An Efficient End-to-End Mutual Authentication Scheme for 2G-GSM System

Mohammed Ramadan, Fagen Li, Chun Xiang Xu, Ahmed Abdalla, Hisham Abdalla
School of Computer Science and Engineering
University of Electronic Science and Technology of China (UESTC)
Chengdu Sichuan 611731, P.R. China
e-mail: nopatia@gmail.com

Abstract-**The security architecture of the mobile networks provides different security features such as authentication, confidentiality, and integrity for both users and network operator. Moreover, the security of mobile communications becomes a hot topic and always need security improvements. GSM cellular system has many weaknesses, especially in the authentication process due to the lack of the physical protection mechanisms in both user and network sides. This paper analyses an existing GSM authentication scheme based on CL-PKC which was proposed in 2014, and it has many weaknesses since it used the basic CL-PKC scheme which has many weaknesses itself. And this paper also proposes an efficient end-to-end scheme for GSM mutual authentication using the concept ofa secure CL-PKC, with some modifications in both security and GSM network architectures.**

Keywords-2G-GSM Security; GSM Mutual Authentication; Certificateless Public Key Cryptography (CL-PKC)

I. INTRODUCTION

The Global System for Mobile communication (GSM) was developed during the 1980s; GSM is the standard Pan European digital cellular system, now accepted as the worldwide wireless communication standard. GSM currently composes of: GPRS designed for web browsing, 3G, which is the system running on third generation standards for multimedia, and EDGE, a technology which allows improved data transmission rates as a compatible extension of GSM. [1-3].

Global efforts to strengthen security mechanisms through research and development have been necessitated by the rapid progress in mobile communication technologies. Since an open channel is used for transmission purposes, the content of the communication may be captured by a third party, resulting in eavesdropping, masquerading, replaying etc. GSM currently lacks in providing mutual authentication, occupies storage overhead and also consumes lot of bandwidth. Further, it is susceptible to a false base station attack without mutual authentication. Despite this, GSM communication technology has gained momentum as a vital mobile communication technology. It provides voice services, bearer services like short messaging services and a set of supplementary services.

The security requirements for the mobile communications networks can be listed as follows [4 -6]:

Confidentiality: This means that the transmitted information is only disclosed to the authorized parties. This also prevents sensitive information from being disclosed to an adversary, such an instance occurring would inspire severe consequences.

Integrity: The assumption that a message is not altered in transit between sender and receiver. Messages however, can be corrupted due to network malfunctioning or malicious attacks.

Authentication: Authentication corroborates the identity of the entities which are communicating. In the absence of authentication mechanisms, an attacker can attempt to violate the security of the network by masquerading as a legitimate entity.

Access control: Access control means that only authorized parties can be allowed to access a service on the network, use a resource, or participate in the communications; any other entity is denied access. The access control assumes the authentication of the entity trying to get access to the network.

Nonrepudiation: If nonrepudiation is guaranteed, the receiver of a wrong message can prove that the originator has been transmitted. This means that the source of a message cannot deny having sent the message. An attacker could generate an incorrect message that appears to be initiated from an authorized party.

Network availability: Availability ensures that all resources of the communications network are always utilizable by authorized parties. An attacker may launch a Denial of Service (DoS) attack by flooding the medium, jamming the communications, or keeping the system resources busy in any other way or by any other means.

For both the user and service provider, the authentication process is considered to be the most important security feature to ensure that the network service will not be obtained duplicitously.

A. Motivation

In this paper, we show that the proposed certificateless signature scheme in [7] does not satisfy the security requirements of GSM security system, in terms of the security architecture and the proposed assumptions. To be more precise, the main vulnerability of the scheme [7] is when an attacker replaces a public key, where they can always successfully forge a signature. Furthermore, we also provide a new scheme which opposes against these vulnerabilities and hence satisfies the security requirements of GSM cellular system.

The rest of the paper is organized as follows: Section II introduces the basic GSM authentication protocol and its

weaknesses; Section III presents briefly the vulnerabilities and some threats in Ref [7] which are the motivations for this paper; Section IV presents our proposed scheme, the system design and the phases of our offered scheme; in Section V we evaluate our advised scheme by analyzing the security and the performance efficiency respectively; Finally, Section VI concludes our work.

II. The Basic Gsm Authentication Protocol

The original protocol is a challenge/response mechanism in which a mobile station is authenticated through message exchanges between the base station and the mobile station. This process is shown as follows [8], [9]:

When a Mobile Station (MS) attempts to access the GSM network, it sends an authentication request to the Visiting Location Register (VLR). The request contains the Temporary Mobile Subscriber Identity (TMSI) and the Location Area Identity (LAI). The VLR obtains the MS's International Mobile Subscriber Identity (IMSI) through analyzing the TMSI, and then sends the IMSI to the Home Location Registers (HLR). Then the HLR generates a 128-bit random number RAND, and uses algorithms A3 and A8 to create *SRES1,* and *K,* respectively. A3 and A8 both take RAND and the MS's secret key *K as* inputs. Finally, the triplet {RAND, *SRES1, K}* is sent to the VLR, and the VLR forwards RAND to the MS. When the MS receives RAND, it also uses algorithms A3 and A8 to generate *SRES2* and *K,* respectively, using the MS's secret key *K* and RAND as inputs. Then the MS keeps *K,* for secret communication and sends *SRES2* back to the VLR. Finally, when the VLR receives *SRES2*, it compares the *SRES2* with *SRES1* which is calculated in advance. If this authentication holds, then MS can get access to the network resources.

The following figure illustrates the basic GSM authentication protocol.

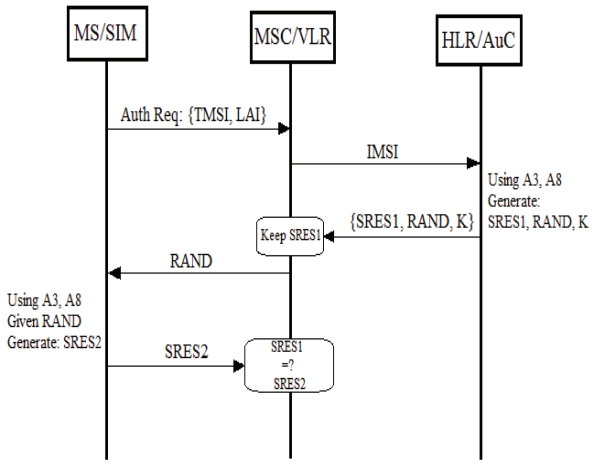

Figure 1. The basic GSM authentication protocol

An important and well-known shortcoming of GSM security is that subscribers cannot authenticate the network, leaving users open to man-in-the-middle attacks. This oversight is the main cause of such false base station attacks. 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, utilize spoof signaling and view user data messages exchanged between the two parties. The required equipment is modified BTS in conjunction with a modified MS [10], [11]. The above reasons require the GSM system to calibrate the communication parameters (Bandwidth, Time delay) with a high security scheme [12].

III. A Review of our Previous Work

In this section, we review Ref [7] scheme and its vulnerabilities. The scheme proposed in [7] has many weaknesses in both security and communications sides. For the security side, the proposed scheme adopts the basic certificate less public key cryptography (signature algorithm CL-PKS) [13].

In the given scheme, there are four algorithms achieved by the HLR/AuC (network side): Setup, Partial Private Key Extract, Set Public key, and Verify. On the mobile station side, there are three algorithms achieved by the MS\SIM (user side): Verify Partial Private Key, Set Private Key, and Sign IMSI as a message.

The AuC can make the main processes in CL-PKC (Setup, Partial Private Key extract, and set public key). These processes depend on the Authentication Center master key S and the Secret key K_0. The output System parameters Psys with the secret key K_0 are used to generate the public key.

The partial private key D is sending to MS via MSC when authentication is requested, The AuC runs the next algorithm (Set public key) immediately and stores it for a specific time period to verify the signature σ, when it is received from the Mobile station (MS).

Mutual authentication algorithm: The proposed scheme in Ref [7] provides a mutual authentication. When the mobile station receives a partial private key D, it will authenticate the network operator as follows:

$e(D, P) = e(Q, P_0)$ Where, $P_0 = SP$, $D = SQ$

So we get, $e(D, P) = e(Q, SP)$

The master key S is not contained in the SIM card (Subscriber side) but the algorithm takes the system parameters and its own *TMSI* which is assigned in the paging process (call setup). It inputs the *TMSI* in the hash function to get Q, and compares the above equation, so that the partial private key can be confirmed to be from the AuC; then the AuC is authenticated.

Signature algorithm: The sign algorithm performs the following steps:

1. Choose random $a \in Z^*_q$
2. Compute:
   $r = e(aP, P) \in G_2$
3. Set $v = H(IMSI, r) \in Z^*_q$
4. Compute:
   $U = v K_S + a P \in G_1$
5. Output as the signature: $\sigma = \langle U, v \rangle$

Verification algorithm: The verify algorithm performs the following steps:

1. Compute: $r = e(U, P).e(Q, -Y)^V$

2. Check: $v = H(IMSI, r)$ holds.

If it does, output (Valid). Otherwise output (Invalid).

A. Review the basic CL-PKC Weaknesses

CL-PKC is first introduced by Al-Riyami and Paterson [13] to solve the key screw problem in the previous Identity-based schemes (IBC) [14]. CL-PKC has been improved in many different security aspects to provide a secure cryptosystem [15-18].

The basic CL-PKE (encryption algorithm) is considered to be secure in a One-Way Encryption (OWE) model, in which Type I and II adversaries have the same capabilities regarding public and private keys, but when there is no decryption queries, and the challenge to the adversary is simply to decrypt a challenge cipher text [13].

The basic CL-PKS (signature algorithm) is considered to be unforgeable against Type II Adversary attack, in which the adversary has access to the master key, but cannot replace the public keys. In contrast, this algorithm is forgeable against Type I Adversary attack, in which the adversary cannot get access to the master key but can perform public keys replacement. Then we can note that the basic CL-PKS does not resist against type I adversary since the adversary can successfully forge a user's signature on a message of its choice. See Ref [19] for the full security proof of the basic CL-PKS.

B. Review the System Assumptions of our Previous Work

In this section we can note that there are many weaknesses in Ref [7] system assumptions as follows:

- We cannot assume that the security architecture for the GSM cellular system is all secure except the air-interface. Therefore, many kinds of attacks can be achieved even via a secure air-interface.
- Assume that the AuC is a KGC and trusted party for all subscribers, because here the AuC can compute all the subscriber's private keys. The AuC entity is a database in the GSM architecture as well as VLR is a database for roaming purposes, and this assumption does not give the system any reliable from the inside attack.
- Suppose that the (SIM card) includes all the necessary information (IMSI, system parameters Psys, K_0, and master key S). The SIM card can be an unsecure entity against cloning attack.
- Using TMSI number as a unique identifier for each subscriber, which is randomly assigned by the (VLR) to every mobile in the area when it is switched on. The weakness in this assumption is that the temporary identifier TMSI is used instead of IMSI to keep the permanent identifier IMSI secure, and hence, in case the mobile station it stay in its home network, so we cannot get any temporary identifier TMSI to assign it as identity to calculate the private/public keys.
- Using IMSI number as a message (M) which stored on both SIM card and AuC. This assumption give more risk to GSM cellular system due to the importance of keeping the permanent identifier IMSI secret as much as we can and to give the system more privacy.
- Assume that all subscribers have a unique key (K_0), and that it illustrates the secret value in the basic CL-PKC. Here the secret value (K_0) is known by both AuC in the network side and the mobile station. This assumption does not make sense for the functionality of CL-PKC due to the lack of the randomness assumption in Ref [7].

C. Security Weaknesses of our Previous Work

The weaknesses found in scheme [7] are not only in security architecture, but also in GSM network architecture. The main vulnerability of scheme [7] {is when the attacker who does not possess the master-key but only can replace a public key (which is related to the user's identity) can successfully forge a signature. Furthermore, we note that the proposed scheme in [7] fails against type I adversary because the users' MS authenticate the MSC/VLR by checking the equality: $e(D, P) = e(Q, P_0)$ holds. However, this is not sufficient to deter against type I adversary. This equality only guarantees that$P_0 = sP$. The test should also cover a mechanism to make sure that the secret value K_0 has been used correctly to obtain the private/public keys, and hence, there is no way to check whether K_0in the public key is identical to the one in the private key. However, this important aspect is abandoned in the design of scheme [7], and the partial private key needs to be delivered securely to user. Therefore, from the above reasons scheme [7] is insecure as well as inflexible.

IV. The Efficient GSM Mutual Authentication Scheme

In this section we provide our efficient scheme which it can solve the weaknesses in scheme [7]. Furthermore the proposed scheme provides high performance security features for GSM cellular system and more flexibility by providing end-to-end mutual authentication, and hence, the proposed scheme has a very important additional benefit which it can reduce the degree of trust that mobile stations MS's need to have in the network operator MS/VLR, HLR/AuC entities in our proposed schemes.

The basic GSM cellular system doesn't provide end-to-end security i.e. between users, but only between MS and BS over the air interface. The proposed scheme is based on end-to-end mutual authentication to provide more security to the subscribers by using secure CL-PKC scheme. The service provider here just provides services for making their calls, and it cannot get any information from the switching processes.

A GSM system implements the following procedures to establish a channel over GSM mobile communications system:

1. Synchronization (Setup: generate system parameters, keys, assign IMSI/TMSI).

2. Location update (Public key exchange, MSC authenticates MS_s).

3. Call Setup (end-to-end authentication i.e. MS_s Authentication).

4. Data Transfer (Encrypt/Decrypt process).

5. Call Clearing (Generate a new keys if necessary).

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 proposed assumptions as follows:

1. Assume LAI parameter as a unique identifier for each user.
2. Let the pre-shared key K_0in the basic protocol A3 to be a master key for each user.

Assume that the message will be signed is the subscriber number SN (Dialing Number)

3. The identifiers IMSI or TMSI (depending on the current location) are using as random numbers for the signature algorithm.

Public key exchange and MSC/VLR authenticates $MS_{A/B}$: After MSs and MSC generate system parameters and private/public keys, then each user send its own public key as service request, this request contains the Location Area Identity (LAI) and the public keys ($X_{A/B}$, $Y_{A/B}$), and hence, VLR obtains the MS's International Mobile Subscriber Identity (IMSI) through analyzing the TMSI, and then sends the IMSI to the Home Location Registers (HLR). Then the HLR generates a 128-bit random number R., then using LAI as a unique identity ID for each user:

$Q_{A/B}= H_1 (\mathrm{LAI}_{A/B})$

Each user will set secret value:

$X_{A/B} \in Z^*_q$

User's public keys:

$T_{A/B}= (A_{A/B}, B_{A/B})=(X_{A/B}P, X_{A/B}K_{A/B}P)$

$Req_{A/B}=Q_{A/B}// K_{A/B}$

When MSC/VLR received the $Req_{A/B}$, it will authenticate ($MS_{A/B}$) i.e. the users as follows:

$e(A_{A/B}, P_0) =?e(B_{A/B}, P)$holds. If not, then abort access.

User-to-user authentication: When the mobile stations receive the other subscriber's public key, it will start to generate the private key by using the pre-shared key $K_{A/B}$ is contained in the all MS's (Subscribers side) as follows:

$S_{A/B}=X_{A/B} K_{A/B}Q_{A/B}$

Sign: This algorithm takes $SN_{A/B}$ (Subscriber number) as a message, and using the private key $S_{A/B}$, and ($IMSI/TMSI_{A/B}$) as a random and unique number, and by using the other user's public key, then perform the following steps:

1. Let ($IMSI/TMSI_{A/B}$)= $R \in Z^*_q$
2. Compute $W= e(RP, P)$
3. Compute $V= H_2 (SN_{A/B}, W, e(S_{A/B}, P))$
4. Compute $U= V S_{A/B}+ RP$
5. Output the signatures $Res_{A/B}= (U, V)$

Verify: When the users receive $Res_{A/B}$ will start to authenticate each other by using its own private key and perform the following steps:

1. Compute $W= e(U, P)\, e(Q_{A/B}, -B_{A/B})^V$
2. Check if:
   $V = H_2(SN_{A/B}, W, e(Q_{A/B}, B_{A/B}))$ holds
   If not, then abort access

The following figure illustrates the processes of the proposed model:

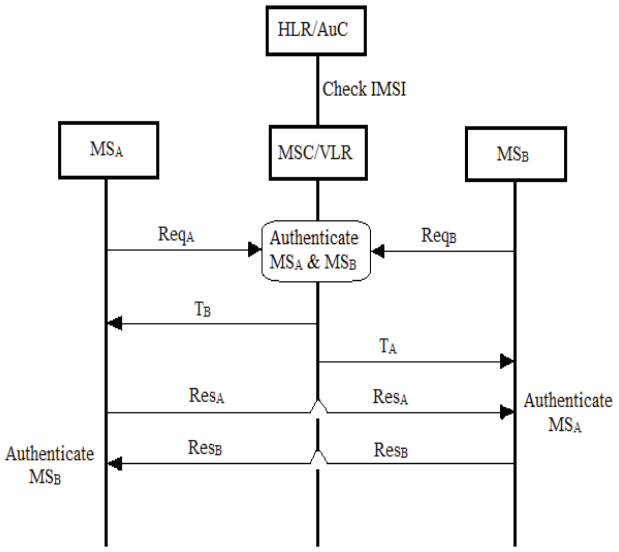

Figure 2. The proposed end-to-end mutual authentication model

Correctness:

When the users $MS_{A/B}$ receive: $Res_{A/B}= (U, V)$

$V= H_2 (SN_{A/B}, W, e(S_{A/B}, P))$, Where, $W= e (RP, P)$

$U= V S_{A/B}+ RP$

It will start to calculate:

$W^*= e(U, P)\, e(Q_{A/B}, -B_{A/B})^V$

$= e(V S_{A/B}+ RP, P)\, e(Q_{A/B}, - X_{A/B}K_{A/B} P)^V$

By using bilinear paring properties:

$W^*= e(V S_{A/B}+ RP, P)\, e(-VX_{A/B}K_{A/B}Q_{A/B}, P)$

$= e(V S_{A/B}+ RP, P)\, e(-V S_{A/B}, P)$

$= e(V S_{A/B}+ RP- V S_{A/B}, P)= e (RP, P)= W$

Then the user use W to calculate V as follows:

$V^* = H_2 (SN_{A/B}, W, e(Q_{A/B}, B_{A/B}))$

$= H_2 (SN_{A/B}, W, e(Q_{A/B}, X_{A/B}K_{A/B} P))$

By using bilinear paring properties:

$V^*= H_2 (SN_{A/B}, W, e(X_{A/B}K_{A/B}Q_{A/B}, P))$

$=H_2 (SN_{A/B}, W, e(S_{A/B}, P))= V$

V. Performance Analysis

In this section we demonstrate that our proposed scheme is more efficient and indeed improves the performance in scheme [7] in the aspects of security and communication.

A. The Security Analysis of the Proposed Scheme

In our proposed scheme we provide a modification to the full CL-PKS. Unlike the scheme in [7], our scheme is secure against type I and II adversaries. The validity of the public key can be checked very efficiently. Assuming that the

bilinear map groups (G_1,G_2) are chosen by a higher level authority HLR/AuC and commonly used by several MSC/VLR's, so the users' MS may generate their public key independently without help of any authority in the system, and this is due to the value $V= H_2$ ($SN_{A/B}$, W, e($S_{A/B}$, P)) which is determined by the message $SN_{A/B}$ (user's dialing number), (IMSI/$TMSI_{A/B}$),and the private key, and hence, the attacker cannot use the value $V$to change the public key of the signer because the private key $S_{A/B}$ is determined only by the user's public key. The following table I shows comparison of the security-based performance efficiency for our proposed scheme with the basic scheme A3 and scheme [7]:

TABLE I. COPARISON OF SECURITY EFFICIENCY

Security Parameters	A3	Ref [7]	Our scheme
Mutual authentication	N	Y	Y
End-to-end security	N	N	Y
Type II attack	N/A	N	Y
Forward/Backward secrecy	N	N	Y
False base station attack	N	Y	Y

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

Making the MSC\VLR the component responsible only for the public key exchange, and here we ignore the third party to achieve end-to-end security. The third party (MSC/VLR) is liable to many kind of attacks, 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 check TMSI depending on their current location, and checks IMSI from HLR/AuC, then exchange the public keys, and this concept is useful for communication reasons the data rate and handshaking reduction (overhead considerations).

The proposed model is considered to be secure against many kind of attacks such as replay attack, forward/backward secrecy attack, and IMSI catcher attack i.e. false base station attack due to the changeable private/public keys by using the changeable LAI, and TMSI identifiers as security parameters, and the hash value (V). The temporary parameters are changeable according to the user's location area, and hence when the attacker replays with the previous security parameters, then the services will be abort. Furthermore, there is no way to send a fake message because the subscriber number SN i.e. the dialing number is used as a message to be signed. If the attacker obtained the secret keys still cannot recover the previous session keys due to the security parameters that used in our proposed assumptions, and the security hard problems [20], [21].

B. The Computational Cost of the Proposed Scheme

In the mobile communication field, the cost of computing is very important. When a user requests a service to a provider with payment way, the users care about the transmission and computational cost [22].

The performance of our proposed scheme is evaluated using the existing calculations in [20], [21] which is based on MIRACLE [23] in a platform with specifications of (Windows XP operating system, 3 GHZ processor, 512 MB memory). From [20], [21] the approximate running time for each operation as follows:

Hash operation: T_1 = 3.04 ms
Pairing operation: T_2 = 20.01 ms
ECC-based scalar multiplication: T_3 = 0.83 ms
Pairing-based scalar multiplication: T_4= 6.38 ms
The other operations will be omitted.

The performance efficiency based on running time of the suggested model is shown in the following table II:

TABLE II. COMPUTATIONAL COST-BASED RUNNING TIME OF OUR PROPOSED SCHEME

Phase	Operation	Running time(ms)
Sign	T_1+2T_2+2T_3+T_4	51.1
Verify	T_1+2T_2	43.06
Total	2T_1+4T_2+2T_3+T_4	94.16

According to the computational cost, we can clearly note that the total running time is 94.16 (ms). In this sense, the proposed scheme is quite practical to be implemented in the real field of the GSM systems.

From the above performance analysis, we can observe that the proposed approach is more efficient than other schemes. In comparison to the basic authentication protocol (A_3) and the proposed scheme in [7], our scheme provides more flexible and secure cryptosystem.

VI. CONCLUSIONS

In recent years, GSM has proven to be convenient in that it is widespread across the world. Many authentication protocols are put forward to improve the original authentication protocol of GSM; our proposed scheme is shown to solve main drawbacks in Ref [7] and the basic scheme with modifying the GSM security architecture. In this paper, we outline an efficient scheme to improve the existing GSM authentication protocol A3 as well as to solve the weaknesses in scheme [7]. Our recommended authentication protocols can not only solve all of the drawbacks, but also increases the efficiency of the protocol. In addition, the security is also enhanced significantly, since mutual authentication is ensured all the time. In a word, our proposed scheme is secure and efficient.

REFERENCES

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

[2] Y.B. Lin, "Mobility management for PCS", Tutorial: First Workshop on Mobile Computing, Applied Research, Bellcore Morristown, NJ, USA, 1995

[3] Moe Rahnema, "Overview of the GSM system and protocol architecture", IEEE Communication Magazine,pp. 92-100, April 1993.

[4] H. Imai, M.G. Rahman, K. Kobara "Wireless Communications Security" ARTECH HOUSE 2006.

[5] K. Hellwig, P. Vary, D. Massaloux, ectl. Speech Codec for the European Mobile Radio System. IEEE Global Communication Conf. 1989: pplO65-1069.

[6] Noureddine Boudriga "Wireless Communications Security", CRC 2010 by Taylor and Francis Group, LLC.

[7] Memon, I., Mohammed, M. Ramadan, Akhtar, R., Memon, H., Memon, M. H., Shaikh, R. A. (2014). "Design and implementation to authentication over a GSM system using certificate-less public key", Wireless Personal Communication. doi:10.1007/s11277-014-1879-8

[8] M. Beller, L.F. Chang, and ***Y.*** Yacobi, "Privacy and authentication on a portable communication system", *IEEE Journal on Selected Areas in Communication,* vol. 11, no. 6, pp. 821-829, 1993.

[9] Refik Molva, Didier Samfat, and Gene Tsudik, "An authentication protocol for mobile users", *IEE Colloquium on Security and Cryptography Applications to Radio System,* London, UK, June 1994.

[10] Gligoric,N. ; Dimcic, T. ; Drajic, D. ; Krco, S. ; Chu, N. Application layer security mechanism for M2M communication over SMS, Page(s): 5–8, 20th Telecommunications Forum (TELFOR), 2012.

[11] Goswami, S. ; Laha, S. ; Chakraborty, S. ; Dhar, A. Enhancement of GSM Security Using Elliptic Curve Cryptography Algorithm, Page(s): 639 – 644, Intelligent Systems, Modelling and Simulation (ISMS), 2012 Third International Conference.

[12] Petracca, M. ; Vari, M. ; Vatalaro, F. ; Lubello, G. Performance evaluation of GSM robustness against smart jamming attacks, Page(s): 1 - 6, Communications Control and Signal Processing (ISCCSP), 2012 5th International Symposium.

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

[14] Boneh, D., & Franklin, M. (2001, January). Identity-based encryption from the Weil pairing. In Advances in Cryptology-CRYPTO 2001 (pp. 213-229). Springer Berlin Heidelberg.

[15] S.S. Al-Riyami, K.G. Paterson. "CBE from CL-PKE: a generic construction and efficient schemes". PKC 2005, LNCS vol. 3386, Springer-Verlag, Berlin, pp. 398-415, 2005.

[16] D. H. Yum and P. J. Lee. Generic construction of certificateless signature. In ACISP'04, volume 3108 of LNCS, pages 200–211. Springer, 2004.

[17] Fagen Li, Pan Xiong, Chunhua Jin. "Identity-based deniable authentication for ad hoc networks". Computing, volume 96, issue 9, pp 843-853. Springer, September 2014.

[18] Huang, Xinyi, et al. "On the security of certificateless signature schemes from Asiacrypt 2003." Cryptology and Network Security. Springer Berlin Heidelberg, 2005. 13-25.

[19] Xinyi Huang, Willy Susilo, Yi Mu, Futai Zhang. "On the Security of Certificateless Signature Schemes from Asiacrypt 2003". Springer. Cryptology and Network Security. Volume 3810 of the series Lecture Notes in Computer Science pp 13-25.

[20] 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.

[21] 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.

[22] M. S. Hwang, C. Y. Liu, "Authenticated encryption schemes: Current status and key issues", International Journal of Network Security, vol. 1, no. 2, PP.61-73, Sep. 2005.

[23] MIRACLE, Multiprecision Integer and Rational Arithmetic C/C++ Library, http://indigo.ie/ Mscott.