

International Conference on Communication, Management and Information Technology (ICCMIT 2015)

Simulink Based Implementation of Developed A5/1 Stream Cipher Cryptosystems

Sattar B. Sadkhan^a, Nibras Hadi Jawad^{b*}

^aUniversity of Babylon- College of Information Technology- Babylon-Iraq

^bUniversity of Al-Qadisiya - College of Education- Al-Qadisiya- Iraq

Abstract

The major aim of this paper is to develop GSM networks security by working on improving of one of the elements of the GSM networks security which is A5/1 encryption algorithm. Since the development facilities of the MATLAB. Process depends on improving the implementation of clocking unit, change the implementation method of the majority function, increase the length of the key stream generator, decrease the time of computation, increase of entropy and develop the link of second register by avoiding three weaknesses that observed by Biham and Barkan in A5/1 in 2005 in the binding process, these processes are very important to increase the randomness of key stream generator and generate force key stream specifically by the used SIMULINK environment.

According to our knowledge, this is the first time to develop a SIMULINK approach for realization the proposed developments of A5/1, and testing their validity of actual application in the real such field. Since the hardware realization is one of the great challenges facing the researchers working in the software field after finishing their implementation of their proposed software development. According to our opinion, this work in such approach offers the following: crossing the barrier separating the software specialists and hardware specialists, offering good background of hardware knowledge to the computer specialists working with this design of a developed key generator or cryptosystem, and offer great trust that the results of the developed algorithms can be applied without any obstacles.

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>).

Peer-review under responsibility of Universal Society for Applied Research

*E-mail address: drengsattar@gmail.com

*E-mail address: st.nibras_hadi@yahoo.com

Keywords: GSM, Encryption, A5/1 stream cipher, Clocking Unit, SIMULINK, Develop, Statistical testing.

1. Introduction

GSM (global system for mobile communications) is called 2G or Second Generation technology. It is developed to make use of same subscriber units or mobile phone terminals throughout the world. There are various GSM standards such as GSM900, EGSM900, GSM1800 and GSM 1900; they mainly differ based on RF carrier frequency band and bandwidth. In 1991 the first GSM based networks commenced operations [1] [2].

A5/1 is a strong version but exhibit weaker due to cryptanalysis. A5/1 based on stream ciphering [3] that is very fast. A5/1 made up of using linear feedback shift register. Initial value of LFSR is called seeds because operation of the LFSRs [4] is deterministic stream values produced by LFSRs is completely determined by its current or previous state. However, LFSR the well-chosen feedback function can produce a sequence of bits which appear random and which has long cycle [5].

GSM Networks need to protect communications by securing them from the risk of theft and eavesdropping, not surprisingly one of the components of the security of the GSM network is the encryption algorithm used to encrypt communications is A5 and implementing several versions. A5/0 which does not have encryption used in countries that have high international sanctions, A5/1 is powerful but specific, A5/2 is weak, and A5/3 is strong [6].

Feedback shift registers is basic building block for many cryptographic primitive. Due to insecurities with LFSRs systems, the use of unit delays becomes very popular. In this paper, an develop structure for A5/1 is proposed. This modification performed on LFSRs through adding (unit delay) to the shift register of LFSR used in original A5/1.

This paper is organized as follows. In section 2 the related work was given. In section 3 description of A5/1 and description of case study of its simulation implementation. While in section 4 a description of developed A5/1 and results analysis was given a comparison between existing A5/1 and modified with using statistical test. Section 5 the important conclusion & future work.

2. Related work

- **Partrik E. and Thomas J. (2002) [7]**, Alex B., et al. [8] Proposed a developed on attack method presented by others, their proposed attack not depend on a time–memory tradeoff is based on an identified correlation.
- **Komninos N., et al. (2002) [9]**, Proposed enhancements to A5/1 encryption algorithm from the (biased birthday attack) and (random subgraph attack). The developments were based on the clocking mechanism of the registers.
- **Imran E. and Emin A. (2005) [10]**, Proposed a modified version of the A5/1 and A5/2 with offering security developments s to the vulnerabilities of the algorithms. The modification was made by just changing the clocking mechanism of the proposed algorithm.
- **David H. and Richard G. (2006) [11]**, Proposed development to the A5/1 stream cipher. A development in security is obtained by introducing dynamic polynomial switching in the LFSRs present in the architecture for pseudo noise sequence generation.
- **Hadi K., et al. (2010) [12]**, Developed an attack on A5/1 that was produced by Maximov, et al. a correlation attack on A5/1. The developed depend on the three weaknesses were found in the A5/1, observed by B. Barkan, they used in developed an attack and by employing graph theory for decoding the estimators.
- **Musheer A. and Izharuddin (2010) [13]**, Enhanced version of A5/1 algorithm. The enhancements were done to mainly develop the clocking mechanism and the combining function of A5/1.
- **Hossein K., et al. (2010) [14]**, Development in biased birthday attack, developd the collision probability that was introduced without changing in the available memory capacity. The approach of their suggestion is based on using multiple data patterns instead of using a single one.

- **Nikesh B. (2011) [15]**, Enhanced the A5/1 through analysis of A5/1 using different Parameters, enhanced was done in two ways. firstly , the feedback tapping mechanism was enhanced by variable taps for LFSRs and random shuffling of LFSRs. Secondly, clocking rule, where that the probability is that any LFSR will clocked (shifted) was 75%, and enhancement reduces the probability to 50%.

3. The A5/1 Stream Cipher

3.1. A5/1 encryption algorithm used for encryption of conversations on GSM mobile phones. This algorithm in its structure depends on the stream cipher that is very fast doing bit by bit XOR. It consists of three linear feedback shift registers (R1, R2 and R3) with a method of majority clocking with total length about 64 bits, and can produce a sequence of bits randomly and have along cycle [16]. And this result of bits in frame of 228 bits is added to encryption plain text, conversations in GSM which are in the form of frames of length of 228 bit to output cipher text [16].

A5/1 consists of three linear feedback shift registers which are (R1, R2 and R3) with lengths are 19 bits, 22 bits and 23 bits, used to produce a sequence of binary bits, with The three registers are maximal length LFSRs with periods $(2^{19} - 1)$, $(2^{22} - 1)$, and $(2^{23} - 1)$ respectively [17].

Will select tap bits to primitive polynomial from three LFSR are:

R1: 18, 17, 16, 13

R2: 21, 20

R3: 22, 21, 20, 7

3.2. Clocking unit applied on the three LFSRs, it tacks one bit from each register to compute clocking depend on the majority function. The **majority function** is a function from (n) inputs to one output. The value of the result is one or zero, when at least $n/2$ arguments are one, and zero otherwise [17], the majority function $F(x_1, x_2, x_3) = (y_1, y_2, y_3)$ is defined by the Table (1). The clocking bits selected for majority function are: bit 8 for R1, bit 10 for R2, and bit 10 for R3 [18].

Table 1: majority function in A5/1

Clocking bit (x_1, x_2, x_3)			Majority function	$F(x_1, x_2, x_3) = (y_1, y_2, y_3)$		
R1	R2	R3		R1	R2	R3
0	0	0	0	1	1	1
0	0	1	0	1	1	0
0	1	0	0	1	0	1
0	1	1	1	0	1	1
1	0	0	0	0	1	1
1	0	1	1	1	0	1
1	1	0	1	1	1	0
1	1	1	1	1	1	1

We will illustrate the diagram of A5/1 generator, see in Fig. (1).

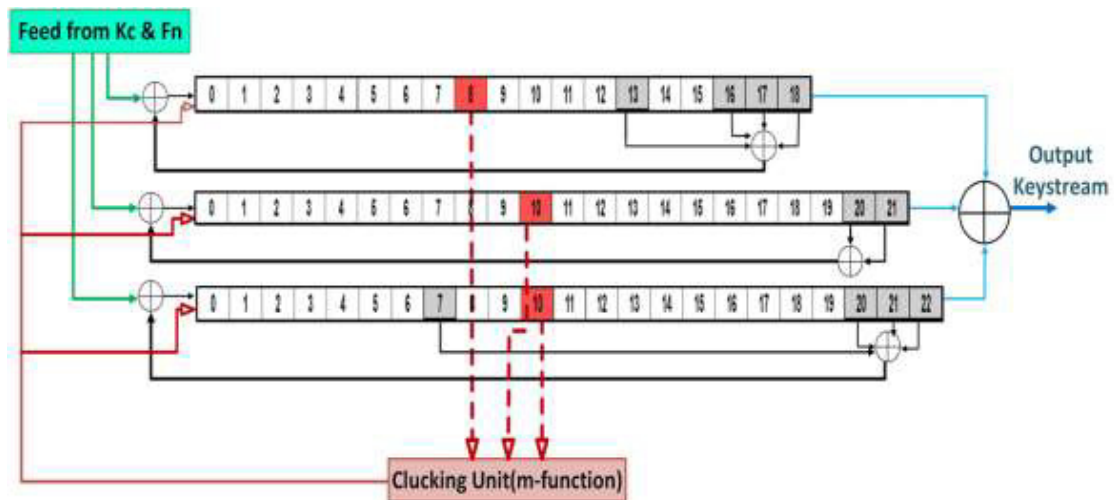


Fig. 1. Structure of A5/1 generator

3.3. Case Study of A5/1 Simulation

An algorithm A5/1 contains three registers sequentially (R1, R2, R3), with lengths 19, 22 and 23. Will be the highest period for the first register with length of $2^{19}-1=524287$ and the highest period for the second register is $2^{22}-1=4194303$ and the highest period for the third register is $2^{23}-1=4294967295$. namely that the length of the overall key stream generated is (9444712697346243690495) including the numbers you are dealing with an algorithm A5/1 is very large and we are unable to deal with and hard to follow key stream generated with this length, so we propose a case study, to minimize of the algorithm A5/1 to be able to calculate the key stream generated and dealing with algorithm A5/1. We will call this case study of A5/1 with A5/1c in order to distinguish between the case study and the original algorithm.

Case study which we have proposed will be as follows:

- 1- The first register (R1) consists of three bits, the taping bits of R1 are at bit positions 1 and 3, after making sure they give a complete period $2^3-1=7$ and the clocking bit for clocking unit is the second bit
- 2- The second register (R2) consists of three bits, the taping bits of R2 are at bit positions 2 and 3, after making sure they give a complete period $2^3-1=7$ and the clocking bit for clocking unit is the third bit
- 3- The third register (R3) consists of four bits, the taping bits of R3 are at bit positions 3 and 4, after making sure they give a complete period $2^4-1=15$ and the clocking bit for clocking unit is the second bit
- 4- Clocking unit has remained as it is because it receives the signal from the three bits, one bit from each register are as follows:
 - Clocking bit to R1 : 1
 - Clocking bit to R2 : 1
 - Clocking bit to R3 : 3

After connecting the case study A5/1c and implementation it as follows:

Generated key stream length is 19 and is much less than the length of the period of the supposed total key stream and which should be 735 bits from $(7 * 7 * 15)$, and because the work in the clocking unit which gives signal stop for the registers at that moment which leading to adoption of the generator on the two or three registers, which stream generation ,

3.4. Problem Statement

We have A5/1 encryption algorithm , its used in communication of mobiles , must be the more save ,security and fast . We have some weakness in the A5/1 encryption algorithm, we want processing these weakness, there are :

Increase length of the key stream generation , decrease the time of computation, increase of entropy , change the implementation method of the majority function in clocking unit and avoiding three weaknesses to increase length of key stream generator and randomness that observed by Biham and Barkan in A5/1 in 2005[19].

4. Developed A5/1

4.1. Implementation Using SIMULINK

The proposed development has been implemented on a case study, where the lengths of shift registers in the proposed case study are (3, 3, and 4). In the algorithm the "original unit" the delay depends on three bits (one bit from each register) to be used as clocking to generate a signal shifting for three used shift registers in the original unit. while the proposed development based on the four bits, each bit from separate shift register.

The development in clocking unit is shown Fig. (2):

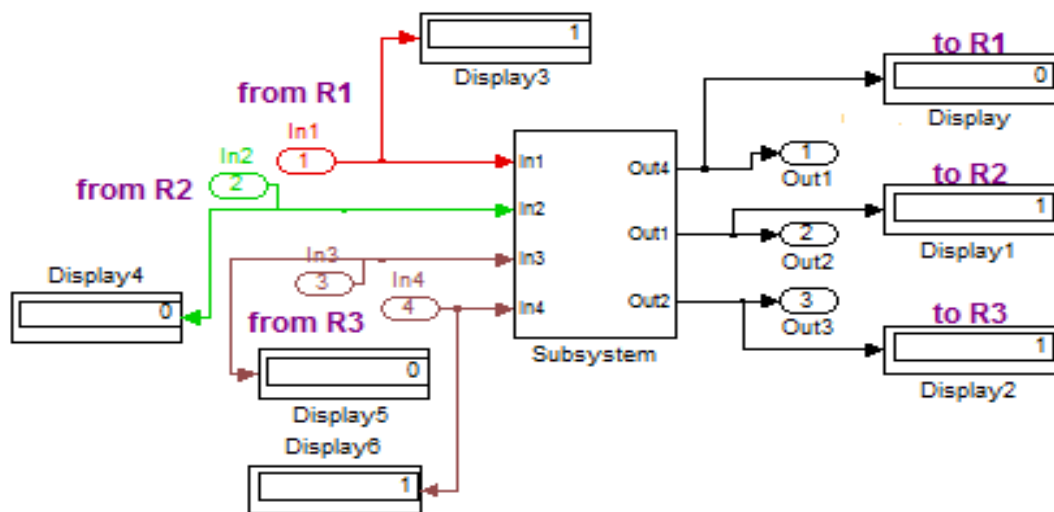


Fig. 2. The development in clocking unit

The work of the majority function will based on comparing the signal comes from:

1. The first register (**first bit**) let $u1$ with the signal comes from the third register (**third bit**) let $u2$.
2. The signal that comes from the second register (**first bit**) let $u3$ with the signal that comes from the third register (**first bit**) let $u4$ with the addition of the (not) to output of the first bit in the third register to reverse of its signal.
3. Check if $(u1 = u2 \ \& \ u3 = u4)$ then : the signal of the clocking unit to all registers are 1. e.g. 1010 $\rightarrow$ 111.
4. Check if $(u1 \sim u2 \ \& \ u3 \sim u4)$ then: the signal of the clocking unit to all registers are invers the input signals. e.g. 1100 $\rightarrow$ 001.
5. Check if $(u1 \sim u2 \ \& \ u3 = u4)$ then : the signal of the clocking unit to the first register is invers the input signal ($u1$), and the signal of the clocking unit to the second register is 1, and the signal of the clocking unit to the third register is invers the input signal ($u2$). e.g. 0010 $\rightarrow$ 010.
6. Check (if $u1 = u2 \ \& \ u3 \sim u4$) then: the signal of the clocking unit to the first register and third register are 1, the signal of the clocking unit to the second register is invers the input signal ($u3$). e.g. 1011 $\rightarrow$ 101.

Table (2) shows the work as follows:

Table (2) Majority function developed in A5/1

Clocking bit(input to MF. from each register)				(output from MF. to each register)		
R1(2)	R3(3)	R2(2)	R3(1)	R1	R2	R3
0	0	0	0	1	1	1
0	1	0	0	1	1	0
0	0	1	0	1	0	1
0	1	1	0	1	0	0
1	0	0	0	0	1	1
1	1	0	0	1	1	1
1	0	1	0	0	0	1
1	1	1	0	1	0	1
0	0	0	1	1	1	1
0	1	0	1	1	1	0
0	0	1	1	1	1	1
0	1	1	1	1	1	0
1	0	0	1	0	1	1
1	1	0	1	1	1	1
1	0	1	1	0	1	1
1	1	1	1	1	1	1

Example:

Suppose that the signal of the first register is 0, the signal of the second register is 0, the signal of the third register (third bit) is 1, and the signal of the third register (first bit) is 0, where will compare the signal of the (second bit) from the first register, which is 0 with the (third bit) from the third register, which is 1 if equal the signals then gives reference 1 and The different will give the invers signal, including that signals different unequal will be the value of the signal to the first register is 1, reverse signal previous, the of signal third register is 0 reverse signal previous (where the signal of the third register will depend on the value of the third bit in the third register in identifying signal value).

As for the signal of the second register will compare the signal of (second bit) from the second register which is 0 with the (first bit) from the third register, which is 0, since the signals are equals in the values, then the signal of the second register is 1 and so on.

Depending on three weakness that observed by Biham and Barkan in A5/1 in 2005[19] are:

- 1- The first weakness of R2 is the fact that the feedback taps of R2 coincide with the bits that are estimated by the correlation equation.
- 2- The second weakness of R2 is that it has only two feedback taps, and these taps are adjacent.
- 3- The third weakness of R2 is that its clock tap is exactly in its center of LFSR.

Implementation of the development in the second register avoiding weakness where illustrate in Fig. (3) the diagram of A5/1 generator development:



Fig. 3. Structure of A5/1 developed generator

4.2. Results:

In this sub section explores the comparison of A5/1c (original) and modified A5/1c (proposed). After implementation of both existing and modified A5/1 algorithms they are with statistical Tests Suite [20] [21].

From the experiment, it is noticed that developed case is acceptable in terms of the statistical tests, where the result appear all within the specified domain, For a significance level of $\alpha = 0.05$, the threshold values F, S, R, P and A are 3:8415, 5:9915, 14:0671, 9:4877, and 1:96, respectively. Developed case is non-linear because the key stream generated for all cases the number of zeros is not equal to the number of one depending on the frequency test. Good results for random.

The execution time is measured per second and since that time the implementation of the algorithm is less than a second. It is shown that the times of execution developed case and original case are equal, so we measured the time of computation in period of 150,000 to see the difference between them.

The developed case is compare with original case in terms of the parameters we have chosen to select the most efficient development, the parameters are time of computation, key length and entropy test, as follows:

1. Time of computation:

The implementation of the developed case is less than the original case, because period 150,000 took 3 seconds, where the original case took 5 second, as shown in table (3), in column (Time of computation).

2. Key length:

Along generated key stream for the original case is 19, while the length of the generated key stream for developed case, the generated key stream length is 80 higher than the original case. As shown in table (3), in column (Key length).

3. Entropy test:

It is clear that the entropy in the developed case is less than the original case, as shown in Table (3), in column (E). As shown in table (3), in column (Entropy test).

It is noted that all the results of developed case are good cryptography randomness so the development can be adopted in developed case.

Table (3) results of tests

	Key length	Time of comp.	Clocking length	Entropy test	Poker test	Run test	Autoc. test	Freq. test	Serial test
Or	19	5 sec	19	0.1914	7.3333	1.9620	0.4737	0.0526	0.1696
Dv	68	3sec	68	0.0730	8.1818	1.9207	0.5294	2.6081	0.9412

Or: original case, Dv: developed case, comp: computation, Autoc: Autocorrelation, Freq: Frequency

5. Conclusion & future work

A5/1 main used for secure communication in mobile network. A5/1 key stream generator is easy to implement and also efficient encryption algorithm used in communication of GSM. The encryption method uses the selective encryption approach where the coefficients selection. That done on MATLAB (R2013a) as result obtained in form of graph. After try to find A5/1 weakness. So, it exhibit weakness like length of LFSRs is short and basic correlation attack. After analysis these things decreased the possibility of correlation attack. A5/1 modified structure has been given which is easy to implement and fast to do. We have proposed a case study to be able to study and follow-up key stream length. The proposed structure is depends on improving the implementation of clocking unit, change the implementation method of the majority function, and develop the link of second register, avoiding three weaknesses to increase length of key stream generator and randomness. This paper proposes a high speed and minimum cost A5/1 key stream algorithms.

Suggestions for Future Works, Determine the mechanism for the appointment of the beginning of the generated key after the completion of the algorithm from initialization of registers.

References

1. Magnus G., Kristian H., Espen H. *Decoding GSM*. Master of Science in Communication Technology; 2010. p. 1-217.
2. Lachu A., Stefano F., Risto M., Basavaraj P., Yousuf S., Sarvesh S., Srinivas S. *Getting to Know Wireless Networks and Technology*; 2003. p.1-13.
3. Elad B., Eli B. *Instant cipher text-only cryptanalysis of GSM encrypted communication*. citeseerx library; 2004. p. 1-18.
4. Patrik E. *On LFSR based stream cipher, analysis and design*; 2003. p.1-157.
5. David M. *GSM Security and Encryption*” George Mason University; 1996. p. 1-16.
6. Yu L. *short Message Service (SMS) Security Solution for Mobile Devices*. M.Sc. thesis, Naval Postgraduate School, Monterey, California; 2006. p. 1-95.
7. Patrik E. and Thomas J. *Another Attack on A5/1*. IEEE Transactions on Information Theory, Vol. 49, No. 1; 2003. p. 284-289.
8. Alex B., Adi S. and David W. *Real Time Cryptanalysis of A5/1 on a PC*. cryptome library. 2000. p. 1-16.
9. Komninos N., Honary B. and Darnell M. *Security Enhancements for A5/1 Without Losing Hardware Efficiency in Future Mobile Systems*. Lancaster University (UK); 2002. p. 1-7.
10. Imran E. and Emin A. *A Modified Stream Generator for the GSM Encryption Algorithms A5/1 and A5/2*. citeseerx library; 2005. p. 1-4.
11. David H. and Richard G. *A Novel Stream Cipher for Cryptographic Applications*. IEEE library; 2006. p. 1-5.
12. Hadi K., Mahmoud A. and Behrouz H. *The New Results of Correlation Attack on A5/1*. IEEE library; 2010. p. 1-6.
13. Musheer A. and Izharuddin. *Randomness Evaluation of Stream Cipher for Secure Mobile Communication*. Proceedings of the 1st International Conference on Parallel, Distributed and Grid Computing (PDGC-2010), 978-1-4244-7674-9/10/\$26.00 ©2010 IEEE; 2010. p.180-183.
14. Hossein K., Hamidreza T. and Majid N. *An Improvement of Collision Probability in Biased Birthday Attack Against A5/1 Stream Cipher*.978-1-4244-6001-4/10/© IEEE; 2010. p. 444-448.
15. Nikesh B. *Effects of Parameters of Enhanced A5/1*. Evolution in Networks and Computer Communications A Special Issue from IJCA journal; 2011. p. 7-13.
16. Chen L. and Gong G. *Communication Systems Security, Appendix B. Design of Stream Ciphers*. Communication Systems Security, Appendix B, Draft, L. Chen and G. Gong; 2008. p. 1-17.
17. Jay S., Ayan M. *A New Guess-and-Determine Attack on the A5/1 Stream Cipher*; 2009. p. 1-14.
18. Timo G. *Hardware-Based Cryptanalysis of the GSM A5/1 Encryption Algorithm*. researchgate library; 2008. p. 1-59.
19. Elad B., Eli B. *An Effective Attack on A5/1*. Springer-Verlag. Volume 1, Issue 3, 2005. p. 159-176,
20. Dhilal M. *Security Evaluation of Cryptosystem Based on Information Theory*. Master of Science in computer Science, university of Babylon; 2013. p.1-120.
21. Menezes A. and vanOorschot P., Vanstone S. *Handbook of Applied Cryptography*. citeseerx library; 1997. p. 169-190.