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 $\mathsf{Accepts}$ the signature, otherwise the verifier $\mathsf{Rejects}$ 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.