Theoretical Computer Science 639 (2016) 42–59

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Provably secure certificateless proxy signature scheme in the standard model

Yang Lu *, Jiguo Li

College of Computer and Information, Hohai University, Nanjing, China

ARTICLE INFO

Article history:
Received 16 August 2015
Received in revised form 25 February 2016
Accepted 14 May 2016
Available online 24 May 2016
Communicated by G. Persiano

Keywords:
Certificateless public key cryptography
Proxy signature
Standard model
Public key replacement attack
Malicious KGC attack
Existential unforgeability

ABSTRACT

Certificateless public key cryptography was introduced to solve the key escrow problem in identity-based cryptography and eliminate the use of certificates. As an extension of proxy signature in the certificateless setting, certificateless proxy signature has attracted much attention and many schemes have been proposed recently. So far, only one certificateless proxy signature scheme without using the random oracles was found in the literature. Unfortunately, cryptanalysis shows that it suffers from some security drawbacks and fails in achieving the existential unforgeability. To overcome the security weaknesses in this scheme, we newly propose a certificateless proxy signature scheme without random oracles. In the standard model, we strictly prove it to be existentially unforgeable against chosen message attacks. Compared with previous certificateless proxy signature scheme without random oracles, the new scheme offers stronger security while enjoying better performance.

1. Introduction

In 1984, Shamir [1] introduced the concept of identity-based cryptography (IBC) to solve the certificate management problem in traditional public key cryptography (PKC). In IBC, a user's public key could be an arbitrary string related to his identity such as e-mail address, telephone number and so on. As a result, IBC eliminates the need for public key certificates and greatly reduces the system complexity. However, the users' private keys should be generated by a trusted authority called private key generator (PKG). Then, IBC has to face with the key escrow problem since all users' private keys are known to the PKG.

To solve the key escrow problem in IBC and eliminate the use of public key certificates, Al-Riyami and Paterson [2] introduced the notion of certificateless public key cryptography (CLPKC) in Asiacrypt 2003. The main idea of CLPKC is that a user should combine two different components to form his private key: one component is a partial private key generated by a trusted third party called key generation center (KGC) and another component is a secret value chosen by the user himself. In addition, a public key computed from the secret value should be published. It is obvious that CLPKC overcomes the key escrow problem inherent in IBC, because KGC does not know any user's private key. Furthermore, CLPKC provides an effective implicit authentication mechanism so that a user does not need to obtain a certificate from the certificate authority for the authenticity of his public key. Following Al-Riyami and Paterson's pioneering work [2], numerous certificateless

* Corresponding author. Postal address: College of Computer and Information, Hohai University, No. 8, Focheng Xi Road, Jiangning District, Nanjing City, Jiangsu Province, 211100, China. Tel.: +86 13401929210.
E-mail addresses: luyangnsd@163.com (Y. Lu), ljg1688@163.com (J. Li).

http://dx.doi.org/10.1016/j.tcs.2016.05.019
0304-3975/

cryptographic schemes have been proposed, including many encryption schemes (*e.g.* [3–6]), signature schemes (*e.g.* [5, 7–10]) and signcryption schemes (*e.g.* [11–13]).

The concept of proxy signature was first introduced by Mambo et al. [14] in 1996. The proxy signature schemes allow an entity, called original signer, to delegate its signing power to other entities, called proxy signer. Then the proxy signers can sign messages to generate proxy signatures on behalf of the original signer. Proxy signature schemes have been found to be useful in many applications, such as distributed shared object systems [15], grid computing [16], global distribution networks [17], mobile agent environment [18], mobile communications [19], *etc.* In 2005, Li et al. [20] introduced proxy signature into certificateless public key cryptography and proposed the first certificateless proxy signature (CLPS) scheme. However, they did not prove the security of their scheme. Moreover, their scheme was pointed out to be insecure against proxy signature forgery attack [21–23]. To improve security, Lu et al. [22] and Choi et al. [23] respectively proposed an improved CLPS scheme. But, no formal security analysis was given in both [22] and [23]. In 2009, Chen et al. [24] presented a formal security model for CLPS and proposed the first provably secure CLPS scheme. To improve performance and security, several provably secure CLPS schemes [25–28] have been proposed in the literature so far.

1.1. Motivation and contribution

Provably security is the basic requirement for CLPS schemes. All the CLPS schemes [24–28] described above were proven secure in the random oracle model proposed by Bellare and Rogaway [29]. Although the random oracle methodology is useful and efficient, a proof in the random oracle model may not necessarily imply the security in the reality [30]. As shown by Canetti et al. in [30], when the random oracles are instantiated with the concrete cryptographic hash functions, the resulting cryptographic schemes may not be practically secure. Therefore, the search for a CLPS scheme that can be proven secure without resorting to the random oracles is of great importance. As far as the authors know, there exists only one CLPS scheme (proposed by Eslami and Pakniat [31]) that does not use the random oracles. However, Eslami and Pakniat [31] merely claimed that their scheme can be proven secure in the standard model without providing a concrete security proof. Unfortunately, our cryptanalysis shows that their scheme does not achieve the existential unforgeability. The insecurity of Eslami and Pakniat's scheme lies in that a public key replacement adversary or a malicious KGC can successfully forge delegation certificates on behalf of an original signer or proxy signatures on behalf of a proxy signer. So, it is fair to say that devising a secure CLPS scheme without depending on the random oracles remains an unsolved problem until now.

In this paper, we first give two concrete attacks to show that Eslami and Pakniat's CLPS scheme [31] does not satisfy the existential unforgeability. Then, we propose a new CLPS scheme without random oracles. Under the square computational Diffie–Hellman assumption, we strictly prove that the proposed scheme is existential unforgeable against adaptive chosen-message attacks in the standard model. Compared with Eslami and Pakniat's CLPS scheme, our new scheme has three advantages. Firstly, it remedies the security flaws existing in Eslami and Pakniat's scheme as it resists both the public key replacement and malicious KGC attacks. Secondly, it offers stronger security guarantee since it is strictly proved to be secure in the standard model. Finally, it enjoys shorter system public parameters and lower computational cost.

1.2. Paper organization

The rest of our paper is organized as follows: In Section 2, we introduce some related notions and the formal model of CLPS. In Section 3, we present our attacks against Eslami and Pakniat's CLPS scheme. The proposed CLPS scheme is described and analyzed in Section 4. Finally, we draw our conclusions and make some further discussions in Section 5.

2. Preliminaries

2.1. Bilinear pairing and complexity assumption

Let G_1 and G_2 be two multiplicative cyclic groups of prime order p and g be a generator of G_1. A map e: $G_1 \times G_1 \to G_2$ is said to be a bilinear pairing if it satisfies the following three properties:

(1) Bilinearity: $e(g^a, g^b) = e(g, g)^{ab}$ for all $a, b \in Z_p$.
(2) Non-degeneracy: $e(g, g) \neq 1$.
(3) Computability: e can be efficiently computed.

The security of our CLPS scheme relies on the following square computational Diffie–Hellman (Squ-CDH) assumption [32].

Definition 1. Given a group G_1 of prime order p with generator g and $g^a \in G_1$ for unknown $a \in Z_p$, the Squ-CDH problem in G_1 is to compute $g^{a^2} \in G_1$.

The advantage of a probabilistic polynomial time (PPT) algorithm $\mathcal{A}$ in solving the Squ-CDH problem is defined as

$$Adv_{\mathcal{A}}^{\text{Squ-CDH}}(k) = \Pr\left[\mathcal{A}(g, g^a) = g^{a^2}\right].$$

We say that the Squ-CDH assumption holds in G_1 if for any PPT algorithm $\mathcal{A}$, the advantage $Adv_{\mathcal{A}}^{\text{Squ-CDH}}(k)$ is negligible.