Certificate-Based Signature: Security Model and Efficient Construction*

Jiguo Li[1], Xinyi Huang[2], Yi Mu[2], Willy Susilo[2], and Qianhong Wu[2]

[1] College of Computer and Information Engineering
Hohai University, Nanjing, P.R. China, 210098
lijiguo@hhu.edu.cn
[2] Centre for Computer and Information Security Research
School of Computer Science & Software Engineering
University of Wollongong, Australia
{xh068,ymu,wsusilo,qhw}@uow.edu.au

Abstract. In Eurocrypt 2003, Gentry introduced the notion of certificate-based encryption. The merit of certificate-based encryption lies in the following features: (1) providing more efficient public-key infrastructure (PKI) that requires less infrastructure, (2) solving the certificate revocation problem, and (3) eliminating third-party queries in the traditional PKI. In addition, it also solves the inherent key escrow problem in the identity-based cryptography. In this paper, we first introduce a new attack called the "Key Replacement Attack" in the certificate-based system and refine the security model of certificate-based signature. We show that the certificate-based signature scheme presented by Kang, Park and Hahn in CT-RSA 2004 is insecure against key replacement attacks. We then propose a new certificate-based signature scheme, which is shown to be existentially unforgeable against adaptive chosen message attacks under the computational Diffie-Hellman assumption in the random oracle model. Compared with the certificate-based signature scheme in CT-RSA 2004, our scheme enjoys *shorter* signature length and less operation cost, and hence, our scheme outperforms the existing schemes in the literature.

Keywords: Certificate-based signature, Key replacement attack, PKI.

1 Introduction

In traditional public key signatures (PKS), the public key of a signer is essentially a random string selected from a given set. Therefore, it is infeasible to prove that a party is indeed the signer for a given signature. This problem was solved by assuming the existence of a trusted third party (or often referred to as a Certification Authority - CA) who can issue (sign) public key certificates which

* The work is supported by the National Natural Science Foundation of China (No. 60673070), Natural Science Foundation of Jiangsu Province (No. BK2006217), and the Project of Jiangsu Province Police Ministry (No. 200503002).

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 110–125, 2007.
© Springer-Verlag Berlin Heidelberg 2007

provide an unforgeable and trusted link between a public key and the identity of a signer. This kind of certificate systems are referred to as the Public Key Infrastructure (PKI). "Third-party query" is considered as a problem in the traditional PKI. Namely, before verifying a signature using the signer's public key, a verifier must obtain the signer's certification status; hence in general he has to make a query on the signer's certificate status to the CA. The verifier must verify the certificate first. If authorization of the CA about the signer's public key is valid, a verifier can then verify the signed message with the given public key from the signer. Therefore, from the verifier's point of view, two verification operations are required. This has been regarded as a drawback due to additional computation time and storage. The apparent need for this infrastructure is often cited as a reason for the widespread use of public-key cryptography. To simplify key management procedures of conventional PKIs, Shamir [1] introduced the concept of Identity-Based Cryptography (IBC) in 1984, which sought to reduce the requirement on the infrastructure by using user's identity as public key. In his seminal paper, Shamir also proposed an identity-based signature scheme. The first practical provably secure Identity-Based Encryption (IBE) scheme [2] was proposed by Boneh and Franklin in 2001. With this approach, certification becomes implicit; that is, the sender of a message does not need to check whether the user is certified or not. Instead, prior to decryption, the receiver must identify himself to a trusted third party called a Private Key Generator (PKG), who will generate and send his private key via an authentication and secure channel. The main practical benefit of IBC lies in greatly reduction of need for public key certification. The PKG can generate the secret keys of all its users, so *private key escrow* becomes an inherent problem in IBC. Moreover, secret keys must be sent over secure channels, which makes secret key distribution a daunting task [9].

To fill the gap between traditional cryptography and identity-based cryptography, Al-Riyami and Paterson proposed a new paradigm called certificateless public key cryptography (CL-PKC) [3]. In CL-PKC, KGC is involved in the process of issuing a partial secret key for each user. The user independently generates a public/private key pair and performs some cryptographic operations in such a way that they can only be carried out when both the partial secret key and the private key are known. Knowing only one of them will not enable anyone to impersonate the user. Therefore, CL-PKC not only solves the key escrow problem, but also eliminates the use of certificates as in traditional digital signature schemes. Due to the lack of public key authentication (certificate), it is important to assume that an adversary in the certificateless system can replace the user's public key with a false key of its choice, which is also known as *key replacement attack*. Cryptographic protocols in certificateless system are easily suffered from this kind of attack. For example, the first certificateless-based signature scheme [3] is not secure against the key replacement attack [5,6]. This problem was later fixed. We will not go into the detail, since it is out of the scope of this paper. Please refer to [5,6] for the detail of the key replacement attack in certificateless system.