

# GSM Security Using Identity-based Cryptography

Animesh Agarwal, Vaibhav Shrimali, and Manik Lal Das

Dhirubahi Ambani Institute of

Information and Communication Technology

Gandhinagar - 382007, India.

{animesh\_agarwal, vaibhav\_shrimali, maniklal\_das}@daiict.ac.in

## Abstract

Current security model in Global System for Mobile Communications (GSM) predominantly use symmetric key cryptography. The rapid advancement of Internet technology facilitates online trading, banking, downloading, emailing using resource-constrained handheld devices such as personal digital assistants and cell phones. However, these applications require more security than the present GSM supports. Consequently, a careful design of GSM security using both symmetric and asymmetric key cryptography would make GSM security more adaptable in security intensive applications. This paper presents a secure and efficient protocol for GSM security using identity based cryptography. The salient features of the proposed protocol are (i) authenticated key exchange; (ii) mutual authentication amongst communicating entities; and (iii) user anonymity. The security analysis of the protocol shows its strength against some known threats observed in conventional GSM security.

**Keywords:** GSM security, Identity-based cryptography, Authentication, Encryption, Mobile communications.

## 1 Introduction

Global System for Mobile Communication (GSM) [1] has been the most widely used technology in connecting mobile devices (e.g., Personal Digital Assistants (PDAs), cell phones) wirelessly, where mobile devices remain connected even on the move and irrespective of their geographical locations. The GSM technology was introduced as an improvement over analog First Generation wireless systems. Earlier GSM was used to transfer only voice and text conversations, but with the introduction of services like mobile banking, secure billing, we surfing, so on and so forth, there is a need to update the current GSM security model. As a result, additional security attributes, such as mutual authentication, dynamic key establishment, non-repudiation are important requirements for securing these applications. However, to the best of authors' knowledge, the main challenges in designing GSM security protocol are i) providing higher level of security while keeping the computational and communication cost low on resource-constrained mobile devices, and ii) compatibility issues amongst devices and applications.

The security philosophy of GSM was driven by the concerns to ensure the following: [2].

- Anonymity of subscriber: Subscriber's identity, which is a unique number IMSI, is not sent through over-the-air channel in clear, for this a temporary identity TMSI is used through which network retrieves IMSI. IMSI is always sent through a secure channel.
- Authentication of subscriber: authentication of the subscriber is done through challenge response mechanism.
- Confidentiality of user and signaling data: in the current GSM scheme a secret key between user and network is established to communicate through over-the-air insecure channel which

ensures confidentiality of user and signaling data.

- One-way authentication: Current GSM security model does not provide mutual authentication.
- The channel between VLR and HLR is assumed to be a secure private channel.

Having observed the merits and limitations of the GSM network, we think the GSM security model has to be evolved in such a way that the network should be used not only in voice communications or text messaging but also it should support adequate security strength for accommodating secure billing, trading, content up/downloading, etc. This paper proposes a scheme which aims at achieving the same. It uses ID-based cryptosystem and Elliptic Curve Cryptography, these two techniques allow us to achieve high level of security at reduced key lengths. In the proposed scheme the resource constraint mobile device does not indulge in any computationally extensive task, thereby providing a high level of performance.

## 1.1 GSM Architecture

There are three main components of GSM architecture:

- The Mobile Station (MS): It consists of mobile wireless equipment (i.e. the hardware) and the subscriber information. The subscriber information is the IMSI (International Mobile Subscriber Identity) which is stored in the SIM (Subscriber Identity Module).
- Base Station Subsystem (BSS): It consists of Base Transceiver Station (BTS) and Base Station Controller (BSC). The BTS contains radio transceivers and engages in radio link protocols with MS, the BSC controls and manages radio resources of several BTSs. Also BSC is responsible for radio channel setup, frequency hopping and handovers between two BTSs that the BSC controls.
- Network Subsystem (NSS): It consists of five entities:
  - Mobile Switching Centre (MSC): It provides functionalities like registration, authentication, location updating and call routing to a roaming subscriber, to the MS.
  - Home Location Register (HLR): It contains the current location of the subscriber registered in the GSM network and manages administrative information about the MS.
  - Visitor Location Register (VLR): The VLR is an agent deputed by HLR with some administrative responsibilities for services to the MS.
  - Equipment Identity Register (EIR): It is a database that stores the list identities of all valid mobile stations in the network.
  - Authentication Centre (AuC): It is a protected database containing the shared secret keys stored in the mobile subscriber's SIM.

## 1.2 Paper contributions

The current GSM security model is based on the symmetric key cryptography, which does not support required security services for security intensive applications such as mobile banking, trading, emailing, etc. The paper is aimed at securing GSM network using identity-based cryptography. The proposed protocol does not require any secure/dedicated channel between the BSS and network servers. As the mobile devices are resource constraint and have limited computing capability, the protocol has been designed in such a manner that mobile devices do not require to compute costly public key operation. The protocol provides mutual authentication, anonymity, replay protection, and mutual key control for establishing session key. After successful authentication between mobile device and authentication server, the transmitted data are being encrypted under a dynamic transient key established by the MS and VLR/HLR.

### 1.3 Paper organization

In section II, we discuss preliminaries that would make the paper self sufficient, followed by related work. In section III, we present our protocol. In section IV, we analyze the proposed protocol. We conclude the paper with Section V.

## 2 Preliminaries and Related Work

In this section we discuss some preliminary concepts that are required for thorough understanding of the proposed protocol. It includes the basic concepts of Elliptic Curve Cryptography and Bilinear Pairing. After that we would discuss the related work done in the fields of ‘Authentication in GSM’ as well as ‘ID-based cryptosystems’.

**Elliptic curve.** An elliptic curve  $E$  over a field  $F$  (in short,  $E(F)$ ) is a cubic curve [3] with no repeated roots. The general form of an elliptic curve is  $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_5$ , where  $a_i \in F$ ,  $i = 1, 2, \dots, 5$ . The  $E(F)$  contains the set of all points  $P(x, y)$  on the curve, such that  $x, y$  are elements of  $F$  along with an additional point called *point at infinity* ( $\mathcal{O}$ ). The set  $E(F)$  forms an Abelian group under elliptic curve point addition operation with  $\mathcal{O}$  as the additive identity. The addition rules are as follows: For all  $P, Q \in E(F)$ , let  $F_q$  be a finite field with order  $q$  and characteristic  $p$ .

#### Point Addition.

1. If  $P = (x_1, y_1) \neq \mathcal{O}$ , then  $-P = (x_1, -y_1)$ .
2. If  $P \neq Q$  and  $P, Q \neq \mathcal{O}$ , then the line joining  $P$  and  $Q$  intersects the curve in another point  $R$ .
3. If  $P = Q$  and  $P, Q \neq \mathcal{O}$ , then the line  $l$  is the tangent at  $P$  and intersects the curve at another point  $-R$ . Then define  $P + Q = 2P = R$ .

**Scalar Multiplication of a Point.** The scalar,  $n$ , multiplication of a curve point  $P$  is defined as  $n$ -times addition of  $P$ , i.e.,  $nP = P + P + \dots + P$  ( $n$ -times). There are algorithms [4, 5] for faster computation of scalar multiplication of a curve point.

### 2.1 Computational Problems

Let there is a randomized parameter generator algorithm and a polynomial time algorithm that takes as input a security parameter  $1^k$  and outputs the required/resultant parameters.

**Discrete Logarithm Problem (DLP).** Let  $p$  and  $q$  be two prime numbers such that  $q|(p-1)$ . Let  $g$  be a random element with order  $q$  in  $\mathbb{Z}_p^*$ , and  $y$  be a random element generated by  $g$ . Then, for any probabilistic polynomial time algorithm  $\mathcal{P}$ , the probability that  $\mathcal{P}(p, q, g, y) = x$  such that  $g^x = y \bmod p$  is a negligible function in  $k$ .

**Elliptic Curve Discrete Logarithm Problem (ECDLP).** Given an elliptic curve  $E(F_q)$ , points  $P$  and  $Q(=xP)$  for  $P, Q \in E(F_q)$ , the ECDLP is to determine the integer  $x$ .

**Computational Diffie-Hellman Problem (CDHP).** Given  $(P, aP, bP)$  for all  $a, b \in \mathbb{Z}_q^*$ , compute  $abP$ . The advantage of any probabilistic polynomial-time algorithm  $\mathcal{P}$  in solving CDHP in  $G_1$ , is defined as  $\text{Adv}_{\mathcal{P}, G_1}^{\text{CDH}} = \Pr[\mathcal{P}(P, aP, bP, abP) = 1 \text{ for all } a, b \in \mathbb{Z}_q^*]$ . And the advantage is negligible in  $k$  for all probabilistic polynomial time algorithms.

### 2.2 Bilinear Pairings

A bilinear pairing [6] is a function that takes as input two group elements and outputs an element of a multiplicative Abelian group. The Weil pairing and the Tate pairing are the two most commonly

used bilinear pairings in cryptography. So far, a large number of schemes and protocols have been proposed using bilinear pairings, and we refer to [7] for various pairing based cryptographic schemes and protocols. Formally, the bilinear pairing is defined as follows:

Suppose  $G_1$  is a cyclic additive group of prime order  $q$ ,  $G_2$  is a cyclic multiplicative group of the same order and  $P$  be a generator of  $G_1$ . A map  $\hat{e} : G_1 \times G_1 \rightarrow G_2$  is called a bilinear pairing if it satisfies the following properties:

- Bilinearity:  $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$  for all  $P, Q \in G_1$  and  $a, b \in \mathbb{Z}_q^*$ .
- Non-degeneracy: There exist  $P, Q \in G_1$  such that  $\hat{e}(P, Q) \neq 1$ .
- Computability: There is an algorithm to compute  $\hat{e}(P, Q)$  for all  $P, Q \in G_1$ .

In general,  $G_1$  is the group of points on an elliptic curve and  $G_2$  denotes a multiplicative subgroup of a finite field. One may refer to [7] for an informative description of various parameters involved in bilinear pairings and its implementation details.

### 2.3 Map-to-Point

Map-to-Point (a special hash function) is an algorithm for converting an arbitrary bit string onto an elliptic curve point. Firstly, the string has to be converted into an integer and then a mapping is required from that integer onto an elliptic curve point. As our scheme uses this special hash operation, we discuss a basic algorithm for Map-to-Point [6] as follows.

Let  $E(F_p)$  be an elliptic curve defined as  $y^2 = f(x)$  and let  $F_p$  has order  $m$ . Let  $P \in E(F_p)$  be a point of prime order  $q$  and  $h : \{0, 1\}^* \rightarrow F_p \times \{0, 1\}$  be a one-way collision-resistant hash function. The algorithm works as follows:

- 1) Given  $M \in \{0, 1\}^*$ , Set  $i = 1$
- 2) Set  $(x, b) = h(i || M) \in F_p \times \{0, 1\}$
- 3) If  $f(x)$  is a quadratic residue in  $F_p$  then
  - Let  $y_0, y_1 \in F_p$  be the two square roots of  $f(x)$
  - Set  $\hat{P}_M = (x, y_b)$  such that  $y_b = \text{Max}(y_0, y_1)$
- 4) Compute  $P_M = (m/q)\hat{P}_M$ . Then  $P_M \in E(F_p)$ .
- 5) Otherwise increment  $i$  and go to step 2.

### 2.4 GSM Security

The GSM security [2, 8] is based on A3, A5, and A8 algorithms using a master secret generated by the NSS and stored at MS and network's authentication server. A5 is based on combination of three 'Linear Feedback Shift Registers(LFSR)'. These are initialized with a 64-bit key whose 10-bits are always zero, therefore the effective key length is 54-bits.

#### 2.4.1 Registration Phase:

During MS registration, AuC registers a 128 bit key  $K_i$  and stores it in the SIM of the MS

#### 2.4.2 Authentication Phase

- MS  $\rightarrow$  VLR : <TMSI>  
Whenever a MS want to connect to the GSM network it sends the nearest VLR its TMSI. Since the subscriber is sending TMSI and not IMSI, he remains anonymous.
- VLR  $\rightarrow$  HLR : <IMSI>  
If MS is not in roaming then VLR itself knows IMSI but if the MS is on roaming scenario then VLR has to send the received TMSI to the previous VLR under whom the MS was held. Upon having IMSI, VLR sends the IMSI to HLR.
- HLR  $\rightarrow$  VLR: <RAND, SRES,  $K_c$  >  
HLR sends back five distinct authentication triplets to VLR. Each triplet consists of three

entities, namely, a random number (RAND), a signed response ( $SRES = A3(RAND, K_i)$ ), and an encryption key ( $K_c = A8(RAND, K_i)$ ).

- VLR  $\rightarrow$  MS:  $\langle RAND \rangle$   
VLR selects one triplet to authenticate the MS and sends RAND to the MS.
- MS  $\rightarrow$  VLR :  $\langle SRES' \rangle$   
MS computes  $SRES' = A3(RAND, K_i)$  and  $K'_c = A8(RAND, K_i)$ . MS then sends back SRES' to the VLR
- VLR upon receiving SRES' compares it with SRES in the authentication triplet. If SRES = SRES' then MS is authenticated else VLR terminate the operation.

## 2.5 Public key cryptography in GSM

GSM security using public key cryptography started back in 1989 with Yacobi and Shimley [9] proposed a key distribution protocol which is based on Diffie-Hellman [10], but this protocol is vulnerable to impersonation attack [11]. Bellar and Yacobi [12] proposed a protocol based on El-Gamal encryption [13], but later this protocol was also proven insecure [14]. Subsequently several protocols [15], [16], [17], [18] have been proposed securing mobile communications using public key cryptography.

## 3 The Proposed Protocol

The proposed protocol uses the fascinating features of identity-based cryptography, where the security of the protocol is based on Computational Diffie-Hellman Problem (CDHP) cited in section II. In 1984, Shamir [19] proposed the first ID based cryptosystems and signature scheme. ID based cryptosystem has a property that the public key can be derived from an identity that can help us identify any user uniquely thus this scheme obviates the need of any public key certificates.

The proposed protocol allows both MS and NSS to authenticate each other, then they establish a transient secret key for securing data to be transmitted in that session. One of the interesting feature of the proposed protocol is that in every session, MS does only hashing, XORing, and one scalar multiplication on elliptic curve point, whereas, HLR and VLR computes public key operations.

The protocol consists of three phases - setup, registration, and authenticated key exchange. The setup and registration phases are a one-time operation, but the authenticated key exchange phase is a dynamic operation, as and when demanded. The symbols and notation used in our protocol are given in Table 1.

### 3.1 Setup Phase.

HLR chooses a random integer  $s \in [1, p-1]$ , where  $p$  is large prime number. Then HLR selects a master secret key  $K$  and generates a public-private key pair  $(HLR_{pub}, HLR_{pri})$  as  $HLR_{pri} = K \cdot H(HLR_{ID})$  and  $HLR_{pub} = H(HLR_{ID})$ , where  $HLR_{pri}$  and  $K$  are secret, and  $HLR_{pub}$  and  $H(\cdot)$  are made public.

### 3.2 Registration Phase.

When a new MS wants to register with NSS, the HLR of that NSS generates a key  $K' = K \cdot H(IMSI)$  corresponding to  $IMSI$  of the MS. It, then, stores this  $K'$  in the  $SIM$  of the MS and also stores a copy of  $K'$  with itself for further verification of the MS.

Notions	Explanations
$IMSI$	International Mobile Subscriber Identity
$TMSI$	Temporary Mobile Subscriber Identity
$VLR_{ID}$	VLR's identity
$HLR_{ID}$	HLR's identity
$HLR_{pub}$	HLR's public Key
$HLR_{pri}$	HLR's private Key
$H(\cdot)$	Map-to-point, a special hash function.
$MS_{pub}$	MS's public key
$A \rightarrow B : m$	message $m$ is sent from an entity A to B
$m_1 \oplus m_2$	Bit-wise XORing of strings $m_1$ and $m_2$
$m_1    m_2$	Concatenation of strings $m_1$ and $m_2$
$E_X(m)$	message $m$ is encrypted using the key $X$
$SIGN_X(m)$	message $m$ is signed using the key $X$

Table 1: Symbols and Notation

### 3.3 Authenticated Key Exchange Phase.

This phase enables both MS and VLR to authenticate each other and after successful authentication they establish a transient session key. All the following message transmissions are done over the public channel. The phase works as follows:

- 1)  $MS \rightarrow VLR : < TMSI >$   
When MS wants to use services of NSS it sends its  $TMSI$ .
- 2)  $VLR \rightarrow MS : < RAND >$   
Upon receiving MS's  $TMSI$ , VLR sends  $RAND$  back to the MS, where  $RAND$  is a nonce used to protect the protocol against replay attacks.
- 3)  $MS \rightarrow VLR : H(K'') || TMSI || RAND''$ .  
After receiving  $RAND$ , MS generates another nonce  $RAND'$  and computes  $RAND''$  as  $RAND'' = RAND \oplus RAND'$ . Then, the MS calculates  $K'' = K' \cdot H(RAND'')$  and sends  $H(K'') || TMSI || RAND''$  to VLR.
- 4)  $VLR \rightarrow HLR : E_{HLR_{pub}}(IMSI || H(K'') || VLR_{ID} || RAND'')$ .  
VLR, now, obtains  $IMSI$  for corresponding  $TMSI$  it received from MS. Then VLR creates a message  $< IMSI || H(K'') || VLR_{ID} || RAND >$  and encrypts it using  $HLR_{pub}$ . Here, the encryption algorithm could use any public key encryption algorithm. However, as we intend to use identity based cryptography, the identity-based encryption [6] by Boneh and Franklin finds an application in our protocol.
- 5) HLR decrypts the message using its private key and gets  $K'$  corresponding to the  $IMSI$  it received. It then generates  $K'' = K' \cdot H(RAND'')$  and checks if calculated  $H(K'')$  is same as the received value. If it does, it authenticates MS. It then authenticates VLR on seeing the  $VLR_{ID}$  it received. If either of VLR or MS is not authenticated, the session is terminated.
- 6)  $HLR \rightarrow VLR : SIGN_{HLR_{pri}}\{H(IMSI || K'' || VLR_{ID})\}, H(IMSI || K'' || VLR_{ID})$ .  
HLR sends  $SIGN_{HLR_{pri}}\{H(IMSI || K'' || VLR_{ID})\}, H(IMSI || K'' || VLR_{ID})$  to the VLR. VLR first verifies the signature, and if the signature is valid then VLR proceeds to next step; otherwise, terminate the session. Here, the short-signature scheme [20] by Boneh et al. is applicable for signing the message.
- 7)  $VLR \rightarrow MS : H(IMSI || K'' || VLR_{ID}), VLR_{ID}$ .  
VLR appends its identity  $VLR_{ID}$  to the message it received from HLR and relays it to MS.

- 8) MS generates  $H(IMS\!I\|K''\|VLR_{ID})$ . If the computed hashed matches the value which it received from the VLR, MS authenticates the NSS (both HLR and VLR); otherwise, the session is terminated.

## 4 Security Analysis

The proposed protocol has two communication channels - one in between MS and VLR and other in between VLR and HLR. It is important to note that both channels are public channels, that is, all transmitted messages are available to the adversary. However, we show that the protocol resists the following attacks, which are potential threats of any authenticated key exchange protocol.

### 4.1 Replay Attack

Replay attack is an offensive attack in which an adversary intercepts a session and then replays some of the intercepted parameters to gain control over a new session. The proposed protocol resists replay attacks, as two nonces are involved in each session. The MS verifies the freshness of  $RAND$  by seeing its current value and previous value. Typically, if the current value of  $RAND$  is greater than the previous one, then MS proceeds further, else, terminate the communication. It is also important to note that one of the nonces is never sent over the network. As a result, if adversary replays the same value of  $RAND$ , then  $K''$  will be different for different sessions. Therefore, replay attack is not succeeded in our protocol.

### 4.2 Mutual Authentication

The protocol provides strong authentication. The communicating entities (MS, VLR, HLR) involved in a session authenticate each other before they agree on a shared session key. The authentication process works as follows.

- **MS authenticating VLR and HLR.** MS sends  $H(K'')$  and  $TMSI$  to VLR. It is the responsibility of the VLR to obtain correct  $IMS\!I$  for the corresponding  $TMSI$  and of the HLR to obtain the value of  $K'$  for the received  $IMS\!I$ . These two responsibilities cannot be done by any other parties other than authentic VLR and HLR. Now, when the MS gets  $H(IMS\!I\|K''\|VLR_{ID})$  from the VLR (which came from the HLR) if the verification of this hash holds correct then MS can be sure that the  $K''$  was correctly computed by the HLR. Consequently, both VLR and HLR authenticity are confirmed.
- **HLR authenticating MS and VLR.** HLR when receives  $E_{HLR_{pub}}\{IMS\!I\|H(K'')\|VLR_{ID}\|RAND''\}$  then HLR authenticates the VLR by decrypting it and then checking the value of  $VLR_{ID}$  and also by verifying the value of  $IMS\!I$ . Further, HLR authenticates MS by recomputing  $K''$  and verifying the  $H(K'')$  it received.
- **VLR authenticating MS and HLR.** The authenticity of HLR is achieved by its signature on  $H(IMS\!I\|K''\|VLR_{ID})$  and MS's authenticity through its  $TMSI$ , which should have a mapping to a valid  $IMS\!I$  stored at VLR's database.

### 4.3 Anonymity

The proposed protocol provides anonymity for the mobile entity (MS). The MS can be identified on the network by the means of a valid  $IMS\!I$ . The  $IMS\!I$  of a MS is not transmitted in public, instead, MS sends its  $TMSI$  over the public channel. Upon receiving  $TMSI$ , the VLR maps the  $TMSI$  to a valid  $IMS\!I$ . If a valid  $IMS\!I$  corresponding to  $TMSI$  is found in VLR's database then VLR sends the  $IMS\!I$  along with other parameter to HLR in an encrypted manner using HLR's public key, so that HLR decrypts it using his private key and get the MS's  $IMS\!I$ . As a result, MS's identity is not disclosed any other party except VLR and HLR.

#### 4.4 Impersonation Attacks

An adversary cannot impersonate MS and HLR for the following reasons:

- MS computes  $H(K'')\|TMSI\|RAND$  that requires to compute  $K''$ , which in turn requires the secret key  $K'$  known to MS.
- VLR and HLR secrecy is based on public key encryption.

#### 4.5 Mutual Key Control

For each session, the protocol generates a new session key  $K''$  which is computed as  $K'' = RAND'' \cdot K'$ , where  $RAND'' = RAND \oplus RAND'$ . Here  $K'$  is generated by the HLR and is stored in the MS.

$RAND$  is generated by the VLR, and  $RAND'$  is generated by the MS.

Therefore, in computation of a session key, the protocol requires components from all the three participating entities. In other words, no one is allowed to be biased in a particular session key, and thus, the protocol provides mutual key control.

#### 4.6 Freshness of Session Key

The protocol run resists the freshness property of the session if the intruder cannot guess a fresh session key with a non-negligible probability. In other words, at the end of the protocol run the intruder should not be able to distinguish a fresh session key, say  $sk$ , from a randomly chosen key from a pool of session keys issued in some of the previous sessions. In order to illustrate the protocol strength against freshness of the session key, we consider the following challenger-intruder game, proposed in [21].

Intruder general query: The intruder makes query to our protocol, for some of the previously issued session keys and obtains a set  $\mathcal{S}$  of session keys.

Intruder special query: The intruder makes a special query to our protocol for a fresh session key and obtains  $sk_{fh}$  as the fresh session key.

Challenger challenge: The challenger asks the intruder to answer the freshness of a session key  $sk_{ch}$  by running the protocol or choosing a sample from  $\mathcal{S}$ . In other words, the query is generated in flipping a fair coin  $b \in \{0, 1\}$  and returning  $sk_{ch}$  if  $b = 0$ , or else a random sample from  $\mathcal{S}$  if  $b = 1$ .

Intruder guess: The intruder now guesses  $b$ . Let intruder's guess is  $result \in \{0, 1\}$ . The advantage that the intruder correctly identifies whether he was given the fresh session key or just a sample from  $\mathcal{S}$  is  $\max\{0, \Pr[result] - \frac{1}{2}\}$ . The protocol run resists the freshness property of the session key if the intruder cannot guess session key's freshness with a non-negligible probability.

### 5 Conclusion

We proposed a secure and efficient protocol for GSM security using identity based cryptography. The proposed protocol does not require any secure/dedicated channel between the BSS and network servers. The protocol does not consume much computational resource on mobile device and provides mutual authentication, anonymity, replay protection, and mutual key control for establishing session key. After successful authentication between mobile device and authentication server, the communicating principals establish a session key by which transmitted data is being protected. The work could be extended in making the protocol secure against denial-of-service and providing forward secrecy.

### References

- [1] T. Halonen, J. Romero, and J. Melero. GSM, GPRS and EDGE performance: evolution towards 3G/UMTS. John Wiley & Sons, 2003.



- [2] GSM Security Papers. (J. Quirke: Security in the GSM System, 2004; T. Huynh, and H. Nguyen: Overview of GSM and GSM Security , 2003; C. Brookson: GSM (and PCN) Security and Encryption, 1994; R. Anderson: A5-The GSM Encryption Algorithm, 1994; M. Briceno, I. Goldberg, and D. Wagner: An implementation of the GSM A3/A8 algorithm, 1998.). <http://www.gsm-security.net/gsm-security-papers.shtml>
- [3] D. Hankerson, A. Menezes and S. Vanstone. Guide To elliptic Curve Cryptography, Springer, 2003.
- [4] V. S. Dimitrov, L. Imbert and P. K. Mishra. Fast elliptic curve point multiplication using double base-chains, <http://eprint.iacr.org/2005/069>.
- [5] N. Koblitz. A Course in Number Theory and Cryptography. Springer, 1994.
- [6] D. Boneh, M. Franklin. Identity-based encryption from the Weil pairing. In: Advances in Cryptology, LNCS 2139, Springer-Verlag, pp.213-229, 2001.
- [7] The Pairing-based Crypto Lounge. <http://www.larc.usp.br/~pbarreto/pblounge.html>
- [8] M. Briceno, I. Goldberg, and D. Wagner. An implementation of the gsm a3, a8 algorithm. April 1998, <http://www.gsm-security.net>
- [9] Y. Yacobi, and Z. Shmueli. On key distribution systems. In Advances in Cryptology, LNCS 2139, pp.34-35. Springer-Verlag, 1989.
- [10] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, vol.22, pp.644-654, 1976.
- [11] G. Horn, K. M. Martin, and C. Mitchell. Evaluation of authentication protocols for mobile environment value-added services. IEEE Transactions on Vehicular Technology, vol.51, no.2, pp.383-392, 2002.
- [12] M. J. Beller, and Y. Yacobi. Fully-fledged two-way public key authentication and key agreement for low-cost terminals. Electronics Letters, vol.29, pp.999-1001, 1993.
- [13] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, vol.31, pp.469-472, 1985.
- [14] C. S. Park. On certificate-based security protocols for wireless mobile communication systems. IEEE Network:50-55, 1997.
- [15] C. Boyd, and D. Park. Public key protocols for wireless communications. In proc. of the International Conference on Information Security and Cryptology, pp.47-57, 1998.
- [16] Advanced security for personal communications technologies. <http://www.esat.kuleuven.ac.be/cosic/aspect/>
- [17] C. H. Lee, M. S. Hwang, and W. P. Yang. Extension of authentication protocol for GSM. IEE Proceedings-Communications vol.150, pp.91-95, 2003.
- [18] C. F. Grecas, S. I. Maniatis, and I. S. Venieris. Introduction of the asymmetric cryptography in GSM, GPRS, UMTS, and its public key infrastructure integration. Mobile Networks and Applications, vol.8, pp.145-150, 2003.
- [19] A. Shamir. Identity-Based Cryptosystems and Signature Schemes. In Proc. of Advances in Cryptology - CRYPTO 84, pp.47-53, 1984.
- [20] D. Boneh, B. Lynn, H. Shacham. Short signatures from the Weil pairing. In: Advances in Cryptology, LNCS 2248, Springer-Verlag, pp.514-532, 2002.

- [21] M. Bellare, and P. Rogaway. Entity authentication and key distribution. In Proc. of Advances in Cryptology, LNCS 773, Springer-Verlag, pp.232–249, 1994.