World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:3, No:1, 2009

Secure Protocol for Short Message Service

Shubat S. Ahmeda and Ashraf M. Ali Edwila

***Abstract*—**Short Message Service (SMS) has grown in popularity over the years and it has become a common way of communication, it is a service provided through General System for Mobile Communications (GSM) that allows users to send text messages to others.

SMS is usually used to transport unclassified information, but with the rise of mobile commerce it has become a popular tool for transmitting sensitive information between the business and its clients. By default SMS does not guarantee confidentiality and integrity to the message content.

In the mobile communication systems, security (encryption) offered by the network operator only applies on the wireless link. Data delivered through the mobile core network may not be protected. Existing end-to-end security mechanisms are provided at application level and typically based on public key cryptosystem.

The main concern in a public-key setting is the authenticity of the public key; this issue can be resolved by identity-based (ID-based) cryptography where the public key of a user can be derived from public information that uniquely identifies the user.

This paper presents an encryption mechanism based on the ID-based scheme using Elliptic curves to provide end-to-end security for SMS. This mechanism has been implemented over the standard SMS network architecture and the encryption overhead has been estimated and compared with RSA scheme. This study indicates that the ID-based mechanism has advantages over the RSA mechanism in key distribution and scalability of increasing security level for mobile service.

***Keywords*—**Elliptic Curve Cryptography (ECC), End-to-end Security, Identity-based Cryptography, Public Key, RSA, SMS Protocol.

I. INTRODUCTION

THE Short Message Service (SMS) is a text message service that enables users to send short messages to other users on the Global System for Mobile communication (GSM) network. SMS Centers (SMSC) is used to store the SMS messages before they are forwarded to the mobile user's service provider or another SMSC. Although the network connections between the SMSC and nodes in a GSM network are usually protected by Virtual Private Network (VPN) tunnels, the SMS messages are stored unencrypted at the SMSC. This means that employees of SMSC operators, or others who can hack into the system, can view all the SMS messages passing through the SMSC. Many SMSCs also retain a copy of the SMS messages for audit, billing and dispute resolution purposes [1]. If an attacker manages to compromise the SMSC, the attacker can also read the SMS traffic.

The cryptography is the process of keeping the information secure. Cryptography, in addition to providing confidentiality, also provides Authentication, Integrity and Non-repudiation. The core of cryptography lies in the key involved and the secrecy of the keys used to encrypt or decrypt. Existing end-to-end security mechanisms are provided at application level and typically based on public key cryptosystem.

In public-key cryptosystem each user has a key pair (PK, SK), where PK is the public key and SK is the private key. The main concern in a public-key setting is the authenticity of the public key. If an attacker convinces a sender that a receiver's public key is some key of the attacker's choice instead of the correct public key, he can eavesdrop and decrypt messages intended for the receiver. This is the well known man-in-the-middle attack [2]. This authentication problem is typically resolved by the use of verifiable information called certificate, which is issued by a trusted third party consisting of the user name and his public key.

In 1984, Shamir [3] introduced the concept of identity-based (ID-based) cryptography where the public key of a user can be derived from public information that uniquely identifies the user. For example, the public key of a user can be simply his/her telephone number or email address, and hence implicitly known to all other users. A major advantage of ID-based cryptosystem is that no certificate is needed to bind user names with their public keys.

The first complete ID-based encryption scheme was proposed by Boneh and Franklin in 2001 [1]. They used a bilinear map (the Weil pairing) over elliptic curves to construct the encryption/decryption scheme. After that, the bilinear pairings have been used to design numerous ID-based schemes, such as key exchange [2] and short signature [4].

ID-based cryptosystem transparently provides security enhancement to the mobile applications without requiring the users to memorize extra public keys. Sending an ID-based encrypted short message is exactly the same as sending a normal short message [3] if the mobile phone number of the short message recipient is used as the public key. Therefore, the mobile user (the sender) does not need to memorize the public key of the receiver. This feature is especially desirable for mobile applications such as bank or stock transactions. However, in the existing ID-based cryptosystem, the pairing computing has significant overhead. Therefore, efficient algorithm for ID-based cryptosystem is essential in mobile devices with limited computing power, an encryption mechanism based on identity based using Elliptic curve to provide an end-to-end security.

In this paper, an encryption mechanism based on ID-based scheme has been implemented. This scheme has been implemented using Elliptic curve to provide end-to-end security for Short Message Service (SMS). The performance of this scheme has been evaluated and compared with RSA

Shubat S. Ahmeda, Department of Computer Engineering, Faculty of Engineering, Elfath University, E-mail: Shubat_ahmeda@yahoo.com.
Ashraf M. Ali Edwila, Department of Computer Engineering, Faculty of Engineering, University of Seventh of April, E-mail: Ashrafa3d@Gmail.com.

scheme.

II. ID-Based Public Key Cryptosystem

Shamir [3] proposed the identity-based (ID-based) public key approach to support public key cryptography without the use of certification. In ID-based public key cryptosystem eliminates the man in the middle attack. User B encrypts a message for user A or verifies a signature from user A using a public key which is derived from user A's identifier IDA (e.g., email address or telephone number). The trusted agent has a new role in ID-based public key cryptosystem, and is renamed as the Private Key Generator (PKG). The PKG issues the private key corresponding to the public key (derived from the identifier IDA to user A over a secure channel).

This issuing action takes place after user A is authenticated by the PKG, see fig.1 To generate private keys, the PKG makes use of a master key which must be kept in secret. The requirement to have an authentic CA's public key for verifying certificates in certificate-based cryptosystem is replaced by the requirement to have authentic PKG's system parameters in ID-based cryptosystem.

The most significant overhead in implementing the ID-based encryption scheme is the computation of Weil pairing (a bilinear pairing) defined on the elliptic curve to be described next.

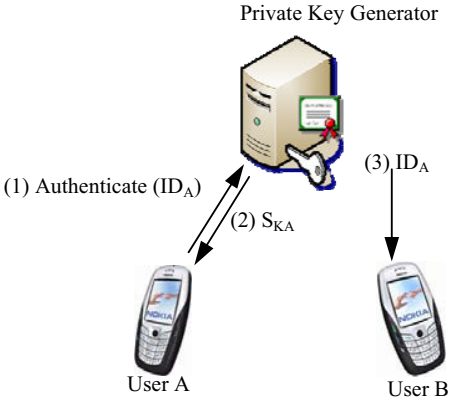

Fig. 1.The ID-based public-key distribution

- *Elliptic Curves*

An elliptic curve over a finite field of size p denoted by GF (p) can be given by an equation of the form: y2 = x3 + ax +b, where a, b ∈ GF (p) and p is a prime number larger than 3. The set of points on the curve is the collection of ordered pairs (x, y) with coordinates in the field such that x and y satisfy the equation defining the curve, plus an extra point O called the infinity point. These points form an abelian group E under a certain addition over GF(p). That is,

E = {(x,y) ∈ O | (x,y) satisfies the equation y2 = x3 + ax +b, x, y∈ GF(p)}.

The group addition operation is defined as follows to add two points P=(x_P, y_P) and Q=(x_Q, y_Q) on the curve, we first pass the straight line through them, find out the third point (x_{P+Q}, y_{P+Q}') intersected with the curve, and then reflect the point over the x-axis to obtain point P+Q=(x_{P+Q}, y_{P+Q}), Assume that P=(xP, yP) and Q=(x_Q, y_Q) are on the curve, λ is the slope of the line passing through P and Q, then the coordinates of P+Q = (x_{P+Q}, y_{P+Q}) are :

$$x_{P+Q} = \lambda^2 - x_P - x_Q$$

$$y_{P+Q} = \lambda^2 (x_P - x_{P+Q}) - y_p$$

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} & if\ P \neq Q \\ \dfrac{3x_P^2 + a}{2y_P} & if\ P = Q \end{cases}$$

The infinity point O plays a role as the identity element, that is, P+O = O+P = P for any point P. Each point P has a unique inverse element -P such that P+(-P)=O. For P=(x_P, y_P) in elliptic curve E over GF(p), the unique additive inverse of P is defined by -P=(x_P, -y_P).

For elliptic curves, the group operation is written as addition instead of multiplication. Thus the exponentiation in general multiplicative group can be appropriately referred to as the scalar multiplication in elliptic curve group [8][2].

III. End-to-End Security for SMS

This section first introduces the short message service (SMS) for GSM. Then the RSA and the ID-based encryption mechanisms for SMS will be presented later.

A. Short Message Service Architecture

The network architecture of short message service in GSM is illustrated in Figure 2. In this architecture, the short message is first delivered from the mobile station (MS) A to a short message service center (SM-SC) through the base station system (BSS), the mobile switching center (MSC), and then the interworking MSC (IWMSC). The SM-SC then forwards the message to the GSM network through a specific GSM MSC called the short message service gateway MSC (SMS GMSC). The SM-SC may connect to several GSM networks and to several SMS GMSCs in a GSM network. Following the GSM roaming protocol, the SMS GMSC locates the current MSC of the message receiver and forwards the message to that MSC. The MSC then broadcasts the message through the BSS to the destination MS B.

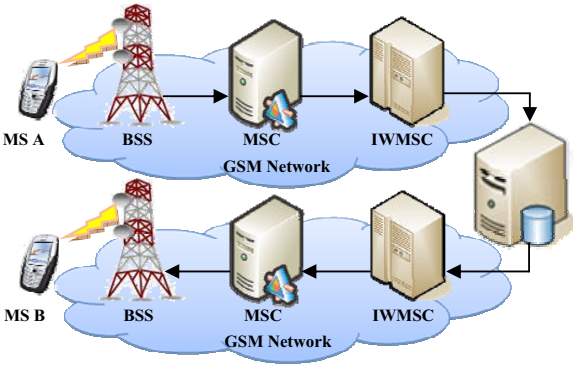

Fig. 2. GSM short message service network architecture

B. RSA Mechanism

The most widely implemented approach to public key encryption is the Rivest-Shamir-Adleman (RSA) scheme [2]. The RSA scheme is a block cipher in which the original non-ciphered text and cipher text are integers between 0 and n-1 for some n. That is, the block size k_{RSA} is determined by the bit length of the integer n and regarded as the key size of the RSA scheme [2]. This scheme consists of the following three functions:

- *Key generation*:
  A user first selects two prime numbers p and q, randomly chooses e with gcd(e, (p-1)(q-1)) = 1, and calculates $d \equiv e^{-1} \bmod (p\text{-}1)(q\text{-}1)$. Then the public key is $P_U = (e, n)$ and the private key is $S_K = (d, n)$, where $n = pq$.
- *Encryption:*
  For a given message represented as an integer M< n, the cipher text is computed by $C=M^e \bmod n$.
- *Decryption:*
  For a given cipher text C, the original non-ciphered text is computed by $M = C^d \bmod n$.

A RSA mechanism for end-to-end secure SMS is introduced as follows. The end-to-end security service provider (ESSP) plays a role as the CA in the certificate-based public key cryptosystem. To access the end-to-end security service, a user first chooses his/her own key pair (P_K, S_K) and subscribes to the ESSP for requesting a certificate of his/her public key P_K. The ESSP signs the certificate with its private key and publishes the certificate in the public key directory for public access. When a mobile user A (the sender) wants to encrypt a short message to user B, he/she first sends a public key request, see figure 3 (1). to the public key directory in short message format. The public key directory retrieves user B's certificate. If it succeeds, user B's certificate is sent to user A as the public key response, see figure 3 (2). Once user A is in possession of B's certificate, he/she verifies the certificate with the ESSP's public key and uses the user B's public key to encrypt short message for B, see figure 3 (3). If the request fails (due to unavailability of user B's certificate), the ESSP will inform user B to subscribe to end-to-end security service if he/she wants to securely communicate with user A.

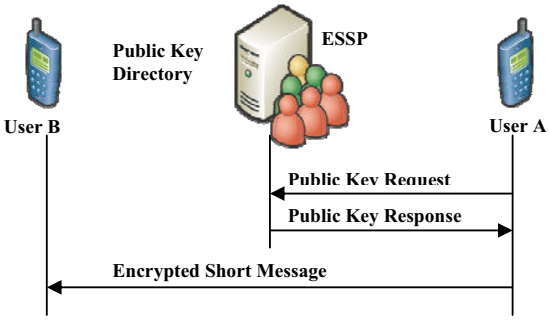

Fig. 3. The RSA procedure for sending an encrypted short message

C. ID-based Mechanism with EC

In the above RSA approach, the sender needs to communicate with the public key directory for requesting the public key. If the request fails (e.g., the directory server is down or there is no certificate exist for the receiver), the sender cannot encrypt short message for the receiver. On the other hand, in an ID-based encryption scheme, the sender simply uses the receiver's ID (i.e., the telephone number) as his public key without any request and verification. Thus, the sender does not need to access any public key directory before sending an encrypted short message.

The first complete and efficient ID-based encryption scheme was proposed by Boneh and Franklin [1]. Which uses a bilinear map called Weil pairing over elliptic curves. The *bilinear map* transforms a pair of elements in group G_1 and sends it to an element in group G_2 in a way that satisfies some properties. The most important property is the bilinearity that it should be linear in each entry of the pair. Assume that P and Q are two elements (e.g., points on elliptic curves) of an additive group G_1. Let e(P,Q) be the element of a multiplicative group G_2, which is the pairing applied to P and Q. Then the pairing must have the following property:

$$e(rP, Q) = e(P, Q)^r = e(P, rQ)$$

Where r is an integer and rP denotes the element generated by r times of additions on P, e.g., 2P=P+P, 3P=P+P+P and so on. Weil pairing on elliptic curves is selected as the bilinear map. That is, the elliptic curve group (the set of point collection on elliptic curves) is used as G_1 and the multiplicative group of a finite field is used as G_2.

The ID-based scheme consists of four algorithms: *Setup*, *Extraction*, *Encryption*, and *Decryption*. Setup is run by the PKG to generate the master key and the system parameters. This is done on input of a security parameter k_{ID}, which specifies the bit length of the group order and is regarded as the key size of the ID-based scheme. The Extraction algorithm is carried out by the PKG to generate a private key corresponding to the identity of a user. As with regular public key cryptography, the Encryption algorithm takes a message and a public key as inputs to produce a cipher text. Similarly, the Decryption algorithm is executed by the

owner of the corresponding private key to decrypt the cipher text. These four functions are described as follows:

- *Setup*:
  With the parameter k_{ID}, the algorithm works as follows:
  1. Generate a random k_{ID}-bit prime p, two groups $(G_1; +)$; $(G_2;*)$ of order p, and the Weil pairing e: $G_1 \times G_1 \rightarrow G_2$. Choose an arbitrary generator $P \in G_1$.
  2. Pick a random number $s \in Zp^*$ and set $Ppub = sP$.
  3. Choose cryptographic hash functions $h1:\{0,1\}^* \rightarrow G1^*$, $h2:G2 \rightarrow \{0,1\}^n$, $h3:\{0,1\}^n \times \{0,1\}^n \rightarrow Zp^*$ and $h4:\{0,1\}^n \rightarrow \{0,1\}^n$ for some n.

  The public system parameters are {p,G1,G2,e,n,P,Ppub, h1, h2, h3, h4} and the master key s is kept in secret by the PKG.
- *Extraction:*
  For a given string $ID \in \{0,1\}^*$ as the public key, the algorithm works as follows:
  1. Compute $Q_{ID} = h_1(ID) \in G_1$.
  2. Set the private key $S_K = sQ_{ID}$, where s is the master key held by PKG.
- *Encryption:*
  To encrypt a message M under the public key $P_K = ID$, the algorithm works as follows:
  1. Compute $Q_{ID} = h_1(ID) \in G_1$.
  2. Choose a random $\sigma \in Z_p^*$ and $r = h_3(\sigma, M)$.
  3. Set the cipher text to be $C = (U, V, W) = (rP, \sigma \oplus h_2(e(Q_{ID}, sP)^r), M \oplus h_4(\sigma))$
- *Decryption:*
  To decrypt a cipher C = (U, V, W) encrypted using the public key $P_K = ID$, if $P_K \notin G1$ reject, the algorithm uses the private key $S_K = sQID \in G1$ do:
  1. Compute $\sigma = V \oplus h_2(e(sQ_{ID}, U))$.
  2. Compute $M = W \oplus h_4(\sigma)$.
  3. Set $r = h_3(\sigma, M)$. Test that $U = rP$. If not, reject the ciphertext.
  4. Output M as the decryption of C.

  This decryption procedure yields the correct message due to the bilinearity of the Weil pairing
  (i.e., $e(sQ_{ID}, U) = e(sQ_{ID}, rP) = e(Q_{ID}, sP)^r$).

Details of Weil pairing for ID-based cryptosystem can be found in [1], and will not be elaborated further in this paper.

An efficient ID-based end-to-end encryption mechanism for mobile services is illustrated in Figure 4. The Public Key generator, see figure 4 (1) constructs the ID-based cryptosystem and uses, for example, the phone number can be used as the identity (ID), see figure 4 (2). Every mobile user involved in the ID-based cryptosystem is given a subscriber identity module (SIM) card at the subscription time, see figure 4 (3). The ID (phone number; e.g., 0912345678 in Figure 4 and its corresponding private key S_K are loaded in the SIM card by the end-to-end security service provider. Note that for standard GSM/UMTS service, SIM card is always given to a mobile user at the subscription time and the proposed ID-based encryption scheme can be pre-loaded into the SIM card without incurring any extra overhead. The mobile station contains two security modules: ID-based encryption module, see figure 4 (4), and ID-based decryption module, see figure 4 (5). When a mobile user A (the sender; figure 4 (6)) wants to encrypt a short message to user B (the receiver), A uses B's phone number 0987654321 (figure 4 (7)) as the public key and encrypts the message through the ID-based encryption module. Once user B receives the cipher (the encrypted message), he/she uses the private key S_K (Figure 4 (8)) stored in the SIM card to decrypt the cipher through the ID-based decryption module and obtain the original non-ciphered message.

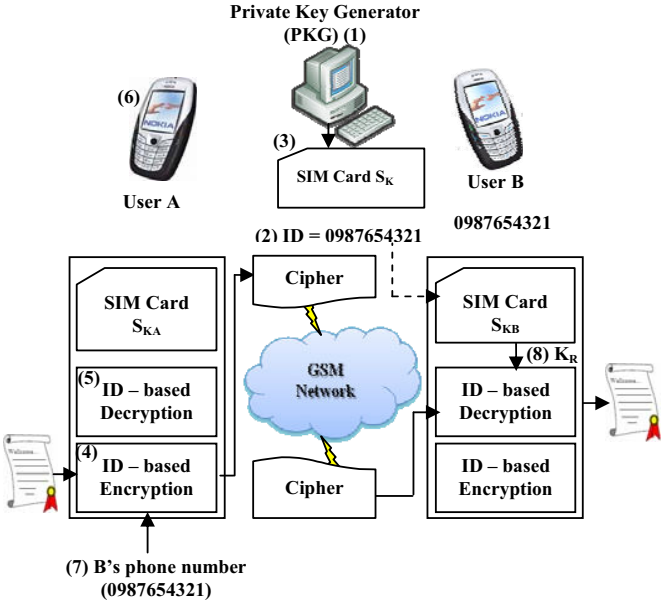

Fig. 4. ID-based end-to-end encryption mechanism

To estimate the encryption overheads between the RSA and the ID-based mechanisms, we implement these two encryption schemes and give the evaluation in the next section.

IV. Performance Comparison

This section compares the transmission (encryption, decryption, and message delivery [7]) delay of ciphered short messages based on the RSA and the ID-based approaches. The experimental environment is illustrated in Figure 5. Both the sender and the receiver are notebooks (Figure 5 (1) and (3)) configured with a Centrino Duo 2 GHz CPU, 1Gbyte main memory, and 120GB disk space, and are running on the Windows XP Professional operating system. To deliver short messages, every notebook or PC is plugged in a NOKIA Card Phone or Light Wave (GSM-GPRS) and the short message is sent via the AL-MADAR GSM network (Figure 5 (2)) from the sender to the receiver.

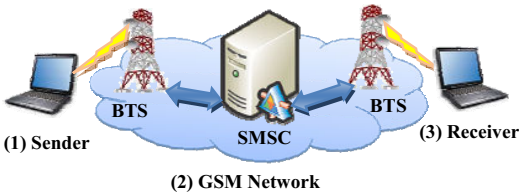

Fig. 5. Encrypted short message experimental environment

At first, it is noted that to support the same security level, the key length for the ID-based and the RSA approaches are different. The ID-based cryptosystem using Weil pairing over elliptic curves, thus its security level depends on the key length of Elliptic Curve Cryptosystem (ECC). As listed in Table 1, a 112-bit ECC key provides the same security level as a 512-bit RSA key, a 160-bit ECC key provides the security level equivalent to a 1024-bit RSA key, and a 224-bit ECC key is equivalent to a 2048-bit RSA key.

TABLE 1
KEY LENGTH FOR EQUIVALENT SECURITY LEVELS

ECC (ID-based)	RSA
112	512
160	1024
224	2048

The processing time required by the RSA and ID-based approaches have been estimated for the same non-ciphered length. Figure 6.1 and Figure 6.2 represented the estimated processing time required for encryption and decryption the message using both RSA and ID-based schemes.

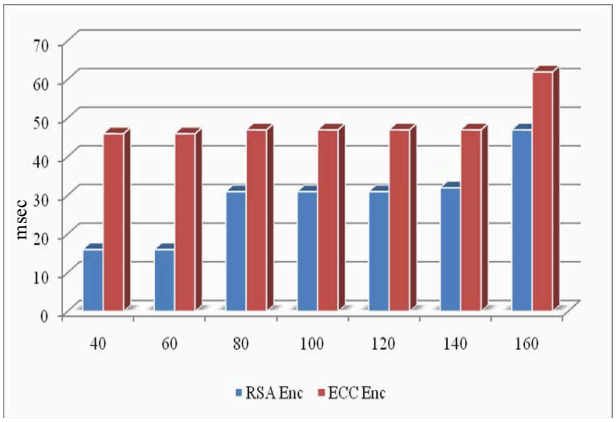

Fig. 6.1. Encryption time (msec)

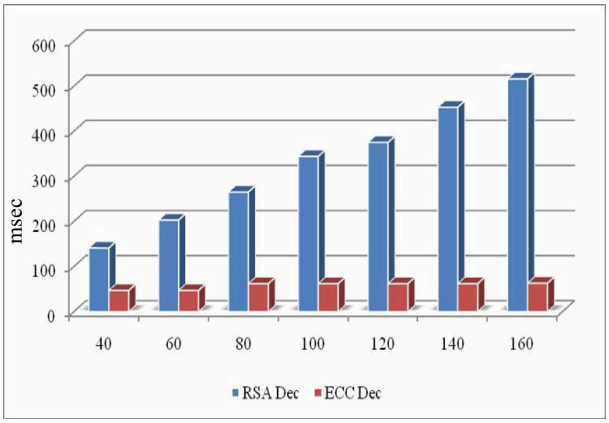

Fig. 6.2. Decryption time (msec)

The RSA approach performs better than the id-based approach during encryption stage. The difference appeared when encryption was made using 1024-bit RSA, then RSA encryption was faster than encryption with 160-bit ID-based Encryption base ECC. Since the size of the SMS message is limited to 160 byte. On the other hand, The id-based approach performs better than the RSA approach during decryption stage. The greatest difference appeared when decryption was made using 160-bit ID-Based decryption base ECC, then ECC decryption was faster than decryption with 1024-bit RSA. Keeping in mind that 160 bit ECC keys is used in contrast to 1024 bit RSA keys. So the overall performance of the ID-based approach is match better than RSA approach.

V. CONCLUSION

In this paper, two applicable end-to-end security mechanisms for SMS based on the RSA scheme and the ID-based scheme are presented, implemented and tested on AL-MADAR GSM network. The ID-based scheme provides a great simplification of key distribution. That is, all public keys can be derived from the identities of the users. Therefore obtaining someone's public key, for encryption or verification, becomes a simple and transparent procedure. This is in contrast to the RSA scheme, where one has to look up the corresponding certificate and verify the CA's signature. Another advantage of the ID-based scheme is the linear scalability of increasing security level. When the security level increases, the key size of the RSA scheme increases faster than that of the ID-based scheme and may not be practical for the SMS applications. Our study concludes that the ID-based scheme offers a convenient end-to-end security mechanism for mobile service such as SMS.

REFERENCE

[1] D. Boneh and M. Franklin, "Identity-based Encryption from the Weil Pairing", Advances in Cryptology-CRYPTO'01, pp. 213–239.
[2] W. Stallings, Cryptography and Network Security, Prentice Hall, fourth Edition 2006.
[3] J.-S. Hwu, R.-J. Chen, and Y.-B. Lin, "An Efficient Identity-based Cryptosystem for End-to-end Mobile Security", Accepted and to appear in IEEE Transactions on Wireless Communications.
[4] Y.-B. Lin and A.-C. Pang, Wireless and Mobile All-IP Networks, John Wiley and Sons, 2005.
[5] A. Shamir, "Identity-based Cryptosystems and Signature Schemes", Advances in Cryptology–CRYPTO'84, pp. 47-53.
[6] R. Revest, A. Shamir, and L. Aldeman, "A Method for Obtaining Digital Signature and Public Key Cryptosystems", Communication of the ACM, February 1978
[7] H.-N. Hung, Y.-B. Lin, M.-K. Lu, and N.-F. Peng, "A Statistic Approach for Deriving the Short Message Transmission Delay Distributions", IEEE Trans. on Wireless Communications, vol. 3, No. 6, 2004.
[8] D. Hankerson, A. Menezes, and S. Vanstone, Guide to Elliptic Curves Cryptography, Springer-Verlag, 2003.