The Journal of Systems and Software 82 (2009) 789–793

Contents lists available at ScienceDirect

The Journal of Systems and Software

journal homepage: www.elsevier.com/locate/jss

Design of DL-based certificateless digital signatures

Lein Harn [a], Jian Ren [b,*], Changlu Lin [c,d]

[a] Department of Computer Science and Electrical Engineering, University of Missouri-Kansas City, MO 64110-2499, USA
[b] Department of Electrical and Computer Engineering, Michigan State University, East Landing, MI 48864-1226, USA
[c] State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences, Beijing 100049, PR China
[d] Key Laboratory of Network Security and Cryptology, Fujian Normal University, Fujian 350007, PR China

ARTICLE INFO

Article history:
Received 5 February 2008
Received in revised form 13 September 2008
Accepted 7 November 2008
Available online 30 November 2008

Keywords:
ID-based cryptosystem
ID-based signature
Provable security
Key escrow
Certificateless digital signature

ABSTRACT

Public-key cryptosystems without requiring digital certificates are very attractive in wireless communications due to limitations imposed by communication bandwidth and computational resource of the mobile wireless communication devices. To eliminate public-key digital certificate, Shamir introduced the concept of the identity-based (ID-based) cryptosystem. The main advantage of the ID-based cryptosystem is that instead of using a random integer as each user's public key as in the traditional public-key systems, the user's real identity, such as user's name or email address, becomes the user's public key. However, all identity-based signature (IBS) schemes have the inherent key escrow problem, that is private key generator (PKG) knows the private key of each user. As a result, the PKG is able to sign any message on the users' behalf. This nature violates the "non-repudiation" requirement of digital signatures. To solve the key escrow problem of the IBS while still taking advantage of the benefits of the IBS, certificateless digital signature (CDS) was introduced. In this paper, we propose a generalized approach to construct CDS schemes. In our proposed CDS scheme, the user's private key is known only to the user himself, therefore, it can eliminate the key escrow problem from the PKG. The proposed construction can be applied to all Discrete Logarithm (DL)-based signature schemes to convert a digital signature scheme into a CDS scheme. The proposed CDS scheme is secure against adaptive chosen-message attack in the random oracle model. In addition, it is also efficient in signature generation and verification.

1. Introduction

Public-key cryptography has become one of the essential techniques in providing security services in modern communications. In traditional public-key cryptosystems, a pair of public/private keys need to be computed by each user. Since the public key is a string of random bits, a digital certificate of the public key is required to provide public-key authentication. Due to the limitations imposed by both the communication bandwidth and computational power of wireless communication devices, public-key cryptography without requiring any digital certificate becomes very attractive in wireless applications.

Shamir (1984) introduced the concept of identity-based (ID-based) cryptosystem to simplify the public-key authentication problem. In this system, each user needs to register at a private key generator (PKG) and identify himself before joining the network. Once a user is accepted, the PKG will generate a private key for the user and the user's identity (e.g. user's name or email address) becomes the corresponding public key. In this way, in order to verify a digital signature or send an encrypted message, a user only needs to know the "identity" of his communication partner and the public key of the PKG, which is extremely useful in cases like wireless communication where pre-distribution of authenticated keys is infeasible.

In the same paper, Shamir proposed the first ID-based signature (IBS) scheme based on integer factorization problem (IFP). Guillou and Quisquater also proposed a "paradoxical" IBS using their interactive zero-knowledge protocol in Guillou and Quisquater (1988, 1989), which has been accepted as an ISO standard (I.S.I, 1999). An IBS scheme using pairing was first proposed independently by Sakai et al. (2000) and Joux (2000). Since then many pairing based IBS schemes have been proposed (Paterson, 2002; Hess, 2003; Cha and Cheon, 2003; Yi, 2003; Chen et al., 2003; Bellare et al., 2004). However, unlike IFP and discrete logarithm problem (DLP), which have been well studied in literature, bilinear pairing is a newly emerging tool and more study is needed before it can be widely accepted.

The major weakness of the IBS is the so-called "key escrow problem". Since PKG issues private keys for all users, PKG is able to decrypt or sign messages for all users without consents of users. A number of proposals have been proposed to overcome the key escrow problem. One possible solution is to involve multiple PKGs

* Corresponding author.
E-mail addresses: harnl@umkc.edu (L. Harn), renjian@egr.msu.edu (J. Ren), lincl@is.ac.cn (C. Lin).

0164-1212/$ - see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2008.11.844

in private key generating process. Since each user's private key is generated by multiple PKGs, this arrangement can reduce the risk of trust on a single PKG. Girault (1991) introduced the concept of self-certified public keys, which was extended in Lee and Kim (2002). In the self-certificated public-key system, each user's private key is chosen by the user himself. The user's public key is computed from the public key of the PKG and the user's identity so that the certificate is "embedded" in the public key. A problem of the self-certified scheme is that each public key is only implicitly authenticated; but not explicitly authenticated. In self-certified digital signature, each user still has to apply for a digital certificate from the authority for his/her long-term public key.

In 2003, Al-Riyami and Paterson proposed the concept of certificateless public-key cryptography (Al-Riyami and Paterson, 2003). In certificateless public-key cryptography, the PKG computes a partial private key for each user using his master key. The user then combines its partial private key with some user selected secret information to generate its actual private key. In this way, each user's private key is not available to the PKG. The public key of each user is computed from its private key and the PKG's public parameter. The user's public key can be made available to other users by transmitting it along with the messages or by placing it in a public directory. There is no authentication required for the public keys. In particular, there is no certificate for each public key. However, the system is no longer identity-based, because the public key cannot be computed from its identity alone. In certificateless encryption, the message sender needs to access the message receiver's identity and public key in order to generate ciphertext. However, in identity-based encryption, the message sender only needs to access the receiver's identity. In certificateless digital signature (CDS), the signer's public key can be attached as part of the digital signature to the verifier. Thus, the CDS provides the same benefit as the IBS. Meanwhile, it does not have the key escrow problem of the IBS. Since 2003, there are many bilinear mapping based proposals for CDS (Al-Riyami and Paterson, 2003; Yum and Lee, 2004; Li et al., 2005; Zhang et al., 2006; Gorantla and Saxena, 2005; Yap et al., 2006; Hu et al., 2007; Du and Wen, 2009).

In this paper, we propose a generalized approach to construct CDS schemes. The proposed construction can convert any DL-based signature scheme to a CDS scheme. The proposed CDS scheme is secure against adaptive chosen-message attack in the random oracle model. In addition, the proposed CDS scheme is efficient in signature generation and verification. To the best of our knowledge, this is the first scheme on designing CDS scheme based on the well-studied DLP.

This paper is organized as follows: In Section 2, the original ElGamal signature scheme and the modified ElGamal signature scheme are reviewed. Our proposed CDS scheme is described in Section 3 followed by security analysis in Section 4. We conclude in Section 5.

2. Review of the ElGamal signature scheme

In this section, we will briefly review the original ElGamal signature scheme as well as the modified ElGamal signature scheme.

2.1. Original ElGamal signature scheme

The signature generation often uses a one-way hash function h. The original ElGamal signature scheme (ElGamal, 1985) contains three algorithms: key generation, signature generation and signature verification.

Key generation algorithm $\mathsf{OK}_g(1^n)$: In all ElGamal-family signature schemes with security parameter 1^n, the message signer runs the random oracle $\mathsf{OK}_g(1^n)$ to generate a large prime p and a generator g of order $p-1$. These two numbers are made publicly known. The signer then selects a random private key $x \in \mathbb{Z}_p^*$ and computes the corresponding public key $y = g^x \bmod p$.

Signature generation algorithm $\mathsf{OSign}(x, m)$: Let m denote the message to be signed. The signer randomly selects a one-time secret $k \in \mathbb{Z}_p^*$ with $\gcd(k, p-1) = 1$, then computes $r = g^k \bmod p$. The parameter r does not depend on the message m and therefore can be computed off-line. In order to generate the signature of message m, the signer uses his private key x to compute s by solving the following linear equation

$$h(m) = sk + xr \bmod (p-1), \tag{1}$$

where h is the one-way hash function. Therefore, $s = k^{-1}(h(m) - xr) \bmod (p-1)$. The pair $\sigma = (r, s)$ is the signature of message m.

There are many variations of the original ElGamal signature scheme. Interested readers are referred to Harn and Xu (1994) for detailed information.

Signature verification algorithm $\mathsf{OVf}(y, m, \sigma)$: To verify the signature corresponding to Eq. (1), one checks whether

$$g^{h(m)} = y^r r^s \bmod p. \tag{2}$$

If Eq. (2) holds, then the verifier Accepts the signature, otherwise the verifier Rejects the signature.

2.2. Modified ElGamal signature scheme

Since the original ElGamal signature scheme ElGamal (1985) is existentially forgeable under both one-parameter and two-parameter forgeries, the scheme cannot achieve probable security. To solve this problem, the modified ElGamal signature (MES) scheme was proposed by Pointcheval and Stern (1996). The only difference between these two schemes is that $h(m)$ in the original ElGamal signature scheme is replaced with $h(m, r)$ in the MES scheme, where h is a one-way hash function used for message signing. It has been proved that the MES scheme is secure against existential forgery in the random oracle model (Pointcheval and Stern, 1996). For this reason, our proposed CDS scheme will be built on the MES, which means that in the proposed CDS scheme, $h(m)$ will be replaced by $h(m, r)$.

Similar to the original ElGamal signature scheme, the modified ElGamal signature scheme, illustrated in Fig. 1, also includes three algorithms.

3. Proposed design of certificateless signature schemes based on discrete logarithm problem

Key escrow is an inherent weakness of the original identity-based cryptographic schemes (Shamir, 1984). In an IBS scheme, the PKG issues private keys for all user using its master private key. As a result, the PKG is able to sign any message on user's behalf. The nature of this property violates the "non-repudiation" requirement of digital signatures.

To solve this problem, in the certificateless signature public-key system, though we still assumes the existence of a trusted PKG, the PKG can only compute a partial private key for each user using its master key. The user then uses the partial private key with the secret information to generate its actual private key. In this way, each user's private key is not available to the PKG. The user can also combine its secret information with the PKG's public parameters to compute its public key. Each user's public key can be made available to other users by transmitting it along with the signature or by placing it in a public directory. There is no authentication required for the public key. In particular, there is no certificate for each public key.

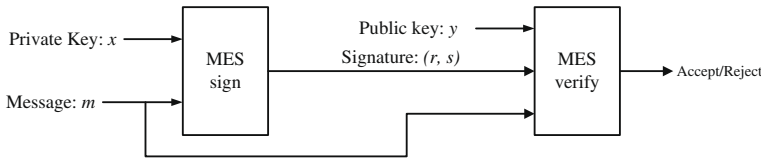

Fig. 1. The modified ElGamal signature scheme.

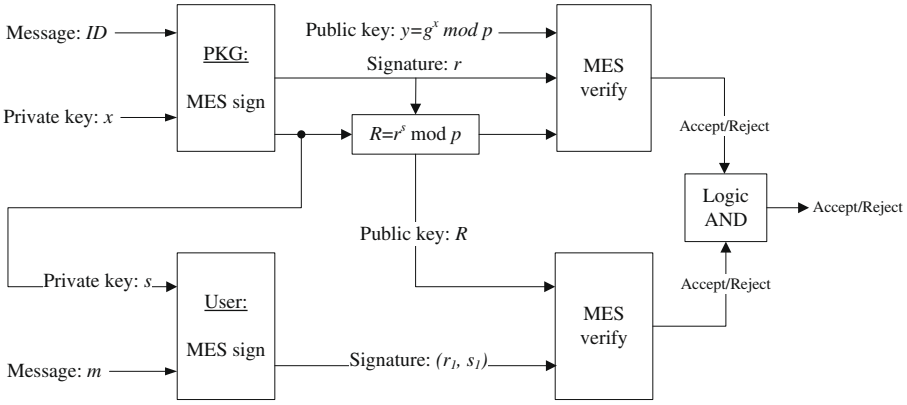

Fig. 2. The proposed CDS scheme.

In this section, an efficient CDS scheme based on DLP is proposed. The proposed scheme is quite easy to understand, implement, and can be applied to the entire ElGamal-family signature variants. The proposed CDS scheme contains four algorithms: PKG key generation, user key generation, message signing and signature verification, which is illustrated in Fig. 2. We now describe the four algorithms in detail.

PKG key generation $\mathsf{K}_{pkg}(1^n)$: This algorithm takes a security parameter 1^n as input, and outputs the public parameters *params* and the master private key of PKG.

(1) Run the random oracle $\mathsf{K}_{pkg}(1^n)$ to generate a large prime p and a generator g of $\mathbb{Z}_p^*$.
(2) Run the random oracle to select a random private key $x \in \mathbb{Z}_p^*$ and computes the public key $y = g^x \bmod p$.
(3) Return $params = (p, g, y)$ as the public parameters of PKG, while keep x as the master private key of PKG.

User key generation $\mathsf{K}_u(params, \mathsf{ID})$: This algorithm takes the public parameters *params* and the user's identity ID as inputs, and it will interact with PKG, then outputs user's private key s and public key (r, R).

(1) User selects a random private key $v \in \mathbb{Z}_{p-1}^*$ with $\gcd(v, p-1) = 1$, and computes $u = g^v \bmod p$. $\{\mathsf{ID}, u\}$ is sent to PKG.
(2) PKG generates a pair (r, z) such that $g^{h(\mathsf{ID},r)} = y^r t^z \bmod p$, where h is a one-way hash function. In order to achieve this aim, PKG first selects a $k \in \mathbb{Z}_{p-1}^*$ with $\gcd(k, p-1) = 1$, then computes $t = g^k \bmod p$ and $r = u^k \bmod p$. PKG solves the linear equation $h(\mathsf{ID}, r) = xr + kz \bmod (p-1) \Rightarrow z = k^{-1}(h(\mathsf{ID}, r) - xr) \bmod (p-1)$. The output (r, z) is sent to user.
(3) User extracts a pair (r, s) such that $g^{h(\mathsf{ID},r)} = y^r r^s \bmod p$. In order to achieve this aim, user computes $s = v^{-1} z \bmod (p-1)$ and $R = r^s \bmod p$. s is each user's private key and (r, R) is each user's public key.

Message signing $\mathsf{Sign}(params, m, s)$: This algorithm takes the public parameter *params*, the message m, and the user's private key s as inputs, and outputs the signature σ on m.

(1) Choose a random $l \in \mathbb{Z}_{p-1}^*$ with $\gcd(l, p-1) = 1$ and compute $r_1 = r^l \bmod p$.
(2) Solve s_1 from $h(m, r_1) = sr_1 + ls_1 \bmod (p-1)$. That is $s_1 = l^{-1}(h(m, r_1) - sr_1) \bmod (p-1)$.
(3) Return $\sigma = (r, R, r_1, s_1)$ as the complete CDS on m.

Signature verification $\mathsf{Vf}(params, \mathsf{ID}, m, \sigma)$: This algorithm takes the public parameter *params*, the user's identity ID, the message m and the signature σ as inputs, and outputs Accept or Reject.

The verification of the CDS σ for an identity ID and public key (r, R) on a message m is based on the following two equations:

(1) $g^{h(\mathsf{ID},r)} = y^r R \bmod p$, and
(2) $r^{h(m,r_1)} = R^{r_1} r_1^{s_1} \bmod p$.

If both equations hold, then the CDS will be Accepted, otherwise the CDS will be Rejected.

We note that there is no certification required for user's public key, that is, the authentication for user's public key is not required in CDS scheme.

Remark 1. The signing phase of our proposed CDS scheme requires one modulo exponentiation, which is identical to any ElGamal-family signature variant. The CDS verification requires four modulo exponentiations, while only two modulo exponentiations are required for ElGamal-family signature variants. Therefore, two additional modulo exponentiations are required in our proposed CDS scheme. The length of CDS is doubled as compared to the length of any ElGamal-family signature variant.

Remark 2. Without loss of generality, we can represent the generalized signing equation for all DL-based signature schemes as $ax = bk + c \bmod (p-1)$ where (a, b, c) are three parameters from the set of values $\{m, r, s\}$. More specifically, each parameter can be a mathematical combination of $\{m, r, s\}$. For example, the

parameter a can be m, r or s. The verification equation is determined accordingly as $y^a = r^b g^c \bmod p$. There are 18 generalized ElGamal-type signature variants (Harn and Xu, 1994). Readers can refer to Harn and Xu (1994) for more discussion on the design of DL-based signature schemes. Among all DL-based signature schemes, the signature component s is always in the exponent of signature verification equations. Thus, by following the same approach as proposed in this section we can convert any DL-based signature scheme to a CDS scheme.

4. Security analysis for our proposed CDS scheme

In this section, we will analyze the security of the proposed CDS scheme. We first describe the attack of the CDS scheme in detail. Then, we prove that the proposed CDS scheme is secure against these attacks. The security analysis is based on discrete logarithm problem (DLP) and discrete logarithm assumption (DLA) in the random oracle model.

Definition 1 (*Discrete logarithm problem (DLP)*). Let p be a large prime and g be a generator of order $p-1$ in $\mathbb{Z}_p^*$, given the elements g, y and p, compute the exponent x such that $y = g^x \bmod p$.

Definition 2 (*Discrete logarithm assumption (DLA)*). It is computationally infeasible to solve the discrete logarithm problem.

In our analysis, we consider three types of attacks. The first two types of attack relate to the security of the PKG key generation and user key generation respectively, while the third type of attack is about security against adaptive chosen-message attack in the random oracle model. We will define the three types of attack formally as follows.

Definition 3 (*Type I attack*). The adversary $\mathscr{A}_I$, who only knows the public parameter, tries to obtain PKG's master private key.

Definition 4 (*Type II attack*). The adversary $\mathscr{A}_{II}$, who can be a dishonest PKG knowing user's public key and user's partial private key in user key generation, tries to obtain user's private key.

Definition 5 (*Type III attack*). The adversary $\mathscr{A}_{III}$, who takes on the ability of the adaptive chosen-message attack as described in Goldwasser et al. (1988), tries to forge a valid CDS. The adversary can be categorized into two types. The first type of adversaries is a dishonest PKG who knows the PKG's master private key and user's partial private key in user key generation. The second type of adversaries is generally a third party who does not know the PKG's master private key and the user's private key.

We will prove that our proposed CDS scheme is secure against Type I and Type II attacks under the DLA (Theorem 1), and is secure against Type III attack under the adaptive chosen-message attack in the random oracle model (Theorem 2).

For an alleged CDS (r, R, r_1, s_1) of a message m signed by a user with identity ID, the signature verification is based on the following two equations:

(1) $g^{h(\mathrm{ID},r)} = y^r R \bmod p$, and
(2) $r^{h(m,r_1)} = R^{r_1} r_1^{s_1} \bmod p$,

where ensures that the public key R for the user with identity ID is generated by the PKG with knowledge of the secret exponent of y) ensures that the signature component (r_1, s_1) of message m is generated by the signer with knowledge of the secret exponent of R, which is equivalent to the public key y in the MES. Therefore, in order for a CDS to be valid, both verification equations need to be satisfied.

It has been proved that the MES scheme is secure against adaptive chosen-message attack in the random oracle model (Pointcheval and Stern, 1996). We will prove that our proposed CDS scheme is also secure against adaptive chosen-message attack in the random oracle model.

Theorem 1. The proposed CDS scheme is secure against Type I and Type II attacks under DLA.

Proof. In the Type I attack, the adversary $\mathscr{A}_I$, who only knows the public parameter, tries to obtain PKG's master private key. The adversary can only try to compute the master private key from the public information. It is obvious that to get the secret exponent x of the master private key from PKG's public key $y = g^x \bmod p$ is equivalent to solving the typical DLP. Thus, it is computationally infeasible for $\mathscr{A}_I$ to obtain x under the DLA.

In the Type II attack, the adversary $\mathscr{A}_{II}$, who can be a dishonest PKG knowing the user's public key and partial private key in user key generation, tries to obtain the user's private key. It is obvious that to get the user's private key s from its public key $R = r^s \bmod p$ is equivalent to solving the typical DLP. In addition, it is computationally infeasible for $\mathscr{A}_{II}$ to compute the user's private key s from its partial private key z in user key generation. This is because $s = v^{-1} z \bmod (p-1)$, where v is a secret randomly selected by the user. On the other hand, the computation of v from $u = g^v \bmod p$ is a typical DLP. □

However, a dishonest PKG may pretend to be a user with identity ID and try to obtain a private key. Then, a dishonest PKG uses it to generate a valid CDS of any given message. This attack is similar to the attack made by a dishonest Certificate Authority (CA). That is, a dishonest CA can pretend to be a user and to obtain a valid public-key digital certificate. In this way, a dishonest CA uses this public-key digital certificate to impersonate the user to communicate with others.

Theorem 2. The proposed CDS scheme is secure against Type III attack, that is, secure against adaptive chosen-message attack under the random oracle model.

Proof. The adversary can be divided into types: The first type of adversaries consists of a dishonest PKG who knows the PKG's master private key and the user's partial private key in user key generation. The second type of adversaries is a general third party who does not know PKG's master private key and user's private key.

In previous theorem we have proved that our scheme is secure against Type II attack under DLA. That is, a dishonest PKG cannot obtain a user's private key. According to the MES, *only* the legitimate user with knowledge of the secret exponent of R, the user's private key, is able to generate a pair of (r_1, s_1) such that $r^{h(m,r_1)} = R^{r_1} r_1^{s_1} \bmod p$. Thus, a dishonest PKG cannot impersonate a user to generate a valid CDS.

For the adversary to be a general third party $\mathscr{A}_{III}$ who does not know PKG's master private key and a user's private key, we will prove that it is impossible to forge a valid CDS. We prove this result by contradictory.

First, we assume that $\mathscr{A}_{III}$ can forge a valid signature $\sigma = (r, R, r_1, s_1)$ under the targeted identity ID and any given message m and the given public parameter. In other words, the forged CDS satisfies both of the following verification equations.

(1) $g^{h(\mathrm{ID},r)} = y^r R \bmod p$, and
(2) $r^{h(m,r_1)} = R^{r_1} r_1^{s_1} \bmod p$.

We know that Eq. (2) is the verification equation of MES scheme of message m, where R is the public key. Since the forged CDS satisfies the Eq. (2) and MES scheme is secure against adaptive

chosen-message attack in the random oracle model, we can conclude that $\mathscr{A}_{III}$ must know the secret exponent of R.

Furthermore, we note that in Eq. (1), the secret exponent of R is one of the components of the MES scheme with the message identity ID, where y is the public key. Since the forged CDS also satisfies the Eq. (1) and the MES scheme is secure against adaptive chosen-message attack in the random oracle model, $\mathscr{A}_{III}$ must know the discrete logarithm of y. This result contradicts to our previous assumption that $\mathscr{A}_{III}$ does not know PKG's master private key. □

5. Conclusions

In ID-based cryptosystems, the public key of the user can be derived from the user's identity. IBS can be verified using the signer's identity and PKG's public keys. There is no authenticated public-key distribution required. However, the IBS schemes bear an inherent weakness, that is the PKG knows the private keys of the users. As a result, the PKG is able to sign any messages on users' behalf, which violates the "non-repudiation" requirement of digital signatures. To solve this problem, the concept of CDS was proposed, which enjoys the benefit of IBS, meanwhile, it does not have key escrow problem. In this paper, we propose a simple method to transform any DL-based signature scheme into a CDS scheme. Our scheme can eliminate key escrow from the PKG since the user's private key is known only to the user himself. The proposed CDS scheme is secure against adaptive chosen-message attack in the random oracle model.

Acknowledgement

This research was supported in part by National Science Foundation under grants CNS-0716039 and CNS-0848569.

References

Al-Riyami, S., Paterson, K., 2003. Certificateless public key cryptography. Advances in Cryptology – AsiaCrypt, LNCS, vol. 2894. Springer-Verlag, pp. 452–473.
Bellare, M., Namprempre, C., Neven, G., 2004. Security proofs for identity-based identification and signature schemes. Advances in Cryptology – EuroCrypt'04, LNCS, vol. 3027. Springer-Verlag, pp. 268–286.
Cha, J., Cheon, J.H., 2003. An identity-based signature from gap Diffie-Hellman groups. Public Key Cryptography – PKC'03, LNCS, vol. 2567. Springer-Verlag, pp. 18–30.
Chen, X., Zhang, F., Kim, K., 2003. A new ID-based group signature scheme from bilinear pairings. WISA'03, LNCS, vol. 2908. Springer-Verlag, pp. 585–592.
Du, H., Wen, Q., 2009. Efficient and provably-secure certificateless short signature scheme from bilinear pairings. Computer Standards & Interfaces 31 (2), 390–394.
ElGamal, T.A., 1985. A public-key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory 31 (4), 469–472.
Girault, M., 1991. Self-certified public keys. Advances in Cryptology – EuroCrypt'91, LNCS, vol. 547. Springer-Verlag, pp. 490–497.
Goldwasser, S., Micali, S., Rivest, R., 1988. A digital signature scheme secure against adaptive chosen-message attack. SIAM Journal of Computing 17 (2), 281–308.
Gorantla, M., Saxena, A., 2005. An efficient certificateless signature scheme. CIS'05, Part II, LNAI, vol. 3802. Springer-Verlag, pp. 110–116.
Guillou, L.C., Quisquater, J.J., 1988. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. Advances in Cryptology – EuroCrypt'88, LNCS, vol. 330. Springer-Verlag, pp. 123–128.
Guillou, L.C., Quisquater, J.J., 1989. A "paradoxical" identity-based signature scheme resulting from zero-knowledge. Advances in Cryptology – Crypto'88, LNCS, vol. 403. Springer-Verlag, pp. 216–231.
Harn, L., Xu, Y., 1994. Design of generalized ElGamal type digital signature schemes based on discrete logarithms. Electronics Letters 30 (24), 2025–2026.
Hess, F., 2003. Efficient identity based signature schemes based on pairings. Selected Areas in Cryptography – SAC'03, LNCS. Springer-Verlag, pp. 310–324.
Hu, B., Wong, D., Zhang, Z., et al., 2007. Certificateless signature: a new security model and an improved generic construction. Designs, Codes and Cryptography 42 (2), 109–126.
I.S.I. 14888-2, 1999. Information technology – security techniques – digital signatures with appendix – part 2: identity-based mechanisms.
Joux, A., 2000. A one round protocol for tripartite diffie-hellman. Algorithmic Number Theory IV-th Symposium (ANTS IV) LNCS, vol. 1838. Springer-Verlag, pp. 385–394.
Lee, B., Kim, K., 2002. Self-certified signatures. IndoCrypt'02, LNCS, vol. 2551. Springer-Verlag, pp. 199–214.
Li, X., Chen, K., Sun, L., 2005. Certificateless signature and proxy signature schemes from bilinear pairings. Lithuanian Mathematical Journal 45, 76–83.
Paterson, K.G., 2002. ID-based signatures from pairings on elliptic curves. Electronics Letters 38 (18), 1025–1026.
Pointcheval, D., Stern, J., 1996. Security proofs for signature schemes. Advances in Cryptology – EuroCrypt'96, LNCS, vol. 1070. Springer-Verlag, pp. 387–398.
Sakai, R., Ohgishi, K., Kasahara, M., 2000. Cryptosystems based on pairing. Symposium on Cryptography and Information Security – SCIS'00, Okinawa, Japan, pp. 26–28.
Shamir, A., 1984. Identity-based cryptosystems and signature schemes. Advances in Cryptology – Crypto'84, LNCS, vol. 196. Springer-Verlag, pp. 47–53.
Yap, W.S., Heng, S.H., Goi, B.M., 2006. An efficient certificateless signature scheme. EUC Workshops 2006, LNCS, vol. 4097. Springer-Verlag, pp. 322–331.
Yi, X., 2003. An identity-based signature scheme from the Weil pairing. IEEE Communications Letters 7 (2), 76–78.
Yum, D., Lee, P., 2004. Generic construction of certificateless signature. ACISP'04, LNCS, vol. 3108. Springer-Verlag, pp. 200–211.
Zhang, Z.F., Wong, D.S., Xu, J., et al., 2006. Certificateless public-key signature: security model and efficient construction. ACNS'06, LNCS, vol. 3989. Springer-Verlag, pp. 293–308.

Lein Harn received the B.S. degree in electrical engineering from the National Taiwan University in 1977, the M.S. degree in electrical engineering from the State University of New York-Stony Brook in 1980, and the Ph.D. degree in electrical engineering from the University of Minnesota in 1984. In 1984, he joined the Department of Electrical and Computer Engineering, University of Missouri-Columbia as an assistant professor, and in 1986, he moved to Computer Science and Telecommunication Program (CSTP), University of Missouri, Kansas City (UMKC). While at UMKC, he went on development leave to work in Racal Data Group, Florida for a year. His research interests include cryptography, network security, and wireless communication security. He has published a number of papers on digital signature design and applications and wireless and network security. He has written two books on security. He is currently investigating new ways of using digital signature in various applications.

Jian Ren received the B.S. and M.S. degrees both in mathematics from Shaanxi Normal University, China, in 1988 and 1991 respectively. He received the Ph.D. degree from Xidian University in 1994. He is now an assistant professor in the Department of Electrical and Computer Engineering, Michigan State University. From 1997 to 1998, he was with Racal Datacom as a security architect. From 1998 to 2002, he was first with Bell-Labs and later with Avaya Labs as a member of technical staff. His research interests include cryptography, network security, sequence design for wireless CDMA communications, E-commerce, and wireless and multimedia communication security.

Changlu Lin received the B.S. degree and M.S. degree in mathematics from the Fujian Normal University, P.R. China, in 2002 and in 2005, respectively. Since September 2005, he is pursuing a doctor degree in information security from the state key laboratory of information security, graduate university of Chinese Academy of Sciences, P.R. China. His research interests include cryptography and information security.