A Modified Cascade Model of a GSM Stream Cipher

Elitsa Gospodinova

Abstract **- This paper presents an optimized method for improving the A5/1 stream cipher encrypting the line from the mobile terminal to the base station in the GSM standard. The method realization is master-slave-based on standardized algorithms, with the realized alternative ciphers being serially applied in rotation with a large non-linearity period. The A5/1 stream cipher modification is a convenient and practical method, minimizing the modification on the software of the end terminals.**

Keywords: security; GSM; stream cipher; A5/1;

I. INTRODUCTION

The advances in computation technology increase the efficiency of the existing kinds of cryptoattacks, and create a flourishing base for developing new kinds. Thus, the contemporary cryptographic algorithms become weaker and less reliable for ensuring the security and confidentiality of the transmitted information. From the cryptoattack viewpoint the radio air is a well protected zone, but from the undesired access viewpoint, it is the weakest component.

The modern broadband and the future more attractive services increasingly attract the interest of persons and organizations wanting to violate the confidentiality of the transmitted information. The security of the wirelessly transmitted data in cellular networks is achieved through encrypting the digital streams to and from the mobile terminal. In GSM communications the encrypting algorithm is A5. It processes all the messages – voice, text and video stream. The A5 algorithm has to be common for all GSM operators, end terminals and base stations, in order the roaming service to be applicable. The A5 realization is twofold – in the end terminal, as well as in the base station.

The GSM specifications allow up to 7 algorithms based on the A5, as well as a non-encryption mode. The earliest realizations A5/1 and A5/2 are widely implemented to date.[1]

- A5/1 – reliable algorithm used in Europe and the Americas;
- A5/2 – "artificially weakened" algorithm used in Eastern Europe and Asia;
- A5/3 – the newest version of the algorithm. It is a stream cipher generating two 114-bit keys and is based on the block cipher KASUMI.

The development of A5/3 is aimed at its application in 3G. It is implemented and standardized [6],[7],[8],[9] for usage in existing cellular networks as well but is not used to the moment.

Elitsa Gospodinova is with the Technical College at Asen Zlatarov University, 8010 Burgas, Bulgaria, E-mail: ed_gospodinova@abv.bg

The weaknesses of the A5 implementations and the many successful attacks [2],[5] require improvement of the security level but the established position of the acting operators, as well as the necessity of large investments make the modification of the infrastructure equipment very unlike, since over 100 million users worldwide would be affected.

Of a primary importance in the cellular networks is the delivery of the offered services without excessive time delay, with offering newer and attractive services demanding large computational resources. This makes it necessary to look for alternative approaches to security improvement, demanding the fewest possible intrusions in the software of the cellular network. In principle, the multiple encryption of the data stream or the series interconnections of ciphers are logical ways to security improvement of a given wireless network since they can be based on standardized and specified algorithms. Their drawbacks such as the time delay for the multiple encryption and need for a specified number of implemented algorithms for the series encryption, make them inapplicable for the cellular networks.

The paper is organized as follows. It begins with a description of a model for generating of ciphers, alternative to A5/1, applied on a rotational principle. Next, new algorithm controlling the sequence of the applied alternative ciphers is presented. After that, conditions for the method realization are noted, as well as its advantages compared to the standard A5/1 are given.

II. CASCADE MODIFIED MODEL OF THE A5/1 STREAM CIPHER

A5/1 is a stream cipher composed of three linear feedback shift registers (LFSR) having 19, 22 and 23 bits, respectively [3]. The most significant bits (MSB) of the LFSRs are modulo 2 summed and determine the output of the generator. The feedback of each register is obtained as a modulo 2 summation of specific bits called tap bits, placed in positions:

$$13, 16, 17, 18 \Rightarrow R1;$$
$$20, 21 \Rightarrow R2;$$
$$7, 20, 21, 22 \Rightarrow R3$$

The cascade will be obtained by changing the positions of the tap bits which will lead to a given number of alternative ciphers of A5/1, with their sequence controlled by the generated by A8 session key (MASTER - SLAVE). For the model description a cascade model of eight modifications of the A5/1 cipher is chosen.

The time-division approach is applied, resulting in obtaining separate time slots. Within each of them the encryption/decryption operation will use different modification of the A5/1 cipher. The different modifications used in the separate time slots are not applied in series but on

a rotational principle. Their sequence is determined according to the state table (Table 1). It visualizes which cipher for which binary combination is applied.

TABLE I
STATE TABLE

SESSION COMBINATIONS	ALTERNATIVE CIPHER	TAP bits									
		R_1				R_2		R_3			
		X_1	X_2	X_3	X_4	Y_1	Y_2	Z_1	Z_2	Z_3	Z_4
000	A5/1/1	13	16	17	18	20	21	7	20	21	22
001	A5/1/2	12	16	15	18	19	21	6	19	21	22
010	A5/1/3	13	15	16	18	18	20	8	19	20	21
011	A5/1/4	11	14	15	17	18	19	6	18	20	22
100	A5/1/5	13	15	17	18	19	20	7	18	19	21
101	A5/1/6	14	13	17	18	17	21	9	18	20	21
110	A5/1/7	12	15	16	17	18	21	8	17	21	22
111	A5/1/8	11	14	16	18	17	20	6	17	20	22

Since a cascade model of eight A5/1 modifications is chosen, the binary code in the state table is required to contain three information bits – session combinations (S_c). The session combinations are fetched serially from the generated by A8 session key (S_k). The S_k has a standard 64-bit length corresponding to 21 whole bit strings. Upon entering the next time slot (in a working state of the system) the current combination is compared with S_c in the state table. This process is repeated until running out of the contained three-bit strings from S_k (Fig. 1).

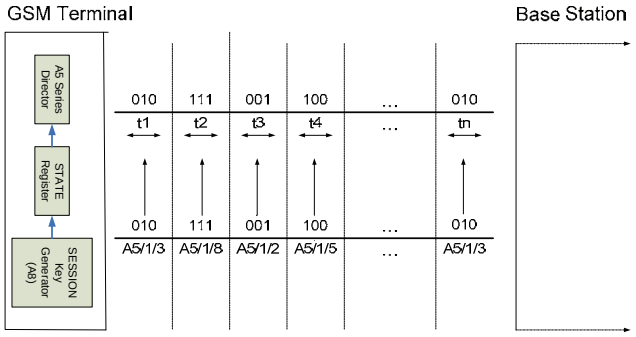

Fig. 1 Cascade modified model of the A5/1 stream cipher

The set of combinations (21) correspond to one whole rotational cycle. It is convenient for the generated by A8 session key to be stored in a specific state register. Upon call initialization between a GSM terminal and a base station the session key is copied into the state register before sending. The three-bit strings corresponding to the sequence of the applied ciphers are fetched from the state register (RS) and have the following sequence:

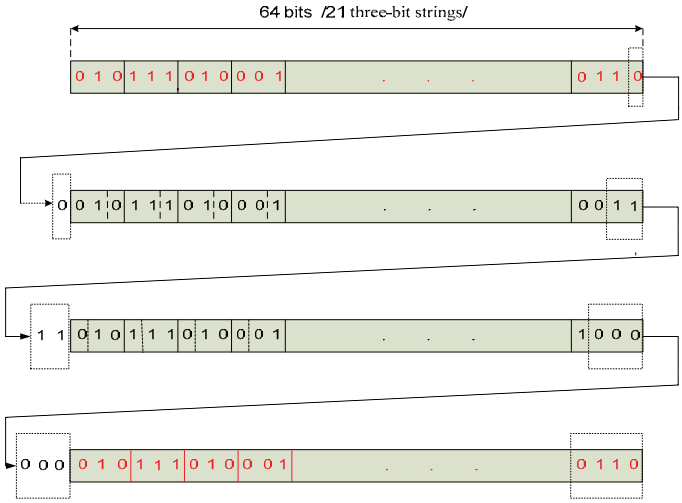

Fig. 2. Algorithm for controlling a rotational sequence of modified ciphers

The bit sequences fetched by the session key and controlling the sequence of rotation of the encryption algorithms are visualized in Fig. 2, based on which the following claim may be constructed:

A series "x" has an equal bit sequence with another series "y" when the following condition is met:

$$M_x - M_y = Z \qquad (1)$$

where:
M – number of bits carried over to the next cycle;
Z – number of information bits in the string, corresponding to one algorithm in the state table;

The expression in Eq.(1) shows same bit sequences generated by the A8 session key in its standard form.

In the particular case Z=3 which leads to a high degree of repeatability of the bit sequences, hence the repeatability of the rotational sequences. This drawback can be overcome by modifying the algorithm as follows. The total length of 21 three-bit strings is equal to 63 bits, and S_k is 64 bits long (Fig. 2). The remainder – 1 bit is the most significant bit (MSB) in the string during the first cycle. It is carried over as the least significant bit (LSB) in the register during the next cycle. It follows that the sequence is 1+64 bits long. In order to keep the same cycle length, the 65th bit is not processed (it is eliminated), and the preceding bit is processed according to the described procedure. The carried over MSB in each next cycle determines the non-repeatability of the rotational sequence of the ciphers (Fig. 3).

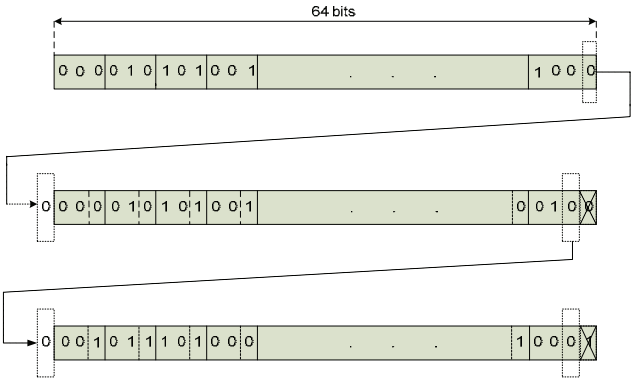

Fig.3 Improved algorithm for controlling a rotational sequence of modified ciphers

$$P_k = S_k^2 + S_k \tag{2}$$

$$N = \frac{S_k - M}{Z} \tag{3}$$

The algorithm for controlling a rotational sequence of modified ciphers may be expressed recursively as:

$$f^0(x_n) = (x_n) \tag{4}$$

$$f^1(x_n) = x_n div 2 + 2^{n-1}(x_n \bmod 2) \tag{5}$$

$$f^m(x_n) = f^{(1)}\left(f^{(m-1)}(x_n)\right) \tag{6}$$

where:

P_k – repeatability of the bit sequences, $[bit]$;

S_k – length of the session key, $[bit]$;

N – number of bit combinations for one rotational cycle;

x_n – key sequence, decomposed into three-bit strings;

n – number of bits in one sequence;

m – number of sequences;

The described algorithm for $2^3 = 8$ ciphers might be applied for 2^7 and 2^9 ciphers as well, with the sequence of the modified ciphers controlled by the MASTER-SLAVE based algorithm presented in Fig. 4.

III. Software realization of the method

For maximum efficiency of the method, the software realization should be optimized with assembly language code. The A5/1 stream cipher is extensively used; the method does not require implementations of new algorithms, but slight changes in the A5/1 software code, with the tap bits being input into the code not as constant values, but as variables, respectively: X_1, X_2, X_3, X_4; Y_1, Y_2; Z_1, Z_2, Z_3, Z_4; During each next cycle their values corresponding to the particular combination generated by the A8 algorithm would be read from the state table. This process guarantees that the data streams are processed with different ciphers for each cycle. Although the state table is static, the control of the sequence of the ciphers is generated by the A8 algorithm which is unique for each session. In practice this guarantees a non-predictable sequence of rotation of the ciphers.

IV. Analysis of the advantages of the method

The many analyses of the A5/1 cipher lead to the conclusion that it has weaknesses determining it as vulnerable to different kinds of attacks [2],[4].Its major weaknesses are the small number of inner states, short key, as well as the linear initialization of the key and the frame counter. The methodology of the present approach aims at avoiding the particular weaknesses. By introducing variable values of the tap bits, the number of inner states of the cipher is increased, that is, it is obtained of eight modified ciphers, with the pseudorandom sequence of rotation of the ciphers being 65 series × 21 three-bit strings = 1365 strings. In addition, the standardized A5/1 consists of three LFSRs, with a total of 10 tap bits, with modulo two summations, forming the feedback of each register. With the MASTER–SLAVE method the tap bits are fetched from the state table and are different for each of the eight alternative ciphers. The complex length of the key with a rotational sequence of the ciphers controlling the A8 algorithm is 87360 bits. A basic advantage of the MASTER–SLAVE method compared to the standardized A5/1 is also the fact that the order of the alternative ciphers is controlled by the A8 algorithm, that is, when an unauthorized access is attempted, data are necessary for the standardized A5/1, the alternative ciphers along with their corresponding tap bits, as well as the A8 algorithm with its corresponding bit sequence for the particular session, which increases the resistance of the method against attacks and overcomes its weaknesses. The slight software intrusions necessary for the realization of the method gives the opportunity the computing resources to be harnessed mainly for providing high-quality broadband services with increased security level of the transmitted data.

V. Conclusion

The described method is very convenient, does not require significant software intrusions into the build infrastructure worldwide. It is based on standardized and certified algorithms and its deployment does not require changes in the authorization and encryption procedures. From the viewpoint of data stream security level the method is comparable to the methods for multiple encryption and use of cascaded ciphers, avoiding the resulting time delay and the need of more powerful energy resources. The method provides an opportunity for a step-by-step deployment, a possibility for optimization for next generation networks. In the future, the method shall be analyzed based on all kinds of attacks for which the standardized A5/1 is known to be vulnerable.

ACKNOWLEDGEMENT

This paper was supported in part by project 213/2010 in the Department of Computer Systems and Technologies in the Faculty of Technical Sciences at Asen Zlatarov University, Burgas.

REFERENCES

[1] Aissi, S., Dabbous, N,. Prasad A., Security for Mobile Networks and Platforms, Artech House Universal Personal Communications, 2006

[2] Birynkov, A., Shamir, A., Wagner D., Real Time Cryptanalysis of A5/1 on a PC, Proc. of Fast Software Encryption –FSE 2000. pp. 1–18

[3] Boudriga, N., Security of Mobile Communications, CRC Press, 2010

[4] Barkan, E., Biham, E., Keller, N., Instant Ciphertext – Only Cryptanalysis of GSM Encrypted Communication (Technical Report CS – 2006 – 07 - 2006)

[5] Ekdahl, P., Johansson, T., Another Attack on A5/1, Abstract, Proceedings of International Symposium on Information Theory (ISIT), Washington, 2001 (http://www.it.lth.se/patrik/publications.html).

[6] Vijaya, C., Authentication and Access Control for Mobile Communications, (http://www.ittc.ku.edu/rvc/documents/865/865_securityreport.pdf.)

[7] European Telecommunications Standards Institute (ETSI), European Digital Cellular Telecommunications System (GSM), General description of a GSM Public Land Mobile Network (PLMN), 1997, (http://www.etsi.org)

[8] GSM 02.17 (ETS 300 509): European Telecommunications Standards Institute (ETSI), European Digital Cellular Telecommunications System, Subscriber identity modules (SIM), Functional Characteristics, (http://www.etsi.org)

[9] GSM 04.07 (TS 100 929): European Telecommunications Standards Institute (ETSI), European Digital Cellular Telecommunications System, Security Related Network Functions, (http://www.etsi.org)