^{19} \quad (4)$$

$$f(x) = 1 + x^{21} + x^{22} \quad (5)$$

$$f(x) = 1 + x^{8} + x^{21} + x^{22} + x^{23} \quad (6)$$

$$f(x) = 1 + x^{14} + x^{17} + x^{18} + x^{19} + x^{24} \quad (7)$$

$$f(x) = 1 + x^{21} + x^{22} + x^{25} \quad (8)$$

The output of the generator is generated by x-or the most significant bits of LFSR1, LFSR2, LFSR3, LFSR4 and LFSR5.

3. Results and Discussion

This part presents the testing process and the results obtained. The purpose of conducting the test is to determine the randomness property that is critical to the design of the key generator. For the test, we conducted the five basic statistical test such as frequency test, serial test, runs test long runs of ones test, and linear complexity test according to the method devises by NIST [4].

Random numbers play a crucial role in different applications especially in cryptography. Common cryptosystems employs keys must be generated in a random fashion. Various statistical tests can be applied to a truly random sequence. For each test, a relevant randomness statistic must be chosen and used to determine the acceptance or rejection of the null hypothesis. In addition, the results of statistical testing must be interpreted with some care and caution to avoid incorrect conclusion about a specific generator [4]. Statistical hypothesis testing is a conclusion-generation procedure that has two possible outcomes either the data is random or the data in non-random. A random sequence has many properties with a high probability. For instance, the frequencies of number of ones and zeroes are likely to be almost equal for long sequences. Such properties can be used to distinguish a pseudo-random sequence from a truly random [5]. We have tested the proposed stream ciphers with several tests which are frequency test, serial test, runs test, longest run of ones test, and the linear complexity test. These tests are based on performing a pass/fail statistical test on 100 bits each produced by our proposed stream cipher. Both proposed stream ciphers have passed the five basic statistical tests. From the test results, we can say that the output generated by the proposed generators satisfies the randomness properties. A binary sequence is said to be random if there is no obvious relationship between the individual bits of the sequence [6]. Software named NIST Statistical Test Suite from National Institute of Standards and Technology (NIST) was used in this research in order to conduct statistical test [4]. This software will be useful in identifying (P)RNGs which produce weak (or patterned) binary sequences, designing new (P)RNGs, verifying that the implementations of (P)RNGs are correct, studying (P)RNGs described in standards, and investigating the degree of randomness by currently used (P)RNGs. Table 4 shows the results of statistical analysis.

The NIST test suite contains sixteen tests which will be useful in studying and evaluating the binary sequences produced by random and pseudo random number generators. As in previous work in this field, statistical tests must be devised which, under some hypothesized distribution, employ a particular test statistic, such as the number of runs of ones or the number of times a pattern appears in a bit stream. The majority of the tests in the test suite either (1) examine the distribution of zeroes and ones in some fashion, (2) study the harmonics of the bit stream utilizing spectral methods, or (3) attempt to detect patterns via some generalized pattern matching technique on the basis of probability theory or information theory [4]. For the majority of the statistical tests, memory must be allocated dynamically in order to proceed. In the event that workspace cannot be provided, the statistical test returns a diagnostic message.

Table 4: The Results of Statistical Analysis

First proposed stream cipher		
Statistical Test	p-value	Success/fail
Frequency	0.230139	Success
Serial	p1:0.498961 p2:0.035777	Success Success
Runs	0.795064	Success
Long Runs of Ones	1.000000	Success
Linear Complexity(block : 50)	0.919689	Success
Second proposed stream cipher		
Statistical Test	p-value	Success/fail
Frequency	0.841481	Success
Serial	p1:0.498961 p2:0.498531	Success Success
Runs	0.686094	Success
Long Runs of Ones	1.000000	Success
Linear Complexity (block : 50)	0.919689	Success

4. Conclusion

In this paper, we have described two modified stream generator models for GSM communication. By just changing the clocking mechanism and add new register, the new generators provide more secure stream cipher. In addition, the maximal period of the proposed stream ciphers are much higher than A5/1 stream cipher. This is one of the characteristics that will produce sequences with good statistical properties. In the future, this algorithm can be improved further to provide the maximum security in GSM communication.

Acknowledgements

The authors would like to express their thanks to Faculty of Science and Technology, Universiti Sains Islam Malaysia for supporting this study.

References

[1] Timo Gendrullis, Martin Novotny, and Andy Rupp, "A Real-World Attack Breaking A5/1 within Hours".
[2] http://en.wikipedia.org/wiki/A5/1, "A5/1", access on 10 June 2010.
[3] http://en.wikipedia.org/wiki/Linear_feedback_shift_register , "Linear Feedback Shift Register", access on 10 June 2010.
[4] Andrew Rukhin, Juan Soto, James Nechvatal, Miles Smid, Elaine Barker, Stefan Leigh, Mark Levenson, Mark Vangel, David Banks, Alan Heckert, James Dray, and San Vo, "A statistical test suite for random and pseudorandom number generators for cryptographic applications", 2008.
[5] Abd Rahim Mat Sidek and Ahmad Zuri Shaámeri, "Comparison Analysis of Stream Cipher Algorithms for Digital Communication", 2007.
[6] John Mattson, "Stream Cipher Design", 2006.