International Journal of Networks and Communications 2020, 10(1): 20-32
DOI: 10.5923/j.ijnc.20201001.03

Chao Athentication and Ciphering Approach to Secure Mobile Networks

Ghazli Abdelkader[1,*], Alipacha Adda[2], Hadj Said Naima[2]

[1]Tahri Mohamed University of Bechar, Algeria (Coding and Information Security Laboratory LACOSI)
[2]University of Sciences and Technology of Oran, Algeria (Coding and Information Security Laboratory LACOSI)

Abstract Mobile networks are the most used networks with wide coverage in the world. Recently, mobile phones are used in several fields, financial, sociological, economical, commercial or even medical fields to monitor the health status of patients at a distance as an example by using many sensors implanted in their Smartphones or even they can be used as authorization passports to manage medical crises like the case of Coronavirus (COVID-19), where we have seen several pay developed some applications to manage this so-called global crisis. Security in mobile phone networks it based on two mechanisms that are the authentication of users, and the encryption of the information exchanging between the network devices. However, these algorithms suffer from a lot cryptanalysis. In this paper an extension of GSM authentication protocol and secure pseudo random bit generator based on chaotic systems are proposed to improve some drawbacks of the current GSM authentication protocol and to make mobile phone encryption algorithms robust and resistive to some attacks such as time memory trade off attacks and algebraic attacks. A basic security analysis shows that the authentication protocol does not change the existing architecture of GSM at all and the new chaotic encryption algorithm is more resisters for cryptanalysis with a good quality of bits stream, and for this reason the proposed solution based chao can be used both to reinforce the security of existing architectures such as 2G, 3G and 4G and can even be used to secure new or future architectures such as 5G.

Keywords Mobile Communication, Security, Authentication, Chao, Stream Cipher, A3, A5

1. Introduction

Mobile subscriptions are growing around three percent year on year globally and reached 7.4 billion in Q1 2016. By 2021 there will be 9 billion mobile subscriptions, 7.7 billion mobile broadband subscriptions and 6.3 billion Smartphone subscriptions. [1]

The mobile phones are not used only for communication but also, in a lot of other things such as mobile banking which use the mobile devices like tablets or Smartphones to perform financial transactions.

In 2016, the worlds of mobile email users total over 1.7 billion.

At the end of 2018, worldwide mobile email users will expect more than 2.2 billion due to the large number of mobile devices and 80% of email users will access their email accounts via a mobile device. [2]

The Global System for Mobile Communication GSM is a second generation 2G network and is the most widely used cellular standard in the world.

Many telecommunication companies still use the old standard of GSM because the cost of the new base station as we show in the figure 1. The GSM comprises of several network components that interact and function with each other.

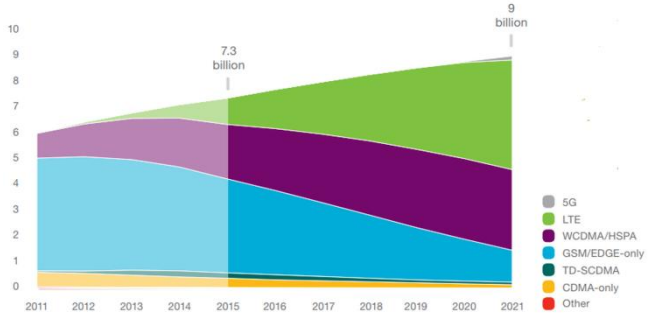

Figure 1. Mobile subscriptions by technology [1]

Generally there are two major security issues in mobile phone communication, authentication and privacy. On the wireless communication, the authentication makes no un-authorized user be able to get required services of an authorized user from the home system.

* Corresponding author:
ghazek@gmail.com (Ghazli Abdelkader)
Published online at http://journal.sapub.org/ijnc

The GSM authentication is based on a challenge/response protocol in which the network sends a challenge to each mobile station MS and the MS must send back an appropriate response. This is a unilateral authentication protocol in which the network cannot be authenticated by the MS.

GSM use A5/x stream generators which is based on Linear Feedback Shift Register LFSRs to secure the user transmitted data, A5/1 is the stronger version and A5/2 is the weaker one.

The encryption and decryption in GSM stream cipher based on XOR operation. The strength and security of these ciphers based of bits sequences produced by the stream generator. [3] A lot of attacks against A5 have been presented in different papers such as algebraic attacks; divide and conquer and time memory trade-off attack. The major issue in A5/1 is the short period problem. In A5/2 version the main problem security is in the mechanism control where one of four registers is used to control the clock mechanism of other registers of A5/2.

In this paper, we propose a new authentication protocol to increases authentication efficiency by introducing a mutual authentication between mobile and the network and also to improve some drawbacks presented in the standard GSM authentication algorithm called A3. In addition a modified version of A5 based chaotic systems called A5C to control the clock of three LFSRs used in A5/1 is presented. our new security mechanism produce a high performance random numbers of no period, which make a lot off attacks impractical and increase the security and degree of complexity of a standard version with a satisfactory statistical test off the key stream sequences.

This paper is organized as follows, section 2 describes the architecture of the GSM network where the basic components of the network are explained. Security in GSM networks is studied in section 3 where the authentication algorithm A3 and the encryption algorithm A5 are illustrated.

Section 4 introduces the chao theory, where the differential equations of the Lorenz attractor are given. A state of the art is presented in section 5 of some GSM improvements authentication and encryption algorithms.

Section 6 describes our new chao based authentication and encryption system to improve security in mobile networks and more specifically that of GSM. A performance and safety analysis of the two proposed algorithms is studied in sections 7, 8 and 9 followed by a synthesis where a comparison of our system with other mechanisms found in the literature is presented. Finally, Section 11 presents our conclusions.

2. Components in GSM Networks

The Global System for Mobile communication GSM is the first global standard for cellular digital radiotelephony, allowing roaming customers in all countries subject to agreements between operators.

In order to the network provide its functionalities and offer services, in addition to the mobile station; it will be composed of several interconnected entities allowing the smooth operation of the mobile network. These entities consist of the following components:

2.1. Mobile Station (MS)

The GSM mobile station (or mobile phone) communicates with other parts of the system through the base-station system.

2.2. Base Station

Is an antenna transmitting and receiving radio signals over a cell in a wireless network. [3]

2.3. Base Station Controller (BSC)

An agent performing functions on behalf of a group of base stations. The BSC handles the allocation of radio channels, controls handovers, performs paging and interfaces with the central network and HLR. [4]

2.4. Cell

A geographical area serviced by a base station in a wireless network, also used to refer to one or more collocated base stations. Cells are the ‘building blocks’ of a cellular network, with overlapping cells defining the coverage area of a particular network.

2.5. Location Area (LA)

In the location areas approach, the service coverage area is partitioned into location areas, and each location area consists of several contiguous cells. The base station of each cell broadcasts the identification (ID) of location area to which the cell belongs. Therefore a mobile station knows which location area it is in. Figure 2 illustrates a service area with three location areas. [4]

A mobile station will update its location whenever it moves into a cell which belongs to a new location area. For example, when a mobile station moves from cell B to cell D as we show in Figure 2, it will report its new location area because cell B and cell D is in different location areas.

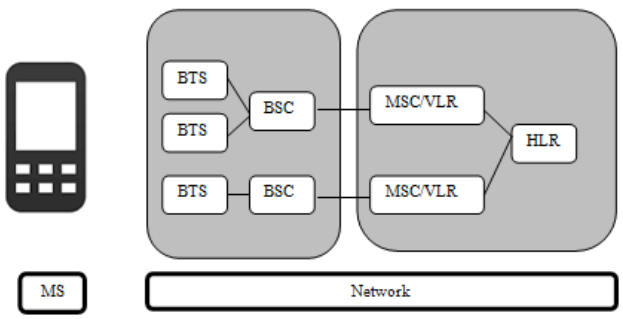

Figure 2. GSM Architecture

2.6. Home Location Register (HLR)

Central database that contains details of each Mobile Subscriber that is authorized to use the GSM core network. HLRs store the information of every SIM card issued by the mobile network operator. SIM cards have a unique identifier called an IMSI which is the primary key to each HLR record. MSISDN (Telephone Number) information is also kept within the SIM and is also primary key in the HLR database. [4]

2.7. Visitor Location Register (VLR)

The GSM visitor location register (VLR) is a database that contains temporary information about subscribers which is needed by the MSC in order to service visiting subscribers. [3]

2.8. Authentication Center (AUC)

The AUC provides authentication and encryption parameters that verify the user's identity and ensure the confidentiality of each call. The authentication center (AUC) also protects network operators from fraud. [3] [4]

2.9. The International Mobile Subscriber Identity (IMSI)

Is an internationally standardized unique number to identify a mobile subscriber. The IMSI consists of a Mobile Country Code (MCC), a Mobile Network Code (MNC) and a Mobile Station Identification Number (MSIN). [5]

2.10. Temporary Mobile Subscriber Identity (TMSI)

TMSI is a temporary identification number that is used in the GSM network instead of the IMSI to ensure the privacy of the mobile subscriber. The TMSI prohibits tracing of the identity of a mobile subscriber by interception of the traffic on the radio link. [5] The TMSI is assigned to a mobile subscriber by the Authentication Centre (AUC). The TMSI is assigned for the duration that the subscriber is in the service area of the associated Mobile Switching Centre (MSC).

2.11. Ki

The secret key shared between MS and HLR.

2.12. Rand

The random number generated by HLR.

2.13. Location Area Identity (LAI)

The location area identity describes the LA of a network operator. It consists of a country code (3 digits), a mobile network code (2 digits), and a location area code (16 bits). [5] [3]

3. Security in GSM Networks

The security issue covers three main aspects: Authentication, Confidentiality, and Anonymity.

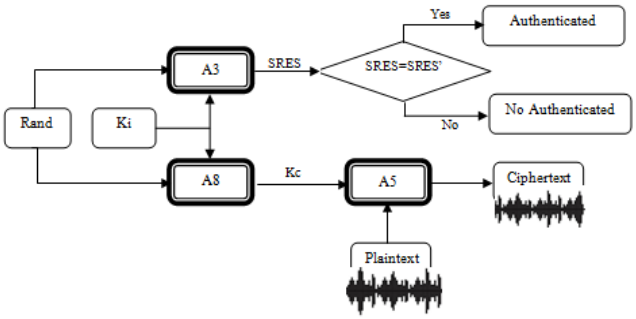

Figure 3. GSM Security Algorithms

Three security algorithms exist in GSM networks, namely the A3 authentication algorithm [9] [10], the A5 ciphering/deciphering algorithm and the A8 ciphering key generation algorithm. These three are used in order to provide different security features and techniques, including authentication and protection of the radio link, which guarantees privacy of calls and user data [5] [8].

3.1. Mobile Station Authentication

The GSM network authenticates the identity of the subscriber through the use of a challenge-response mechanism. A 128-bit random number (Rand) is sent to the MS. The MS computes the 32-bit signed response (SRES) based on the encryption of the random number (Rand) with the authentication algorithm (A3) using the individual subscriber authentication key (Ki).

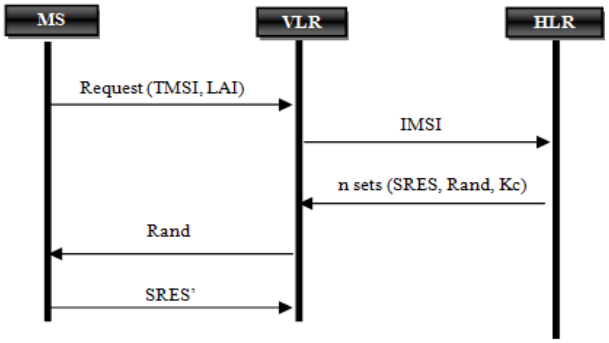

Figure 4. Authentication in GSM Network

Upon receiving the signed response (SRES) from the subscriber, the GSM network repeats the calculation to verify the identity of the subscriber. [6] [9] [3]

Note that the individual subscriber authentication key (Ki) is never transmitted over the radio channel. It is present in the subscriber's SIM, as well as the AUC, HLR, and VLR databases as previously described. If the received SRES agrees with the calculated value, the MS has been successfully authenticated and may continue. If the values do not match, the connection is terminated and an authentication failure indicated to the MS. [11] [12]

Several drawbacks found in GSM authentication protocol is shown as follows:

(1) The major setback In GSM architecture that the Mutual authentication between MS and VLR is not

provided. Only MS is authenticated by VLR, but VLR is not authenticated by MS. Thus supporting unilateral authentication.

(2) There are n copies of triplet authentication parameters stored in VLR's database for each MS in the visiting VLR. This approach results in the storage overhead.

(3) If MS stays in the same VLR for a long time and consumes all of the authenticating parameters, VLR will request HLR again for n copies of authenticating parameters. Consequently, the bandwidth consumption between HLR and VLR will increase.

4) It is possible for MS to move frequently to several VLR's in a short period. Each VLR will request HLR for n copies of triplet authentication parameters. Consequently, the bandwidth consumption and the loads of HLR will increase badly.

5) Man in the middle and impersonating attacks are easily to be practical in the existing protocol; an attacker can impersonate himself as VLR because a VLR is not authenticated by the MS. [13] [11] [14]

3.2. Ciphering In Mobile Phone Communication

In mobile phone communications, encryption is performed between the mobile station and the BTS. There are three versions of the algorithm A5 that are A5/0, A5/1 and A5/2, depending on the allowed level of encryption. In GPRS, a new version of the A5 algorithm called A5 / 3 is designed especially for the transmission of packets. [4] [3]

3.2.1. A5/1 Stream Cipher

The A5/1 is one of the stream cipher algorithm that currently is using by the most countries around the world in order to ensure privacy of conversations on GSM mobile phones. The A5/1 consists of three linear shift registers named R1, R2 and R3 of length 19, 22 and 23 respectively. [15]

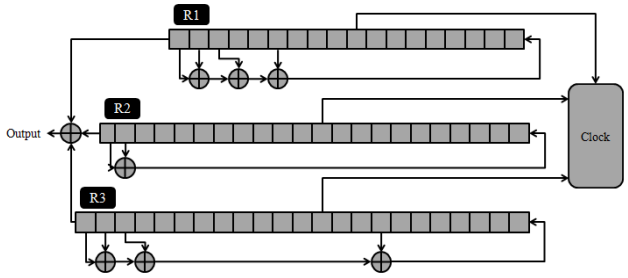

Figure 5. A5/1 Stream cipher

The taps of R1 are at bits 13,16,17,18 and the taps of R2 are at positions 20, 21; and the taps of R3 at bit positions 7,20,21,22.

Each LFSR has a single clocking tap in bit 8 for R1, bit 10 for R2 and R3.the output is produced by xoring the most significant bits of each register. Clocking mechanism for each register is determined according to the majority rule.

The initialization of registers will be done by 64 bit of KC and 22 bit frame number Fn which these are first shifted into the left side of all threes registers and xored with the feedbacks. Then A5/1 is clocked by using the majority clocking for 100 cycles to mix the bits. Then, the next 114 bits of output from A5/1 are xored with the plaintext to encrypt or decrypt data. [16]

3.2.2. A5/2 Stream Cipher

The A5/2 is the 2nd stream cipher algorithm that currently support by GSM protocol in many countries. A5/2 use four register of lengths 19,22,23,17 denoted by R1, R2, R3 and R4 respectively. The feedback functions are the same of A5/1. The R4 control the clock of R1, R2 and R3.

If majority of bits 3, 7 and 10 of R4 is the same as R4 (3) then R2 is clocked, if the result is the same as R4 (7) then R3 is clocked and if the result is the same as R4 (10) then R1 is clocked. The output is produced by xoring all the majorities and the right most bit from each register. [17]

4. Chao Theory

Chaotic behavior is the basis of many natural systems, such as weather or climate. Chaos theory has applications in several fields: meteorology, sociology, physics, computer science, engineering, economics, biology and philosophy.

The chaotic signal, which possesses natural randomness, sensitivity of initial state and controlling parameters, can be used for information encryption as sequence cipher.

Chaos or more grandly chaotic behavior is nonlinear dynamical systems, predictable from simple deterministic equations. Chaotic system used attractors which are a set of states (points in the phase space), invariant under the dynamics evolves over time. Chaotic maps present many desired cryptographic qualities such as simplicity of implementation that leads to high encryption rates, and excellent security. [18] Chaotic behaviour can be studied through analysis using chaotic mathematical models. Mathematically, a dynamical system is described by a problem where data are only the starting values of the state variables. It may have a time component discrete or continuous.

The evolution of dynamic systems using a discrete time applications can be represented by:

$$X_{n+1} = T(X_n, \Lambda)$$

Where n is a natural number, X0 is the initial condition and Λ the parameter vector.

4.1. Lorenz Attractor

In 1963 Edward Lorenz, One of the fathers of chaos theory, studied numerically a system of three differential equations of chaotic behaviour for certain values of the parameters. His system was a very simplified modelling governing the convection rolls in the atmosphere in order to improve long-term weather forecasts.

Figure 6 shows the evolution of ensembles of initial points on the famous Lorenz "butterfly" attractor. [19]

Figure 6. Lorenz butterfly

The Lorenz attractor is generated by the differential equation written by:

$$dx/dt=s\ (y-x)$$
$$dy/dt=rx-y-xz$$
$$dz/dt=xy-bz$$

Where s, r and b are positive real numbers.

5. Related Works

To solving drawbacks of the GSM authentication and ciphering mechanism, many authentication protocols and ciphering algorithms are proposed. However, most of them change the basic architecture for GSM an also cannot fix all of the drawbacks mentioned. In addition, some protocol are changed to the public cryptograph which is most cost in computational furthermore some revised GSM authentication protocol and ciphering algorithm require that some additional hardware be added to the standard GSM System and others proposed authentication protocols are not suitable for the roaming users.

In 1999 Park and all proposed a secure method for GSM by changing the GSM architecture which can resolve some of the drawbacks mentioned above. In 2004, Hwang and all proposed a new protocol based secret and public cryptosystem which is very high cost in componential. [14]

Lee and all proposed a new method in 2003 to solve all of the above drawbacks without changing the existing GSM architecture. However, the Mutual authentication between MS and VLR is not provided in the second call. [13]

In 2006 Ammayapan and all [20] proposed an improvement protocol to the GSM authentication by using the Elliptic curve cryptography (ECC) but the model change the GSM architecture and the computational cost is high.

In 2009 Fanian and all proposed a new protocol which can provide a bilateral authentication nevertheless changed the architecture of GSM network and is not suitable for roaming users. Later,

In 2011 Cheng and all proposed an efficient authentication protocol for mobile communication which solves all drawbacks mentioned but it can be more adapted to reduce bandwidth consumption between VLR and HLR. [11]

In their paper "Security Enhancement in GSM using A3 algorithm" published in 2014, Arpita Gupta and all present an improved version of the A3 algorithm to increase the level of security offered by the GSM standard. The researchers added encryption in the authentication phase to improve safety during this process. The signed response generated (SRES), which is the result of A3 algorithm is encrypted on the SIM card or mobile station (MS) and sent to the mobile switching center (MSC) which in turn has at deciphering this response to authenticate the user. The proposed scheme is coded in C #. NET in Microsoft Visual Studio 2012. [21]

In 2016, Mohammed Shafiul and all reported in their article that the GSM mobile phone system provides only unilateral authentication of the mobile phone network; this limitation allows a range of attacks. While adding support for mutual authentication would be very beneficial, by changing the way of functioning of GSM networks is not practical. For this reason, they proposed a further change in the relationship between a subscriber identity module (SIM) and its domestic network that allows mutual authentication without changing the existing mobile infrastructure. [22] Their proposal requires two major changes in authentication centers and in the SIMs card.

Mid-Og Park and all proposed in 2004 in their article "Modified A5 / 1 stream cipher using S-boxes" another strategy to strengthen security of the A5 / 1 stream cipher using 4x16 s-boxes [23]. The results show that the proposed model has the best characters of random and serial correlation if we compared to the classical version of the A5 algorithm.

In 2011, Nikesh B has proposed two techniques to enhancing security in A5/1 algorithm by analyzing it with different settings. The improvement was made in two ways, the first in the feedback mechanism that was reinforced by using variable valve which increases the complexity of the algorithm and the second in the shift function rules of different registers. He decreases the probability that an LFSR (R1, R2 or R3) will be shifted to 50% which was 75%. [15]

Rosepreet Kaur and Nikesh Bajaj [24] proposed in 2012 a modified version of A5/1 fast and easier to implement. The quality of bit stream produced by the generator was analysis by statistical tests given by national institute of standards and technology (NIST). The proposed structure includes minor increase in hardware by converting LFSR to NLFSR and change in combining function for feedback polynomials.

Darshana Upadhyay and all proposed in their paper "Randomness analysis of A5 / 1 stream cipher for secure mobile communications", published in March 2014 a new approach to improving A5 / 1, the strongest encryption algorithm among all the cryptographic algorithms used in mobile phone communication. They presented a cryptographic system based on NLFSRs (Non Linear

Feedback Shift Register) instead of the LFSR using a non-linear combinatorial generator. It was observed that the proposed system is much better and stronger with a minor increase in hardware. [25]

In 2014 and to increase the length of the generated keystream, authors in [26] proposed an Improvement of A5/1 encryption algorithm by applying a unit delay in the A5/1 algorithm. This was simulated in Simulink.

Authors in 2014 in their paper entitled LFSR Based Stream Cipher (Enhanced A5/1) [27] proposed a new version of the A5/1 algorithm use four LFSRs of length 30, 32, 29 and 37 instead of three in the conventional A5/1. Two of which are used for mutating of the main back-bone LFSR while the fourth LFSR mutates the final output. The proposed algorithm is simulated by using MATLAB and the Keystream generated was been have been tested using Randomness Test Suit given by National Institute of Standard and Technology (NIST). The results show that the proposed scheme is robust and resistive to the cryptographic attacks as compared to the conventional A5/1 stream cipher.

Hala Bahjat and Mohanad Ali in 2016 introduced new improvements to the encryption algorithm A5/ 1 stream cipher to overcome some weaknesses that appear in the shift control mechanism used in this one. They use S-box to increasing the efficiency of the majority function of the A5 / 1 algorithm and improve the randomness characteristics. [28] In their proposed scheme, it is observed that the register is shifted much better and the ciphertext of the proposed algorithm has more complexity when compared with the ciphertext of the original A5/1.

Ria Elin Thomas &all in 2017 try to improve the security provided by the A5/1 algorithm by XORing the keystream generated with a pseudo random number, without increasing the time complexity and does not need any extra hardware requirements. [29]

To improve the efficiency of A5/1 majority function, a new S-box generation is proposed by Divyabharathi Marappan in 2017. In the proposed algorithm, the A5/1 algorithm is modified with two more LFSRs added to the original algorithm with new polynomials. [30] Divyabharathi Marappan found that the proposed approach has more regularity in its clocking operation and consequently, the cipher text of the proposed algorithm is more complex compared with the original algorithm A5/1.

In 2019 and in the second International Conference on Engineering Technology and its Applications, Sattar B. Sadkhan and Zainab Hamza propose an enhancement of A5/1 by adding fourth register to the conventional A5/1 architecture to increase the total security of their proposed algorithm. They also apply a new filtration functions on each register to strengthen the linear combination function (XOR). [31]

Authors in [32] propose an enhancement technique of A5/1 stream cipher based non-linear function using MOSFET which is the most frequently used transistor that can be found in both analog and digital circuits, instead of the existing a5/1 algorithm that use a linear function based xor-ing operation to produce the keystream. The proposed work increases the complexity by using non-linear function and by increasing the data size of the session key to 128, increasing the size of the LSFR and by altering the tapped bits.

According to the observations and results obtained from different tests, authors concluded that the proposed scheme is robust enough from cryptographic attacks in comparison to the standard A5/1 stream cipher.

6. Our Contribution: Chaotic approach

Our objective is to propose a secure solution to improve some drawbacks of the current GSM authentication protocol including: not supporting bilateral authentication; huge bandwidth consumption between VLR and HLR and storage space overhead in VLR and also to make mobile phone encryption algorithms robust and resistive to some known attacks such as time memory trade off attacks, divide and conquer and algebraic attack.

A new authentication protocol is presented which does not change the architecture of the standard GSM and a secure ciphering algorithm based on the use of chaotic systems which are highly sensitive to initial conditions suitable to applications requiring a high flow as the case of mobile phone communications. The proposed solutions solve a lot off drawbacks of the current authentication protocol and ciphering mechanism of the GSM architecture. Our contribution does not change the security architecture of GSM network and it is suitable for roaming user with minimum bandwidth consumption between HLR and VLR and also it applicable to different generations of mobile phones including 3G and 4G.

6.1. Authentication Phase

To solve the drawbacks mentioned above, a new authentication protocol of GSM suitable for roaming users is proposed in this section. The proposed protocol is based on [11] and [10] schemes where the VLR have the permission to authenticate the MS by using a new temporary secret key called KCn which is derivate over a secret key Ki. Moreover, the temporary key KCn stored in the VLR after the first authentication and it is never transmitted over the air between the MS and the network.

As a result, the VLR does not turn back to the HLR for another set of authentication parameters after the first authentication, consequently; the bandwidth consumption between VLR and HLR is reduced.

The robustness of the new protocol is also based on the use of GSM security algorithms A3, A5 and A8 which is used correctly to minimize the bandwidth consumption between HLR and VLR.

6.1.1. The First Authentication of Mobile Station

Firstly, we propose that each VLR have a unique identification value called VLRID which can help the MS

to authenticate the VLR. The detail of authentication for the first time between MS and VLR are described as follow:

While the MS enters a new area, it sends the TMSI, LAI to the visited VLR.

The new VLR can use the TMSI to get the IMSI from the old VLR After receiving the TMSI from the MS. Then the new VLR sends the VLRID, IMSI, to HLR through a secure channel.

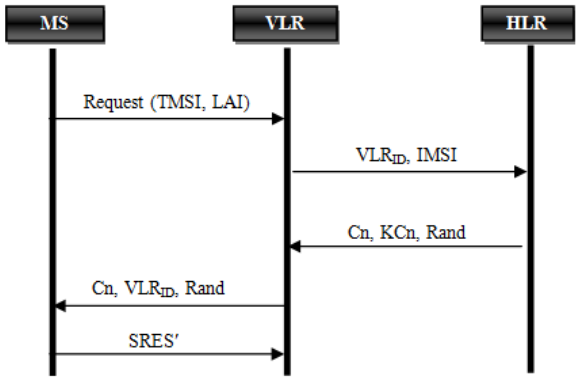

Figure 7. First Authentication of MS

When HLR receives the information, it first checks whether the identity VLRID of the visiting VLR is legal or not. The authentication process is terminated if the VLRID is not valid. Otherwise, HLR computes Cn = A3 (VLRID, Ki) and KCn= A8 (Rand, Ki). Then the HLR sends Cn, Rand, and KCn to the VLR through a secure channel.

Once VLR receives the information from HLR, it stores the KCn in the database and computes SRES= A5 (KCn, Cn). after that, VLR sends VLRID, Rand and Cn to MS.

When MS receives the messages, it first authenticate the VLR by computing Cn′= A3 (VLRID, Ki), and then compares it with the received Cn. If they are not the same, the process is terminated; otherwise, VLR is authenticated.

The MS then computes KCn= A8 (Rand, Ki) and SRES′ = A5 (KCn, Cn). Finally, the MS sends SRES′ back to VLR.

Once the VLR receives SRES′ from the MS, it compares it with the SRES. If they are the same, the MS is authenticated; otherwise, the MS is not a legal user.

6.1.2. MS Authentication for the N Time

The details of the authentication are described as follows:

While MS asks for new communication in the same service area of the same visiting VLR, it computes new Cn = A5 (KCn, Cn) = Keystream 1 + Keystream 2 and send request include TMSI to the VLR where Keystream1is uplink Keystream generating by A5 and Keystream 2 is the downlink one.

The VLR receive the TMSI and compute the new Cn= A5 (KCn, Cn) = Keystream 1' + Keystream 2'. after that the VLR compute a CERT= A5 (VLRID, Keystream 1') and send its VLRID and CERT to the MS.

Once MS receives the messages, it first authenticate the VLR by verifying its CERT which must be the same as CERT' = A5 (VLRID, Keystream 1), then its compute the SRES = A5 (KCn, Keystream 2) and send the value to the VLR.

When VLR receives the request from MS, it computes SRES′ = A5 (KCn, Keystream 2') where KCn is the session key stored in its database for the previous authentication. Then VLR compares SRES′ with the received one. If they are not the same, the process is terminated; otherwise the authentication process is succeeding.

6.1.3. Roaming Between Two VLR's

When the MS move to the new LA it sends to the new VLR TMSI and Cn.

When the new VLR receives the information it send VLRID and TMSI to HLR which identified the new VLR by its VLRID before continues the authentication process.

After its identification, the HLR sends TMSI to the old VLR which calculate RSRES = A5 (KCn, Cn) = KeyS1 + KeyS2 on forward it to the HLR.

Upon receiving RSRES the HLR send it to the new VLR and the process of authentication between MS and the new VLR is started.

The new VLR send a KeyS1 to the MS which calculate RSRES' = A5 (KCn, Cn) =KeyS'1+KeyS'2 and compare the KeyS1to KeyS'1, if it is equal the MS send the KeyS'2 to the new VLR to authenticate him. Otherwise the process is terminated.

When the KeyS'2 it getting by the new VLR it compare it with KeyS2 If they are not the same, the process is terminated, otherwise the authentication process is succeed.

The new VLR sends a location update message to HLR which updates the location of the MS accordingly and send TMS-C to the old VLR.

Finally HLR returns an acknowledgement for the location and the old VLR transmit the KCn to the new VLR.

6.2. Encryption and Decryption Phase

In the new chaos based encryption mechanism, the first step is to calculate the value of X0 which present the initialization parameters of the chaotic system of the new chaotic generator called A5C. X0 is calculated by the A3 function using the session key Kcn and Cn as input values. After that the value of X0 is sent to the VLR which will forward it to the base station BTS that communicate with the mobile phone using the air interface.

When the VLR receives X0, it calculates the keystream of 228 bits by the new chaotic generator A5C to encrypt and decrypt the flux interchanged with mobile station.

The mobile can encrypt and decrypt the messages by calculating the keystream using the same A5C algorithm implemented in the mobile phone. The A5C generator uses the X0 value to initialize the chaotic system of the generator; this value is calculated by the A3 algorithm implemented in the SIM card of the mobile using the values of Cn and the session key Kcn calculated during the authentication phase.

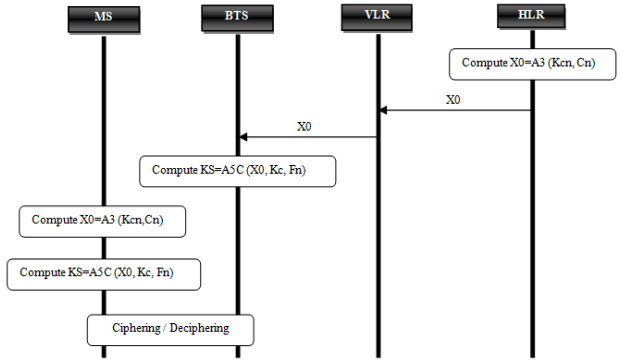

Figure 8. Ciphering and deciphering in chaotic mechanism

6.3. The Chaotic Generator A5C

To not change the architecture of the GSM network, the proposed chaotic generator called A5C is based on the standard A5/1 generator by just introducing some minor modifications to overcome its drawbacks especially in the control mechanism and the Boolean function which is not resistive to algebraic attacks.

6.3.1. A5C Description

The A5C based on three modifications on the standard A5. The first is to introduce a chaotic mechanism to control the clocking of registers. The second one is in the output function and the last one the input values of the Boolean function. The architecture of the proposed scheme is shown in figure 9. The proposed generator consists of three LFSRs as chosen the same as those of A5/1. For each clock cycle we generate new values of variables X, Y, Z by using the Lorenz equations.

$$dx/dt=-10x+10y$$
$$dy/dt=28x-y-xz$$
$$dz/dt=-8/3z+xy.$$

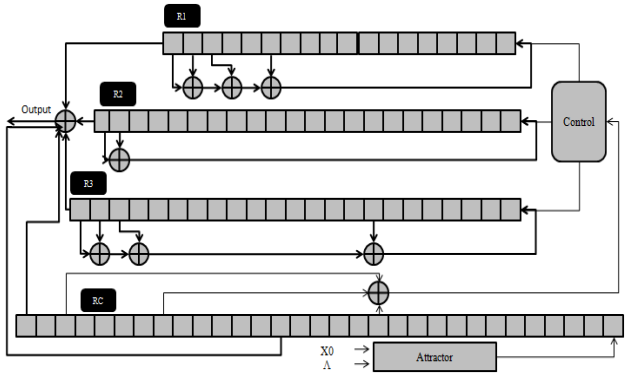

Figure 9. The chaotic stream cipher A5C

After that we convert a value off x into binary using IEE 754 norm. The binary sequence converted is our new chaotic register RC of 32 bit.

6.3.2. Output Function

The output of conventional A5/1 is calculated by xoring the most significant bits of registers R1, R2 and R3.

Table 1. Boolean Function Values

Inputs	Output	Inputs	Output
00000	1	10000	1
00001	1	10001	0
00010	0	10010	1
00011	1	10011	0
00100	0	10100	0
00101	1	10101	1
00110	0	10110	1
00111	0	10111	0
01000	0	11000	0
01001	0	11001	0
01010	1	11010	0
01011	1	11011	1
01100	1	11100	1
01101	0	11101	1
01110	0	11110	1
01111	1	11111	0

We use a high non linear Boolean function as shown in Table 1 with three input variables of conventional A5/1 and two RC bits in positions 16 and 29.

6.3.3. Correlation Immunity

The correlation immunity of a Boolean function is a measure of the degree to which its outputs are uncorrelated with some subset of its inputs. The Boolean function used is a highly non-linear balanced Boolean function with an excellent Correlation-Immunity because the result from probability point of view for all variables is equal to ½. Therefore the designed function is more robust to correlation attack.

6.3.4. Algebraic Degree

It is important that almost every Boolean function has a high algebraic degree to be suitable for cryptographic applications. The algebraic degree of the used equation is equal to 4 which is the maximum level for 5 variables. Therefore, each output random bit of this function can successfully resist in faced to algebraic attack.

6.3.5. Inputs of Output Function

The Boolean function used in this paper use 5 variables to produce one bit of the output sequence. The inputs of the function are the last significant bits of three registers with two bits from RX in positions 32 and 16.

6.3.6. Control Mechanism

In the modified A5 we propose to introduce a chaotic map to control the clocking of LFSR because most of attacks against A5/1 and A5/2 make use of the security flaws in clocking mechanism. We offer a new clocking mechanism for A5 stream generator, which is works as follows:

For each clock cycle a variable M is calculated by xoring bits of RX in positions 11,22 and 29.if M=1 then the majority rule of clocking taps R1 (14), R2 (9) and R3 (3) is applied. However if M=0 the registers whose taps value equals 1 is clocked. If all taps are 0 then three registers are clocked. The probability that any LFSR can be clocked is 75% for the conventional A5/1, but for this new clocking mechanism; it has been reduced to 68%.

7. Efficiency Analysis

We have proposed this new authentication and chaotic ciphering algorithm called A5C to improve and solve a lot of drawbacks mentioned above but also to increase the efficiency of some proposed protocols. Our propositions accomplish its goals in the differences ways:

7.1. VLR Storage Space

In the authentication protocol of GSM, VLR have to save all copies (SRES, Rand, KC) sends by HLR in its database to authenticate the mobile station MS, this creates the overloaded of the VLR's database. But in our proposed authentication protocol, in the first authentication phase, VLR have to save only the secret sessions key KCn and its identification Cn. When the mobile moves to the new VLR, the session secret key KCn will be send by the old VLR to the new one that can authenticate the mobile with the same session secret key KCn stored in the mobile phone from the last authentication process.

7.2. Consumption between VLR and HLR

In our proposed authentication protocol as a long as MS stays in the coverage area of the same VLR is authenticated by the same VLR using the secret sessions key KCn and the Cn without need to the HLR .this process reduce efficiently the bandwidth consumption between VLR and HLR. However in the authentication protocol of standard GSM every time VLR request HLR for authenticity of MS especially when the VLR consumes the triplets (SRES, Rand, KC) stored in its database and request the HLR for a new sets of triplets.

7.3. Key Exchange and Algorithms Selection

An important key called KCn was created in our new authentication protocol which is a variant of the secret key Ki stored only on the network and the mobile phone and does not never exchanging over the air interface of the network to not be intercepted by the attackers. In our contribution we don't exchange this new Key called KCn in all authentication and ciphering phases to save the secret of the mobile SIM card.

To not changing the architecture of the GSM network we have using just the algorithms ensuring the security in GSM networks which are the authentication algorithm A3, key agreement algorithm A8 and the A5 stream cipher used for encryption.

Our authentication protocol essentially is proposed to reduce more the bandwidth consumption between VLR and HLR. A lot of proposed protocol don't choose the good algorithms specially when choosing the algorithms A3 or A8 to authenticate MS by the VLR because these algorithms is implemented in the HLR/AUC, if we use one of them in the authentication process, necessary we will not reduce the bandwidth consumption between VLR and HLR. As a result, a VLR turn back up to the HLR in each authentication process.

8. Security Analysis

8.1. Mutual Authentication

The Mutual authentication is improved in each phase of our authentication protocol, the MS and the VLR will be authenticated each one in each phase of authentication process.

In the first authentication mechanism the VLR can get it authorization Cn computing by the A3 algorithm which is implemented just in the HLR/AUC and the SIM card of the mobile station MS. So the VLR can't get it without the help of its HLR.

The mobile station is capable to authenticate the VLR when the visiting VLR send request for its authentication includes Rand, Cn and its identification VLRID.

When the MS asks the VLR for authentication for the n time, VLR use KCn and Cn as the inputs through A5 to compute the certificate CERT, then VLR request a message include CERT and VLRID to the MS. The CERT is then used for MS to authenticate VLR. The VLR can authenticate the MS throw the comparison of its SRES calculated by the A5 algorithm.

In the roaming phase the VLR is authenticated for the first time by its HLR and the VLR can authenticate the MS throw the SRES computing by A5 using the secret session key KCn transferred from the old VLR to the new one through a secure channel.

8.2. Impersonating Attack

An impersonation attack is an attack in which an adversary successfully assumes the identity of one of the legitimate parties in the system of communications protocol. In the stronger identification protocol of our contribution no one can impersonate the mobile station MS or the VLR. in our proposed scheme if an attacker tries to impersonate the MS he cannot generate the correct SRES because he don't know the correct identifier Cn of the VLR transmitted by the HLR in the first authentication processes when the HLR verify the identity of the VLR. That's why the impersonate attack is invisible in our protocol.

8.3. Quality of a Random Bits Generated By A5C

Statistical tests designed to measure the quality of a

generator purported to be a random bit generator.

Each statistical test determines whether the sequence possesses a certain attribute that a truly random sequence would be likely to exhibit. [33]

According to National Institute of Standards and Technology (NIST), all important cryptography tests have applied on our new designed stream cipher algorithm to test some bits sequences produced by our genetic stream cipher.

Table 2. Statistical Tests Results

Statistical Test	P-Value	Success / Fail
Frequency Monobit	0.511101	Success
Block Frequency	0.551856	Success
Serial	0.538095	Success
Runs	0.453840	Success
Long Runs of ones	0.514994	Success
Linear complexity	0.501444	Success

All of the five basic tests such as frequency test, serial test, runs test, long runs of ones test and linear complexity test passed successfully as shown in Table 2. we can say that all sequences generated by our chaotic generator have a good quality to be as random with high degree complexity.

8.4. Boolean Function Security

The choice of Boolean function is very important in the design of any stream cipher because any bit of the keystream generated is calculated by this Boolean function. For this raison, we present in table 3 some comparisons about the probability that any register can be clocked and some cryptographic characteristic of the Boolean function of our stream cipher generator and the conventional A5/1 stream cipher.

Table 3. Boolean Function Characteristic

Characteristic	**A5C**	**A5/1**
Probability that any register can be clocked	68%	75%
Algebraic degree of the Boolean function	HIGH	LOW
Correlation Immunity of the Boolean function	HIGH	LOW

Anyone can clearly observe that our ciphering algorithm A5C offer a good characteristic of the Boolean function which have a degree equal to 4 which is the maximum level for 5 variables equation furthermore the Boolean function have an excellent Correlation-Immunity because the result from probability point of view for all variables is equal to ½ Therefore the designed function is more robust to algebraic and correlation attacks.

8.5. Chaotic Stream Cipher A5C Security

In our new proposed generator design called A5C, the essential point is the use of chaotic system to generate random values which it uses like a RX register.

Chaotic Systems are sensitive to initial condition this makes them sensitive to minimal change of inputs information.

The security in our design is that the known of inner state of RX it is not sufficient to know the system structure because the next values of RX depend to a chaotic system, for that reason the attacker must know the parameters of chaotic system which is not invisible for him and it will be changed any time when the mobile station request the network for a new authentication. So in this part we applied some attacks against A5C to prove the security and the complexity of our new proposed design.

8.5.1. Time Memory Data Trade of Attack

A generic attack that can be applied to a large class of cryptographic primitives, and on stream ciphers in particular, is the time-memory-data trade-of attack. it has been shown that solution space N can be distributed between time T and memory M, where the inequality TM < = N must be hold for the success of the attack where N represents total number of solution space for LFSR's internal state, M represents total of required memory and T represents necessary computational time of the attack.

In the proposed stream generator, there are four LFSR's of total length 96, so according to this model the memory increases to $M.2^{96}$ and its need 2^{96} times more. As a result the attack becomes infeasible.

8.5.2. Divide-And-Conquer Attacks

Divide-and-conquer attacks work by guessing a part of the secret internal state of the stream cipher and then deducing the unknown part of the state.

Golic has described a divide and conquer attack on A5/1 stream cipher in [34]. The main idea of the attack is getting 63.32 linear equations and then obtaining internal state of LFSR's by solving these equations.

The complexity becomes about $2^{40.16}$ linear equation set solving which is enough to obtain internal state of LFSRs. In [35], E. Barkan and all. described a different type of divide and conquer attack as "Basic Attack" which requires $2^{39.91}$ total work complexities with 2.36 minutes of conversation plaintext.

In both of the attacks mentioned above some bits are guessed, then by using clocking mechanism of A5/1, linear equations are obtained and unknown bits of LFSRs are recovered.

If anyone attempts to apply a similar technique on the proposed cipher, he has to guess all bits of RX to understand which rule for the clocking mechanism (majority rule or match rule) of R1, R2 and R3 is used. Otherwise guessing any small portion of the R1, R2 or R3 does not appear to help to determine the initial state of the generator. Guessing RX results in 2^{32} extra computational times, so totally attack requires about 2^{72} time complexity. Table 4 group all the complexity of attaks mentioned above of our chaotic system A5C and the conventional A5/1 stream cipher.

Table 4. Complexity of Somme Attacks

	Complexity	
Attack	A5/1	**A5C**
Time memory data trade of attack	M	$M.2^{96}$
Golic attack	$2^{40.16}$	$2^{72.16}$
Barkan and all attack	$2^{39.91}$	$2^{71.91}$

As we show in the table 4, all attacks mentioned below are more complex to complete of our proposed chaotic stream cipher called A5C which is based on chaotic system to control the shuttling mechanism of other register compose the A5C stream cipher design . Furthermore the chaotic systems are sensitive to initial condition and the initialization of chaotic design it based on the authentication phase because the initialization parameters X0 is depend an authentication values. Therefore un attacker which is not authenticated cannot find these values offers with our new authentication process schemes more robust and secure if we compared with the GSM conventional authentication process called A3.

9. Authentication Protocol Performance

To evaluate the performance of our protocol, in this section, we make a comparison of our proposed protocol with the related schemes.

In table 5, we compare the goals of our authentication protocol with some other GSM authentication schemes. The symbols used in table 5 are defined as follow:

CH: The computation cost for HLR
CV: The computation cost for VLR
CHV: The communication cost between HLR and VLR
SV: The space overhead for VLR
MA: Mutual authentication between MS and VLR

According to table 5, we can observe that our protocol is more efficient of it compared with the GSM protocol algorithm. It used a few number of arguments in each phase of our authentication mechanism which can minimize the flow of information in the network.

Table 5. Comparison Between Some GSM Authentication Protocols

	Our protocol	**[11]**	**GSM**
CH	LOW	HIGH	HIGH
CV	LOW	LOW	LOW
CHV	VERY LOW	LOW	HIGH
SV	LOW	LOW	HIGH
MA	YES	YES	NO

In addition our protocol reduces more the bandwidth consumption between VLR and HLR and doesn't use the A3 algorithm where the VLR authenticate the MS instead of HLR such as the protocol presented in [11].

10. Synthesis

Firstly, the majority of the proposed solutions is interested either authentication or encryption in mobile phone communications, our contribution is interested in both authentication and encryption while we have trying to give solutions to each of them since in reality the authentication algorithm A3 is implemented with the key generation algorithm called A8 which provided the encryption key Kc to the encryption algorithm A5.

Table 6. Comparison with other authentication Algorithms

	Based	**Change**	**Cost**	**Problems**
[13]	A3,A8 and A5	MINOR	LOW	Mutual authentication just in the first time
[20]	ECC	MAJOR	High	Change GSM Architecture
[11]	A3, A5, and A8	MINOR	LOW	Bandwidth consumption between VLR and HLR
[21]	Encryption of SRES	MAJOR	High	Major changes in AUC and SIMs
[22]	RAND Hijacking	MAJOR	High	Major changes in AUC and SIMs
OUR	A3, A8 and A5	MINOR	LOW	

Table 7. Comparison between chaotic A5 and some enhanced algorithms

	Based	**Change**	**Cost**	**Problems**
[23]	Using 4x16 s-boxs	MAJOR	High	Change the Architecture
[15]	Feedback and shift function rules	MINOR	LOW	Algorithm became complex
[24]	NLFSR	MINOR	LOW	Change the Architecture
[25]	System based on NLFSRs	MINOR	LOW	Change the Architecture
[26]	Unit delay	MINOR	LOW	Minor increase in hardware
[27]	Adding Registers	MAJOR	LOW	increasing the number of LFSRs of A5/1
[28]	S-box	MAJOR	High	Using 5 LFSR
[29]	XORing the keystream with a random number	MINOR	LOW	Generation of the pseudo random number
OUR	Chaotic A5	MINOR	LOW	

As we can show in Table 6, a lot of contributions have been presented in the literature to overcame some drawbacks finding in the GSM authentication protocol include the bandwidth consumption between HLR and VLR, unilateral authentication and the storage overhead in VLR. A number of these approaches require a big change in the authentication center AUC and also in the SIM card [21] [22] where the implementation algorithm is implemented and others include bandwidth consumption between VLR and HLR [11] without forgetting a high computational cost presented in others protocols. [20] [21] [22].

The proposed solution provides a secure bilateral authentication system, decreases the bandwidth consumption between VLR and HLR and not requires a major change in the mobile network architecture.

Our chaotic encryption system based on chaotic system, which it derives its strength from some chaotic feature such as initial sensitivity to conditions and consequently a small variation in the initialization values of chaotic generator produces a very different keystream values.

A lot of enhancement of the standard A5 algorithm has been proposed in the literature but the majority of them changes the architecture of the generator or increase a high computational cost to generate the final keystream.

In the other hand our protocol among a very limited number of contributions that offers a complete solution for both authentication and encryption.

11. Conclusions

Security in mobile telephony was and always remains a subject of worry for telecommunication operators and this mainly due to the new services offered by this technology where the mobile has not become just a tool to telephone or send short messages, but it occurs in several activities of our daily life which affects sensitive areas such as E-payment and E-health.

GSM system is still used and widespread because of its simplicity and efficiently. Many telecommunication companies still use the old standard of GSM because the cost of the new base station is still very high.

In this paper, we have proposed a new protocol to enhance the standard GSM authentication protocol and a new chaotic stream cipher design called A5C is proposed to make ciphering mechanism in mobile phone communication robust and more secure. The proposed solution not only provides a secure bilateral authentication mechanism, but also decreases the bandwidth consumption between VLR and HLR. It can not only solve all of the drawbacks but also increase the efficiency by reducing the number of arguments using in the authentication process.

The new generator A5C provides a cryptographically more secure with respect to some popular attacks as algebraic attacks; divide and conquer and time memory trade-off attack. Furthermore, the period of the proposed generator is higher and robust to Berleykamp Massey attack if we compared to the convetionnal A5/1. In addition, The chaotic A5C algorithm has passed all of basic cryptographic tests of NIST successfully so it present a good characteristic for a stream generator that has to be suitable for cryptographic applications.

Our proposed mechanism including authentication and ciphering can also be applied to future mobile systems such as 4G or 5G and it's suitable for roaming users. In a word, our proposed system is very secure and efficient.

REFERENCES

[1] ERICSSON, Mobility Report. Retrieved from https://www.abc.es/gestordocumental/uploads/internacional/EMR_June_2016_D5%201.pdf, June 2016.

[2] Sara Radicati,.Mobile Statistics Report 2014-2018, Retrieved from www.radicati.com, February 2014.

[3] Noureddine Boudriga, Security of Mobile Communications. Auerbach Publications Taylor & Francis Group, 2010.

[4] EFORT. Sécurité Mobile 2G, 3G et 4G: Concepts, Principes et Architectures, Retrieved from http://www.efort.com.

[5] Xavier Lagrange, Philipe Godlewski, SamiTabbane, Réseaux GSM, 5iéme edition, Hermes Science Publication: Paris, 2006.

[6] K. Al-tawil, A. Akrami, and H. Youssef, "A new authentication protocol for GSM network." Proceedings of IEEE 23rd Annual Conference on Local Computer Networks, pp. 21-30, October 1998.

[7] B. Mallinder, "An overview of the GSM system." Proceedings of Third Nordic Seminar on Digital Land Mobile Radio Communication, pp. 12-15, Copenhagen, Denmark, September 1998.

[8] EFORT, GSM : Global System for Mobile Communications Architecture Interfaces et Identités, Retrieved from http://www.efort.com.

[9] L. Harn and H. Y. Lin, "Modification to enhance the security of the GSM protocol." Proceedings of the 5th National Conference on Information Security, pp.416-420, Taipei, Taiwan, May 1995.

[10] C. H. Lee, M. S. wang, and W. P. Yang, "Enhanced privacy and authentication for the global system for the mobile communications." Wireless Networks, Vol. 5, pp. 231-243, 1999.

[11] C. C. Lee, M. S. Hwang, and I.E. Liao, An efficient protocol for mobile communication. " Springer, January 2011, Vol. 46, No.1, pp 31-41, January 2011.

[12] A. Aziz and W. Diffie, "Privacy and authentication for wireless local area networks." IEEE Personal Communications, pp. 24-31, Jully 1993.

[13] C. C. Lee, M. S. Hwang, and W. P. Yang, "Extension of authentication protocol for GSM. Proceedings of IEE on Communication, Vol. 150, No. 2, pp. 91-95, April 2003.

[14] C. H. Lee and M. S. Hwang, "Authenticated key-exchanged in mobile radio network". European Transactions on Telecommunication, pp. 265-269, 1997.

[15] B. Nikesh, "Effects of Parameters of Enhanced A5/1." International Journal of Computers and Applications IJCA Special Issue on Evolution in Networks and Computer Communications, July 20111.

[16] H. Zakaria, Kamaruzzaman. S and I. Abdullah, "Modified A5/1 Based Stream Cipher For Secured GSM," Communication. IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.2, February 2011.

[17] S. Petrovic and A. Fuster-Sapater, "Cryptanalysis of the A5/2 Algorithm," Cryptology ePrint Archive, Report 2000/052, http://eprint.iacr.org, 2011.

[18] Vinod. P and K. K. Sud, "A Novel Pseudo Random Bit Generator Based on Chaotic Standard Map and its Testing, " Electronic Journal of Theoretical Physics EJTP 6, No. 20, p327–344, 2009.

[19] A. Ali-Pacha, N. Hadj-Said, A. M'Hamed, A. Belghoraf, "Lorenz's Attractor Applied to the Stream Cipher (Ali-Pacha Generator)," Elsevier Science: Chaos, Solitons & Fractals, Vol.33/5 pp.1762-1766, August 2007.

[20] K. P Kumar, A. Kavitha, A., "Mutual Authentication and Key Agreement based on elliptic curve cryptography for GSM," International Conference on advanced computing and communication, December 2006.

[21] Arpita Gupta, Prateek Singh Chandel, "Security Enhancement in GSM using A3 algorithm," International Journal of Computer Applications, Vol.108, No.1, December 2014.

[22] Mohammed Shafiul, Alam Khan, Chris J Mitchell, "Retrofitting mutual authentication to GSM using RAND hijacking," 12th International Workshop of Security and Trust Management, STM, September 2016.

[23] Mi-Og Park, Yeon-Hee Choi, Moon-Seog Jun, "Modified A5 stream cipher using S-boxes", The 6th International Conference on Advanced Communication Technology, February, 2004.

[24] Rosepreet Kaur, Nikesh Bajaj, "Enhancement in Feedback Polynomials of LFSR used in A5/1 Stream Cipher", International Journal of Computer Applications, Vol.57, No.19, November 2012.

[25] Darshana Upadhyay, Priyanka Sharma, Sharada Valiveti, "Randomness analysis of A5/1 Stream Cipher for secure mobile communication", International Journal of Computer Science & Communication, Vol.5, No.1, page 95-100, September 2014.

[26] Sadkhan S B and Jawad N H," Improvement of A5/1 Encryption Algorithm Based on Using Unit Delay", Iraqi Academic Scientific Journal 22 622–63, 2014.

[27] Amandeep Singh Bhal, Zhilmil Dhillon, "LFSR BASED STREAM CIPHER (ENHANCED A5/1)", International Journal of Advanced Computational Engineering and Networking, ISSN: 2320-2106 Vol.2, No.12, December 2014.

[28] Hala Bahjat, Mohanad Ali, "Improvement Majority Function in A5/1 stream cipher Algorithm", International Journal of Engineering & Technology, Vol.34 No.1, 2016.

[29] Ria Elin Thomas, G Chandhiny, Katyayani Sharma, H Santhi and P Gayathri, "Enhancement of A5/1 encryption algorithm", IOP Conference Series: Materials Science and Engineering, 263. 042084. 10.1088/1757-899X/263/4/042084, 2017.

[30] Divyabharathi Marappan, "Securing Mobile Technology of GSM using A5/1 Algorithm", International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 01, January 2017.

[31] Sattar B. Sadkhan and Zainab Hamza, "Proposed Enhancement of A5/1 stream cipher", 2019 2nd International Conference on Engineering Technology and its Applications (IICETA), August 2019.

[32] Farhan Rahman, Siddharth Singh," Enhancement of A5/1 Stream Cipher with Non-Linear Function using MOSFET", International Journal of Engineering and Advanced Technology (IJEAT), December 2019.

[33] Siti Yohana Akmal Mohd Fauzi, Marinah Othman, Farrah Masyitah Mohd Shuib, Kamaruzzaman Seman, Khairi Abdulrahim," Randomness Evaluation of Modified A5/1 Stream Cipher for Global System for Mobile Communication", Malaysian Journal of Science Health & Technology, Vol.2, 2018.

[34] J. Golic, "Cryptanalysis of alleged A5 stream cipher", Proceedings of Eurocrypt'97, Lecture Notes in Computer Science, vol. 1233, pp. 239-255, 1997.

[35] E. Barkan, E. Biham, and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Journal of Cryptology, 21(3): p.392-429, 2008.