MJoSHT
Malaysian Journal of Science, Health & Technology
[mjosht.usim.edu.my]

Article

Randomness Evaluation of Modified A5/1 Stream Cipher for Global System for Mobile Communication

Siti Yohana Akmal Mohd Fauzi[1], Marinah Othman[2,a], Farrah Masyitah Mohd Shuib[2,b], Kamaruzzaman Seman[2,c], Khairi Abdulrahim[2,d]

[1]*Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai Negeri Sembilan. Malaysia*
Email:sy.akmal91@gmail.com

[2]*Faculty of Engineering and Built Environment, Universiti Sains Islam Malaysia, 71800 Nilai Negeri Sembilan. Malaysia*
E-mail: [a]marinah@usim.edu.my, [b]farrah@usim.edu.my, [c]drkzaman@usim.edu.my, [d]khairiabdulrahim@usim.edu.my

***Abstract*— While the A5/1 stream cipher encryption is known to aid in providing security and privacy for the mobile communication, it actually has numerous security vulnerabilities that leave it susceptible to attacks. Although newer technology standards have been developed, the majority of the mobile phones around the world still make use of the A5/1 stream cipher design, hence the urgent need to strengthen the latter. Numerous works have been done to improve the security of the A5/1, such as by altering its clocking mechanism, and the length of the linear feedback shift register, leading to the ultimate goal of producing a stream of random bits which are difficult to crack, with the National Institute of Standards and Technology (NIST) Statistical Toolsuite used to analyse the randomness property of the results. However, none of them, to the best of the author's knowledge actually carried out the analysis of the results according to the guideline as per recommended by the NIST, despite the fact that the interpretation of the results is crucial in determining the strength of the stream cipher, as to whether it is robust to attacks, or otherwise. In this paper, a new modified A5/1 stream cipher is proposed and tested using the NIST test suite. The results, interpreted according to the NIST guidelines, by analysing the proportion of sequences passing test and the uniformity of the P-value, shows that the new modified design is random and is a good alternative to the conventional A5/1 stream cipher. A selective review of the weaknesses of a few of the interpretations by the other researchers will also be included.**

***Keywords*— A5/1 stream cipher; GSM; linear feedback shift register; LFSR, NIST test suite.**

I. INTRODUCTION

Since the first official attack on A5/1 stream cipher in 1999, numerous other attacks followed on by targeting the weak points of the encryption design [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11], [12]. Some of the weak points are simple and linear combinational function, positioning of the clocking bit, short LFSR length and LFSR correlation [13], [14], [15], [16].

While several efforts have been done to improve the A5/1 stream cipher design and tested the generated bit stream using the NIST test suite, none of them, as far as in author's knowledge, have actually done a proper analysis as recommended by NIST. For instance, Bajaj [17] and Bhal et al. [13] used the NIST test suite to do a statistical analysis of the randomness pattern of the bit stream generated by their modified version of the A5/1 stream cipher. Instead of using the interpretation method outlined by NIST, they calculated the average for the resulted p-value of each test as the pass/fail outcome.

Also, some of the previous works did not properly run the test as per suggested by NIST as they either run only some of the tests listed or did not generate enough bit stream to be tested [18], [19]. The issue is that since the test is not run and analyzed as per suggested by NIST, how credible is the result is that is to say that the proposed design is successful as it could generate secure bit stream.

In this paper, three modified designs of A5/1 stream cipher are proposed whereby each of the design is altered based on the characteristics of the conventional design that is said to weaken its security strength. The designs will then be tested using the NIST test suite and analyzed using interpretation methods suggested by NIST. Section 2 will look into how randomness helps in providing security, how A5/1 stream cipher works as well as some previous works done on A5/1 stream cipher. In Section 3, proposed designs by authors are described, followed by the result of the NIST test of each designs in section 4.

II. A5/1 STREAM CIPHER: RANDOMNESS AND SECURITY

Randomness is a term used to describe an unpredictable event that happens independently and not being biased by external factors. In security system, a highest degree of randomness property is desirable to achieve a strong and secure system. The randomness property is largely

dependent on the cryptographic algorithm that acts as the random number generator (RNG) which generates sequences of random bit stream. A good RNG will produce sets of bit stream with good randomness property. RNG can be categorized into three types: true RNG (TRNG), pseudo-random number generator (PRNG) and cryptographically secure PRNG (CSPRNG).

TRNG, besides being costly [20], do not generate the same output each time it is run just like the probability of getting head when flipping coin. PRNG is computed with an initial value or seed and could generate an output almost like TRNG. CSPRNG, on the other hand, is an unpredictable PRNG that behaves exactly like TRNG. Although CSPRNG seems ideal to be used in the design, the downside of the CSPRNG is that since it is unpredictable, decryption will not be possible [21]. Among these three RNG, PRNG is the common type of RNG to be used in cryptographic algorithm.

A. A5/1 Stream Cipher Design Structure and Bit Stream Generation Process

Categorized under PRNG, the A5/1 stream cipher computes the seed fed to it into sequences of random bit stream. The A5/1 stream cipher has long been used for GSM communication – a prominent mobile standard technology [22]– to provide security for the users. It produces sequences of bit streams which are called the secret key (Ki).

The conventional design of A5/1 stream cipher mainly consists of three sets of linear feedback shift register (LFSR) clocked using a majority logic (ML) function to produce one bit of key at a time. The design structure of the conventional A5/1 stream cipher is as shown in Fig. 1.

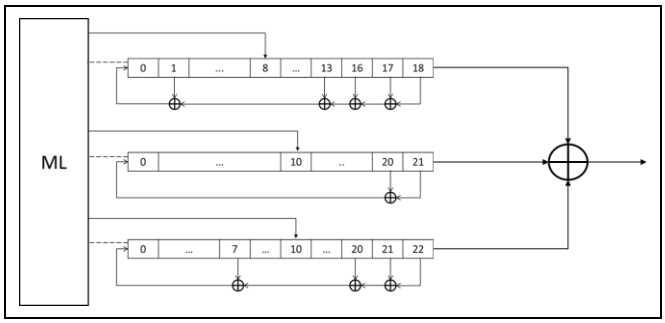

Fig. 1 Design structure of conventional A5/1 stream cipher

The leftmost box labelled as ML is the majority logic function that controls the shifting of each LFSR. The smaller boxes grouped together are the linear feedback shift registers whereby the number labeled on the boxes are the tapping bits of each LFSR and the symbol $\oplus$ denotes XOR that serves as the combinational function.

The majority logic works by comparing the clocking bit – a bit register that is situated within the center of register – of the three LFSRs such that if the clocking bit agrees with majority logic, the corresponding LFSR will be shifted.

For the LFSRs, the tapping bits are XOR-ed to feed the least significant bit (LSB) that is on the rightmost bit register, labelled as 0. The most significant bit (MSB) is situated on the leftmost bit register which signifies the size of the LFSR. The tapping bits can be represented in term of polynomials as follows:

LFSR 1: $f(x) = x^{19} + x^{18} + x^{17} + x^{14} + 1$ (1)

LFSR 2: $f(x) = x^{22} + x^{21} + 1$ (2)

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

The process of generating sequences of random bit stream can be broken into two phases as follows:

Phase I: Initialization Phase

First, all the bit registers of the LFSRs are set to zero. Next, 64 bits key session (KC) and 22 bits frame number (FN) are fed into the LFSRs in parallel, bit by bit. Once the LFSRs have finished being fed with KC and FN, the LFSRs will then be shifted according to the majority logic rules for 100 cycles.

Phase II: Secret Key Generation Phase

The LFSRs will continue to be shifted according to the majority logic rules, but the difference is that the most significant bit (MSB) of each LFSR will be XOR-ed to produce Ki.

In a session, the maximum amount of Ki that can be generated is 228 bits per frame which means if more bits of Ki are needed; the process should be repeated over several times until the desired bit stream is achieved. In this study, a bit stream of 100 million bits is generated which is then tested for its randomness property.

B. Bit Stream Randomness Evaluation

There are several tests available to test the randomness property of the bit stream generated, but one of the most used test set is the NIST test suite. NIST test suite is published by National Institute of Standards and Technology and has been used in numerous studies to evaluate the randomness property of the generated bit stream [13], [17], [18], [19], [23], [24], [25], [26], [27]. It consists of sixteen different tests that compute p-value based using different types of approach of analyzing the randomness property such as frequency monobit test, overlapping template matching test, cumulative sum (CuSum) test, longest runs of one test, etc. [28].

The p-value computed in each of the NIST statistical test is used to determine whether the test is considered as successful or failed such that if the p-value is more than or equal to 0.01, then the test is considered as successful and vice versa [28]. To the best of the author's knowledge, none of the published works on modified A5/1 stream cipher that used NIST test suite has run the software and evaluate the result as per suggested by NIST [13], [17], [18], [19]. Based on the manual released by NIST, there are two approaches that can be done to interpret the empirical result of the p-value that are the proportion of sequences passing a test and the uniformity of the p-value distribution.

C. Previous Works of Improvement of A5/1 Stream Cipher

Throughout the year since the first leak of the covert design, there are numbers of efforts that had been made to improve the structure of A5/1 stream cipher to make it more secure. Table I depicts several works which have been done and used the NIST to evaluate the randomness of the generated bit stream.

TABLE I
LIST OF PREVIOUS WORKS ON A5/1 STREAM CIPHER

	Detail on Modification	Detail on NIST Test Run and Evaluation
Bajaj [17]	Proposed two modifications – feedback tapping units and clocking mechanisms.	- Run all 16 tests with 10 sequences of size 10000 bits. - The p-value is analysed by computing the average.
Zakaria et al. [19]	Proposed two modified designs for A5/1 – changed the clocking mechanism and added up LFSRs.	- Run 6 tests only with 1 sequence of size 1 million bits. - The generated p-value is used as the final result.
Bhal & Dhillon [13]	Proposed a design consisting of 4 registers that sums up to 128 bits.	- Only run 11 tests with 100 sequences of size 100000 bits. - The p-value is analysed by computing the average.
Upadhyay et al. [18]	Substitute LFSR into NLFSR.	- Only run 11 tests with 100 sequences of size 100000 bits. - The p-value is analysed by computing the average.

D. Proposed Modification of A5/1 Stream Cipher

Bhal and Dhillon [13] suggested that the use of larger LFSR size could help in avoiding time-memory trade-off (TMTO) attack. This attack works by having a database of all possible arrangements of the register value. Larger register value or LFSR means more arrangement possibility thus making the design to be more robust from attack.

In this study, a new modified design with larger LFSR size is proposed. The new design has an LFSR size of 40-, 43- and 45-bits which sums up to bits of 128-bits and makes it larger compared to conventional A5/1 stream cipher design which only has 64-bits. However, most of the characteristics of the conventional design are preserved such as the number of the LFSR, clocking mechanism and also the combinational function. The new polynomial to be used in the LFSR design is as shown in Equation (4), (5) and (6).

LFSR 1:

$$(x) = x^{40} + x^{36} + x^{28} + x^{18} + x^{7} + x^{6} + 1 \quad (4)$$

LFSR 2:

$$f(x) = x^{43} + x^{35} + x^{32} + x^{30} + x^{25} + x^{8} + 1 \quad (5)$$

LFSR 3:

$$f(x) = x^{45} + x^{33} + x^{27} + x^{23} + x^{15} + x^{14} + 1 \quad (6)$$

Using the modified design, a bit stream of 1-million-bit length with 100 sequences are generated.

III. RESULT AND DISCUSSION

In order to evaluate the randomness property of the proposed design, NIST statistical test suite is used.

A. NIST Statistical Test Suite

NIST is a special software used to evaluate RNG in terms of its randomness property which consequently determine the security strength of the RNG. It is developed by the National Institute of Science and Technology (NIST) that offers 16 types of different tests to check the randomness pattern of the generated keystream. The NIST team has released a report together with the source code for the tests in order to guide the researchers on how to implement the statistical test [28], [29].

The p-value computed from each of the NIST tests is used to determine as to if the tested keystream passed or failed the test whereby if the p-value falls into the range of $\geqslant 0.01$, the test is considered to have successfully passed the test. The result can be interpreted empirically in two ways: proportion of sequences passing test and the distribution of p-value.

B. Proportion of Sequences Passing Test

By using the pass/fail decision from the p-value obtained, the number of sequences that passed the test over the number of sequences tested is calculated such that:

$$\text{Proportion of sequences thats passed} = \frac{\text{Total sequence(s) that passed the test}}{\text{Total sequences tested}} \quad (7)$$

Using Equation (7), the result obtained from all 16 NIST tests in both conventional and proposed design of A5/1 stream cipher is tabulated as in Table II. It is observed that the proposed design successfully passed all the tests.

TABLE II
PROPORTION OF SEQUENCES PASSING TEST

No	Test	Proposed Design
1	Frequency	0.972222
2	Block frequency	0.990741
3	Runs	0.194444
4	Longest run of ones in a block	0.962963
5	Binary matrix rank	0.981481
6	Discrete Fourier transform (spectral)	1.000000
7	Non-overlapping template matching	0.987051
8	Overlapping template matching	0.981481
9	Maurer's "Universal Statistical"	0.981481
10	Lempel-Ziv compression	0.962963
11	Linear complexity	1.000000
12	Serial	0.842593
13	Approximate Entropy	0.972222
14	Cumulative Sum (CuSum)	0.967593
15	Random Excursion	0.996527
16	Random Excursion Variant	0.999338

C. Uniformity of P-Value

The uniformity of the p-value is determined by calculating the number of occurrences of the p-value within a certain interval. The histogram provides a straight forward observation of the uniformity of the P-value thus making it easier to compare between the tests. If the P-value is normally distributed, then it can be concluded that the

distribution of the P-values are uniform [28]. It is to be noted that, one distribution table is done per test which means that for each design, there will be a total of 16 distribution tables.

The result is then plotted into histogram to have better observation of the distribution of the p-value. Fig. 2 shows an example of the histogram of the distribution of p-value of frequency test for the proposed design. The interval is broken into 10 and it can be seen that the distribution of p-value is uniform. It is found that the generated bit stream from the proposed design passed the uniformity test for all 16 tests.

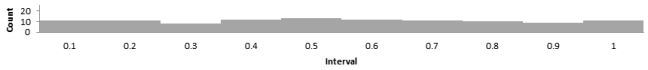

Fig. 2 Histogram of frequency test for proposed design

IV. Conclusion

Upon randomness evaluation using both proportion of sequences passing test and the uniformity of p-value, the proposed design by author successfully pass the tests.

Acknowledgment

This research was supported by USIM Special Grant (USIM/PPP/KHAS_FKAB/30/10117). SYAMF acknowledges a graduate fellowship through the MyBrain15 programme.

References

[1] A. AlHamdan, B. Harry, E. Dawson, L. Simpson, and K. K.-H. Wong, "Weak key-IV Pairs in the A5/1 Stream Cipher," in *Twelfth Australasian Information Security Conference*, 2014, vol. 149, pp. 23–36. Auckland, New Zealand: Australian Computer Society.

[2] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication," *Journal of Cryptology*, vol. 21, pp. 392–429, 2008

[3] T. Gendrullis, M. Novotný, and A. Rupp, "A Real-World Attack Breaking A5/1 Within Hours," in *Cryptographic Hardware and Embedded Systems*, 2008, 5154, pp.266–282.

[4] A. Jain, and N. S. Chaudhari, "Two Trivial Attacks on A5/1:A GSM Stream Cipher," *Cryptography and Security (cs.CR)*, 2013.

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

[6] A. Mahalanobis, and J. Shah, "An Improved Guess-and-Determine Attack on the A5/1 Stream Cipher," *Computer and Information Science*, vol. 7(1), pp. 115–124, 2014.

[7] S. Meyer, "Breaking GSM With Rainbow Tables," *Cryptography and Security (cs.CR)*, 2010.

[8] K. Nohl and C. Paget, "GSM: Srsly?." (Slide). 26th Chaos Communication Congress, 2009.

[9] K. Nohl, "Attacking Phone Privacy Crypto Basics Time-Memory Trade-Offs," BlackHat 2010 Lecture Notes, 1–6.

[10] J. Shah, A. Mahalanobis, "A New Guess-and-Determine Attack on the A5/1 Stream Cipher," *Cryptography and Security (cs.CR)*, 2012.

[11] H. Wu, Cryptanalysis and Design of Stream Ciphers. 2008.

[12] C. Xenakis, and C. Ntantogian, "Attacking the Baseband Modem of Mobile Phones to Breach the Users' Privacy and Network Security," in *Proceedings of the 7th International Conference on Cyber Conflict*, 2015, pp. 231–244.

[13] A. S. Bhal, and Z. Dhillon, "LFSR Based Stream Cipher (Enhanced A5/1)," *International Journal of Computer Applications*, vol. 57(19), pp. 32–35, 2014.

[14] M. Madani, and S. Chitroub, "Enhancement of A5 / 1 Stream Cipher Overcoming its Weaknesses," in D. Krstic & M. C. A. Torres (Eds.), T*he Tenth International Conference on Wireless and Mobile Communications*, 2014, pp. 154–159.

[15] F. Masoodi, S. Alam, and M. U. Bokhari, "Article: An Analysis of Linear Feedback Shift Registers in Stream Ciphers," *International Journal of Computer Applications*, vol. 46(17), pp. 46–49. 2012.

[16] S. B. Sadkhan and N. H. Jawad, "Improvement of A5/1 Encryption Algorithm Based on Using Unit Delay," *Iraqi Academic Scientific Journal*, vol. 22(2), pp. 622–633, 2014.

[17] N. Bajaj, "Effects of Parameters of Enhanced A5/1," *International Journal of Computer Applications*, vol. 2(2), pp. 7–13, 2011.

[18] D. Upadhyay, P. Sharma and S. Valiveti, "Randomness Analysis of A5/1 Stream Cipher for Secure Mobile Communication," *International Journal on Soft Computing (IJSC)*, vol. 5(March-September), pp. 95–100, 2014.

[19] N. H. Zakaria, K. Seman, and I. Abdullah, "Modified A5/1 Based Stream Cipher for Secured GSM Communication," *International Journal of Computer Science and Network Security* (IJCSNS), vol. 11(2), pp. 223–226. 2011.

[20] Wijesinghe, W., Jayananda, M., & Sonnadara, D. "Hardware Implementation of Randon Number Generators". In *Proceedings of the Technical Session*, 22, pp. 28-38, 2006. Retrieved from http://www.ip-sl.org/procs/ipsl063.pdf.

[21] Paar, C., & Pelzl, J. "Stream Cipher", *Understanding Cryptography*, pp 29-55, 2010. Retrieved from http://doi.org/10.1007/978-3-642-04101-3.

[22] Ericson. "Ericson Mobility Report," (June), 1–32, 2014.

[23] M. Bakhtiari and M. Aizaini, "An Efficient Stream Cipher Algorithm for Data Encryption," *International Journal of Computer Science Issues*, Vol. 8 (3), pp. 247–253, 2011

[24] S. Fauzi, M. Othman, F. M. Shuib and K. Seman, "Improving GSM Security by Enhancing the Randomness Property of the A51 Design," *Australian Journal of Basic and Applied Science*, vol. 9(32), pp. 209–214. 2015.

[25] S. Fauzi, K. Seman and M. Othman, "Design of FPGA- based Modified A5/1 Stream Ciphers, 1–5, 2015

[26] H. A. Wahab and M. A. Mohammed, "Improvement A5/1 Encryption Algorithm Based On Sponge Techniques," *IEEE*, pp. 2–6, 2015.

[27] N H. L. @ A. Zawawi, K. Seman and N. J. M. Zaizi, "A New Proposed Design of a Stream Cipher Algorithm : Modified Grain - 128," *International Journal of Computer and Information Technology*, vol. 3(5), pp. 902–908, 2014.

[28] A. Rukhin, J. Soto, J. Nechvatal, S. Miles, E. Barker, et al. "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *National Institute of Standards and Technology*, vol. 800(22), 131 pages, 2001.

[29] J. Zaman, and R. Ghosh, "Review on fifteen Statistical Tests proposed by NIST," *Journal of Theoretical Physics and Cryptography*, vol. 1, pp. 18–31, 2012.