On the Security of Certificateless Signature Schemes from Asiacrypt 2003*

Xinyi Huang[1], Willy Susilo[2], Yi Mu[2], and Futai Zhang[1,**]

[1] College of Mathematics and Computer Science,
Nanjing Normal University, P.R. China
xinyinjnu@126.com, zhangfutai@njnu.edu.cn
[2] Centre for Information Security Research,
School of Information Technology and Computer Science,
University of Wollongong, Australia
{wsusilo, ymu}@uow.edu.au

Abstract. In traditional digital signature schemes, certificates signed by a trusted party are required to ensure the authenticity of the public key. In Asiacrypt 2003, the concept of certificateless signature scheme was introduced. In the new paradigm, the necessity of certificates has been successfully removed. The security model for certificateless cryptography was also introduced in the same paper. However, as we shall show in this paper, the proposed certificateless signature is insecure in their defined model. We provide an attack that *can successfully forge* a certificateless signature in their model. We also fix this problem by proposing a new scheme.

Keywords: Certificateless Signature, Certificateless Cryptography, Attack Model, Bilinear Pairing.

1 Introduction

In traditional digital signature schemes, the binding between a user and his public key needs to be ensured. A typical way to provide this assurance is by providing certificates that are signed by a trusted third party. In [13], Shamir introduced a new notion called identity-based cryptography (and hence, identity-based signature scheme) where the user's public key is indeed his identity (such as an email, IP address, etc.). This way, the need of certification can be avoided. However, this approach creates a new inherent problem namely the key escrow of a user's private key, since the trusted third party called the Private Key Generator (PKG) must be completely trusted, since he has the knowledge of the user's secret key.

* This work is supported by ARC Discovery Grant DP0557493.
** Partially supported by Ministry of Education of Jiangsu Province Project 03KJA520066 and Open Project of Key Laboratory on Computer Network and Information Security of Ministry of Education of China.

Y.G. Desmedt et al. (Eds.): CANS 2005, LNCS 3810, pp. 13–25, 2005.

To fill the gap between traditional cryptography and identity-based cryptography, Al-Riyami and Paterson proposed a new paradigm called *certificateless cryptography* in [1]. In contrast to traditional cryptography, certificateless cryptography does not require the use of any certificates to ensure the authenticity of public keys. Certificateless cryptography relies on the existence of a trusted third party who has the master-key. In this sense, it is similar to identity-based cryptography. Nevertheless, certificateless cryptography does not suffer from the key escrow property that seems to be inherent in identity-based cryptography. We note that the concept of certificateless cryptography has been around [7, 9, 10, 12], but the first formalization was provided in [1].

Intuitively, the characteristic of certificateless cryptography is as follows. The trusted third party, called the KGC, does not have access to the users' private keys. The KGC only supplies a user with a *partial private key* D_i, which the KGC computes from an identifier ID_i. As in the identity-based cryptography, the partial private key needs to be delivered securely to the user. Then, the user combines his partial private key D_i with some secret information to generate his actual private key S_i. This way, the user's private key is *not* available to the KGC. The user also combines his secret information with the KGC's public parameters to generate his public key P_i. The user's public key P_i needs to be made available to the other participants by transmitting it along with messages, in the case of message signing. Hence, it is no longer an identity-based cryptography, since the public key needs to be provided (but in contrast to the traditional cryptography, the public key does not require any certificate).

Due to the lack of public key authentication, it is important to assume that an adversary can replace the user's public key by a false key of its choice [1]. In order to provide a secure certificateless signature scheme, this type of attacks must not be able to produce signatures that verify with the false public key [1]. An assumption that must be made is that the KGC does not mount a public key replacement attack since he is armed with a partial private key. Hence, we must assume that the KGC, who posses the master-key and hence all partial private keys, is trusted not to replace user's public keys. This way, the level of trust is similar to the trust in a CA in a traditional PKI. We will review the adversarial model defined in [1] in the next section.

Following, the work of [1], there are several certificateless public key encryption proposed (eg. [3, 5, 4, 15]). In [14], a generic construction of certificateless signature from any identity-based signature scheme and a secure public key signature scheme in the sense of [8] was proposed.

Our Contribution

In this paper, we show that the proposed certificateless signature scheme in [1] *does not* satisfy the security requirement of certificateless cryptography, in terms of the defined adversarial model in [1]. To be more precise, we show that an attacker who does *not* posses the master-key but can only do a public key replacement attack, can always successfully forge a signature. We also provide a new scheme that resists against this type of attacks and hence, it satisfies the requirements of certificateless signature schemes as defined in [1].