Oriental Journal of Computer Science & Technology Vol. **2**(1), 87-94 (2009)

A Security Analysis of GSM Security using ECC Technique

TARUN KUMAR

Department of Computer Science and Information Technology,
Radha Govind Engineering College Anuyogipuram Meerut - 250 004 (India).

(Received: January 20, 2009; Accepted: April 02, 2009)

ABSTRACT

GSM (Group Special Mobile or System for Mobile Communications) is the PAN-EUROPEAN standard for digital cellular communication. GSM provides enhanced features when compared with the older analog-based wireless systems. A GSM network is more vulnerable to unauthorized access and eavesdropping when compared with the traditional fixed wired networks due to the mobility of users, the transmission of signals through open-air and the requirement of low power consumption by a mobile user. This paper focuses on the security techniques used within the GSM standard as well as current GSM security system vulnerabilities. In this paper, we proposed two new security protocols for GSM using Elliptic Curve Public Key Cryptography (ECC) technique and a security analysis of the proposed protocol.

Keywords: GSM security, Wireless Security, Elliptic Curve Cryptology.

INTRODUCTION

GSM (Group Special Mobile or System for Mobile Communications) is the PAN-EUROPEAN standard for digital cellular communication. GSM provides enhanced features when compared with the older analog-based wireless systems, which are summarized below:

Total Mobility

The subscriber has the ability of communication in any area served by a GSM cellular network using the same assigned telephone number, even outside of his home location.

High Capacity and Optimum Spectrum Allocation

When compared with the older analog-based systems, GSM system is capable of serving a greater number of subscribers. Using FDMA, TDMA, efficient proposed speech coding, and the Gaussian Minimum Shift Keying modulation scheme achieve this.

Services

The list of services available to GSM users typically include: voice communication, facsimile, voice mail, short message transmission, data transmission and supplemental services such as call forwarding.

Security

The security methods standardized for the GSM System make it the most secure cellular communications standard currently available.

The rest of the paper is organized as follows: Section 2 gives the brief description of current GSM Security techniques. In Section 3 we summarize Elliptic Curve Cryptography (ELCC) Protocol of GSM Security. Proposed protocols are analyzed on security terms in Section 4.

GSM Network Architecture and GSM Security

A GSM network can be divided into three areas: Mobile Station, Base Station Subsystem and Network Subsystem. A Mobile Station (MS) consists of two main elements: The Mobile Equipment and the Subscriber Identity Module. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem performs the switching of calls between mobile users and between mobile and fixed network (ISDN, PST, etc.) users.

As shown in Fig. 1, security parameters of the GSM are distributed among the Subscriber Identity Module (SIM), the Mobile Equipment and the GSM network [1], [2], [4]. Security in GSM is comprised of the following [2], [3], [4],[5], [6]:

Subscriber Identity (IMSI) Authentication

When a mobile user transitions from one domain to another, the user identity must be established at every domain boundary encountered.

Subscriber Identity (IMSI) Confidentiality

The privacy of the identities of the subscribers who are using the GSM network resources must be protected.

User Data and Signaling Element Confidentiality

User information exchanged on the GSM traffic channels must not made available or disclosed to unauthorized individuals, entities or processes.

Evaluation of the Current GSM Security System

The security and the authentication mechanisms incorporated into GSM make it the most secure mobile communication standard currently available. Part of the GSM security is implicit in the utilization of Gaussian Minimum Shift Keying, digital modulation, slow frequency hoping and TDMA architecture [1], but these techniques are not the main elements comprising the GSM security architecture [3]. GSM security is based mainly on authentication and encryption techniques. Unfortunately these techniques have several important security flaws, which are as follows:

1. Confidentiality of a call and anonymity of the GSM subscriber are only guaranteed on the radio channel (air interface) between the mobile station and the base station subsystem [1], [3], [4], [6]. This leads to possibility of eavesdropping of voice data on the fixed infrastructure of the GSM network (between BSS and MSC, HLR, VLR, AUC, etc.).
2. During the inter-domain visits of GSM subscribers, some important authentication parameters, such as the encryption key, are sent from the HLR to the new VLR in the clear. Security of this HLR ®VLR (or VLR ®VLR) communication depends on the security of the intermediate transport network between these two registers. The need for this secure transport network cannot be satisfied in a large or global scale, administratively heterogeneous network environment.
3. The user identity confidentiality is violated by transmitting the user identities (IMSI) in unprotected form through the intermediate transport networks between the GSM registers.

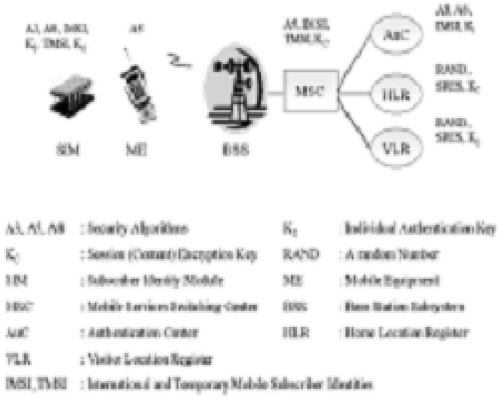

A3, A8, IMSI,
Ki, TMSI, Kc
A5
A5, IMSI,
TMSI, Kc
AuC
A3, A8,
IMSI, Ki
RAND,
SRES, Kc
HLR
RAND,
SRES, Kc
VLR
MSC
SIM
ME
BSS
A3, A5, A8 : Security Algorithms
Ki : Individual Authentication Key
Kc : Session (Content) Encryption Key
RAND : A random Number
SIM : Subscriber Identity Module
ME : Mobile Equipment
MSC : Mobile Services Switching Center
BSS : Base Station Subsystem
AuC : Authentication Center
HLR : Home Location Register
VLR : Visitor Location Register
IMSI, TMSI : International and Temporary Mobile Subscriber Identities

Fig. 1: Distribution of GSM Security Parameters

4. In addition to the SIM cards, individual authentication keys of the users are also stored in the GSM authentication centers. Any person who has the rights and capabilities to access to authentication center can obtain the authentication key of a valid subscriber to impersonate that mobile user. An unauthorized person can thus capture and decipher the encrypted traffic on the radio channel between the mobile station and the base station.
5. 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.

6. In the GSM authentication phase, two related parameters, RAND and SRES, are transmitted on the air interface in the clear. So any listener on the air interface can perform a known plain text attack on the RAND - SRES pair to obtain the authentication key.

Evaluation of the Proposed Security Systems for Wireless Networks

Two security protocol proposals for wireless networks are evaluated. One of the protocols uses private key techniques. The other uses public key encryption techniques. Private Key based security protocol has the following enhancements and flaws:

1. The proposed protocol does not address a solution for the confidentiality of calls within the fixed infrastructure of the mobile network.
2. The proposed solution does not include any assumption about the security of the intermediate network between the foreign and the home network authentication centers. All sensitive information is sent in encrypted form through this intermediate network.
3. After the first authentication of a mobile user in a new VLR area, a temporary and changing identity to be used in this domain is provided. This protects the user identity confidentiality except for the first time a user interacts in a foreign domain.
4. In the proposed protocol, the user's secret keys are stored in their home networks as in the GSM.
5. Known and accepted algorithms such as DES and MD5 are used in these protocols.

Public-key based authentication and key exchange protocols has the following enhancements and flaws:

1. End-to-end privacy of the communication between two mobile users is protected.
2. No protocol for performing secure communication between the foreign and the home network authentication centers is defined.
3. Digital certificates defined in this protocol include user identities in clear form. These certificates are exchanged between the users and the network in unencrypted form, so the user's identity confidentiality is violated.
4. Since this system uses public key cryptography techniques, there is no need to store the private keys of the users in home network databases.
5. Known and accepted security algorithms such as DES and MD5 are used in these protocols.
6. Classical public key cryptography techniques such as the Diffie-Hellman (DH) protocol are used in the proposed system. These techniques are characterized by higher key sizes and lower speed performance, which are not acceptable in mobile network environment where the mobile equipment has smaller storage area and limited computing power.

ECC Protocols for GSM Security

As previously described, the current GSM security architecture and the proposed enhancements have many security flaws. In order to address these flaws, new security protocols are proposed in the following sections. A relatively new public key cryptography technology, the Elliptic Curve Public Key Cryptosystem, is used in these protocols. Reduction in key size brings the advantage of less storage area and less required bandwidth, which are important requirements of wireless network architectures. In addition, ECC permits the implementation of high-speed and efficient network security protocols requiring less power and smaller code sizes as compared to classical public key techniques such as RSA and DH.

Protocols to be proposed are based on the following requirements:

o The mobile user's secret information shall be stored only in their smart cards.

o The user identity confidentiality shall be enforced both in home (local) and foreign (remote) domains.

o Minimal assumptions about the security of intermediate transport network between home and visited networks shall be made.

- o Authentication in a foreign domain shall have minimal overhead impact on the user interface with respect to the home domain authentication process.
- o Computational overhead for the mobile users shall be minimized.

The following sections describe the protocol building blocks, authentication and key distribution in a new VLR area, local authentication and an end-to-end mobile user security protocol.

Protocol Building Blocks - Elliptic Curve Diffie-Hellman (ECDH)

The ECDH protocol (Fig. 2) is used to produce a secret key K_{UN}, shared between two communicating parties (e.g. the user and the GSM network). This secret value can then be used to distribute the content encryption key that encrypts sensitive data. EC public keys of the communicating parties can be distributed by using EC digital certificates that contain the following fields (Fig.3):

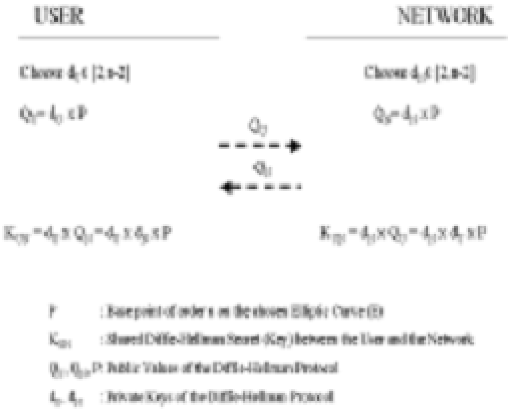
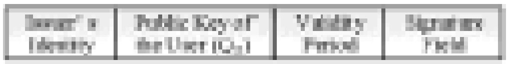

USER
NETWORK
Choose $d_U \in [2, n-2]$
Choose $d_N \in [2, n-2]$
$Q_U = d_U \times P$
$Q_N = d_N \times P$
Q_U
Q_N
$K_{UN} = d_U \times Q_N = d_U \times d_N \times P$
$K_{UN} = d_N \times Q_U = d_N \times d_U \times P$
P : Base point of order n on the chosen Elliptic Curve (E)
K_{UN} : Shared Diffie-Hellman Secret (Key) between the User and the Network
Q_U, Q_N, P: Public Values of the Diffie-Hellman Protocol
d_U, d_N : Private Keys of the Diffie-Hellman Protocol

Fig. 2: Elliptic Curve Diffie-Hellman (ECDH)



Issuer's Identity	Public Key of the User (Q_U)	Validity Period	Signature Field

Fig. 3: ECDH Certificate for the Mobile Users

Issuer Identity

Identity of the certificate issuer, which is the user's home network.

Public Key of the User: ECDH public key of the user, Q_U.

Validity Period: The time interval in which the user's certificate is valid.

Signature Field

Issuer's EC Digital Signature Algorithm (ECDSA) signature computed over the following fields: the issuer identity, the certificate holder (user) identity, the public key of the user and the validity period certificate. The user certificate does not contain the identity of the subscriber in explicit form; but the identity of the user is considered during the signature generation operation. This hides the user's identity to prevent unauthorized tracking of the user during the certificate exchanges.

Authentication and Key Distribution in a New VLR Area

When a mobile user transitions from one domain to another domain, there must be protocols between the user's home network, the visited network and the user to authenticate this subscriber in the new network area. This section focuses on authentication and key distribution protocols used when a mobile user enters into a new VLR area.

As shown in Fig. 4, the user and the visited network jointly contribute to the generation of the content (data) encryption key. In this protocol all authentication operations are performed through the ECC methods. By examining first few digits of the TMSI of the user, the visited network (VLR) recognizes that the user is foreign and extracts the identity of the home network (HLR) of that user. The first few digits of the TMSI indicate the HLR of the user or the VLR to which the user had been most recently registered.

1. The user generates the session (content encryption) key and the signed response. SRES and d_{U-1}.$RAND_U$ are sent to the visited network where dU is the user's ECDH private key and dU -1 is the inverse of the dU in the chosen EC Group.
2. In order to protect the privacy of the ECDH private value d_U, the random number used in this step ($RAND_U$) must be of the same order of the private keys. A random number that is at least 90-bits long ensures the

privacy of the ECDH inverse private key.

3. Modular inversion is an essential and widely used arithmetic operation for many cryptographic applications, Recent works on ECC technology have made a secure and speed optimized implementation of the inversion operation on a small hardware chip possible.
4. The visited network (VLR) establishes a communication path with the user's home network (HLR) and sends the parameters indicated in Fig. 4 to the home network.

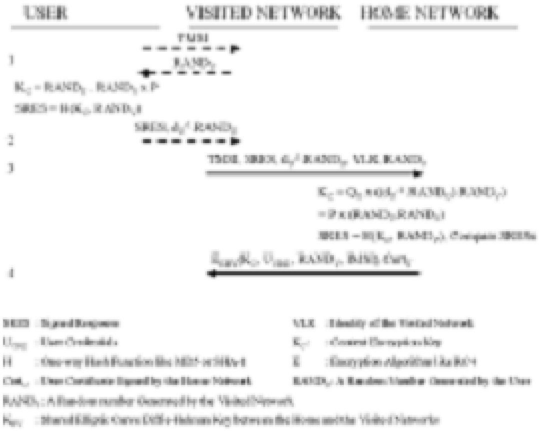

USER
VISITED NETWORK
HOME NETWORK
TMSI
1
RAND
2
3
4
SRES : Signed Response
VLR : Identity of the Visited Network
H : One-way Hash Function like MD5 or SHA-1
E : Encryption Algorithm Like RC4
RAND : A Random Number Generated by the User

Fig. 4: Remote Domain Authentication and Key Distribution

5. From the TMSI sent by the VLR, the HLR finds the IMSI and the ECDH certificate of the user. The HLR calculates the content encryption key in the chosen Elliptic Curve Group as:

$$K_C= Q_U \text{ x } (d_U \text{ -1 .}RAND_U) \text{ . } RAND_V$$
$$= d_U \text{ x P x } (d_U \text{ -1 .}RAND_U) \text{ . } RAND_V$$
$$= \text{P x } (RAND_U.RAND_V).$$

6. A match in the SRES, calculated by the HLR and sent by the visited network, establishes the authenticity of the subscriber to the home network.
7. After authenticating the user, the HLR sends two parameters, EKHV(KC, UCRE, RANDV, IMSI) and Cert$_U$, to the VLR. EKHV represents a symmetric key encryption operation where E is an encryption algorithm such as RC4. KH$_V$ is the DH secret key shared between the HLR and VLR. It is generated by the HLR by using the ECDH certificate of the VLR¹. By inserting the VLR's random number into the E$_{KHV}$ expression, the HLR establishes its identity to the visited network and avoids replay attacks that can be performed on the E$_{KHV}$ expression.

UCRE consists of the following parameters

Authentication Flag: Indicates whether the HLR permits the user access the services of the visited domain.

Validity Period

The time interval during which the user is permitted the services of the visited network. If this interval expires, the VLR and the user's HLR perform a new authentication operation on that subscriber.

Insertion of the UCRE into the EKHV expression ensures the integrity of this parameter.

Since the IMSI of the user is not contained in the user certificate, the VLR uses the IMSI sent by the HLR and the HLR's ECDH certificate to verify the integrity of the user certificate. In this step, IMSI's are transferred in encrypted form to provide the user identity confidentiality service on the air interface.

Public key cryptography based user authentication used in this protocol makes it possible to store the user specific secret keys in only the SIM cards of the subscribers. This is not possible for the current GSM security system. After the user authentication phase of this proposal, known and accepted symmetric key encryption algorithms such as RC4 and AES can be used to establish encrypted traffic between the VLR and the user. The content encryption key (KC) forms the secret key to these encryption algorithms. In this protocol, all of the sensitive traffic between the GSM registers is encrypted to eliminate the need for a secure intermediate transport network that is necessary for the existing GSM architecture.

DH Key Agreement and Authentication

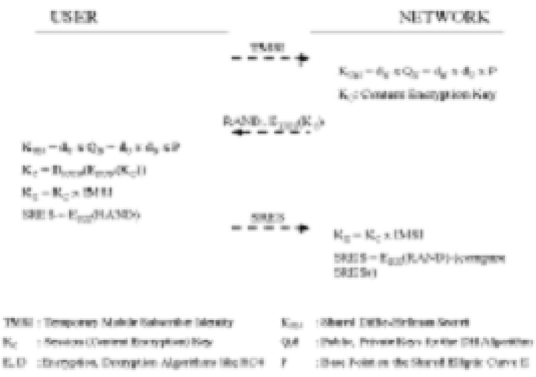
As shown in Fig. 5, the ECDH secret key value can be used to distribute the content encryption key between the visiting user and the visited network. Besides distributing the content encryption key, the GSM user and the network can use this protocol to authenticate each other.

The protocol depicted in Fig. 5 uses a challenge response based authentication technique where the network's random number is the challenge and the signed response is the response of the user.

The correct signed response can be generated only if the user has the correct ECDH secret key K_{UN} to decrypt the $E_{KUN}(K_C)$ expression. It can be seen that in the SRES expression $K_X = K_C$ x IMSI is used as the key to the encryption algorithm E. The purpose of this operation is to avoid a known plaintext attack on the SRES - K_C pair.

End-to-End Mobile User Security Protocol

End-to-end user security protocol described in this section is used to establish a secure communication between two mobile users in such a way that the secret key used in the encryption operation is generated by using the ECDH parameters of both users.



USER
NETWORK
TMSI
K_C : Content Encryption Key
RAND, $E_{KUN}(K_C)$
SRES
$K_X = K_C$ x IMSI
TMSI : Temporary Mobile Subscriber Identity
K_C : Session (Content Encryption) Key
E, D : Encryption, Decryption Algorithms like RC4
K_{UN} : Shared Diffie-Hellman Secret
Q, d : Public, Private Keys for the DH Algorithm
P : Base Point on the Shared Elliptic Curve E

Fig. 5: ECDH Key Agreement and Authentication

This ensures that only the two communicating users can obtain or calculate the content encryption key K_C (Fig. 6). Other entities, including the GSM registers, do not have access to the content encryption key KC.

Mobile user A establishes secure communications with mobile user B as follows:

1. A and B (U_A and U_B) are authenticated by the registers that control their corresponding regions. VLR_A transfers the certificate of U_A to VLRB and VLRB transfers the certificate of U_B to VLR_A. All traffic contents are signed by the registers to ensure the integrity of the user certificates. Since IMSI's are not contained in the user certificates, VLR_A cannot verify the integrity of the UB certificate by using the certificate of U_B's home network. The same reasoning applies to the VLR_B - U_A pair.).
2. User A and user B generates the shared DH key between them and use it to encrypt the data traffic.

The correct key to decrypt the user-to-user traffic can only be generated by these end users. This procedure ensures the confidentiality of calls within the fixed infrastructure of the GSM network.

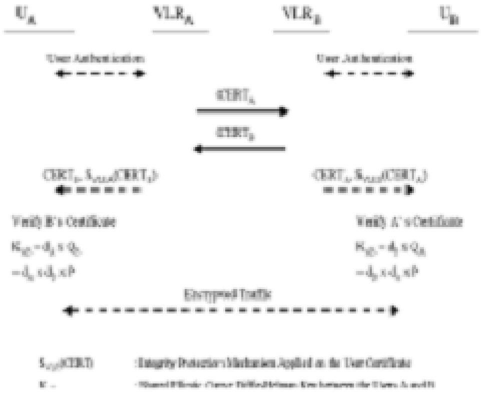
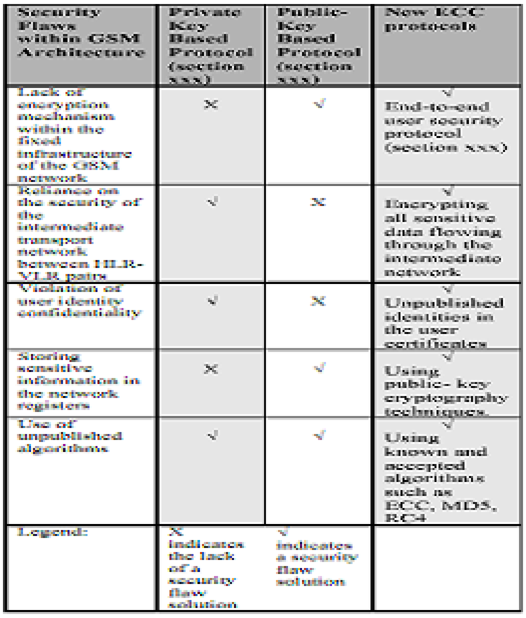


Fig. 6: ECDH End-to-End Mobile User Security Protocol

Security Analysis of the Proposed Protocols

This section is related to the security analysis of GSM and the proposed protocols to enhance GSM security. The first column of the table identifies the security flaws within the GSM infrastructure. The second and third columns indicate whether or not these flaws are addressed by the private-public key methods. The fourth column summarizes how the ECC-based novel protocols proposed address all of the identified security flaws.

Table 1. Security Analysis of the Protocols



Security Flaws within GSM Architecture	Private Key Based Protocol (section xxx)	Public-Key Based Protocol (section xxx)	New ECC protocols
Lack of encryption mechanism within the fixed infrastructure of the GSM network	✗	√	√ End-to-end user security protocol (section xxx)
Reliance on the security of the intermediate transport network between HLR-VLR pairs	√	✗	√ Encrypting all sensitive data flowing through the intermediate network
Violation of user identity confidentiality	√	✗	√ Unpublished identities in the user certificates
Storing sensitive information in the network registers	✗	√	√ Using public- key cryptography techniques.
Use of unpublished algorithms	√	√	√ Using known and accepted algorithms such as ECC, MD5, RC4
Legend:	✗ indicates the lack of a security flaw solution	√ indicates a security flaw solution	

It was shown that the existing GSM system has many security flaws. It is also shown that proposed enhancements to address these security flaws are not completely effective. To address these security issues the Elliptic Curve Cryptology which is characterized by efficiency both in key sizes and speed performance, are favored over classical public key systems. The use of the ECC public key cryptography methods, in user authentication and the key distribution services, ensures that mobile user's private parameters are stored only in their SIM cards. Public key certificates used in the proposed system do not contain the identities of their owners which ensure user identity confidentiality on the air interface. However, the digital signatures on these certificates do make use of the user identities to ensure the binding between the certificates and their owners. Since all of the data flowing through the intermediate transport network between the home and the visited networks is encrypted with a private key algorithm, the proposed protocols do not rely on the security of that intermediate network.

The security protocols developed were explained in terms of the GSM environment. Consideration during the design of these protocols makes them extensible to any wireless network architecture. Implementation and integration of the designed protocols in UMTS 3G wireless networks is planned for the future work.

REFERENCES

1. David Margrave, "GSM Security and Encryption", George Mason University.
2. B. Kasým, L. Ertaul, "Evaluation of GSM Security", in Proc. of the 5th Symp. on Com. Networks (BAS 2000), (2000).
3. S.H. Redl, M. K. Weber, M. W. Oliphant, "An Introduction to GSM", Artech House, (1995).
4. ETSI, "Digital Cellular Telecommunications System (Phase 2); Security Related Network Functions", GSM 03.20 version 4.4.1.
5. ETSI, "Digital Cellular Telecommunications System (Phase 2+); Security Aspects", GSM 02.09 version 5.1.1.
6. ETSI, "Digital Cellular Telecommunications System (Phase 2+); Security Management", GSM 12.03 version 7.0.1 (1998).
7. R. Molva, D. Samfat and G. Tsudik, "Authentication of Mobile Users", IEEE Network, pp. 26-34 (1994).
8. W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Trans., on IT, pp. 644-654 (1976).

9. A.J. Menezes, D. B. Johnson, "EC-DSA: An Enhanced DSA", Invited Talks - 7 th Usenix Sec., Symp., pp. 33-43 (1998).
10. Certicom Corp., "Certicom ECC Tutorials".
11. Certicom Corp., "Remarks on the Security of the ECC systems", ECC White Papers, (2000).
12. K. Lauter, "The Advantages of Elliptic Curve Cryptography for Wireless Security," IEEE Wireless Communications, vol. 11, no. 1, pp. 62-67, (2004).
13. M. Aydos, T. Tanýk, Ç. K. Koç, "High-Speed Implementation of an ECC-based Wireless Authentication Protocol on an ARM Microprocessor", IEE Pro.: Comms, pp 273-279 (2001).
14. R. L. Rivest, A. Shamir and L.M. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Comms of the ACM, v. 21-n.2, pp. 120-126 (1978).
15. A.K. Lenstra, E. R. Verheul, "Selecting Cryptographic Key Sizes", ECC 99, Waterloo Canada (1999).