Information Processing Letters 114 (2014) 492–499

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Certificateless signature scheme with security enhanced in the standard model

Yumin Yuan *, Chenhui Wang

School of Applied Mathematics, Xiamen University of Technology, China

ARTICLE INFO

Article history:
Received 27 December 2012
Received in revised form 14 November 2013
Accepted 6 April 2014
Available online 13 April 2014
Communicated by V. Rijmen

Keywords:
Cryptography
Certificateless signature
Standard model
Provably secure

ABSTRACT

Certificateless cryptography is an attractive paradigm, which combines the advantages of identity-based cryptography (without certificate) and traditional public key cryptography (no escrow). Recently, to solve the drawbacks of the existing certificateless signature (CL-S) schemes without random oracles, Yu et al. proposed a new CL-S scheme, which possesses several merits including shorter system parameters and higher computational efficiency than the previous schemes. However, in this work, we will point out that their CL-S scheme is insecure against key replacement attack and malicious-but-passive KGC attack. We further propose an improved scheme that overcomes the security flaws without affecting the merits of the original scheme. We prove that our scheme is existentially unforgeable against adaptive chosen message attacks under the computational Diffie–Hellman assumption in the standard model.

1. Introduction

In a traditional public key cryptography (PKC), a user selects a public/private key pair and publishes public key. This leads to a problem of how the public key is associated with the user. In these cryptosystems the binding between public key and identity of the user is obtained via a digital certificate. Therefore, a conventional public key infrastructure (PKI) requires heavy management and communication cost to achieve authenticity of the public keys of users.

To reduce this burden, Shamir [9] proposed the concept of ID-based cryptography (ID-PKC) wherein, a user's public key can be obtained directly from his unique identifier information, while the user's private key is generated by a trusted third party called Private Key Generator (PKG). However, an inherent problem of such ID-PKC is key escrow, i.e., the PKG knows all user's private key.

To solve the key escrow problem in ID-PKC and eliminate the use of certificates in PKC, Al Riyami and Paterson [1] introduced the concept of certificateless public key cryptography (CL-PKC). In CL-PKC, a semi-trusted third party called Key Generation Center (KGC) is also involved, which is responsible for generating user's partial private key *psk* based on his identity. In such certificateless cryptosystem, a user's actual key consists of partial private key *psk* for the user identity ID generated by the KGC and public/secret key pair (*upk*, *usk*) generated by the user himself. In CL-PKC, to generate valid signatures of a user with the identity ID under the public key *upk*, one needs to know both the partial private key of ID and the corresponding secret key *usk* of *upk*. While verifier can directly use the user's public key *upk* to verify signatures, without checking the certificate of the user's public key.

The concept of certificateless signature (CL-S) scheme was initially introduced by Al Riyami and Paterson [1], who also proposed the first CL-S scheme in the same literature. Following the work of Al Riyami and Paterson [1], many researchers have done a lot of work in this field. However, most of the existing schemes in the certificateless setting

* Corresponding author.
E-mail addresses: yuanymp@163.com (Y. Yuan), chwang@xmut.edu.cn (C. Wang).

http://dx.doi.org/10.1016/j.ipl.2014.04.004
0020-0190/

were proven secure in the random oracle model proposed by Bellare and Rogaway [4]. Although the random oracle methodology leads to the construction of efficient and provably-secure schemes, it has received a lot of criticism. It has been shown that when random oracles are instantiated with concrete hash functions, the resulting scheme may not be secure [3,5].

To make up for this, based on the identity-based signature scheme proposed by Paterson and Schuldt [8], the first CL-S scheme without random oracles was proposed by Liu et al. [7]. After that, Xiong et al. [13] and Huang et al. [6] independently pointed out that Liu et al.'s CL-S scheme cannot achieve unforgeable against malicious-but-passive KGC [2] attack. To eliminate the security problems in Liu et al.'s scheme, Xiong et al. provided a countermeasure in [13]. However, Shim et al. [10] pointed out that their scheme is in fact still insecure in the face of a malicious-but-passive KGC attack. In addition, Xia et al. [12] demonstrated that the existing CL-S schemes in the standard model [7,13,15] share a common flaw, i.e., given a signer's signature on a message, an adversary can replace the public key of the signer and forge valid signatures on the same message under the replaced public key. To overcome the common flaw of those schemes, Yu et al. [14] further proposed an improved certificateless signature scheme, which has several merits including shorter system parameters and higher computational efficiency than the previous schemes. Although they claimed that their scheme was stronger security than the previous schemes, in this work, we will point out that their scheme is not secure against the key replacement attack. Moreover, Yu et al.'s CL-S scheme is insecure against a malicious-but-passive KGC attack (note that our malicious-but-passive KGC attack does not refute the security claims made in [14], since their security model does not consider this attack).

To remedy these security flaws, we further propose an improved scheme, which is shown to be existentially unforgeable against adaptive chosen message attacks under the computational Diffie–Hellman assumption in the standard model. It not only preserves the advantages of Yu et al.'s scheme such as shorter system parameters and higher computational efficiency than the existing related works, but also improves the efficiency of [14] by reducing the signature size.

2. Bilinear maps and complexity assumption

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two cyclic multiplicative groups of prime order p. A map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is called a bilinear map if it satisfies the following properties:

1. Bilinear: $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$ for all $g_1, g_2 \in \mathbb{G}$ and all $a, b \in \mathbb{Z}_p$.
2. Non-degeneracy: There exist $g_1, g_2 \in \mathbb{G}$ such that $e(g_1, g_2) \neq 1$.
3. Computable: There is an efficient algorithm to compute $e(g_1, g_2)$ for any $g_1, g_2 \in \mathbb{G}$.

The security of our scheme relies on the hardness of the following problems.

Definition 1. Computational Diffie–Hellman (CDH) Problem is that given three elements $g, g^a, g^b \in \mathbb{G}$ for unknown randomly chosen $a, b \in \mathbb{Z}_p$, compute g^{ab}.

Let $\mathcal{A}$ be an algorithm, and we say that $\mathcal{A}$ has advantage ϵ in solving the CDH problem on $\mathbb{G}$ if

$$\Pr\left[\mathcal{A}\left(g, g^a g^b\right) = g^{ab}\right] \geq \epsilon.$$

We say that the CDH assumption holds on $\mathbb{G}$ if there is no random algorithm $\mathcal{A}$ that can solve the CDH problem with a non-negligible advantage ϵ.

Definition 2. Square Computational Diffie–Hellman (Squ-CDH) Problem [16] is that given two elements $g, g^a \in \mathbb{G}$ for unknown randomly chosen $a \in \mathbb{Z}_p$, compute g^{a^2}.

Let $\mathcal{A}$ be an algorithm, and we say that $\mathcal{A}$ has advantage ϵ in solving the Squ-CDH problem on $\mathbb{G}$ if

$$\Pr\left[\mathcal{A}\left(g, g^a\right) = g^{a^2}\right] \geq \epsilon.$$

We say that the Squ-CDH assumption holds on $\mathbb{G}$ if there is no random algorithm $\mathcal{A}$ that can solve the Squ-CDH problem with a non-negligible advantage ϵ.

It is easy to prove that the Squ-CDH assumption is equivalent to the CDH assumption.

3. Review of Yu et al.'s certificateless signature scheme and its security weaknesses

In this section, we first review Yu et al.'s certificateless signature scheme [14]. Then we show that the scheme is insecure by giving two concrete attacks.

3.1. Review of Yu et al.'s scheme

Yu et al.'s CL-S [14] is composed of five phases as follows.

Setup. The KGC chooses two cyclic groups $\mathbb{G}$ and $\mathbb{G}_T$ of prime order p, a random generator g of $\mathbb{G}$ and a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$. It also randomly chooses $s \in \mathbb{Z}_p^*$, $g_2 \in \mathbb{G}$ and sets $g_1 = g^s$. Furthermore, it chooses four random elements $u', m_0, m_1, v \in \mathbb{G}$, and a random vector $\boldsymbol{U} = (u_i) \in \mathbb{G}^n$. $H_0 : \{0,1\}^* \to \{0,1\}^n$ and $H : \{0,1\}^* \times \mathbb{G}^2 \to \mathbb{Z}_p$ are two collision-resistant hash functions. Let Q be a point in $\mathbb{G}$. Define a function $f(Q)$ as follows. If the x-coordinate of Q is odd, then $f(Q) = 1$; else, $f(Q) = 0$. The public parameters are $params = \{\mathbb{G}, \mathbb{G}_T, e, g, g_1, g_2, u', m_0, m_1, v, \boldsymbol{U}, H_0, H, f\}$ and the master secret key is $msk = g_2^s$.

Partial-secret-key-extract. Given an identity ID, KGC first computes $H_0(\mathrm{ID})$. Let $\mathfrak{u}[i]$ denote the i-th bit of $\mathfrak{u} = H_0(\mathrm{ID})$ and $\mathcal{U}_{\mathrm{ID}} = \{i \mid \mathfrak{u}[i] = 1, 1 \leq i \leq n\}$. The KGC randomly selects $r \in \mathbb{Z}_p$, computes $psk_{\mathrm{ID}} = (g_2^s \cdot (u' \prod_{i \in \mathcal{U}_{\mathrm{ID}}} u_i)^r, g^r) = (psk_{\mathrm{ID},1}, psk_{\mathrm{ID},2})$ as the partial secret key of the user with identity ID.

User-key-generation. User with identity ID selects a secret value $x \in \mathbb{Z}_p$ as his secret key usk_{ID}, and computes his public key as $upk_{\mathrm{ID}} = (e(g, g_1)^x, g_1^x) = (upk_{\mathrm{ID},1}, upk_{\mathrm{ID},2})$.