Information Sciences 286 (2014) 29–34

Contents lists available at ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

Security analysis of an identity-based strongly unforgeable signature scheme

Kwangsu Lee, Dong Hoon Lee *

Korea University, Anam-dong, Seungbuk-gu, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 21 April 2014
Received in revised form 2 July 2014
Accepted 19 July 2014
Available online 29 July 2014

Keywords:
Cryptography
Identity-based signature
Strongly unforgeability
Security analysis
Bilinear map

ABSTRACT

Identity-based signature (IBS) is a specific type of public-key signature (PKS) where any identity string *ID* can be used for the public key of a user. Although an IBS scheme can be constructed from any PKS scheme by using the certificate paradigm, it is still important to construct an efficient IBS scheme with short signature under the standard assumption without relying on random oracles. Recently, Kwon proposed an IBS scheme and claimed its strong unforgeability under the computational Diffie–Hellman (CDH) assumption. In this paper, we show that the security proof of Kwon is seriously flawed. To show the flaws, we first show that there exists a distinguisher that can distinguish the distribution of simulated signatures from that of real signatures. Next, we also show that the simulator of Kwon's security argument cannot extract the solution of the CDH problem even if there exists an adversary that forges the signature. Therefore, the security of the Kwon's IBS scheme is not related to the hardness of the CDH assumption.

1. Introduction

Identity-based signature (IBS) is a specific type of public-key signature (PKS) such that an identity string *ID* can be used for the public key of a user. The concept of IBS and the first IBS scheme were proposed by Shamir [8]. The main advantage of IBS is that the certificate management problem of PKS can be solved by replacing a public key with an identity string. Although an identity-based encryption (IBE) scheme requires a strong primitive like bilinear maps, an IBS scheme can be easily derived from any PKS scheme by using the certificate paradigm [1,4]. However, the signature size of this general IBS scheme derived from a PKS scheme is long since the signature should contain a public key and a certificate on the public key and an identity string. Gentry and Silverberg [5] showed that an IBS scheme (with short signature) can be derived from a two-level hierarchical IBE scheme. Although many IBS schemes were proposed without random oracles [7,3], it is still important work to construct an efficient IBS scheme with short signature that is secure under the standard assumption without random oracles.

Recently, Kwon [6] proposed an IBS scheme that is strongly unforgeable under the computational Diffie–Hellman (CDH) assumption without random oracles. The IBS scheme of Kwon is a hierarchical combination of the PKS scheme of Waters [11] and the weakly secure (modified) PKS scheme of Boneh and Boyen [2]. Kwon also devised a new mechanism to provide the

* Corresponding author.
E-mail addresses: guspin@korea.ac.kr (K. Lee), donghlee@korea.ac.kr (D.H. Lee).

http://dx.doi.org/10.1016/j.ins.2014.07.022
0020-0255/

strong unforgeability. Compared with previous IBS schemes that are secure under the CDH assumption without random oracles [7,3], the IBS scheme of Kwon has shorter public parameters and provides the strong unforgeability.

In this paper, we show that the security argument of Kwon is flawed. In a correct security argument, the distribution of simulated private keys and simulated signatures should be indistinguishable from that of original one, and a simulator could extract the solution of the CDH problem from the forged signature of an adversary. We first show that there exists an algorithm that can distinguish whether signatures are generated from the real signing algorithm or not with high probability if the algorithm requests a polynomial number of signature queries. Next, we show that the simulator of Kwon cannot extract the solution of the CDH problem even if there exists an adversary that outputs a forged signature. Therefore, the security argument of Kwon is not valid since the distribution of simulated game is distinguishable and the security argument is not related with the hardness of the CDH assumption.

The paper is organized as follows: We first review the IBS scheme of Kwon and its security argument in Section 2. After that, we present our security analysis in Section 3.

2. The review of Kwon's identity-based signature

In this section, we review the IBS scheme of Kwon and its security proof under the CDH assumption.

2.1. Bilinear groups and complexity assumption

Let $\mathbb{G}$ and $\mathbb{G}_T$ be two multiplicative cyclic groups of same prime order p and g be a generator of $\mathbb{G}$. The bilinear map $e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$ has the following properties:

1. *Bilinearity:* $\forall u,\ v\in\mathbb{G}$ and $\forall a,\ b\in\mathbb{Z}_p$, $e(u^a,v^b)=e(u,v)^{ab}$.
2. *Non-degeneracy:* $\exists g$ such that $e(g,g)$ has order p, that is, $e(g,g)$ is a generator of $\mathbb{G}_T$.

We say that $\mathbb{G}$ is a bilinear group if the group operations in $\mathbb{G}$ and $\mathbb{G}_T$ as well as the bilinear map e are all efficiently computable. Furthermore, we assume that the description of $\mathbb{G}$ and $\mathbb{G}_T$ includes generators of $\mathbb{G}$ and $\mathbb{G}_T$ respectively.

Assumption 2.1 (*Computational Diffie–Hellman, CDH*). Let $(p,\mathbb{G},\mathbb{G}_T,e)$ be a description of the bilinear group of prime order p. Let g be generators of subgroups $\mathbb{G}$. The CHD assumption is that if the challenge tuple $D=((p,\mathbb{G},\mathbb{G}_T,e),\ g,g^a,g^b)$ is given, no PPT algorithm $\mathcal{A}$ can output $g^{ab}\in\mathbb{G}$ with more than a negligible advantage. The advantage of $\mathcal{A}$ is defined as $\boldsymbol{Adv}_{\mathcal{A}}^{CDH}(\lambda)=\Pr[\mathcal{A}(D)=g^{ab}]$ where the probability is taken over random choices of $a,b\in\mathbb{Z}_p$.

2.2. The original IBS scheme

The IBS scheme consists of **Setup**, **GenKey**, **Sign**, and **Verify** algorithms. The IBS scheme of Kwon [6] has the same private key structure with that of Waters [11] and it uses the modified structure of Boneh and Boyen [2] for signature generation.

Let $\chi(d)$ be a mapping from an element $d\in\mathbb{G}$ to $\gamma\in\{0,1\}$ where γ is the rightmost bit of x coordinate of d. Let $H:\{0,1\}^*\times\mathbb{G}\times\mathbb{G}\to\mathbb{Z}_p$ be a collision-resistant hash function. The IBS scheme is described as follows:

Setup(1^λ): This algorithm takes as input a security parameter 1^λ. It generates bilinear groups $\mathbb{G},\ \mathbb{G}_T$ of prime order p. Let g be the generator of $\mathbb{G}$. It chooses random elements $g_2,\ u_0,\ u_1,\ \ldots,\ u_n,\ v_0,\ v_1,\ w\in\mathbb{G}$ and a random exponent $\alpha\in\mathbb{Z}_p$ where $n=2\lambda$. It outputs a master key $MK=g_2^\alpha$ and public parameters $PP=((p,\mathbb{G},\mathbb{G}_T,e),g,g_1=g^\alpha,g_2,u_0,u_1,\ldots,u_n,v_0,v_1,w)$.

GenKey(ID,MK,PP): This algorithm takes as input an identity string $ID=(I_1,\ldots,I_n)\in\{0,1\}^n$ where I_i is a bit string of ID at ith position, the master key MK, and the public parameters PP. It selects a random exponent $r\in\mathbb{Z}_p^*$ and outputs a private key $SK_{ID}=\left(K_1=g_2^\alpha\left(u_0\prod_{i=1}^n u_i^{I_i}\right)^r,K_2=g^r\right)$.

Sign(M,SK_{ID},PP): Let $SK_{ID}=(K_1,K_2)$. It obtains γ by computing $\chi(K_2)$. Next, it selects a random exponent $s\in\mathbb{Z}_p^*$ and computes $h=H(M\|ID,K_2,g^s)$. It outputs a signature $\sigma=\left(S_1=K_1\cdot\left(v_\gamma w^h\right)^s,S_2=K_2,S_3=g^s\right)$.

Verify(σ,ID,M,PP): Let $\sigma=(S_1,S_2,S_3)$. It obtains γ by computing $\chi(S_2)$. It computes $h=H(M\|ID,S_2,S_3)$ and verifies that $e(S_1,g)\stackrel{?}{=}e(g_2,g_1)\cdot e\left(S_2,u_0\prod_{i=1}^n u_i^{I_i}\right)\cdot e(S_3,v_\gamma w^h)$. If this equation holds, then it outputs 1. Otherwise, it outputs 0.

2.3. The security proof

In this subsection, we briefly review the simulator in the security proof of Kwon [6] that solves the CDH problem by using an adversary.

Suppose there exists an adversary $\mathcal{A}$ that requests q_k number of private key queries and outputs a forged signature for the above IBS scheme with a non-negligible advantage. A simulator $\mathcal{B}$ that solves the CDH problem using $\mathcal{A}$ is given: a challenge tuple $D=((p,\mathbb{G},\mathbb{G}_T,e),g,g^a,g^b)$. Then $\mathcal{B}$ that interacts with $\mathcal{A}$ is described as follows: