Indonesian Journal of Electrical Engineering and Computer Science
Vol. 24, No. 1, October 2021, pp. 357~366
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v24.i1.pp357-366

Evolutionary approach to secure mobile telecommunication networks

Abdelkader Ghazli[1], Adda Alipacha[2], Naima Hadj Said[3]
[1]Tahri Mohamed University of Bechar, Bechar, Algeria
[1,2,3]Coding and Information Security Laboratory (LACOSI), Bechar, Algeria

Article Info

Article history:

Received Dec 14, 2020
Revised Aug 2, 2021
Accepted Aug 5, 2021

Keywords:

A5/1
Evolutionary
LFSR
Mobile network
PSO
Security
Stream cipher

ABSTRACT

A series of encryption algorithms called A5 is used to secure mobile telephone communications, producing a pseudo-random sequence that will be exclusive OR (XORed) with the data flowing in the air interface in order to secure them. These algorithms are essentially composed of shift registers with linear feedback, controlled generally by a function or with another register in order to favor the randomness character of the keystream generated. Evolutionary algorithms are bioinspired calculation methods, whose principle is inspired by the theory of evolution, which consists in evolving a set of solutions to a problem given in order to find better results. This paper presents an improvement of the A5/1 algorithm by an evolutionary approach based on the use of particle swarm optimization algorithm (PSO) in order to limit some weaknesses and drawbacks found in the conventional A5/1 version, which have been cryptanalysed and several attacks have been published such as time memory trade off attacks and guess and determine attacks. Our technique does not alter the A5/1's architecture, but it does help to improve its shifting system by an evolutionary approach, which guarantees the quality of the keystream generated and makes it more complex and more secure.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Abdelkader Ghazli
Department of Mathematics and Computer Sciences
Tahri Mohamed Univercity of Bechar
B.P 417 kenadsa Street, Bechar, Algeria
Email: Ghazek@gmail.com

1. INTRODUCTION

Today, almost everyone has a cellular phone connected to the internet or some other networks. People's life has changed and new features have emerged such as M-commerce where monetary transactions are conducted via a mobile network. Mobile communication uses wireless connectivity in order to communicate at any time and from any location. The openness of mobile communication, on the other hand, offers a number of security risks, and as a result, the mobile operators use some techniques to ensure the security of subscriber communications including the encryption of information interchanged in the air interface between the mobile device and its network.

Stream ciphers, which are symmetric key ciphers that generate pseudorandom binary patterns used to encrypt message signals on a bit-by-bit basis, are used to encrypt message signals in mobile phone conversations. Stream ciphers are much quicker than block ciphers and need far less hardware and software resources to implement. Stream ciphers are therefore better suited to telecommunications applications such as mobile phone networks. Information security through mobile communication networks is critical and poses a

significant threat to mobile communications security. Voice calls in mobile phone conversations are encrypted using a family of algorithms known as A5 to provide anonymity over the air. A5/1 is the more powerful variant, whereas A5/2 is the less powerful, and A5/3 is a block cipher used in 3G. The A5/1 method is made up of three linear feedback shift registers (LFSR) that are controlled by a clocking mechanism that uses a majority function to determine whether or not a register is shifted.

A5/1 is vulnerable to a number of attacks, including biased birthday attack [1], time memory trade off attacks, guess and determine attacks, and the random subgraph attack, due to a security flaw in its architecture. The majority of these attacks take advantage of a flaw in the clocking mechanism's security [2]. As a result, many A5/1 attacks have been made public [3]. Particle swarm optimization (PSO) is a powerful technique for finding near-optimal or ideal solutions to problems. It's simple to use, and it's proven to be both efficient and effective when applied to a variety of optimization situations.

In order to improve the shift control mechanism of the various registers that create the traditional A5/1, several ways have been offered in the literature. Many of these approaches define new mechanisms that attempt to construct a pseudo-random generator that produces binary sequences of good random characteristics but without using any decisive factor that has assured the convergence of the algorithm to a desired solution. The present approach makes the problem of shifting of registers as a problem of optimization using the particle swarm optimization algorithm. Our recommended strategy is as follows : the shift of any register is performed by satisfying a certain function, which serves to maximize the random character quality produced by our generator called A5/PSO.

A new technique is also used to shift linear feedback shift registers R1, R2 and R3 that build the conventional A5/1 which is shifting any register using a certain speed that designates the number of times a register is shifted in a clock top. This new functionality attempts to load the register in question rapidly by new values so that the generator can produce binary sequences of good randomness. The primary objective of this research is to develop a novel method. for building pseudo-random generators based on self-controlling mechanism, in which the quality of the keystream is improved by an optimization function that maximizes the randomness of the generated sequences.

2. SECURITY IN MOBILE TELECOMMUNICATION NETWORKS

Many cryptosystems are used in mobile telecommunication networks in order to satisfy the requirements of confidentiality and integrity of communications and to authenticate mobile terminals. The choice of a cryptosystem depends essentially on the intended security function and the network generation considered, i.e. global system for mobile communications (GSM), universal mobile telecommunications service (UMTS) or other new generations. The authentication protocol used in GSM networks is based on a symmetric cryptosystem called A3 as we shown in Figure 1. The authentication of a mobile device consists of calculating a signed response, designated special report on emissions scenarios **(**SRES) of 64 bits, requires a 128-bit symmetrical Ki key and a 128-bit RAND challenge sent by the operator. The calculation of SRES is carried out jointly by the smart card of the mobile and by the authentication center of the operator. Authentication is accepted in case of equality of values of SRES calculated by the authentication center of the operator and that are sent by the mobile device.

A8 is a key derivation procedure that generates a symmetric key Kc of 64 bits from Ki and RAND. This session key Kc serves to encrypt the communications; it is generated by the terminal's smart card and by the Authentication center, on the other hand. The smart card provides Kc to the mobile terminal for encrypting mobile communication. Cryptographic algorithms are implemented to protect the confidentiality of data exchanged through radio frequency communications. Encryption covers all the traffic and the signaling. Actually, there is a series of cryptographic algorithms grouped under the name A5 including A5/1, A5/2 and A5/3. The choice of the algorithm to be used for a communication is negotiated; the network chooses an algorithm from the list of the ones proposed by the terminal. This list contains at least A5/1.

A GSM conversation is divided into time blocks, each of which is 4.6 milliseconds long and comprises 2×114 bits for both communication channels. In order to create the starting state of a pseudorandom number generator that yields 228 bits, a session key Kc is combined with block counters Fn. After an exclusive OR (XOR) with data from both channels, these are utilized for encryption.

2.1. Description of the A5/1 stream cipher

A5/1 is a stream cipher used in the second generation of cellular phones to offer over-the-air communication privacy. It's popular in both Europe and the United States. Transmission on GSM networks is driven by a series of frames sent every 4.615 milliseconds. The frame length is 228 bits, with 114 bits for each direction of transmission. A5/1 is utilized to generate a 228-bit key stream for each frame, which is XORed with the frame's 228 bits. Figure 2 shows the A5/1 algorithm's architecture, which is made up of

three short linear feedback shift registers (LFSRs) with lengths of 19, 22, and 23 bits, indicated by R1, R2, and R3, respectively. A5/1 is set up with a 64-bit key named Kc and a 22-bit frame counter called Fn, which is public knowledge. R1 has taps at bit locations 13, 16, 17, and 18. R2 taps at bit positions 20, 21, and R3 taps at bit positions 7, 20, 21, and 22.

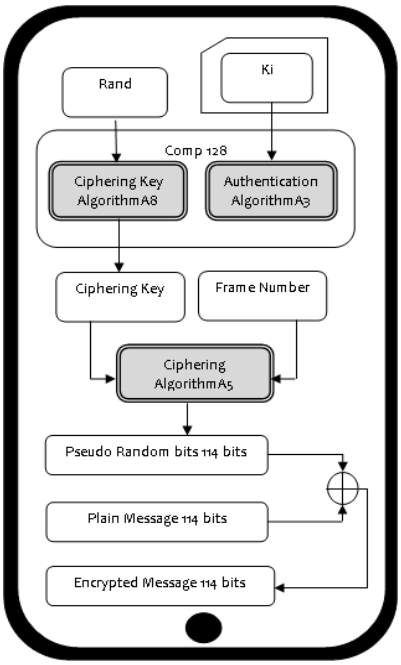

Figure 1. GSM security algorithms

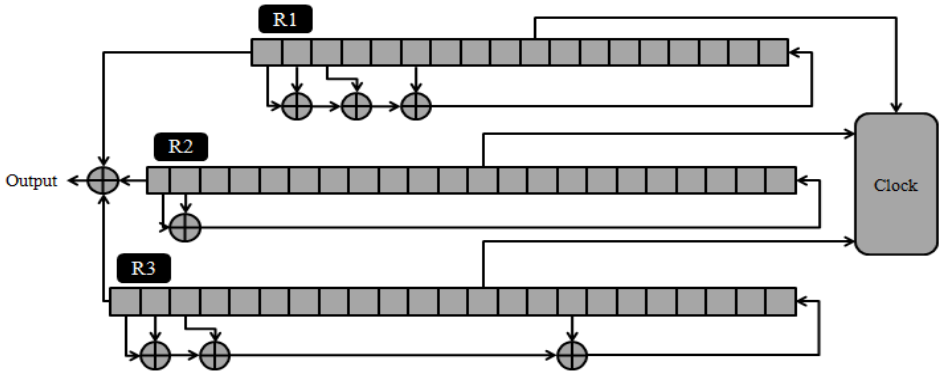

Figure 2. A5/1 structure

The algorithm A5 is unfolded in four steps:
Step 1: Reset: all the registers R1, R2 and R3 are initialized to zero.
Step 2: Initialization: Load 64 bits of the ciphering key Kc and 22 bits of frame number Fn into all of the three registers by xoring each bit of Kc and Fn with the least significant bits of each register, registers clocked regularly.
Step 3: Warm-up: Clock for 100 cycles and discard the output, registers clocked irregularly.
Step 4: Execution: Clock for 228 cycles, generate 114+114 bits, registers clocked irregularly.

3. PARTICLE SWARM OPTIMIZATION

Optimization finds the optimum solution to a problem given a set of conditions. Swarm intelligence (SI) is based on the collective behavior of decentralized, self-organized systems. It could be natural or created by humans. In nature, SI can be seen in ant colonies, fish schooling, bird flocking, and bee swarming.

Particle swarm optimization (PSO) is an evolutionnary methodology similar to genetic algorithms. Kennedy and Eberhart came up with the idea in 1995. This method has been used to tackle a variety of optimization problems and classification difficulties. The PSO is launched with a population of m random solutions of the fitness function. Each individual solution pi, i = 1, 2, ..., m, in the swarm is considered as a particle. Essentially, PSO algorithm is identified by two parameters: velocity and position. In each iteration, each particle's velocity Vi and position Xi are updated based on the fitness values of the updated individuals. Each particle's personal best position pBest and the global best position gBest among all particles are both updated [4].

The personal best position pBest and the global best position gBest have an impact on each particle pk. As a result, the PSO seeks the global optimum solution by modifying each particle's trajectory toward its personal best position as well as the global best position.

V i= w*V i+c 1*r1*(pBesti -Xi)+c2 * r 2*(gBest-Xi)

V i = Xi+Vi where:

Xi isthe current position of the particle, Vi isthe current velocity of the particle, i =1,2,…..,m, PBest is the personal best position of the particle, gBest is the global best position of all the particles, w is the inertia used to control the impact of previous velocities value. A larger inertia weight ω facilitates global exploration (searching new areas) while a smaller inertia weight tends to facilitate local exploration [5], r 1 and r 2 are random numbers, which are used to maintain the diversity of the population, and are uniformly distributed in the interval [0, 1], c 1 is a positive constant, called coefficient of the self-recognition component; c 2: is a positive constant, called coefficient of the social component [6]. According to the above description about the PSO, the following is a description of its pseudo code:

```
For each particle
Initialize particle
End For
Do until maximum iterations or minimum error criteria
        For each particle
        Calculate Data fitness value
        If the fitness value is better than pBest then SetpBest = current fitness value
        If pBest is better than gBest Then SetgBest = pBest
        End For
        For each particle
        Calculate particle Velocity
        Use gBest and Velocity to update particle Data
End For
```

The stopping condition depends on the type of problem being solved. Usually, the algorithm is run until a defined error bound is met or for a fixed number of iterations.

4. SEMINAL WORKS

Park *et al*. offered another technique to increase the security of the A5/1 stream cipher using 4x16 s-boxes in their article "Modified A5/1 stream cipher utilizing S-boxes" in 2004. When compared to the conventional form of the A5 algorithm, the findings reveal that the suggested model has the best random and serial correlation characteristics [7]. Nikesh offered two ways in 2011 to improve the security of the A5/1 algorithm by studying it with various settings. The algorithm was improved in two ways: the first was in the feedback mechanism, which was reinforced by utilizing variable valve, which increased the algorithm's complexity, and the second was in the shift function, which used various register rules. It reduces the chances of an LFSR (R1, R2, or R3) being shifted to 50% from 75% previously [8].

In 2012, Kaur and Bajaj [9] suggested a faster and easier-to-implement version of A5/1. The generator's bit stream was subjected to statistical tests conducted by the National Institute of Standards and Technology (NIST). Converting LFSR to NLFSR and changing the combining function for feedback polynomials are included in the suggested structure.

Upadhyay *et al*. [10] offered a novel way to improve A5/1, the strongest encryption algorithm among all the cryptographic algorithms used in mobile phone communication, in their work “Randomness analysis of A5/1 stream cipher for secure mobile communications,” published in March 2014. Instead of employing a non-linear combinatorial generator, they offered a cryptographic system based on NLFSRs (non linear feedback shift registers). With only a little increase in hardware, the proposed system is significantly better and stronger [10].

Sadkhan and Jawad [11] presented an improvement to the A5/1 encryption method by adding a unit delay to the A5/1 algorithm to lengthen the generated keystream. Simulink was used to model this. Authors developed a new version of the A5/1 algorithm in 2014 in their article “LFSR based stream cipher (enhanced A5/1)” [12], which used four registers of length 30, 32, 29, and 37 instead of three in the regular A5/1. The

main backbone LFSR is mutated by two of these algorithms, while the final output is mutated by the fourth. The suggested technique is simulated in MATLAB, and the keystream generated is tested using the National Institute of Standards and Technology's Randomness Test Suit. In comparison to the traditional A5/1 algorithm, the results reveal that the suggested method is more resilient and resistant to cryptographic attacks.

The exclusive OR (XOR) function employed in the traditional A5/1 contributes to the vulnerability of the stream cipher created, as it may be easily cryptanalyzed, according to Fauzi and colleagues in 2015. In contrast to the XOR combinational function, the authors proposed a new architecture based on a multiplexer (Mux). The new design was written and simulated in C++, and the generated keystream was evaluated for randomness using the NIST test suite, demonstrating that the new design is a viable option for improving the strength of the stream cipher generated [13].

In 2016, Bahjat and Ali announced additional modifications to the A5/ 1 stream cipher to fix a number of issues in the shift control method utilized in this one. They employed S-box to improve the efficiency of the A5/1 algorithm's majority function as well as the randomization characteristics [14]. When compared to the ciphertext of the original A5/1, the register is shifted considerably better in their suggested scheme, and the ciphertext of the proposed algorithm is more sophisticated.

To make the A5/1 algorithm's security more secure, Thomas *et al*. introduced E-A5/1 in 2017, a new upgraded version of A5/1. Without raising the time complexity, they xor the key stream generated with a pseudo random integer [15]. Because it does not necessitate any additional hardware, the suggested algorithm is low-cost.

An improvement of the A5/1 protocol by adding two new registers of length 24 and 25 has been presented in [16]. In 2017 order to overcome some drawbacks finding in the most secure and popular algorithm called as A5/1 used to ensure the security over the air in mobile communications networks. The enhancement was applied by using new clocking function based on new method using sbox.

The authors found out that the new generator has more regularity in its clocking and the keystream generated by the new approach is more efficient and of good quality. An evaluation of a new secure communication protocol based on the A5/1 algorithm was presented by Fauzi *et al*. in their paper entitled published in 2018 in the Malaysian Journal of Science Health & Technology [17]. Unlike other approaches, the evaluation was applied by the NIST Statistical Toolsuite with respect of guidelines. By analysis of the results, authors concluded that their proposed generator presents good randomness with an analysis respecting the conditions of NIST. In 2019 and in international conference on engineering technology and their applications, Sadkhan and Hamza proposed an enhancement of A5/1 by adding a fourth register to the other ones constituting the conventional A5/1 and by applying filtering to each register in order to improve the performance of the bit sequences created by the use of the XOR function [18].

Rahman and Singh, in 2019, used non-linear function implemented by MOSFET, It can assist in the implementation of digital non-linear logic to resolve some various vulnerabilities finding in the conventional A5/1 Algorithm caused by the linear function used to generate the keystream. By an analysis of the results obtained based essentially on statistical tests, the authors have concluded that their approach based MOSFET is more robust and secure to some known attacks because of the high level of complexity of the new algorithm proposed [19].

5. OUR CONTRIBUTION: A5/PSO

Authors' goal is to create such a robust secure generator known as A5/PSO, ready for deployment in order to ensure that mobile phone communications are secure. Our approach consists in developing a new generator that is essentially based on the conventional A5/1 and by the integration of a new optimization function guaranteeing the quality of the keystream provided by our generator in order to get over the conventional A5/1's constraints caused especially by its shift system based on a so-called majority function.

The taps bits of R1 are defined at places 13, 16, 17, 18 in the A5/PSO algorithm, whereas the taps of R2 are defined at positions 20, 21, and the taps of register R3 are defined at positions 7, 20, 21, 22. Each particle or register has a single clocking bit in position 8 for R1, 10 for R2 and R3. The output that presents 228 bits of the keystream is generated by xoring the most significant bits of each registerIn order to solve the problems with A5/1's clocking system and make it more sophisticated, In the A5/PSO, a new clocking mechanism is introduced in order to control the clocking of registers in the last step of the algorithm where the key stream is produced. The clocking mechanism of the proposed scheme based PSO contain two rules: the majority rule and the PSO rule. Table 1 compares the traditional A5/1 algorithm with the proposed A5/PSO algorithm.

The majority rule consistsin a register that can be clocked according to the majority function M, which presents the majority of the clocking bit of each register R1 [8], R2 [10] and R3 [10] and any register whose clocking bit equals to M, should be clocked. In the PSO rule, any register presents a particle that can be clocked or not according to an objective function that favorites the random characteristic of the keystream produced by the algorithm.

Table 1. Comparison between the original A5/1 and A5/PSO

	Original A5/1	A5/PSO
Inputs	Kc, Fn	Kc, Fn, Fitness Function
Outputs	228 bits	228 bits
Clocking Rule	Majority Rule	Majority Rule
Quality Rule	-	PSO Rule

The main objective of any optimization algorithm is to minimize or maximize an objective function. The optimization problem considered here is to maximize the randomness of the key stream generated by our generator called A5/PSO. Unlike the other computation techniques, each particle in PSO has a velocity and it moves in the search space and adjusts its velocity dynamically according to its previous behaviors.

In the proposed stream cipher, each register presents a particle and the velocity of each particle is the number of times that the register will be shifted. The register that will be shifted with a high speed means that its values are not really random so it has to be shifted several times in order to be able to change its values rapidly. A register that will be shifted with a small speed means that its behavior is nearer to the random. According to the PSO's previous description, the A5/PSO operation is broken down into the following steps:
Input: Kc, Fn and The Fitness Function F.
Output: Keystream.
Step 1: Initialization

- All the registers to zero.
- Initialization of Kc and Fn.
- Initialization of particles, where each particle is presented by one register of the conventional A5/1 as follows P1=R1, P2=R2, P3=R3.
- Define the Fitness Function F= $\sum$ $Pvalue_i$/N; where i=1...N and N is the number of statistical Test.

Step2: Introducing Kc

- The 64 bits of the key Kc are interred by XORing, each bit with the feedback bit calculated for each register by using its taps values.
- Registers are clocked regularly.

Step3: Introducing Fn

- The 22 bits of the key Fn are interred by XORing each bit with the feedback bit calculated for each register by using its taps values.
- Registers are clocked regularly.

Step4: Warm up: Clock for 100 cycles and discards the output according to the Majority Rule

```
For i=1 to 100 do
 Calculate M= Majority (R1 [8], R2 [10], R3 [10]))
  If (R1 [8] =M) then clock R1
  End if
    If (R2 [10] =M) then clock R2
    End if
  If (R3 [10] =M) then clock R3
  End if
End for
```

Step5: Execution applying PSO Rule

```
For each particle Pi: Calculate Fitness FRI
  Unitizing each particle Pi best fitness by: PBestRi=FRi
  Initialized gBest = the higher value of (FR1, FR2, FR3)
  Initializing all velocities VR1, VR2, VR3 of all particles P1, P2, P3 to zero
    For J=1 to 228 do
     Calculate F= Fitness (Key stream+ (R1 [19] ^ R2 [22] ^ R3 [23]))
      If (F>gBest) clock all registers irregularly using to the majority Rule and produce
      one bit of the Keystream
        Else
          For i=1 to 3 do
          For each particle PI: Calculate Fitness FRi
           Update pBestRi : if (FRi>pBestRi)then pBestRi= FRi end if
          End for
        Update gBest
          For I=1 to 3 do
           Calculate the Velocity of each register using the equation
            VRI= VRI+C1 X Rand1 X (pBestRI- FRi) + C2 X Rand2 X (gBest - FRi)
          End for
```

```
            Shift each register according to its velocity VRI and produce one bit of the
            keystream
        End if
End for
```

6. PERFORMANCE EVALUATION OF A5/PSO

Table 2 presents a comparison between some previous works, where the authors have tried to increase the security of mobile communications networks, especially the traditional A5/1, which ensures the confidentiality of data transmitted through the air interface between the mobile device and the network. Almost all of these proposal approaches have tried to overstate the different weaknesses presented in the standard version of the A5/1 including the size of the key and the function that manages the clock of the different registers that compose A5/1. As the Table 2 shows, Some authors have attempted to use NLFSR instead of LFSR, others have directed to use sboxes in order to strengthen the mobile phone's safety cryptosystem, and other authors have tried to increase the number of registers composes A5/1 or to implement a control unit jointly with the majority function in order to manage better the shift operations of the different registers compose the A5/1 stream cipher.

Table 2. Comparison between some enhanced versions of A5/1

Ref	Year	Algorithm	Hardware Change	Time Complexity	Approach	Quality Factor
A5/1	1999	A5/1	-	-	Majority Rule	No
[7]	2004	-	Major	High	S-boxes	No
[8]	2011	Enhanced A5/1	Major	High	Feedback Mechanism+ M Rule	No
[9]	2012	-	Minor	Low	NLFSR+ Majority Rule	No
[10]	2014	-	Medium	Medium	NLFSR	No
[11]	2014	-	Minor	Low	Unit delay+ Majority Rule	No
[12]	2014	Enhanced A5/1	Major	High	4 LFSR+ Majority Rule	No
[13]	2015	-	Minor	Low	MUX + Majority Rule	No
[14]	2016	-	Major	High	S-box + Majority Rule	No
[15]	2017	E-A5/1	Minor	Low	XOR+ Majority Rule	No
[16]	2017	-	Major	High	5 LFSR+Sbox	No
[18]	2019	-	Major	Low	4 LFSR+Filtring	No
[19]	2019	-	Minor	Low	MOSFET	No
OUR	2021	A5/PSO	Minor	Low	Majority Rule	PSO Rule

Unfortunately, none of these approaches includes a mechanism that guarantees the quality of the generated keystream and the majority, if not all the authors, uses the NIST statistical tests to ensure that the resulting keystream is of good quality. Even if keysteam has a good quality, the majority of the authors do not discuss the initialization parameters of their enhanced versions of the A5/1 algorithm because a little change in these parameters including Kc and the Fn can influence vitally the quality generated keystream.

A5/PSO proposes a new way to improve the security of the traditional A5/1 generator by making it more complicated, safe, and resistant to known assaults. Our approach integrates a small mechanism that intelligently controls a shifting of the different registers that compose A5/1. This new function is based on an optimization algorithm known as particle swarm optimization algorithm.

7. SECURITY ANALYSIS OF A5/PSO

The A5/1 algorithm is massively deployed, but it does not offer absolute privacy protection. A5/1 has been cryptanalysed and several attacks against A5/1 have been published since the late 1990 [20]. In this section, the authors try to present some known attacks against the standard A5/1 in order to discuss the feasibility of applying these attacks on our modified version known as A5/PSO.

7.1. Guess and determine attacks

Anderson used a guess and determine attack on A5/1 in 1994. He advocated guessing all bits of registers R1 (19 bits) and R2 (19 bits) as well as 11 bits of R3 (22 bits) in order to establish the generator's initial state, where the attacker would examine roughly 2^{52} (19+22+11=52) scenarios to get the correct unknown bits of R3 [21].

Later in 1997, Golic [22] proposed an attack on the algorithm A5/1 based on the resolution of a system of equations in which the first, half of the initial values for all the registers R1, R2, and R3 were guessed to determine the values of these registers based on information extracted from a known keystream by solving a set of 64x64 linear equations. The attack's complexity was around 240 and necessitated so many resources. The attack had a complexity of 2^{40} by using the Gaussian Elimination method to solve more than 40 linear equations.

A new clock control mechanism is proposed in our A5/PSO in order to boost the algorithm's complexity. This new mechanism is not based just only on the majority function that takes three input bits (R1 [8], R2 [10], R3 [10]) and produces a single output bit. The new PSO rule used in our approach needs all the values of all the registers in order to produce a bit output. Guessed a small number of bits do not seem enough to be able to make an attack. Mahalanobis and Shah [23] proposed a better version of the Guess and Determine attack against the A5/1 cipher in 2014; it required roughly $2^{48.5}$. First, 19 bits of register R1 are guessed using the 64 bits of the keystream available to cryptanalyst, and then the initial values of registers R1 and R2 are calculated in the second phase. Following that, a state set will be created, or each new state will designate a candidate generator.

Each generator will be started to generate a set of bits that will subsequently be compared to the 64 bits of keystream that are available. The initial values of registers R1, R2, and R3 represent the values of the secret key requested if the outputs of the candidate generator match the Keystream available. The attack was portrayed in two stages: pre-determination and post-determination. The decomposition process is similarly split into two halves. Processing Phase 1 calculates the most important bits of registers R2 and R3 using the most significant bits of register R1 and the available keystream bits. The clocking bits of registers R2, and R3 were considered in the second step, which was dubbed processing phase2. The complexity of certain Guess and Determine attacks on the A5/1 algorithm is shown in Table 3

The assault is 100 percent successful and consumes 5.65 GB of storage space. The attack is predicated on the majority function's vulnerability, which is used to clock the registers R1, R2, and R3. After 11 clocking rounds, the number of complete state candidates that contain the genuine key grows, and the likelihood of discovering the key among all complete state candidates grows as well. Table 4 shows the complexity of certain known Guess and Determine attacks on the A5/PSO.

In A5/PSO, the keystream is generated in the last step of the algorithm that produces 228 bits of the keystream by applying the PSO rule. Concerning the first phase of determination, there is not a possibility to determine the bits of the register R2 and R3 from a few bits of the keystream available for the attacker because the PSO Rule required that all the values of all the registers R1, R2, R3 are known. Secondly, even if an attacker builds a list of complete states candidates, he does not know the criterion of optimization carried by the PSO rule. This regards the fitness function assigned to the PSO Rule, since this fitness function is never interchanged between the mobile station and the network. For all these reasons, the complexity of this attack is 2^{64}.

Table 3. The difficulty of some A5/1 guess and determine attacks

Attack	Bits Guessed	Keystream Available	Complexity
Anderson	52 bits	0 bits	$\mathbf{2^{52}}$
Golic	32 bits	0 bits	$\mathbf{2^{40}}$
Mahalanobis& Shah	19 bits	$\mathbf{2^6}$=64 bits	$\mathbf{2^{48.5}}$

Table 4. Resistance of A5/1 to some known guess and determine attacks

	Original A5/1		Complexity	
Attack	**Bits Guessed**	**Complexity**	**Bits Guessed**	**Complexity**
Anderson	52 bits	$\mathbf{2^{52}}$	64 bits	$\mathbf{2^{64}}$
Golic	32 bits	$\mathbf{2^{40}}$	64 bits	$\mathbf{2^{64}}$
Mahalanobis& Shah	19 bits	$\mathbf{2^{48.5}}$	64 bits	$\mathbf{2^{64}}$

7.2. Correlation and time memory trade of attacks

Ekdahl and Johansson proposed a new correlation attack of the A5/1 encryption scheme in 2002, which investigates the weak key initialization that separates the session key from the frame number [24]. The attack has a high success rate of over 70%, yet the assault's complexity is merely linear in the length of the shift registers, relying instead on the number of irregular clocks before the keystream is generated. The attack recommends 40 initial bits from 2^{16} frames, which is nearly 5 minutes of unencrypted GSM conversation. Biryukov *et al*. developed biased birthday attack [25], an improved time memory trade off attack, in 2001. The fundamental idea behind this attack is to look at sets A and B that aren't selected using a uniform probability distribution across all conceivable states.

In 2001, Biryukov *et al*. presented an improved time memory trade off attacks called biased birthday attack [25]. The main idea of this attack is to consider sets A and B, which are not chosen through the uniform probability distribution among all the possible states. The reason that makes this attack efficient is that in the standard GSM A5/1, the register bits that affect the clock control and the register bits that affect the output are unrelated for about 16 clock cycles. This decreases the state (2^{64}=2^{19}+2^{22}+2^{23}) to be sampled to 2^{48}=2^{64}-2^{16}. Because the register bits that impact the clock control and the register bits that control the output

are unrelated for around 16 clock cycles in the standard GSM A5/1, this approach is efficient. This reduces the sampled state from $2^{64}=2^{19}+2^{22}+2^{23}$ to $2^{48}=2^{64}-2^{16}$.

These attacks primarily focus on the flaws in the original A5/1 algorithm's usage of the majority function. These attacks will not work on the A5/1, which has been improved and is now known as the A5/PSO, because the weaknesses of this so-called majority function that handles the shifting of the original A5/1 registers is improved by the use of a new function, which is based on a criterion of optimization using particle swarm optimization algorithm. The minimization of the search field of this attack is not taken into consideration in this new approach, since the generation of the output bits does not dependonlyon some specific bits of each register but rather on all the bits constituting the A5/PSO.

8. CONCLUSION

Cellular networks must more than ever meet security requirements to ensure best the various security objectives including confidentiality, integrity, and availability. Several articles have been published in recent years aiming to improve security in mobile telephone networks and more particularly they propose improvements to the series of algorithms ensuring the confidentiality of mobile communications named A5, whose A5/1 version is the most robust. However, none of these approaches incorporates a mechanism to control the quality of the keystream generated by their pseudo-random generators. By the way, the majority of authors, if not all, use NIST tests to be able to validate and ensure the quality of the keystream generated with a limited number of initialization parameters, or the authors will not discuss it in the majority of cases. Such a generator can give good quality pseudo-random sequences with certain initialization parameters but the quality may be degraded while using other initialization parameters.

This paper is initiated to a new class of pseudo random generators where the quality of the generated sequences is guaranteed. Our approach is based on the evolutionary algorithm known as Particle Swarm Optimization Algorithm that has been used in this article to improve security in mobile networks. In this paper, a new version of the A5/1 stream cipher called A5/PSO has been proposed in order to improve the randomization property of A5/1 algorithm to make it robust and resistive to some known attacks.

After the analysis of the different results, it has been shown that the proposed stream cipher has improved the randomness performance because of the good characteristic of randomness of the output bit stream generated by the enhanced scheme. When compared to the traditional ciphering technique A5/1, a security examination of the new scheme reveals that it is very secure and stronger. This type of generator is a great way to create new pseudo random generators that guarantee the quality of the generated keystream.

REFERENCES

[1] H. Kourkchi, H. Tavakoli, and M. Naderi, "An improvement of collision probability in biased birthday attack against A5/1 stream cipher," *2010 European Wireless Conference (EW)*, 2010, pp. 444-448, doi: 10.1109/EW.2010.5483496.

[2] S. Babbage, "A Space/Time Tradeoff in Exhaustive Search Attacks on Stream Ciphers," *European Convention on Security and Detection, IEE Conference publication*, no. 408, May 1995, doi: 10.1049/cp:19950490.

[3] AlAschkar, S. E., and El-Hadidi, M. T., "Known attacks for the A5/1 algorithm: A Tutorial," *International Conference on Information and Communications Technology (ICICT03*), pp. 229-251, 2003.

[4] C. C. Chen, "Hierarchical Particle Swarm Optimization for Optimization Problems," *Tamkang Journal of Science and Engineering*, vol. 12, no. 3, pp. 289-298, 2009, doi: 10.6180/jase.2009.12.3.08.

[5] S. Asta, "A Novel Particle Swarm Optimization Algorithm," M. Sc Thesis*,* Istanbul Technical University Graduate School of Science Engineering and Technology, Turkey, Jan. 2012, doi: 10.13140/2.1.1669.5361.

[6] I. K. Ali, and A. I. Jarullah, "A New Keystream Generator Based on Swarm Intelligence," *Diyala Journal for Pure Sciences*, vol. 8 no. 2, pp. 169-177, Apr. 2012.

[7] M. O. Park, Y. H. Choi, and M. S. Jun, "Modified A5/1Stream Cipher using S-boxes," *The 6th International Conference on Advanced Communication Technology*, Feb. 2004, doi: 10.1109/icact.2004.1292921.

[8] 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*, vol. 2, no. 2, pp. 7-13, Jul. 2011.

[9] R. Kaur, and N. Bajaj, "Enhancement in Feedback Polynomials of LFSR used in A5/1 Stream Cipher," *International Journal of Computer Applications*, vol.57, no.19, pp.32-35, Nov. 2012.

[10] D. Upadhyay, P. Sharma, and S. Valiveti, "Randomness analysis of A5/1 Stream Cipher for secure mobile communication," *International Journal of Computer Science & Communication*, vol.5, no.1, pp. 95-100, Sep. 2014.

[11] S. B. Sadkhan and N. H. Jawad, "Improvement of A5/1 Encryption Algorithm Based on Using Unit Delay," *Al-Qadisiyah Journal of Pure Science,* vol.19, no.3, pp. 211-222, 2014.

[12] A. Singh Bhal, and Z. Dhillon, "LFSR based stream cipher (Enhanced a5/1)," *International Journal of Advanced Computational Engineering and Networking*, vol. 2, no. 12, pp. 85-90, Dec. 2014.

[13] M. Fauzi, S. Y. A., M. Othman, M. Shuib, F. M. and K. Seman, "An Enhanced A5/1 Stream Cipher Utilising An Improved combinational Function For GSM Communication," *Proceeding of The Third International Conference en Intelligence and Computer Sciences AICS2015*, Sep. 2015.

[14] H. Bahjat, and M. Ali., "Improvement Majority Function in A5/1 Stream Cipher Algorithm," *International Journal of Engineering & Technology*, vol. 34, no. 1, 2016.
[15] R. E. Thomas, G. Chandhiny, K. Sharma, H. Santhi, and P. Gayathri, "Enhancement of A5/1 encryption algorithm," In *IOP Conference Series: Materials Science and Engineering,* 2017, vol. 263, no. 4, doi: 10.1088/1757-899x/263/4/042084.
[16] D. Marappan, "Securing Mobile Technology of GSM using A5/1 Algorithm," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4 no. 1, Jan. 2017.
[17] M. Fauzi S. Y. A, M. Othman, M. Shuib F. M, K. Seman, and A. Rahim, K., "Randomness Evaluation of Modified A5/1 Stream Cipher for Global System for Mobile Communication," *Malaysian Journal of Science Health & Technology*, vol. 2, pp. 31-34, 2018.
[18] S. B. Sadkhan and Z. Hamza, "Proposed Enhancement of A5/1 stream cipher," In *2009 2nd International Conference on Engineering Technology and its Applications (IICETA)*, 2019, pp. 111-116, Aug. 2019, doi: 10.1109/iiceta47481.2019.9013008.
[19] F. Rahman, and S. Singh, "Enhancement of A5/1 Stream Cipher with Non-Linear Function using MOSFET," *International Journal of Engineering and Advanced Technology (IJEAT)*, vol.9, pp. 101-105, Dec. 2019, doi: 10.35940/ijeat.a1021.1291s319.
[20] L. Jiao, Y. Hao, and D. Feng, "Stream cipher designs: a review," *Science China Information Sciences*, vol. 63 no. 3, 2020, doi: 10.1007/s11432-018-9929-x.
[21] R. Anderson, "A5 (was: Hacking digital phones)," *Newsgroup Communication*, 1994.
[22] J. Golic, "Cryptanalysis of alleged A5 stream cipher, Advances in Cryptology," In *International Conference on the Theory and Applications of Cryptographic Techniques*, 1997, pp.239-255, doi:10.1007/3-540-69053-0_17.
[23] A. Mahalanobis, and J. Shah, "An Improved Guess-and-Determine Attack on the A5/1 Stream Cipher," *Computer and Information Science*, vol. 7, no. 1, 2014, doi: 10.5539/cis.v7n1p115.
[24] P. Ekdahl, and T. Johansson, "Another attack on A5/1," *IEEE Transactions on Information Theory*, vol. 49, no. 1, pp. 284-289, 2003, doi:10.1109/tit.2002.806129.
[25] A. Biryukov, A. Shamir, and D. Wagner, "Real Time Cryptanalysis of A5/1 on a PC," In *Fast Software Encryption Workshop 2000*, 2000, pp. 1-18, doi: 10.1007/3-540-44706-7_1.

BIOGRAPHIES OF AUTHORS

Abdelkader Ghazli is a Ph. D in computer Science. He received the diploma of teaching in Computer Science from the University of University of Science and Technology USTO of Oran, ALGERIA in 2009. He is a lecturer at the University of Tahri Mohamed of Bechar Algeria, His research interests are cryptography and security.

Adda Alipacha is a lecturer in electronics and Computer Science. He is a teacher at the University of Science and Technology of Oran Usto, Algeria. His research interests are coding, cryptography and security FPGA.

Naima Hadj Said is a lecturer in Computer Science. She teaches at the University of Science and Technology of Oran Usto, Algeria. His research interests are coding, cryptography and security.