Implementation of Cryptographic Algorithms for GSM Cellular Standard

1Alpesh R. Sankaliya, 2V.Mishra(Senior MIEEE) and 3Abhilash Mandloi
Department of Electronics
Sardar Vallabhbhai National Institute of Technology, Surat-395007
Gujarat, India
1alpeshrs@yahoo.com, 2vive@eced.svnit.ac.in and 3asm@eced.svnit.ac.in

Abstract—GSM is most widely used cellular standard in the world. Mobile network is the shared media and any user of the media can intercept the network. When the media are shared, any one can listen to or transmit on the media. Thus communication is no longer private. When media are shared, privacy and authentication are lost unless some method is established to regain it. Cryptography provides the mean to regain control over privacy and authentication. A5/x are the encryption algorithms used in order to ensure privacy of conversations on GSM mobile phones. A5/x algorithms to secure the information sent over the air interface. The strong version A5/1 is used in most countries. A5/2 is weaker version used in countries on which export restrictions apply. A5/3 encryption algorithm used for GSM and ECSD and GEA3 encryption algorithm for GPRS. The following paper is based on simulation of A5/1 and A5/3 algorithms.

Keywords-GSM, security, Cryptography, Cipher text, A5/1, A5/3.

I. INTRODUCTION

Encryption in mobile communication is very crucial to protect information of the subscribers and avoid fraud. There are various methods for providing privacy and security in GSM System. Secret key cryptographic systems can be categorized into either block or stream ciphers. Block ciphers are memory less algorithms that permute N-bits blocks of plaintext data under the influence of the secret key and generate N-bits blocks of encrypted data. Stream ciphers contain internal states and typically operate serially by generation a stream of pseudo-random key bits, the keystream (stream ciphers are also called keystream Generators). The keystream is then bitwise XORed with the Data to encrypt/decrypt. Stream ciphers do not suffer from the error propagation, as in the block ones, because each bit is independently encrypted/decrypted from any other. They are generally much faster than block ciphers and they have greater software efficiency.

In the GSM security layer, A5 stream cipher is used, which employs a 64-bit secret key [1]. Versions A5/1 and A5/2 were kept secret for a long period of time. Since the GSM A5 algorithm was developed, the climate for cryptography has changed substantially [2]. Recently, A5/1 and A5/2 were reverse-engineered from a GSM handset and published by Briceno et al. [2]. Afterwards A5/2 was cryptanalysis and proved to be completely insecure. The attack required very few pseudo random hits and only 216 steps [1][3]. A new security algorithm, known as A5/3 provides users of GSM mobile phones with an even higher level of protection against eavesdropping than they have already [4][5]. A5/3 has been developed by a joint working party between the GSM Association Security Group and the 3'rd Generation Partnership Project (3GPP), for use in GSM systems. It will also be applicable for the General Packet Radio Service (GPRS) where it will be known as GEA3, and other GSM modes such as High Speed Circuit Switched Data (HSCSD) and Enhanced Data Rates for GSM Evolution (EDGE) [5][6]. The A5/3 encryption algorithm specifically supplies signaling protection, so that sensitive information such as telephone numbers is protected over the radio path, and user data protection, to protect voice calls and other user generated data passing over the radio path [4][5][6]. The A5/3 and GEA3 algorithms are based on the 3GPP ciphering algorithm, for which Mitsubishi holds essential patents [12].

II. A5/1 CIPHERING ALGORITHM

A GSM conversation is sent as a sequence of frames every 4.6 millisecond. Each frame contains 114 bits representing the digitized X to Y communication and 114 bits representing the digitized Y to X communication. Each conversation can be encrypted by a new session key Kc. For each frame, Kc is mixed with a publicly known frame counter Fn, and the result serves as the initial state of a generator which produces 228 pseudo random bits. These bits are XOR'ed by the two parties with the 114+114 bits of the plaintext to produce the 114+114 bits of the cipher text[15][16].

The A5/1 cipher is composed by three Linear Feedback Shift Registers (LFSRs), R1, R2, and R3 of lengths 19, 22, and 23 bits, respectively. Each LFSR is shifted, using clock cycles that are determined by a majority function. The majority function uses three bits; C1, C2, and C3. Among these bits, if two or more of them are 0 then the majority m = 0. Similarly, if two or more of them are 1, then the majority m = 1. If Ck = m then Rk is shifted, where k=1,2,3. The feedback polynomials for R1, R2, R3 are: x19 + x3 + x2 + x + 1, x22 + x + 1 and x23 + x15 + x2 + x + 1, respectively. At each clock cycle, after the initialization phase, the last bits of each LFSR are XORed to produce one output bit. The proposed architecture for the hardware implementation of the A5/1 cipher is shown in Fig. 1.
The process of generating the keystream bits from the key $K_c$ and the frame number $F_n$ is performed in four steps. In step 1, The Three LFSRs are initialized to zero. Then, clocked for 64 cycles, ignoring the majority function. During each cycle, the each bit from $K_c$ is XORed in parallel into the lsb’s of the three registers.

In step 2, the 22 bits of $F_n$ are fed in using the same process as in step 1. In step 3, 100 additional cycles are performed using the majority function, but without any output. Finally in step 4, The three registers are clocked for 228 additional clock cycles with the majority function in order to produce the 228 output bits. At each clock cycle, one output bit is produced as the XOR of the msb’s of the three registers.

The idea behind the $A5/1$ are good. It is very efficient. It passes all known statistical test; it’s only known weakness is that its registers are short enough to make exhaustive search feasible. Fig. 3 gives the simulation result by using the Sample time = 0.1ms, $KEY = [1 2 3 4 5 6 7 8]$. III. SYSTEM SECURITY OF 3GPP

Third generation mobile system offering mobile users content rich services, wireless broadband access to internet, and worldwide roaming. However, this includes serious security vulnerabilities. In this document are specified three ciphering algorithms: A5/3 for GSM, A5/3 for ECSD and GEA3 for GPRS (including EGPRS). The algorithms are stream ciphers that are used to encrypt/decrypt blocks of data under a confidentiality key $K_C$. Each of these algorithms is based on the KASUMI algorithm which is a block cipher that produces a 64-bit output from a 64-bit input under the control of a 128-bit key. The algorithms defined here use KASUMI in a form of output-feedback mode as a keystream generator. The three algorithms are all very similar. KGcore function is shown in Fig.4. Table 1 gives the detail of variables used in figure. Each of these algorithms is based on the KASUMI. KASUMI is a block cipher that produces a 64-bit output from a 64-bit input under the control of a 128-bit key. KASUMI used in these algorithms is the Feistel cipher with eight rounds with associated subkeys (KL, KI and KO)

![Figure 1. A5/1 stream cipher architecture](image)

![Figure 2. Simulation of A5/1 Algorithm using Matlab](image)

![Figure 3. Simulation result for A5/1 Algorithm](image)

![Figure 4. KGcore Core Keystream Generator Function with KM=0x55555555555555555555555555555555 (in hex)](image)

<table>
<thead>
<tr>
<th>GSM A5/3</th>
<th>ECSD A5/3</th>
<th>GEA3</th>
</tr>
</thead>
<tbody>
<tr>
<td>CA</td>
<td>000010111</td>
<td>000010111</td>
</tr>
<tr>
<td>CB</td>
<td>0000000000</td>
<td>0000000000</td>
</tr>
<tr>
<td>CC</td>
<td>0_0/COUNT</td>
<td>0_0/COUNT</td>
</tr>
<tr>
<td>CD</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CE</td>
<td>CIPHER KEY REPEATED TO FILL 128 BITS</td>
<td></td>
</tr>
<tr>
<td>CK</td>
<td>BLOCK1 BLOCK2</td>
<td>BLOCK1 BLOCK2</td>
</tr>
</tbody>
</table>

Which is generated from $CK$ using rounding manner. It operates on a 64-bit data block and uses a 128-bit key. Its eight rounds are shown in Fig 5. Each KASUMI operator uses FL and FO functions. In each odd round of KASUMI
operator uses $R_i = \text{FO} (\text{FL}(L_{i-1}, K_{Li}), KO_i, K_{Ii})$ function and for each even round uses $R_i = \text{FL} (\text{FO}(L_{i-1}, KO_i, K_{Ii}), K_{Li})$. The FL and FO algorithms based on number of iteration round with substitutions (S-Boxes) and permutations (PBoxes) shown in Fig 6 and 7.

In FL algorithm $R' = R \oplus \text{ROL}(L \oplus K_{Li1}), L' = L \oplus \text{ROL}(R \oplus K_{Li2})$. In FO algorithm $R_j = \text{FI}(L_{j-1} \oplus \text{ZO}(R_{j-1}) \oplus K_{Ij,1}, L_j = S_{9}[L_{j-1}] \oplus \text{TR}(L_{j-1}) \oplus K_{Ij,i,1})$ for 4th round out $= S_{7}[L_{j-1}] \oplus \text{TR}(L_{j-1})$.

Figure 5. KASUMI algorithm

Figure 6. FL algorithm

Figure 7. FI algorithm

Figure 8. FO algorithm
IV. A5/3 Ciphering Algorithm

The GSM A5/3 algorithm produces two 114-bit keystream strings, one of which is used for uplink encryption/decryption and the other for downlink encryption/decryption. Figure 9 shows simulation of A5/3 algorithm.

Figure 9. Simulation of A5/3 Algorithm using Matlab

Result of Simulation block of A5/3 algorithm is shown in Fig. 10 by taking sampling time=0.1ms, key=[1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16], count=32.

Figure 10. Simulation result of A5/3 Algorithm

V. PERFORMANCE ANALYSIS

The simulation works were carried out on a Pentium dual core processor with 2 GB of RAM running on Window XP. Codes for A5/1 and A5/3 were written and executed in MATLAB 7.8

Figure 11. Speech ciphered by A5/1

Figure 12. Speech ciphered by A5/3

Speech is the very complex signal representing different kind of sound voiced, unvoiced and silence. The speech signal can be visualized well through a spectrogram, which is the three dimensional representation that has time, frequency and energy density as dimension. Fig.10 shows the spectrogram of ‘Hello’ word sound in Matlab. The dark bands in Fig 10 are called formants and are frequency of resonance. The darkness of these bands is energy, which serves as the third dimension in the spectrogram [9].

Modern speech secrecy systems are mainly based on digital enciphering techniques. In the area of speech ciphers, mainly symmetric key algorithms are used. Fig 11 and 12 shows the spectrograms of the plain speech ciphered by A5/1 and A5/3 algorithms respectively and easily compared the energy band of ciphered signals. A5/3 provides very low key set up time than others.

We can see in A5/1 ciphering still having the originality of speech and we can hear voice sound with ‘Hello’ word superimposed with some spidery noise. While in A5/3 we can only hear non-voice sound. Hence, no one can clearly understand the original plain speech. Normally the length and characteristic of the key specify the depth of encryption. As the key length of the A5/1 is only 64-bit while A5/3 is
the variable length encryption with key length varies from 64-128 bit. Hence, it is very difficult to guess the key. We can also see that the spectrogram of $A5/3$ is very much different. Therefore, $A5/3$ is more secure than the others.

VI. FUTURE ENHANCEMENT

A new security algorithm, known as $A5/4$, will provide users of GSM mobile phones with an even higher level of protection. It will ensure that, even if a prospective attacker manages to pull a GSM phone call out of radio waves, he will be completely unable to make sense of it, even if he throws massive computing resources at the task. $A5/4$ for GSM, $A5/4$ for ECSD, and GEA4 for GPRS algorithms are stream ciphers that are used to encrypt/decrypt blocks of data under a confidentiality key KC. Each of these algorithms is based on the KASUMI algorithm. The new algorithm was designed by the Security Algorithm Group of Expert (SAGE) of the European Telecommunication Standard Institute (ETSI), based on a requirement specification produced by 3GPP’s working group SA3. The development was carried out with the support of the GSM Association, 3GPP and the United States’ T1 Standard Committee, sponsored by the Alliance for Telecommunications Industry Solutions (ATIS).

VII. CONCLUSION

Exponential increase in mobile subscribers, it has been estimated that computing power doubles every two years. An algorithm that is secure today may be breakable in next few years. Since any system being designed today must work for many years after design, a reasonable requirement is that the procedures must last at least 12-15 years. Thus, the algorithm design must consider the vest cracking algorithms available today and must have provision for being upgraded in the field.

REFERENCES