AL-Qadisiyha Journal For Science Vol.19 No. 3 Year 2014
Sattar B.Sadkhan\ Nibras Hadi Jawad ISSN 1997-2490

*Improvement of A5/1 encryption algorithm based on Using Unit Delay

Received : 16\1\2014 Accepted : 9\3\2014

Sattar B. Sadkhan

Iraq- University of Babylon- College of Information Technology

Nibras Hadi Jawad

University of Babylon- College of Sciences

St.nibras_hadi@yahoo.com

Abstract :

The authentication and the security mechanism are very important in mobile networks because the GSM networks are susceptible to many attacks aiming to penetrate the conversation and access to data transmitted through the network. The GSM security and encryption algorithms are used to provide authentication and radio link privacy to users on GSM network. Encryption algorithm is one of the elements of the GSM networks security where it depends on the encryption algorithm A5/1. A5/1 is strong 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, where the sequence key generated must have large period, and good statistical properties. The aim of this paper is to improve GSM network security by improving one of the components of the GSM network security which is A5/1encryption algorithm, with applying (unit delay) to increase length of generated key stream sequence. The Simulation of A5/1 encryption algorithm was implemented in SIMULINK.

Keywords: GSM, Encryption, A5/1 stream cipher, Clock Controlling Unit, Unit delay, 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

***The Research is apart of on MSC. Thesis in the case of the First researcher**

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 improve 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 Unit Delay. While in section **4** a description of case study of its simulation implementation. In section **5** a description of improved A5/1 and results analysis was given a comparison between existing A5/1 and modified with using statistical test. Section **6** the important conclusion.

2. Related work

- **Partrik E. and Thomas J. (2002) [7],** Biryukov, at el….. [8] Proposed attack on the A5/1, which can break A5/1 in seconds using huge precomputation time and memory. Whereas time–memory tradeoff attacks have a complexity which was exponential with the shift-register length. Partrik E. and Thomas J. [9] proposed adeveloped attack method based on the attack method given by Biryukov, at el….. [8], their proposed [9] based on an identified correlation. The complexity of the proposed attack was almost independent of the shift-register length. Their Proposed attack not depend on a time–memory tradeoff, but used completely different properties of the cipher. It explored the weak key initialization which allowed the separation the session key from the frame number in binary linear expressions. The complexity of the proposed attack was only linear in the length of the shift registers based on the number of irregular clocking's before the key stream was produced. The proposed attack was implementation in a few minutes (2 up to 5) minutes.

- **Komninos N. , at el….. (2002) [10],** Proposed security enhancements to improve A5/1 encryption algorithm from the (biased birthday attack) and (random subgraph attack). The improvements that made both attacks impractical based on the clocking mechanism of the registers. It based on implementation of majority function in the clocking unit and select two tap bits from each register instead of one bit, and their key setup routine. The session key was mixed with the frame counter in a random way which made it difficult to be extracted from the initial state. Furthermore, they increased the linear complexity of A5/1 to make the solution of the linear equations impractical in real time systems. Both original algorithm and modified algorithm of A5/1 were implemented in a complex programmable logic device (CPLD) device for 3Rd generation mobile systems.

- **Mi-Og P. , at el….. (2004) [11],** they proposed a new mechanism to made unsafe A5 algorithm secure, which was a stream cipher in GSM system. Proposed mechanism used some 4x16 s-boxes only if bit was 0, s-box decision method and s-box rowcolumn method in order to achieve proposed mechanism. In s-box passed step, proposed s-box decision method decides to the order of s-box to use among s-boxes. Proposed s-box rowcolnmn method decides certain row and column to use. By analyzed test results, they proved the proposed model has better randomness and serial correlation characteristic than A5.

- **Imran E. and Emin A. (2005) [12]**, Proposed a modified versions of the A5/1 and A5/2 with offering security improvements to the vulnerabilities of the algorithms. The LFSR's and primitive polynomials of the proposed algorithms were the same as those of A5/2. The modification was by just changing the clocking mechanism of the proposed algorithm. They

applied some known attacks on the proposed algorithm with respect to the stream generator to show its security enhancements. The proposed generator provided a cryptographically more secure stream cipher with respect to some popular attacks as "divide and conquer" and "time memory trade-off". Furthermore, the period of the proposed generator was higher compared to A5/1. This was a considered as a good design characteristic for a stream generator.

- **Mohamed S. , at el….. (2005) [13]**, They proposed an algorithm instead of A5 algorithm used in GSM networks. They proposed the inverse taps of the standard LFSR were used to generate the output key-stream bits. The proposed LFSR design called a complex LFSR. The performance of the inverse taps and the Complex LFSR has been assessed using the NlST suite of statistical tests and demonstrates good cryptographic randomness. The proposed LFSR design can be effectively applied in software or hardware to provide a low cost and high speed encryption capability.

- **Hadi K. , at el….. (2010) [14]**, Proposed the improved attack on A5/1 that was in produced by Maximov, Johansson and Babbage a correlation attack on A5/1 in 2005 [15]. Improved attack depend on three weaknesses that observed by Bihamand Barkan in A5/1 in 2005 [9] and by employing graph theory for decoding the estimators. The comparison between the previous work of the [15] and the proposed improved attack, showed good results in proposed improved attack.

- **Musheer A. and Izharuddin (2010) [16]**, Proposed enhanced version of A5/1 algorithm. The enhancements were done to mainly improve the clocking mechanism and the combining function of A5/1. They noted that the clocking unit was more irregular in the proposed scheme and uses two different rules to clock the registers. Two nonlinear combining functions were employed that dynamically switch to each other. It has been demonstrated that the proposed enhancements exhibit excellent statistical properties. Based on the statistical results, they conclude that the proposed scheme has much better performance in terms of randomness than the A5/1 stream cipher used in GSM.

- **Nikesh B. (2011) [17],** Proposed enhanced to A5/1 algorithm through analysis A5/1 with used different Parameters, enhanced was done in two ways (first way) feedback tapping mechanism which was enhanced by variable taps for LFSRs and random shuffling of LFSRs, which increases the complexity of the algorithm without compromis the properties of randomness and (second way) clocking rule, where that the probability that any LFSR will clocked (shifted) was ¾ which was 75% probability that any LFSR (R1, R2 or R3) will be clocked, an enhanced was reduce the probability to 50%. The modification has been proposed keeping the ease of implementation in mind. It was observed that the changing of feedback taps and the shuffling of LFSRs was an effective to make the generator stronger. Cryptanalyst has to identify four feedback polynomials instead of one for each LFSR. This generator was also robust to Berleykamp Massey attack. Algorithm become more complex to break due to introduced shuffling of LFSRs. Though algorithm became complex but it was easy to realize. Based on the observations and results, it can be concluded that the proposed scheme was robust to the cryptographic attacks compare to the conventional A5/1 stream cipher. Hence the proposed scheme generates cryptographically better binary sequence than the A5/1 stream cipher of GSM with minor increase in the hardware.

3. The A5/1

- **A5/1 is encryption algorithm** used to encrypt 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 is consist from three linear feedback shift registers (R1, R2 and R3) with method of majority clocking with total length are 64 bits, can produce a sequence of bits which appear random and has along cycle. And add this result of bits in frame of 228 bits to encryption plain text, conversations in GSM are in the form of frames as length of 228 bit to output cipher text [1][18].

A5/1 is 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 [19].

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

R1: 18, 17, 16, 13

R2: 21, 20

R3: 22, 21, 20, 7

Clocking control applied on the three LFSRs, it tackes 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 [19], the majority function F(x1,x2,x3) = (y1,y2,y3) 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 [20].

Table 1: majority function in A5/1

Clocking bit (x_1,x_2,x_3)			Majority function	$F(x_1,x_2,x_3)=(y_1,y_2,y_3)$		
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 in figure (1) the diagram of A5/1 generator.

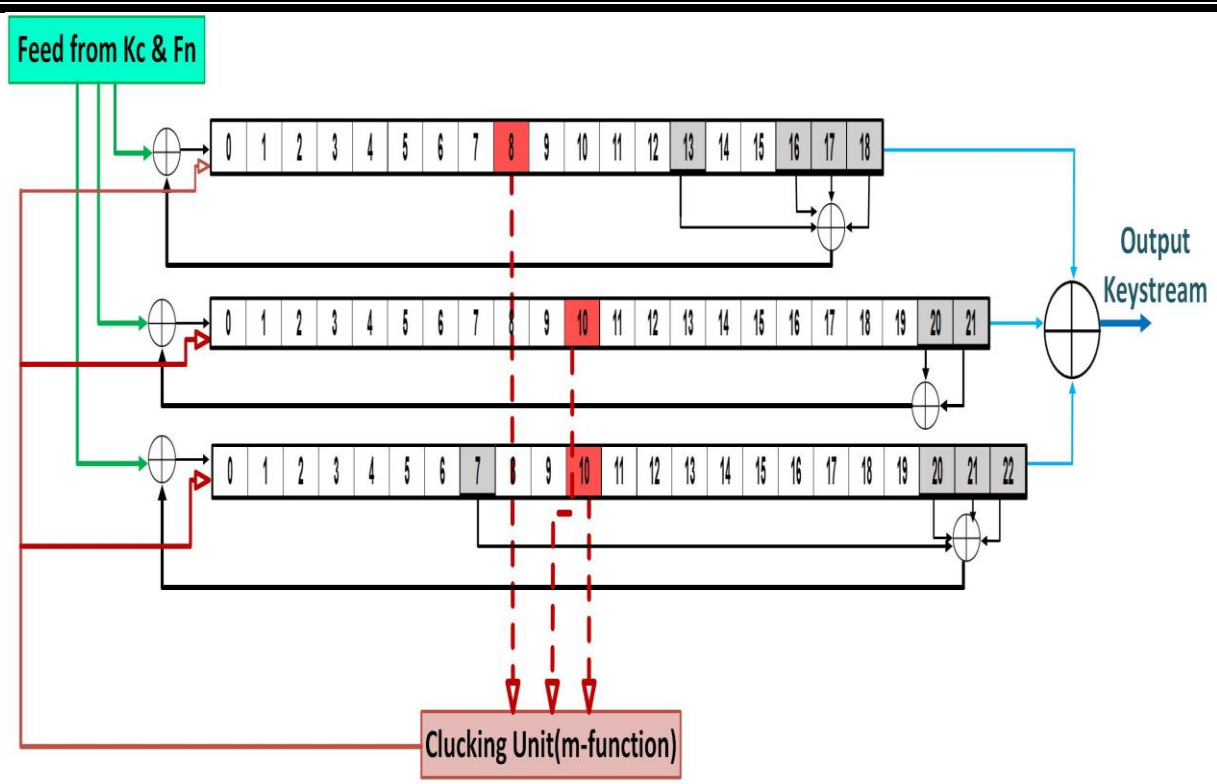

Figure (1) structure of A5/1 generator

The steps of algorithm of the A5/1 algorithm go as follows from initialization to 228-bits of key stream [1]:

Step1. All three registers are set to 0.

$R1 = R2 = R3 = 0$

Step2.the key with a size of 64 bits is put into all registers simultaneously. Then, for 64 cycles, the key is mixed into the registers in parallel using the following algorithm:

For *i* = 0 to 63 do

$R1[0] = R1[0] \oplus Kc[i]$

$R2[0] = R2[0] \oplus Kc[i]$

$R3[0] = R3[0] \oplus Kc[i]$

Clock all three registers ignoring the stop/go clocking unit

End for

Step3. the registers are clocked as usual .then the 22 bit frame number of the GSM frame is inserted into the registers in the same way, 22 addition cycles are clocked, still overlooking the majority function. During this period the frame number is XORed into the l select bit of the registers in the same way as with the key, that is:

For i = 0 to 21 do

$R1[0] = R1[0] \oplus COUNT[i]$

$R2[0] = R2[0] \oplus COUNT[i]$

$R3[0] = R3[0] \oplus COUNT[i]$

Clock all three registers ignoring the stop/go clocking unit

End for

Step4. For i = 0 to 99 do

$$z = R1[cb_8] \oplus R2[cb_{10}] \oplus R3[cb_{10}]$$

If $R1[cb_8]$ = z then
$Clock_1=1$
Else
$Clock_1=0$
If $R2[cb_{10}]$ = z then
$Clock_2=1$
Else
$Clock_2=0$
If $R3[cb_{10}]$ = z then
$Clock_3=1$
Else
$Clock_3=0$

Discard the first 100 bits of the key-stream, 100 additional clocks are performed with the regular majority clocking mechanism activated, but the output is discarded. The content of the registers at the end of this state is what we refer to as the initial state of A5/1.

Step5. 228 bits (clocks) are performed to produce 228 bits of key stream. 114 bits are used to encrypt data from the network to the mobile phone, and the other 114 bits are used to encrypt data from the phone to the network.

- **Unit Delay**

The Unit Delay block delays its input by the specified sample period. The unit accepts one input and generates one output, which can be either both scalar or both vector. If the input is a vector, all elements of the vector are delayed by the same sample period. We specify the block output for the first sampling period with the Initial conditions parameter. Careful selection of this parameter can minimize unwanted output behavior. The time between samples is specified with the sample time parameter [21].

4. Simulation

a- The Case Study

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= 7 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 : 2
- 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 leading to increase the sequence of the key stream generated.

5. Improved A5/1

a- Implementation of Using Simulink

Addition two from (unit delay) to the third register, where its location in the (first) after of XOR which combine FBSR and feeding from session key (Kc) and frame counter (Fn) and the other (second) at output of second bit, as in the figure (2) look at the circle dashed :

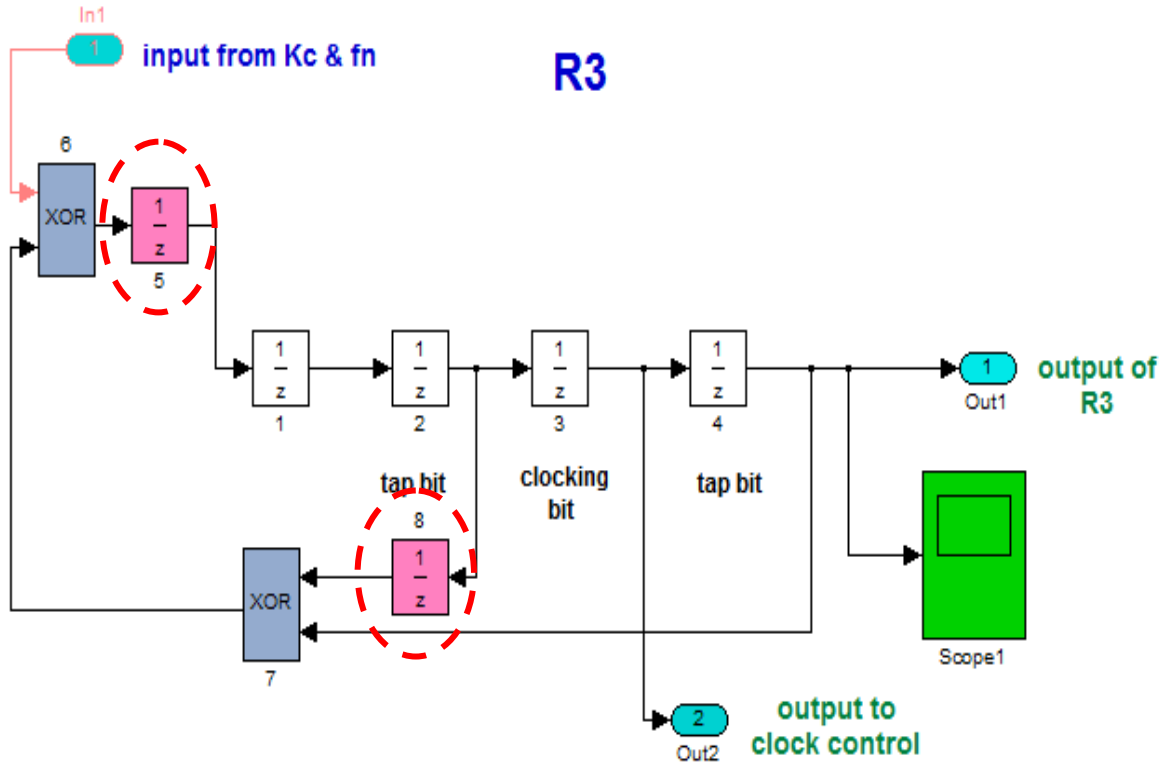

Figure (2) improved in third register in A5/1

We note the key stream generated length is 49 bits, as in the figure (3):

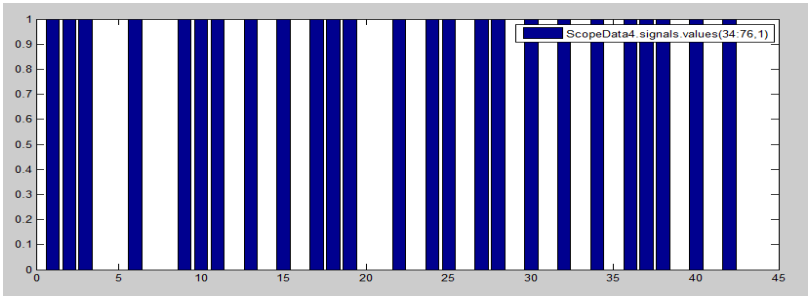

Figure (3) key stream length

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 [22].

From the experiment, it can be seen that modified A5/1, design provides good source of random number for cryptographic purposes.

As in figure (2), the generated key streams of A5/1c came we have tested. The statistical test used as in table (2), Consider **poker test** in this test the let generated random key streams S is divided into k = n/m non-overlapping parts each of length m, where m be a positive integer such that $\lfloor \frac{n}{m} \rfloor \geq 5 \cdot (2^m)$, Let n_i be the number of occurrences of the i^{th} type of key streams of length m, where $1 \leq i \leq 2^m$. The Poker test determines the key streams of length m, each appear approximately the same number of times in S [23]. **Runs Test** in this test, we determine whether the number of runs of various lengths in the key streams S is as expected in the random key streams [24]. **Serial Test** (two bit test) in this test, we determine whether the number of occurrences of 00, 01, 10 and 11 as subsequences of random key streams S are approximately the same, as would be expected for a random key streams. **Frequency Test** (mono bit test) in this test, we determine the number of zeros and ones in the generated random key streams [24]. **Autocorrelation Test** in this test the correlations between the key streams S and its (non-cyclic) shifted version are checked [24]. **Entropy test** it is clear that the entropy in the developed case is less than the original case. As shown in table (2).

Table (2) results of tests

	Poker	7.3333	12.2857	Acceptable
	Run	1.9620	6.2168	Acceptable
	Serial	2.9766	5.9103	Acceptable
	Frequency	2.5789	5.2326	Acceptable
	Entropy	0.1878	0.1021	Acceptable
	Autocorrelation function	0.4737	0.5349	Acceptable
	Length of key stream	19	43	Acceptable
	Run time	5 sec in period 1000	3 sec in period 1000	Acceptable

6. Conclusion

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 used (unit delay) to increase length of key stream generator and randomness. This

paper proposes a high speed and minimum cost A5/1 key stream algorithms but minor increase in hardware.

7. Reference

1- Magnus G., Kristian H., Espen H. **(**2010) ***"Decoding GSM"*** *Master* of Science in Communication Technology, pages (1-217), http://www.divaportal.org/smash/get/diva2:355716/FULLTEXT01.pdf .

2- Lachu A., Stefano F., Risto M. , Basavaraj P. , Yousuf S. , Sarvesh S. , Srinivas S. (2003) ***"Getting to Know Wireless Networks and Technology"*** pages (1-13), http://www.informit.com/articles/article.aspx?p=98132 .

3- Elad B. , Eli B. (2004) ***"Instant cipher text-only cryptanalysis of GSM encrypted communication"*** citeseerx library, pages (1-18), http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.3.7651 .

4- Patrik E. (2003) ***"On LFSR based stream cipher, analysis and design"*** pages (1-164), ftp://ftp.kemt.fei.tuke.sk/KEMT414_AK/_materialy/Cvicenia/GSM/UTOKY/Ekdahl_thesis_E5ref.pdf .

5- David M. **(**1996) ***"GSM Security and Encryption" George Mason University "*** pages (1-17) http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html .

6- Yu L. (2006) ***"short Message Service (SMS) Security Solution for Mobile Devices''*** master's thesis, researchgate library, pages (1-113) https://www.researchgate.net/publication/235046021_Short_Message_Service_(SMS)_Security_Solution_for_Mobile_Devices .

7- Patrik E. , Thomas J. (2002) ***"Another Attack on A5/1"*** citeseerx library, pages (284-289), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.98.8121&rep=rep1&type=pdf.

8- Biryukov A., Adi S. , David W. (2001) ***"Real Time Cryptanalysis of A5/1 on a PC"*** cryptome library, pages (1-16), http://cryptome.org/a51-bsw.htm.

9- Elad B. , Eli B. (2005) ***"Conditional Estimators: An Effective Attack on A5/1"*** pages (1-19), http://dl.acm.org/citation.cfm?id=2180542 .

10- Hadi Khorrami, Mahmoud Ahmadian, BehrouzHajian (2010) ***"The New Results of Correlation Attack on A5/1"*** IEEE library, pages (1-6), http://ieeexplore.ieee.org/xpl/articleDetails.jsp?tp=&arnumber=4685010&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D4685010.

11- Mi-Og P. , Yeon-Hee C. , Moon-Seog J. (2004) ***"Modified A5/1Stream Cipher using S-boxes"*** IEEE library, pages (508-511), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1292921&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F9073%2F28786%2F01292921 .

12- Imran Erguler, and Emin Anarim (2005) ***"A Modified Stream Generator for the GSM Encryption Algorithms A5/1 and A5/2"*** pages (1-4), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.103.9435&rep=rep1&type=pdf.

13- Mohmed S. , Hala A. , HalaH.Zayed, M L Shore (2005) ***"a complex linear feedback shift register design for the A5 key stream generator"*** IEEE library, pages (1-8), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1502156&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D1502156 .

14- Komninos N. , Honary B. , Darnell M. (2002) ***'' Security Enhancements for A5/1 Without Loosing Hardware Efficiency in Future Mobile Systems''*** Lancaster University (UK), pages (1-7), http://openaccess.city.ac.uk/2494/ .

15- Maximov A., Johansson T., and Babbage S. (2005) ***"An Improved Correlation Attack on A5/1"*** pages (1-18), http://books.google.iq/books?id=hty4AMwQrPgC&pg=PA1&lpg=PA1&dq=An+Improved+Correlation+Attack+on+A5/1.+In+Selected+Areas+in+Cryptography&source=bl&ots=_HbA

Vzg37w&sig=QnjUgSd_wpWLLsKbP6d9Q2xx0w&hl=ar&sa=X&ei=fy7mUoqbI8PmywPYj4KwDA&ved=0CE8Q6AEwBA#v=onepage&q=An%20Improved%20Correlation%20Attack%20on%20A5%2F1.%20In%20Selected%20Areas%20in%20Cryptography&f=false .

16- Musheer A. , Izharuddin (2010) ***"Randomness Evaluation of Stream Cipher for Secure Mobile Communication"*** IEEE library, pages (180-183), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5679889&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5679889 .

17- Nikesh B. (2011) ***"Effects of Parameters of Enhanced A5/1"*** researchgate library, pages (7-13), https://www.researchgate.net/publication/230802146_Effects_of_Parameters_of_Enhanced_A51 ,.

18- Chen L. , Gong G**.** (2008) ***"Communication Systems Security, Appendix B. Design of Stream Ciphers"*** pages (1-17), http://www.crcpress.com/product/isbn/9781439840368 .

19- Jay S. , Ayan M. (2009) ***" A New Guess-and-Determine Attack on the A5/1 Stream Cipher''*** pages (1-14), http://eprint.iacr.org/2012/208.pdf .

20- Timo G. (2008) ***"Hardware-Based Cryptanalysis of the GSM A5/1 Encryption Algorithm''*** researchgate library, pages (1-73), https://www.researchgate.net/publication/239923937_HardwareBased_Cryptanalysis_of_the_GSM_A51_Encryption_Algorithm .

21- On line http://www.mathworks.com/help/simulink/.

22- Dhilal M. (2013) ***" Security Evaluation of Cryptosystem Based on Information Theory"*** Master of Science in computer Science, university of Babylon, pages (1-137).

23- Sheena M. , Paulose K. (2005) ***" A New Fast Stream Cipher: MAJE4''*** IEEE library, pages (60-63), http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=1590124&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F10601%2F33509%2F01590124.pdf%3Farnumber%3D1590124 .

24- Menezes A. , vanOorschot P. , Vanstone S. (1997) ***" Handbook of Applied Cryptography''*** citeseerx library, pages (1-794), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.99.2838&rep=rep1&type=pdf .

AL-Qadisiyha Journal For Science Vol.19 No. 3 Year 2014
Sattar B.Sadkhan\ Nibras Hadi Jawad ISSN 1997-2490

*تحسين خوارزمية التشفير A5/1بأستخدام وحدة التاخير

تاريخ الاستلام:16\1\2014 تاريخ القبول :9\3\2014

ستار بدر سدخان
جامعة بابل /كلية تكنولوجيا المعلومات

نبراس هادي جواد
جامعة بابل / كلية العلوم

الخلاصة :

المصادقة و آلية ألامنية مهمة جدا في شبكة الهاتف النقال، حيث ان شبكة GSM عرضة للعديد من الهجمات و اختراق المحادثات و الوصول للبيانات المنقولة عبر الشبكة. تستخدم شبكة GSM الأمنية و خوارزميات التشفير لتوفير مصادقة و سرية روابط النقل الرادوية للمستخدمين على شبكة GSM . خوارزمية التشفير هي إحدى مكونات أمنية شبكات GSM حيث انها تعتمد على خوارزمية التشفير A5/1 وهي ذو هيئة التشفير الانسيابي وهو سريع جدا. وقد اثبتت خوارزمية التشفير A5/1 على مدى قوة و صعوبة التنبأ بالمفتاح السري المتولد والمستخدم لتشفيرالنص الصريح او البيانات المرسلة من خلال الشبكة، حيث يجب أن تكون سلسلة المفتاح المتولد ذو فترة كبيرة ، وذو خصائص إحصائية جيدة. في هذه الورقة تحسين لأمنية شبكة GSM من خلال تحسين واحدة من مكونات امنية الشبكة GSM وهو خوارزميةاتشفير A5/1 ، مع تطبيق (وحدة تأخير) لزيادة طول الفترة لسلسلة المفتاح المتولد. سيتم محاكاة خوارزمية التشفير A5 / 1 واختبار النتائج بواسطة MATLAB / SIMULINK .

***البحث مستل من رسالة ماجستير للباحث الثاني**