EEE-GSM: End-to-End Encryption Scheme over GSM System

Mohammed Ramadan[1, 2], Guohong Du[2], Fagen Li[1] and Chun Xiang Xu[1]

[1]*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Gaoxin West Zone, Chengdu 611731, P.R.China*
[2]*School of Electronic Engineering, Chengdu University of Information Technology, Xuefu Road, Chengdu 610225, P.R.China*
nopatia@gmail.com

Abstract

GSM system is widely used by hundreds of millions of people. In fact there is no encryption scheme provides the reasonable security level (user-to-user encryption), it's just provide the Air-interface encryption i.e. between the mobile station and the base station. Furthermore, there are other wireless links are vulnerable to attacks. It is therefore of great importance to provide reasonable security techniques to ensure the privacy of the mobile users especially circuit switching-based services, as well as prevent unauthorized use of the service. In this paper, a new approach is proposed to provide end-to-end encryption for the GSM system (EEE-GSM). This is achieved by using CL-PKC with some modifications and follow some assumptions in GSM system architecture in order to make the scheme compliant to the GSM cellular system. However, the proposed scheme not only efficient due to end-to-end security, but can also provide a secure system against IMSI catcher, man-in-the-middle, and replay attacks.

Keywords*: End-to-end security, GSM Security, GSM Encryption, Certificateless Public Key Cryptography*

1. Introduction

The name GSM first came from a group called (Group Special Mobile), and then became the short term for (Global System for Mobile communication) which was formed in 1982 for European countries. Security has become a crucial topic in current mobile and wireless networks, and the security procedures for such networks elevates as well as the techniques used to attack the wirless networks. Wireless communication security is therefore the measures or techniques used to protect the wirless communication between certain entities [1].

GSM system needs more security to protect the entities from any third party attacks, such as revealing a particular identity, data modification, data-hijacking, eavesdropping, and impersonation, and hence protection mechanisms are used. Devoted technologies for securing data and communication are mandatory in wireless networks, and they vary according to the category of wireless technology deployed. In mobile networks, security handles a diversity of issues, from user authentication, to data integrity and encryption [2].

Among the digital communication systems, the security process is very easy to be realized for GSM. In GSM systems, the security processes consists of four parts: authentication, encryption, TMSI reallocation, and equipment identification. However, there are some possible vulnerability issues which are a concern among many researchers. Most of them are the weakness in the basic algorithms used for authentication such as COMP128, and the algorithms used for encryption such as A5/1, A5/2. In the past, these algorithms were considered to be secure, but nowadays the advancement of technology has made these algorithms vulnerable to attacks. Recently, countermeasure against these vulnerabilities has been considered and under implementation. A5/3 and MILENAGE

algorithms are expected to be used for the new security system. They are also open for the cryptographic community to help examine the algorithm and improve it and make less susceptible to man-in-the-middle attack [3].

The network operator provides mobile services to the users, Figure 1 shows the network architecture from the mobile station to the core system:

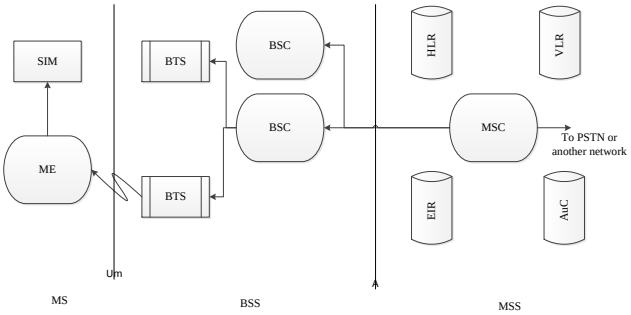

Figure 1. GSM Network Architecture

The rest of the paper is organized as follows: Section 2 introduces briefly the security issues in GSM cellular system, the basic encryption algorithm A5 and its vulnerabilities; Section 3 presents our proposed scheme and shows some assumptions and definitions for our proposed model; Section 4 gives the performance evaluation of our proposed scheme by analyzing the security requirements and the computational cost respectively; Finally Section 5 concludes this work.

2. GSM Security Issues

The cellular system 2G-GSM provides several security functions such as: authentication of the subscriber, data confidentiality, and anonymity of the subscriber. However, the most important and well-known shortcoming of GSM security is that, it does not provide a means for subscribers to authenticate the network. This oversight allows for false base station attacks or IMSI catcher attack [2]. The security methods standardized for the GSM System made it the basic standard for the recent generations e.g. 3G-CDMA and 4G-LTE. Although the confidentiality of a call and anonymity of the GSM subscriber is only guaranteed on the radio channel, this is a major step in achieving end-to-end security. The subscriber's anonymity is ensured through the use of temporary identification numbers. The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping which could only be realized using digital systems and signaling. Particularly in comparison to the previous analog systems, and hence part of the enhanced security of GSM is due to the fact that it is a digital system utilizing a speech coding algorithm, Gaussian Minimum Shift Keying (GMSK) digital modulation, slow frequency hopping (FH), and Time Division Multiple Access (TDMA) time slot architecture. However, to intercept and reconstruct this signal would require more highly specialized and expensive equipment to perform the reception, synchronization, and decoding of the signal. Nonetheless, there have been many attacks on the GSM system in the last few years [4].

Man-in-the-middle is the capability whereby the intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signalling and user data messages exchanged between the two parties by modified BTS in conjunction with a modified MS. Therefore, the above reasons make the GSM system needs hard work to balance the communication parameters (bandwidth, data rate, communication overhead, *etc.*,) with a high security scheme [5, 6].

2.1. Encryption Algorithm (A5)

COMP128 is basically a keyed hash function that takes a 128 bit key Ki, and 128 bit of data RAND, to output a 96 bit hash value. The input RAND is the random challenge supplied by the BTS. The first 32 bits of the hash are used as the response SRES to the challenge and sent back to the network. The remaining 64 bits are used as the session key Kc for voice encryption using some version of the A5 algorithm [7].

The ciphering procedure is presented on the following figure:

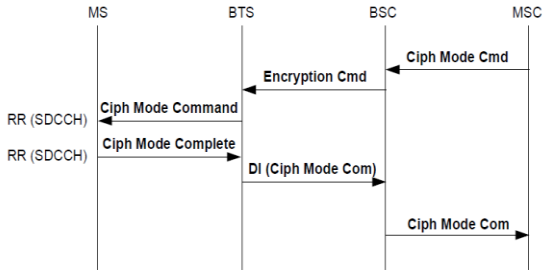

Figure 2: Ciphering Process

- If the authentication procedure is successfully performed, the ciphering mode setting procedure can be initiated by the MSC/VLR (depending on the exchange property setting in the MSC/VLR), which then sends the Ciphering Mode Command to the BSC (See Figure 2), and this is a BSSMAP message which contains the *Kc*, and then forwarded by BSC to the BTS.
- The BTS stores *Kc* and tells the MS to start ciphering, BTS starts the deciphering process, and the Ciphering Mode Command message from BTS to MS will be sent in clear.
- The MS inserts *Kc* and TDMA frame number into algorithm A5, which yields a ciphering sequence that is added to the message to be sent, and this message called Ciphering Mode Complete, and it does not have any parameters, it only tells the BTS that ciphering mode has started.
- When the BTS receives the Ciphering Mode Complete message or any other correctly deciphered layer 2 frame, ciphering is started on the network side, then Ciphering Mode Complete will be sent in a DI frame to the MSC [8].

2.2. Weaknesses of Encryption Algorithms

A Biryukov, A Shamir, and D Wagner presented two cryptanalytic attacks on A5/1, in which a single PC can extract the encryption key K_c in realtime from a small amount of the generated output. Furthermore all these attacks are related to each other, but each one of them optimizes a different parameter. For instance, the first attack called the Biased Birthday attack, and it requires two minutes of data (known key stream) and one second of processing time, whereas the second attack, called the Random Subgraph attack, and it requires two seconds of data and several minutes of processing time. Back in 2002 Alex Biryukov et al. [9] presented the attack on A5/2. It took them less than a day to crack the algorithm, and the information used for these methods was never published. Therefore, the information available on homepages of the authors has been used. The time complexity of the attack is very low, and the session key is found within milliseconds and demonstrates that A5/2 provides weak security. However, the problem with this attack is that it requires the knowledge of the XOR of the key stream used for encryption of two frames that are exactly (2^{11}) frames apart (approximately six seconds apart), and hence if this knowledge is provided, then the key can be found in approximately 10 milliseconds; and this is a softer

requirement than the attack on A5/1 since it requires much less knowledge of the plaintext [10,11,12].

3. Proposed End-to-End Encryption Scheme over GSM (EEE-GSM)

The basic GSM system does not perform end-to-end encryption i.e. user-to-user security, but only between MS and BSS over the air interface. The proposed scheme is based on end-to-end encryption to provide a high security level to the subscribers. The service provider here just provides services for making their calls, and it can not get any information from the switching processes.

The GSM system implements some procedures for making a call over a mobile communications: synchronization, location update, call setup, data transfer, and call clearing. Building on that, the basic process for making a call is (Call Setup process), and all the security services provided in this step. The design proposed for CL-PKC [13] related to the procedure (Call Setup), has two handshaking processes to setup the encryption process (ciphering mode). The proposed scheme also requires two handshaking processes between users and network provider, and it is only for public keys exchange. Furthermore, this proposed design provides end-to-end encryption by ignoring the third party (Network side), and making the MSC\VLR the component responsible only for the public key exchange, and hence by ignoring the third party to achieve end-to-end encryption.

The third party (MSC/VLR) is liable to many kind of attaks, so the most important thing here is that, the step (partial private key extract) in the CL-PKC scheme is totally eliminated, because a third party (the network provider- MSC\VLR) is untrusted, and it can't compute the subscriber's private keys, but it can only do its own function which is to assign TMSI for each user in the roaming status depending on their current location, and checks IMSI from HLR/AuC, then sends the public keys (Y) to the subscribers on the air-interface link, and it's also useful to ignore this step for communications purposes such as reducing the handshaking processes, and low communication overhead.

3.1. Definitions and Assumptions

Definitions:

Here we present some definitions which we need in our proposed scheme [14]:

- ***Mobile station (MS):*** The Mobile Station consists of two parts, the Mobile Equipment (ME) and an electronic "smart card" called a Subscriber Identity Module (SIM card).
- ***Mobile Switching Center (MSC*)**: The main function of MSC is for call- switching in GSM system. Its overall purpose is the same as that of any telephone exchanger.
- ***Visitor Location Register (VLR*)**: The VLR contains a copy of most of the data stored at the HLR. However, it is a temporary data that exists for only as long as the subscriber is "active" within the VLR coverage.
- ***International Mobile Subscriber Identity (IMSI*)**: Each registered user is uniquely identified by its international mobile subscriber identity (IMSI). It is stored in the subscriber identity module (SIM). A mobile station can only be operated if a SIM with a valid IMSI is inserted into equipment with a valid IMEI.
- ***Temporary Mobile Subscriber Identity (TMSI):*** The Temporary Mobile Subscriber Identity (TMSI) is the identity that is sent between the mobile and the network, and it is randomly assigned by the VLR to every mobile in the area, when it is switched on. The number is local to a specific area, and so it has to be updated each time the mobile moves to a new location area. The network can also change the TMSI of the mobile at any time, and it normally does so, in order to avoid the subscriber from being identified by third party attackers, and tracked by eavesdroppers on the radio interface.

- ***Subscriber number (SN):*** It's simply the phone number, and it is not associated with a certain device but with the SIM cards, which is personalized for a user. The SN follows the ITU-T standard E.164 for addresses.
- ***Local Area Identity (LAI):*** Identifies the current location of the subscriber.
- ***Pre-shared key (K_0):*** This is used to authenticate the SIM card, stores in both the SIM card and the Authentication Center AuC.

Assumptions:

The proposed model needs some modifications for suitability of the basic GSM system and in the security model to be compatible to implement in our proposed scheme, and without losing the generality of CL-PKC [13], we only describe the Sign and Verify algorithms as well as the proposed assumptions as follows:

- Let the pre-shared key K_0 in the basic protocol (A5) to be the master key for each user.
- Assume the unique identity (ID) for each user is the subscriber number combine with the area identifier (SN, LAI).
- The identifiers IMSI and TMSI (depending on the current location) are using as random numbers.

3.2. Proposed EEE-GSM Design

The main description of this idea is to let the MSC/VLR assign the subscriber's TMSI or use the specific IMSI and then hash it and send the hashed assignment to the AuC (given that in the basic GSM system the TMSI never transmits to the AuC for security purposes). When this TMSI is allocated in advance by MSC\VLR and it will be sent to the specific MS in the call setup process or in the paging process in case the MS is called from the network. Note that there is no master key provided by the third party (MSC\VLR), and it is replaced by the pre-shared key ($K_{A/B}$).

There is only one algorithm achieved by the MSC\VLR framework and it's Setup (Psys), in addition to the public key distribution. On the mobile station side, there are four algorithms achieved by the MS\SIM, if the user receives a call (MTC) or wants to make a call (MOC), the first step is to compute its own public key ($Y_{A/B}$) and send it to MSC\VLR, then compute its own private key (S_A) depending on the parameters: $K_{A/B}$, $SN_{A/B}$, $LAI_{A/B}$, and $ITMSI_{A/B}$, which are changeable parameters, and related to the current location, then encrypt using the receiver's public key ($Y_{A/B}$), and decrypt using its own private key ($S_{A/B}$). In our proposed design, firstly when a MS requests access to the network, the MSC/VLR will normally authenticate the users MS. The MSC will forward the IMSI to the HLR or check the specific TMSI in its database by the entity VLR, and when the HLR receives the IMSI and the authentication request, it first checks its database to make sure the IMSI is valid and its a part of the network. Once it has accomplished this step, then it will forward the IMSI and authentication request to the Authentication Center (AuC). The proposed EEE-GSM scheme consists of five algorithms as follows:

Setup:

The two users whom want to call each other start to calculate the system parameters P_{sys}: $\{G_1, G_2, e, n, P, P_0, H_1, H_2, H_3, H_4\}$ in the synchronization process, then set secret value $X_{A/B} \epsilon Z^*_q$

Set public key:

Public key can be calculated for the two users by the following steps:

$A_{A/B} = X_{A/B}\, P$

$B_{A/B} = X_{A/B}\, S_{A/B}\, P$

$Y_{A/B} = (X_{A/B}\, P, X_{A/B}\, S_{A/B}\, P)$

After the users calculated their public keys, then they exchange the keys through the network (MSC/VLR) in the call setup process.

Set private key:

When the mobile station receives the other subscriber's public key, it will start to generate the private key by using the following algorithm:
Using the secret value: $X_{A/B}$, and the identity:
$ID_{A/B}= (SN/LAI)_{A/B}$
Compute:
$Q_{A/B}=H_1(SN/LAI)_{A/B}$
Then set the private key: $S_{A/B}=X_{A/B}\ K_{A/B}\ Q_{A/B}$
The master key $K_{A/B}$ is contained in the all MS's (Subscribers side), the algorithm takes the secret value X_A and the preshared key $K_{A/B}$ and it inputs the $(SN/LAI)_{A/B}$ number in the hash function to get (Q_A), then the MS generate the prvate key.

Encrypt:

After $MS_{A/B}$ generates the temporary private/public keys depending on the subscriber's number $SN_{A/B}$, the next algorithm is executed to encrypt a message, and this algorithm runs in the MS. It takes as inputs system parameter (P), a message (M) to be encrypted, and a public key for the receiver (Y_B) which was generated in the previous algorithm, and the receiver phone number and local area identity $(SN/LAI)_{A/B}$, and it outputs the ciphertext (C), then send it to the MSC\VLR to switch it to the receiver as a ciphertext, the encryption algorithm performs the following steps:
User $MS_{A/B}$ checks the other side public key $Y_{A/B}$ as follows:
$e(A_{A/B}, P_0) = e(B_{A/B}, P)$ If not, then abort the call. If holds, then run the encryption process: Compute:
$Q_{A/B}=H_1(SN/LAI)_{A/B}$
Use $(IMSI/TMSI)_{A/B}$ as a random number
For convenience, let N denotes to TMSI or IMSI depending on the switching network and location.
Calculate:
$R=H_3\ (N, M)$
$U= R\ P$
$V= N \oplus H_2(\mathrm{e}(Q_{A/B}, B_{A/B})^R)$
$W= M \oplus H_4(N)$
Compute $C= < R\ P, N \oplus H_2(\mathrm{e}(Q_{A/B}, B_{A/B})^R), M \oplus H_4(N) >$
Then outputs the ciphertext: $C = < U , V , W >$

Decrypt:

This algorithm runs at the receiver and it takes as inputs the ciphertext C, and its own private key $(S_{A/B})$, and it outputs the plaintext (M), the decryption algorithm as follows: Calculate:
$N= V \oplus H_2(e(S_{A/B},U))$
$M= W \oplus H_4(N)$
Then compute:
$R= H_3(N, M)$, and check $U= RP$, If not, then abort the call.
If holds, then the reciever user outputs the plaintext: $M= W \quad H_4(N)$
The main processes of EEE-GSM shown in Figure 3 which are encrypt and decrypt algorithms:

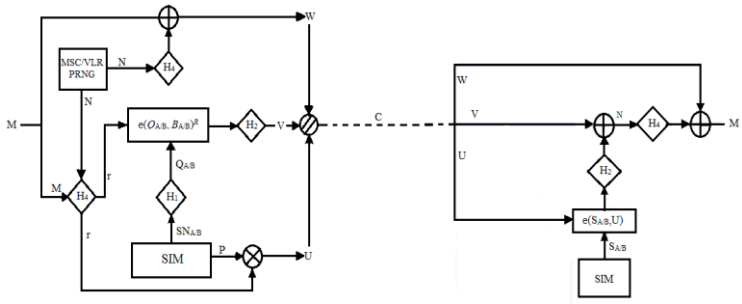

Figure 3. Encrypt/Decrypt Algorithms

If one of the security parameters entered wrong such as P_{sys} or $S_{A/B}$ then the encrypt\decrypt algorithms abort, and these parameters can be manipulated by changing $K_{A/B}$, TMSI/IMSI, or $SN_{A/B}$ by the attacker. However, this approach make the GSM system efficient and secure against such attacks as shown in Section 4.1 for the security analysis of our proposed EEE-GSM scheme.

3.3. Correctness

The $MS_{A/B}$ possesses the public keys $Y_{A/B}$ and exchange the keys in the call setup process and when the $MS_{A/B}$ receives the ciphertext from the other end:
$C = < U , V , W >$
$U= RP$, $V= N \oplus H_2(e(Q_{A/B},B_{A/B})^R)$, $W= M \oplus H_4(N)$
Here, $B_{A/B}= X_{A/B} K_{A/B} P$, $S_{A/B}=X_{A/B} S_{A/B} Q_{A/B}$
then it start to calcuate the parameters N and M using its own private as follows:
$N= V \oplus H_2(e(S_{A/B}, U))$ and $M=V \oplus H_4(e(S_{A/B}, U))$
Using U, V, and $S_{A/B}= X_{A/B} K_{A/B} Q_{A/B}$
$N= N \oplus H_4(e(Q_{A/B}, B_{A/B})^R) \oplus H_4(e(X_{A/B} K_{A/B} Q_{A/B}, RP))$
By using the pairing properties (Bilinear property):
$M= M \oplus H_4(e(Q_{A/B}, B_{A/B})^R) \oplus H_4(e(Q_{A/B}, X_{A/B} K_{A/B} P)^R)$ for $B_B=X_{A/B} S_{A/B} P$
Then, $N= N \oplus H_4(e(Q_{A/B}, B_{A/B})^R) \oplus H_4(e(Q_{A/B},B_{A/B})^R)$
As well as we get N then we can compute the plaintext:
$M= W \oplus H_4(N)$, and $M= M \oplus H_4(N) \oplus H_4(N)= M$

4. Performance Evaluation

In this section we demonstrate that our proposed scheme is efficient and secure in both security and computational complexity aspects:

4.1. Security Analysis

Security algorithms of the GSM (A3, A5, and A8) are all unpublished, secret algorithms. Researchers have reverse-engineered these algorithms and they have shown that these algorithms have many important security flaws, for example in the GSM authentication phase, two related parameters, RAND and SRES, are transmitted on the air interface in clear. So any listener on the air interface between MS and BTS or between BTS/BSC and MSC can perform a known plain text attack on the RAND - SRES pair to obtain the authentication key, and then the attacker can further obtain the encryption key [15]. Therefore, due to the weaknesses in the GSM system, the GSM systems requires a lot of work to calibrate the communication parameters with high security schemes in order to prevent such vulnerabilities, and the GSM does not provide end-to-end encryption (user-to-user security) and the users always want to be in secure hand and they don't trust the service providers, and by this proposed scheme we can build up the trust again.

Furthermore, The proposed scheme makes the system more robust against many kind of attacks such as false base station attack, core system attack, and Man-in-the-middle attack.

Proposition 1. EEE-GSM provide end-to-end security.

EEE-GSM scheme provide end-to-end encryption and somehow mutual authentication, the first authentication when user A get guarantee user B public key, and its message will encrypt for user B { $e(A_B, P_0) = e(B_B, P)$}, the second authentication when user B checks the value {$U= RP$} by computing N and R and make sure this message comes from user A, so there is no way the intruder puts itself in between the network components for eavesdropping, and it's the most important problem for the GSM security. This problem can be solved by the proposed scheme, because the adopted scheme CL-PKC is robust against these type of attacks, and by providing end-to-end encryption making the system more secure [16].

Proposition 2. EEE-GSM is secure against IMSI catcher attack.

IMSI catcher attack AKA False base station is a widespread attack in the field of mobile communication security, generally the attacker can tap conversations in real time by performing a man-in-the-middle attack, and the the user's identifiers can act as a false base station between the mobile station and base station to act as a real base station. For more details, when the user encrypt a message using algorithm A5/2, Then the attacker can implement ciphertext only attack to get the user secret key K_0 in a very short period of thime (less than second), and then the attacker sends a response to the network operator. Building on that, and when the network start encryption mode the attacker can start encrypt his data using algorithm A5/1 or A5/3, and the attacker already gets the correct secret key K_0, and then can send the response encrypted by using algorithm A5/1 or A5/3. Thus, the network operator will treat the attacker as a legal valid user. Furthermore, the delay of this attack can not be useful to detect such attack, because it needs less than one second, and the delay allowed by the GSM standard is 12 seconds. However, our proposed scheme is secure against such attack due to the identifiers protection by using hash, and the pre-shared key K_0 as a master key. In addition, the using the secret value and IMSI/TMSI parameters, and hence, the proposed scheme provides more security level to the users somehow by using temporary identifiers (TMSI) instead of (IMSI) when the user is in the roaming mode [17].

Proposition 3. EEE-GSM is secure against replay attack.

To prevent the cryptosystem from such attack, we often use random numbers, sequence number, or timestamp, and each of these techniques has its own boundaries to use. The EEE-GSM scheme is free from this attack by using IMSI/TMSI as a random numbers and will be changeable when the user moves from the current location area to another one, which make the private/public keys changeable, accordingly giving more security features to the proposed scheme, and by using the secret value $X_{A/B\ to}$ compute the private/public keys. Moreover, the parameters SN/LAI are used as a unique identity for each user, which ensures the freshness of the private/public keys. In this sense, there is another level of security to the system by checking SN/LAI parameters in addition to the public keyin the call setup processes by default [18].

Proposition 4. EEE-GSM is secure against type II adversary attack.

Certificateless cryptography (CL-PKC) is an interesting alternative to traditional PKI. It makes use of identities, which are users' public keys made of arbitrary strings, in place of certificates. Besides, it's infrastructure is lightweight and can be deployed at relatively lower cost. Additionally, it offers transparent encryption, so that non-technical users could easily secure their data easily because of the CL-PKC features especially the lack of key escrow property. Moreover, to encrypt a message to another user, three pieces of information are needed (the other user's public key, identity, and the third party's public parameters), to decryption process a user just needs to use their private key. For tight security, a certificateless system has to prove its security against two types of adversaries. Type I adversary attack refers to any third party who can fake the user's public keys,

corresponding to the user's random secret value. Type II adversary attack refers to a compromised or malicious KGC, who has access to the partial public and private keys of all users, more details in Ref [19]. However, The proposed EEE-GSM scheme is secure against theses attacks, and the attacker can not get the plaintext without the knowledge of the all secret parameters.
The following table (Table 1) illustrates the comparison of security-based performance efficiency for our proposed scheme with the basic scheme A5 and scheme [20] [21]:

Table 1. Comparison of security-based performance evaluation

Security Parameters	A5	Ref [20]	Ref [21]	EEE-GSM
End-to-end security	N	N	Y	Y
IMSI catcher attack	N	Y	N	Y
Replay attack	Y	Y	Y	Y
Type II attack	N/A	N	N	Y

Y: Robust; N: Not robust; N/A: Non-Applicable

The proposed approach is more efficient than other competing topologies. In comparison to other schemes, such as A8 or A5 algorithms in a GSM system, and schemes [20] [21], due to the flexiblity of Certificate-less Cryptography and provide a secure cryptosystem.

4.2. Computational complexity

Since GSM systems offer a relatively high performance as mentioned in the introduction section, the security feature can be enhanced using the new network utilities as much as a strong security is needed. However, the only practical problem might be a relatively higher computational cost than A5, but it will be improved as new mathematical propositions are implemented.
The performance of our proposed scheme is evaluated using the existing experimental setup of [22] [23] [24] for a variety of cryptographic operations using MIRACLE [25] in PIV 3 GHZ processor with Windows XP operating system and 512 MB memory. From [22] [23] [24] the relative running time for the operations we employed in our proposed model as follows:
T_h: Hash function= 3.04 ms.
T_p: Pairing operation time complexity= 20.01 ms.
T_m: Pairing-based scalar multiplication= 6.38 ms.
T_e: ECC-based scalar multiplication= 0.83 ms.
The other operations: Omitted.
The following table (Table 2) illustrates the performance efficiency based on running time of our proposed model:

Table 2. Computational complexity-based performance evaluation

Phase	Operation	Running time(ms)
Encrypt	$3T_h+T_p+T_m+T_e$	36.34
Decrypt	$3T_h+T_p$	29.13
Total	$6T_h+2T_p+T_m+T_e$	65.47

According to the computational cost we clearly can note that the total running time in MS side is 65.47 (ms). That means, the proposed model scheme is quite reliable to be

implemented in the real field of the GSM mobile communication systems. Generally, from the above analysis and results it can be noted that the proposed EEE-GSM scheme has reasonable computational complexity and provide efficient and secure system.

4. Conclusion

The users and the service providers would never want their resources and services to be used by unauthorized users. In this work, a technique to provide end-to-end encryption for the GSM system with a little handshaking procedures was demonstrated using Public Key Infrastructure approach PKI, similar to the A5 algorithm. GSM system is being used as a basis for the next generation of mobile communication technologies (3G and 4G) in the world. Certificate-less cryptography can be the most suitable scheme for the mobile communication security because its lightweight infrastructure, and it's lack of certificates, and CL-PKC is a promising solution improving several weaknesses of PKI and Identity-Based Cryptography IBC. The proposed EEE-GSM scheme is made as suitable as possible for the GSM system. Although the scheme is rather complex, it allows for many details to be hidden so that end-users are not concerned with manual handling of data security.

References

[1] M900/M1800 GSM SYSTEM, Training Documents, Huawei Technologies CO. Ltd. Training Center.

[2] Jorg Eberspacher, Hans-Jorg Vogel, Christian Bettstetter, "GSM, switching, Services and Protocols", 2nd edition, (WILEY), 2001.

[3] European Telecommunications Standards Institute (ETSI), Digital cellular telecommunications system (Phase 2+); Mobile Station – Base Stations System (MS – BSS) Interface Data Link (DL) Layer Specification, TS 100 938 (GSM 04.06), http://www.etsi.org.

[4] Goswami, Sukalyan, et al. "Enhancement of GSM Security Using Elliptic Curve Cryptography Algorithm." Intelligent Systems, 2012 Third International Conference on Modelling and Simulation (ISMS). IEEE, 2012.

[5] Petracca, Marco, et al. "Performance evaluation of GSM robustness against smart jamming attacks." Communications Control and Signal Processing (ISCCSP), 2012 5th International Symposium on. IEEE, 2012.

[6] Barkan E, Biham E, Keller N, „Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communications", Journal of Cryptology, 21(3), pp. 392-429. DOI: 10.1007/s00145-007-9001-y, June 2008.

[7] ETSI, Recommendation GSM 02.09: security aspects, Technical Reports, European Telecommunications Standards Institute, ETSI, 1993.

[8] Alberto Peinado, "Privacy and authentication protocol providing anonymous channels in GSM", Computer Communications Vol. 27, pp. 1709-1715, 2004.

[9] Alex Biryukov, Adi Shamir, David Wagner, "Real Time Cryptanalysis of A5/1 on a PC", Springer, Volume 1978 of the series Lecture Notes in Computer Science, pp. 1-18, January 2002.

[10] LI Lei, LIU XiangHui, WANG Zheng, LIFengHua, „An improved attack on clock-controlled shift registers based on hardware implementation", SCIENCE CHINA Information Sciences, Vol. 56, Issue: 112107(10), DOI: 10.1007/s11432-012-4682-8, September 2012.

[11] Gligoric, N., et al. "Application-layer security mechanism for M2M communication over SMS." Telecommunications Forum (TELFOR), 2012 20th. 2012.

[12] Chakraborty, Satarupa. "Furtherance of Elliptic Curve Cryptography Algorithm in the field of GSM security", International Journal Of Scientific & Engineering Research, Volume 3, Issue 10, ISSN: 2229-5518, October 2012.

[13] Al-Riyami, Sattam S., and Kenneth G. Paterson. "Certificateless public key cryptography." Advances in Cryptology-ASIACRYPT 2003. Springer Berlin Heidelberg, pp.452-473, 2003.

[14] European Telecommunications Standards Institute (ETSI), Digital cellular telecommunications system (Phase 2+); Physical layer on the radio path; General description, TS 100 573 (GSM 05.01), http://www.etsi.org.

[15] Alexander Maximov, Thomas Johansson, Steve Babbage, "An improved correlation attack on A5/1", proceedings of SAC 2004, LNCS 3357, pp. 1–18, Springer-Verlag, 2005.

[16] Jerry Rick Ramstetter, Yaling Yang, Danfeng Yao, "Applications and Security of Next-Generation, User-Centric Wireless Systems", Future Internet 2010, 2, 190-211; doi: 10.3390/fi2030190, July 2010.

[17] Shahnaz Saleem, Sana Ullah, Kyung Sup Kwak, "A Study of IEEE 802.15.4 Security Framework for Wireless Body Area Networks", Sensors 2011, 11, 1383-1395; doi: 10.3390/s110201383, January 2011.

[18] Simone Cirani, Gianluigi Ferrari, Luca Veltri, “Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithmic Overview”, Algorithms 2013, 6, 197-226; doi: 10.3390/a6020197, April 2013.
[19] Alexander W. Dent, Caroline Kudla, “On Proofs of Security for Certificate-less Cryptosystems”, Cryptology ePrint Archive Report 2005/348, January 2005.
[20] Sukalyan Goswami, Subarna Laha, Satarupa Chakraborty, Ankana Dhar, “Enhancement of GSM Security Using Elliptic Curve Cryptography Algorithm“, 2012 Third International Conference on Intelligent Systems, Modelling and Simulation (ISMS), DOI: 10.1109/ISMS.2012.137, February 2012.
[21] Heshem A. El Zouka, “PROVIDING END-TO-END SECURE COMMUNICATIONSIN GSM NETWORKS”, International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.4, July 2015.
[22] Mohammed Ramadan, Fagen Li, Chun Xiang Xu, Ahmed Abdalla, Hisham Abdalla, “An Efficient End-to-End Mutual Authentication Scheme for 2G-GSM System“, In Proc. 2016 IEEE International Conference on Big Data Analysis (ICBDA 2016), March 2016.
[23] Mohammed Ramadan, Fagen Li, Chun Xiang Xu, Abdeldime Mohamed, Hisham Abdalla, Ahmed Abdalla. ” User-to-User Mutual Authentication and Key Agreement Scheme for LTE Cellular System”. International Journal of Network Security, Vol.18, No.4, pp.769-781, July 2016.
[24] Mohammed Ramadan, Fagen Li, Chun Xiang Xu, Kwame Oteng, Hesham Ibrahim. “Authentication and key agreement scheme for CDMA cellular system”. 2015 IEEE International Conference on Communication Software and Networks (ICCSN), IEEE Xplore Digital Library, 10.1109/ICCSN.2015.7296138, pp.118 – 124, June 2015.
[25] MIRACLE, Multiprecision Integer and Rational Arithmetic C/C++ Library, http://indigo.ie/ Mscott.