ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Improving GSM Security by Enhancing the Randomness Property of the A5/1 Design

Siti Yohana Akmal binti Mohd Fauzi, Marinah binti Othman, Farrah Masyitah binti Mohd Shuib, Kamaruzzaman bin Seman

Faculty of Science & Technology, University Sains Islam Malaysia (USIM, Bandar Baru Nilai, 71800 Nilai, Negeri Sembilan

ARTICLE INFO

Article history:
Received 3 August 2015
Accepted 28 October 2015
Available online 31 October 2015

Keywords:
A5/1 stream cipher, NIST test suite, pseudo-random number generator (PNRG), randomness analysis

ABSTRACT

Background: A5/1 is well-known as the encryption standard for GSM communication, one of the most largely used cellular system in the world. Despite the popularity, its credibility was severed when its design was leaked in 1999 which consequently posed a threat to user's privacy and confidentiality. The disclosure, incidentally, unveiled some weaknesses of the A5/1 stream cipher design such as short register phase, collision problem and simple combinational function. In this paper, a modified A5/1 is described. The proposed design looked at the effect of altering the combinational function from that of XOR to one using a 4-to-1 multiplexer (Mux) to increase the complexity of the algorithm which in turn will enhance its random features, and thus making it more secure overall. The generated output from the proposed design will be tested using the National Institute of Standard and Technology (NIST) test suite. The result will then be compared with that obtained using the modified design by Zakaria et. al. (2014), and next, analyzed. **Objective:** The objective for this study is to analyze and compare the use of different parameter toward the randomness of modified A5/1 structure by using the NIST test suite. **Results:** The analysis computed by the NIST test suite shows that the author's proposed version is more secure compared to that of Zakaria et. al.'s version**. Conclusion:** The author's version is shown to be more secure compared to that of Zakaria et. al. (2011), and while its randomness is comparable to that of the original A5/1 version, its structure is not that of public's knowledge and will therefore minimize its probability of being deciphered.

To Cite This Article: Siti Yohana Akmal binti Mohd Fauzi, Marinah binti Othman, Farrah Masyitah binti Mohd Shuib, Kamaruzzaman bin Seman.. Improving GSM Security by Enhancing the Randomness Property of the A5/1 Design. ***Aust. J. Basic & Appl. Sci.,*** *9(32): 209-214, 2015*

INTRODUCTION

GSM, short for Global System for Mobile communication, dominates the mobile communication networks with its total number of subscribers well exceeding that of the other mobile network standard's subscribers such as Code Division Multiple Access (CDMA) and Universal Mobile Telecommunications System subscribers such as Code Division Multiple Access (CDMA) and Universal Mobile (UMTS) by almost 90% globally (Mobi Thinking, 2014).

It is a well-known fact that the GSM network is encrypted with the A5/1 stream cipher to secure the two-way communication between that of the user and the receiver. Unveiled as the encryption standard for GSM communication in 1987, the A5/1 stream cipher has since then successfully played its role in providing confidentiality and privacy for both voice and text messaging for over a decade (Madani & Chitroub , 2014; Mitchell & Dent, 2004), emerging as the solution for the vulnerability of the GSM communication that was not cloaked with any encryption whatsoever, thus making it susceptible to be 'snooped' or eavesdropped by irresponsible third party that may have something up on their sleeve. The 'no-cloaking' communication is denoted as A5/0 encryption which implied that the communication consisted purely of plaintext, which is an euphemism for the real conversation that is not concealed with some weird coding to make it appear nonsensical in case it is tapped.

A5/2, which was subsequently introduced, garnered much concern rather than appreciation. While the reason for its debut was solely due to export constraint, once the version was proven to be critically weaker than that of A5/1, many countries chose to revoke the use of A5/2 in the mobile devices (Mitchell & Dent, 2004).

However, the credibility of A5/1 does not last long when the covert design structure of A5/1 was finally leaked leading to numerous attacks which were aimed at its weak features, specifically on the seed (Nohl, 2010; AlHamdan et. al., 2014), the clocking mechanism (Gendrulllis et. al., 2008), the fixed feedback polynomial based linear feedback

Corresponding Author: Marinah binti Othman, Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, egeri Sembilan.
E-mail: marinah@usim.edu.my

shift register (LFSR)(Meyer, 2010; Mahalanobis & Shah, 2014), the non-invertible clocking mechanism (Kalenderi et. al., 2012; Jain & Chaudhari, 2013; Upadhyay et. al., 2014), and the need for frequent resetting (Shah & Mahalanobis, 2012).

Nevertheless, there in an ongoing effort to improve the security of A5/1, mainly by altering its original architectural design such as the clocking mechanism (Colbert et. al., 2011; Bajaj, 2011; Madani & Chitroub, 2014; Upadhyay et. al., 2014), the length of the linear feedback shift register (LFSR), as well as the development of a more secure (random) polynomial structure (Zakaria et. al., 2011) to ensure that the encryption is less vulnerable to attacks.

In this paper, a new algorithm is proposed, aimed to make up for the weaknesses of A5/1, and then tested for its randomness property using the NIST test. Sections 2 and 3 will look in more detail at the A5/1 stream cipher, as well as the design of the proposed stream cipher respectively, followed by a discussion on the analysis of the data obtained from the NIST test in section 4. Section 5 then concludes the work.

2. A5/1 Stream Cipher:

Stream cipher is a type of encryption that processes the plaintext which is typically in binary form, bit-by-bit into ciphertext. Stream cipher is generally considered as an efficient encryption method due to its faster encryption capability that continuously encrypt stream of plaintext. The block cipher, in contrast, has a complex circuitry that weighs down the speed of the hardware. There is also the risk of increased transmission error as the result of propagation error (Mitchell & Dent, 2004) (Al-Rasedy & Al-Swidi, 2010) (Pornin & Stern, 2000) (Salih, Al-Safi, & Ali, 2014) (Galanis, Kitsos, Kostopoulos, & Sklavos, 2005). A5/1 stands out as one of the well-known stream cipher algorithms aside from E0, RC4, Helix and W7 cipher that is being used in bluetooth, wireless network, Message Authetication Code (MAC) and high data rates hardware respectively.

2.1 Architectural Design of A5/1:

In general, the basic design of A5/1 can be summarized into four distinct parts that are linear feedback shift register (LFSR), polynomials, clocking mechanism, and combinational function (Kostopoulos et. al., 2004; Sankaliya et. al., 2011). According to Mitchell and Dent (2004), the standard design of a stream cipher consists of both a keystream generator (KG) and an output function as stated in ISO/IEC 18033-4. In this case, LFSR set is equivalent to that of the KG, while the output function refers to the combinational function used to produce the ciphertext.

The LFSRs consists of 3 sets each made up of 19-, 22-, and 23 bits respectively, giving a total of 64 bits, with each being fitted with a different polynomial as shown in Equations (1), (2) and (3), that denotes the tapping bits.

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

$$f(x) = x^{22} + x^{21} + 1 \quad (2)$$

$$f(x) = x^{23} + x^{22} + x^{21} + x^{8} + 1 \quad (3)$$

Interestingly, each polynomial used is a primitive polynomial or in a more familiar term, ‘irreducible polynomial’ as it circumvents the possibility of redundancy within the polynomial that may lead to the LFSR being vulnerable to attacks.

Based on the polynomial, the LFSR will be tapped and if it agrees with the majority logic (ML), it will be shifted by one bit. Next, the most significant bit (MSB) from each of the LFSR will be forwarded to the combinational function.

Combinational function can be considered the vital point in A5/1 as it plays the role of ensuring the output sequence to be unpredictable. Conventional A5/1 made use of the XOR which is prone to attacks by means of linear cryptanalysis as mentioned by Madani & Chitroub (2014).

The overall design of A5/1 is shown in Figure 2.1.1.

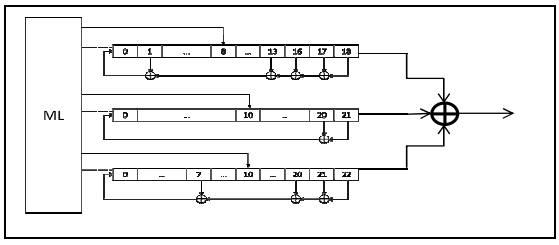


Fig. 2.1.1: A5/1 design architecture.

The clocking bits (which are 8, 10, 10 respectively; based on Figure 2.1.1) will determine as to whether the LFSR is to be clocked. If the clocking bits agree with the majority logic (ML), the register will be clocked and vice versa. The tapping bits of each register will then be ‘XOR’-ed (Meyer, 2010). The overall process flow for single clocking of the A5/1 stream cipher can be seen in Figure 2.1.2.

2.3 NIST Statistical Test:

NIST is an agency of the U.S. Department of Commerce specializing in the development of

science and technology, aimed at improving both the economic security as well as quality of life. The NIST statistical tool suite is one of the many Standard Reference Materials (SRMs) published by the NIST.

The test suite offers a set of 16 tests that can be used to check the randomness characteristics of a binary string. Each of the test is unique and scrutinize the randomness of the stream in a distinctive manner.

The test has been set on default value with different minimum bit requirement in order for the test to be valid. The default value however, can be changed to suit the user's design.

In brief, the test would analyze the frequency and the pattern of occurrence of 1s and 0s within the stream that is whether it is predictable or otherwise (National Institute of Standard and Technology, 2010, p. 13).

2.4 Altering A5/1 Parameter:

A5/1 consists of several distinct characteristics which can be used to enhance its randomness property. The choices vary from changing the LFSR length, modifying clocking mechanism, or the selection of new tapping bits.

The modified design by Zakaria et. al. (2011), as shown in Equations (4) to (6), focused on changing the polynomial or the tapping bits.

$$f(x) = x^{19} + x^{16} + x^{15} + x^{12} + 1 \quad (4)$$

$$f(x) = x^{22} + x^{19} + 1 \quad (5)$$

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

They however, preserved the XOR combinational function, which is not necessarily a good choice because as per mentioned earlier, XOR is more likely to be cracked due to its linearity simplicity. Between both the tapping bits and the combinational function, the former would contribute less in generating random binary sequence.

In this paper, a new algorithm will be proposed by modifying its combinational function from that of the conventional XOR to one using a Mux. The effect of altering the different parameters, i.e. tapping bits by Zakaria et. al. (2011) and combinational function by the author's proposed design, will be looked at in terms of the randomness of the output.

3. Proposed A5/1 Design:

The design that will be proposed in this paper focuses on the use of a new combinational function whilst preserving the total number of LFSRs and their combined length at both 3 and 64 bits respectively. The polynomials used are the same as that in Equations (1) to (3) to ensure that the modified version preserves its original characteristics which eventually will ease its future hardware implementation.

Multiplexer or Mux is a type of switch that operates based on a predetermined selection which has been programmed into it such that only one of the many input signals will be forwarded.

In this design, a 4-to-1 Mux will be used and further customized such that each selection will XOR function either 2 or more LFSRs, which in turn makes it harder to be cracked. The details on the selection and Mux choices are not disclosed here such that its confidentiality is more robust.

The new architectural design is as shown in Figure 3.1, while the details of the different characteristics between that of the two designs being looked at in this work are listed in Table 3.2.

4. Analysis on Generated Output:

Once the design architecture has been programmed, it is then simulated to generate a stream of binary which is stored in a file. One of the NIST test suite has a minimum bit requirement for the testing of 1,000,000 bits – the number which has been taken for this study. The stored bits will then be used for the randomness test.

Some of the tests are parameterized such that the values need to be set. Fortunately, NIST also provide a handbook to give guidelines on the default value that can be used according to the minimum input. The details for the value of the parameterized test used for the NIST test is shown in Table 4.1.

5. Conclusion:

In summary, the design by Zakaria et. al. (2011) has been found to fail one of the statistical tests, believed to be due to them not using an irreducible type of polynomial. The computed analysis using the NIST test suite has shown that the proposed design by the author has a good randomness property thus making it a good substitute for conventional A5/1, suggesting that the manipulation of the complex combinational function turn will enhance its random features via the generation of the random binary sequence, and thus making it more secure overall.

ACKNOWLEDGEMENT

This research was supported by the RAGS grant, under the Ministry of Higher Education Malaysia. (USIM/RAGS/FST/36/50813). SYAMF acknowledges a graduate fellowship through the MyBrain15 programme.

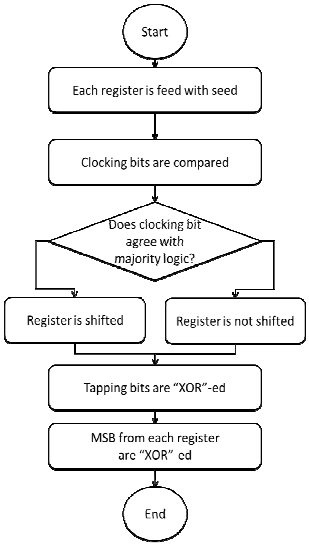


Fig. 2.1.2: Single process of A5/1 clocking.

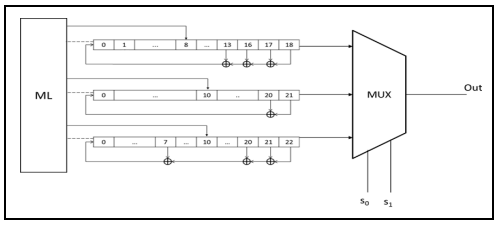


Fig. 3.1: Architectural design of proposed A5/1.

Table 3.2: Details on the characteristic of A5/1 design between Zakaria et. al. (2014) and author's proposed design.

	Zakaria et. al.	Proposed
Bit length	64	64
Number of LFSR	3 LFSR	3 LFSR
Tapping bits	$f(x) = x^{19} + x^{16} + x^{15} + x^{12} + 1$ $f(x) = x^{22} + x^{19} + 1$ $f(x) = x^{23} + x^{20} + x^{19} + x^{6} + 1$	$f(x) = x^{19} + x^{18} + x^{17} + x^{14} + 1$ $f(x) = x^{22} + x^{21} + 1$ $f(x) = x^{23} + x^{22} + x^{21} + x^{8} + 1$
Clocking Mechanism	Majority logic	Majority logic
Combinational function	XOR	Mux

Table 4.1: Input value for the parameterized tests

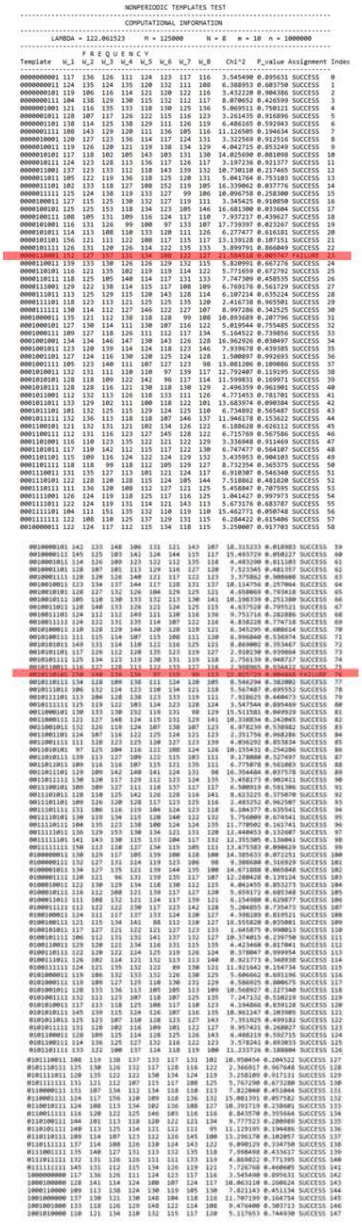
Test	Input value (bit)
Block frequency test	Block length = 128
Non-overlapping template matching test	Template length = 10
Overlapping template matching test	Template length = 9
Maurer's "Universal Statistical" test	Number of Blocks = 7 Block length = 1280
Linear complexity test	Block length = 500
Serial test	Block length = 16
Approximate entropy test	Block length = 10

All 16 tests from NIST test suite are executed in this study and the data computed is tabulated as in Table 4.1.1.

Table 4.1.1: Result from NIST test for Zakaria's and author's proposed design.

		Zakaria et. al.	Proposed
Frequency		0.944194	0.871306
Block Frequency		0.021784	0.807510
Runs Test		0.448454	0.307741
Longest Runs		0.495429	0.380238
Binary Matrix		0.431913	0.309042
Spectral		0.860923	0.835507
Non-Overlapping Template		Fail	Success
Overlapping		0.425947	0.637205
Universal		0.157400	0.973745
Lempel-Ziv		0.076962	0.750961
Linear Complex		0.691752	0.585877
Serial		0.653244	0.409125
		0.548623	0.542520
Approximate Entropy		0.017461	0.636243
Cumulative Sum	Forward	0.627394	0.300836
	Reverse	0.692331	0.403653
Random Excursion		Success	N/A
Random Excursion Variant		Success	N/A

Table 4.1.2: Statistical test result of non-overlapping template for design by Zakaria et. al.



REFERENCE

AlHamdan, A., Harry, B., Dawson, E., Simpson, L., & Wong, K. K. H., 2014. Weak key-IV Pairs in the A5/1 Stream Cipher. Twelfth Australasian Information Security Conference (AISC 2014), 23-36.

Al-Rasedy, S. A., & Al-Swidi, A. A., 2010. An Advantages and Disadvantages of Block and Stream Cipher, 294-296.

Galanis, M., Kitsos, P., Kostopoulos, G., & Sklavos, N., 2005. Comparison of the Hardware Implementation of Stream Cipher. The International Arab Journal of Information Technology, 2: 267-274.

Gendrulllis, T., Martin, N., & Andy, R., 2008. A Real-World Attack Breaking A5/1 Within Hours. Cryptographic Hardware and Embedded Systems – CHES 2008, 5154: 266-282.

Jain, A., & Chaudhari, N. S., 2013. Two Trivial Attacks on A5/1: A GSM Stream Cipher.

Kalenderi, M., Pnevmatikatos, D., Papaefstathiou, I., & Manifavas, C., 2012. Breaking the GSM A5/1 Cryptography Algorithm with Rainbow Tables and High-End FPGAs. 22nd International Conference - Field Programmable Logic and Applications (FPL), 747-753.

Kostopoulos, G., Sklavos, N., Galanis, M., & Koufopavlou, O., 2004. VLSI Implementation of GSM Security; A5/1and W7 Ciphers.

Madani , M., & Chitroub , S., 2014. Enhancement of A5/1 Stream Cipher Overcoming its Weaknesses. The Tenth International Conference on Wireless and Mobile Communications (ICWMC), 11(2): 154-159.

Mahalanobis, A., & Shah, J. , 2014. An Improved Guess-and-Determine Attack on the A5/1 Stream Cipher. Computer and Information Science, 7(1).

Meyer, S., 2010. Breaking GSM with rainbow Tables.

Mobi Thinking, 2014. Global Mobile Statistics 2014 Part A: Mobile Subscribers; Handset Market Share; Mobile Operators. MobiForge: http://mobiforge.com/research-analysis/global-mobile-statistics-2014-part-a-mobile-subscribers-handset-market-share-mobile-operators. Retrieved 20 January, 2015.

Mitchell, C. J., & Dent, A. W., 2004. International Standards for Stream Ciphers : A Progress Report.

National Institute of Standard and Technology., 2010. A Statistical Test Suite for the Validation of Random Number Generators and Pseudo Random Number Generators for Cryptographic Applications. National Institute of Standard and Technology.

Nohl, K., 2010. Attacking Phone Privacy. Blackhat 2010 Lecture Notes.

Pornin, T., & Stern, J., 2000. Software-Hardware Trade-Offs: Application to A5/1 Cryptanalysis. In Ç. K. Koç, & C. Paar, Cryptographic Hardware and Embedded Systems — CHES 2000, 318-327.

Salih, M. M., Al-Safi, M. G., & Ali, F. H., 2014. Dynamic Stream Ciphering Algorithm. IOSR Journal of Computer Engineering (IOSR-JCE), 16(2)3: 72-78.

Sankaliya, A. R., Mishra, V., & Mandloi, A., 2011. Implimentation of Cryptographic Algorithm for GSM and UMTS Systems. International Journal of Network Security & Its Applications (IJNSA), 3(6): 81-88.

Shah, J., & Mahalanobis, Ayan. (2012). A New Guess-and-Determine Attack on the A5/1 Stream Cipher. Cryptography and Security (cs.CR).

Upadhyay, D., Sharma, P., & Valiveti, S., 2014. Randomness Analysis of A5/1 Stream Cipher for Secure Mobile Communication. International Journal on Soft Computing (IJSC), 5(1): 95 - 100.

Zakaria, N. H., Seman, K., & Abdullah, I., 2011. Modified A5/1 Based Stream Cipher for Secured GSM Communication. International Journal of Computer Science and Network Security, 12: 223-226.