Security Analysis of an Identity-Based Strongly Unforgeable Signature Scheme

Kwangsu Lee* Dong Hoon Lee†

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 signature from that of real signatures. Next, we also show that the simulator of Kwon's security argument cannot extract the solution of the CDH assumption 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.

Keywords: Identity-based signature, Strongly unforgeability, Security analysis, Bilinear maps.

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 problem of certificate management problem in 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 [3, 7], 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 strong unforgeability. Compared with

*Korea University, Korea. Email: guspin@korea.ac.kr.
†Korea University, Korea. Email: donghlee@korea.ac.kr.

IBS schemes that are secure under the CDH assumption without random oracles [3, 7], 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 assumption from the forged signature of an adversary. We first show that there exists an algorithm than 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 assumption 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 $D = \left((p, \mathbb{G}, \mathbb{G}_T, e), g, g^a, g^b\right)$ 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 $PP = \big((p, \mathbb{G}, \mathbb{G}_T, e),\ g,\ g_1 = g^\alpha,\ g_2,\ u_0, u_1, \ldots, u_n,\ v_0, v_1, w\big)$.

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 $SK_{ID} = \big(K_1 = g_2^\alpha \big(u_0 \prod_{i=1}^n u_i^{I_i}\big)^r,\ K_2 = g^r\big)$.

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 $\sigma = \big(S_1 = K_1 \cdot \big(v_\gamma w^h\big)^s,\ S_2 = K_2,\ S_3 = g^s\big)$.

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 $e(S_1, g) \stackrel{?}{=} e(g_2, g_1) \cdot e(S_2, u_0 \prod_{i=1}^n u_i^{I_i}) \cdot e(S_3, v_\gamma w^h)$. 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 assumption 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 assumption 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:

Setup: Let $m = 2q_k$. $\mathcal{B}$ first picks $k \in \{1, \ldots, n\}$. It chooses random values $x_0, x_1, \ldots, x_n \in \{0, \ldots, m-1\}$ and random exponents $u_0', u_1', \ldots, u_n', v_0', v_1', h^*, w' \in \mathbb{Z}_p$. It implicitly sets $\alpha = a$ and publishes the public parameters PP as

$$g,\ g_1 = g^a,\ g_2 = g^b,\ u_0 = (g^b)^{-mk+x_0} g^{u_0'},\ u_i = (g^b)^{x_i} g^{u_i'}\ \forall i \in \{1, \ldots, n\},$$
$$v_0 = g^{v_0'},\ v_1 = g_2^{h^*} g^{v_1'},\ w = g^{w'}.$$

We define $F(ID) = -mk + x_0 + \sum_{i=1}^n x_i I_i$ and $J(ID) = u_0' + \sum_{i=1}^n u_i' I_i$.

Private-Key Query: $\mathcal{B}$ handles a private key query for an identity ID as follows: If $F(ID) \equiv 0 \mod p$, then it aborts the simulation since it cannot create a private key. If $F(ID) \not\equiv 0 \mod p$, then it selects random exponents $r' \in \mathbb{Z}_p$ and creates a private key by implicitly setting $r = -a/F(ID) + r'$ as

$$K_1 = \big(g^a\big)^{-J(ID)/F(ID)} \big(u_0 \prod_{i=1}^n u_i^{I_i}\big)^{r'},\ K_2 = \big(g^a\big)^{-1/F(ID)} g^{r'}.$$

Note that the probability of $F(ID) \equiv 0 \mod p$ is $\frac{1}{m} = \frac{1}{2q_k}$ from the analysis of Waters [11].

Signature Query: $\mathcal{B}$ handles a signature query on a message M for an identity ID as follows:

- **Case** $F(ID) \not\equiv 0 \mod p$: It first generates a private key for ID as the same as the private key simulation and creates a signature on M for ID by running the normal signing algorithm since it has a private key. In this case, we have that $\Pr[\chi(S_2) = 0] = \frac{1}{2}$ and $\Pr[\chi(S_2) = 1] = \frac{1}{2}$ since the exponent r' is randomly selected.

- **Case** $F(ID) \equiv 0 \mod p$: It first selects random exponents $r, s' \in \mathbb{Z}_p$ such that $\chi(g^r) = 1$. It computes $h = H(M \| ID, g^r, (g^a)^{-1/h^*} g^{s'})$ and creates a signature by implicitly setting $s = -a/h^* + s'$ as

$$S_1 = \left(u_0 \prod_{i=1}^{n} u_i^{I_i}\right)^r \left(g^a\right)^{-(v_1' h + w')/h^*} (v_1 w^h)^{s'},\ S_2 = g^r,\ S_3 = \left(g^a\right)^{-1/h^*} g^{s'}.$$

  In this case, a signature with $\chi(S_2) = 0$ is not generated since the exponent r with $\chi(g^r) = 1$ is always selected.

Note that we re-organized the description of the signature generation of Kwon to simplify the simulation of signatures. We should note that a signature with $F(ID) \equiv 0 \mod p$ and $\chi(S_2) = 0$ cannot be generated by the simulator of Kwon.

Output: $\mathcal{A}$ finally outputs a forged signature $\sigma^* = (S_1^*, S_2^*, S_3^*)$ on a message M^* for an identity $ID^* = (I_1^*, \ldots, I_n^*)$. If $F(ID^*) \equiv 0 \mod p$ and $\chi(S_2^*) = 0$, then $\mathcal{B}$ computes $h = H(M^* \| ID^*, S_2^*, S_3^*)$ and outputs the CDH value by calculating

$$g^{ab} = S_1^* \cdot (S_2^*)^{-J(ID^*)} \cdot (S_3^*)^{-(v_0' h + w')}.$$

Otherwise, $\mathcal{B}$ fails to extract the CDH value and stops.

2.4 A Modified IBS Scheme

The simulator $\mathcal{B}$ in the security proof of Kwon creates a signature by selecting a random S_2. However, the signature algorithm of the Kwon's IBS scheme just creates a signature by using the element K_2 of a private key for the element S_2 of the signature without randomization. To remove this difference, the signature algorithm of the IBS scheme should be modified to create a signature after randomizing a private key. If the signature algorithm does not randomize the private key, then the security proof goes wrong since an adversary can easily distinguish two games by examining the distribution of the signature element S_2. The modified signature algorithm is described as follows:

Sign(M, SK_{ID}, PP)**:** Let $SK_{ID} = (K_1, K_2)$. It first re-randomizes the private key components as $K_1' = K_1 \cdot (u_0 \prod u_i^{I_i})^{r'}, K_2' = K_2 \cdot g^{r'}$ by selecting $r' \in \mathbb{Z}_p$. 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 $\sigma = \left(S_1 = K_1' \cdot \left(v_\gamma w^h\right)^s,\ S_2 = K_2',\ S_3 = g^s\right)$.

3 Our Security Analysis

In this section, we first review the overall structure of a general security proof by using hybrid games, and then we present two lemmas that claim there are serious flaws in the security proof of Kwon [6] by showing two algorithms that attack the security proof.

3.1 Overview of Hybrid Games

To proving the security of a cryptographic scheme is relatively complex. A security proof that uses hybrid games can reduce the complexity of the security proof by presenting the proof as a sequence of games [9]. We briefly overview the structure of a valid security proof for IBS. Security for IBS is defined as an attack game between a challenger and an adversary (or a forger). Note that the formal security game of the strongly unforgeability under chosen-message attacks for IBS is defined in [6]. The security proof of IBS that uses hybrid games consists of the following games.

Game $\mathbf{G}_0$. This game is the original security game. That is, a challenger generates a master key and public parameter by itself, and handles the private key and signature queries of an adversary by running the normal algorithms with the master key. Let S_0 be the event that the adversary wins the game.

Game $\mathbf{G}_1$. In this game, a challenger (or a simulator) is given a challenge tuple of a complexity assumption and handles the private key and signature queries of an adversary by simulating private keys and signatures without knowing the master key. Finally the simulator extracts a solution of the complexity assumption from the forged signature of the adversary. Let S_1 be the event that the adversary wins the game.

To argue the security of an IBS scheme, we should show that $\Pr[S_0]$ that is the probability of S_0 in the real game $\mathbf{G}_0$ is negligible. This can be achieved if we can show the security proof satisfies the following two conditions: 1) There is no polynomial-time algorithm than can distinguish the real game $\mathbf{G}_0$ and the simulated game $\mathbf{G}_1$ with non-negligible probability; 2) In the simulated game $\mathbf{G}_1$, if there is an adversary that forges a signature, then a simulator can extract a solution for the assumption from the forged signature with non-negligible probability. If a security argument satisfies two conditions, then we have $\Pr[S_0] - \Pr[S_1] \leq neg_1$ from the first condition and $\Pr[S_1] \leq neg_2$ from the second condition since the probability of solving the assumption is negligible where neg_1 and neg_2 are negligible values in a security parameter. Therefore, we obtain $\Pr[S_0] \leq neg_1 + neg_2$.

3.2 Attacking Algorithms

By presenting two lemmas, we show that the security argument of Kwon [6] does not satisfy the two conditions of hybrid games that were mentioned before. At first, we show that there is a probabilistic polynomial-time (PPT) algorithm that can distinguish the real game $\mathbf{G}_0$ from the simulated game $\mathbf{G}_1$ with non-negligible probability.

Lemma 3.1. *There exists a PPT algorithm $\mathcal{D}$ that can distinguish whether it interacts with the real game $\mathbf{G}_0$ or the simulated game $\mathbf{G}_1$ of Kwon with probability $1-\delta$ if $\mathcal{D}$ makes at most $O(\log(\delta^{-1})q_k^2)$ number of signature queries.*

Proof. The basic idea is that if an adversary request a signature $\sigma = (S_1, S_2, S_3)$ on a message M for an identity ID, then there is a difference between the distribution of $\chi(S_2) = 0$ and $\chi(S_2) = 1$ since the simulator of Kwon [6] cannot create a signature with $\chi(S_2) = 0$ if $F(ID) \equiv 0 \mod p$. Although this difference is small, the adversary can distinguish this difference by requesting a polynomial number of signature queries since the difference probability of two distribution is non-negligible. Let L be an integer value that is determined later. A distinguishing algorithm $\mathcal{D}$ is described as follows:

1. It sets $c = 0$.
2. For $i = 1$ to L, $\mathcal{D}$ performs the following steps:
   (a) It selects a random identity ID_i and a random message M_i.
   (b) It requests a signature on M_i for ID_i and receives a signature $\sigma_i = (S_{i,1}, S_{i,2}, S_{i,3})$.
   (c) If $\chi(S_{i,2}) = 1$, then it increases c by one.
3. If $\frac{c}{L} \leq \frac{1}{2} + \frac{1}{8q_k}$, then $\mathcal{D}$ outputs 0. Otherwise, it outputs 1.

Note that the above algorithm $\mathcal{D}$ is a valid adversary since it only requests a polynomial number of signature queries.

We now analyze the success probability of $\mathcal{D}$. If $\mathcal{D}$ interacts with the real game $\mathbf{G}_0$, then $\Pr[\chi(S_{i,2}) = 0] = \frac{1}{2}$ and $\Pr[\chi(S_{i,2}) = 1] = \frac{1}{2}$ since the signing algorithm uses a re-randomized private key to create a signature in the real game. However, if $\mathcal{D}$ interacts with the simulated game $\mathbf{G}_1$ of Kwon, then $\Pr[\chi(S_{i,2}) = 0] = \frac{1}{2} \cdot \left(1 - \frac{1}{2q_k}\right)$ and $\Pr[\chi(S_{i,2}) = 1] = \frac{1}{2} \cdot \left(1 + \frac{1}{2q_k}\right)$ since the simulator of Kwon cannot create a signature with $\chi(S_{i,2}) = 0$ and $F(ID) \equiv 0 \mod p$. The reason is that the probability of $F(ID) \equiv 0 \mod p$ in the simulated game $\mathbf{G}_1$ is $\frac{1}{2q_k}$ for a random identity ID.

Let X_i be a random variable such that $X_i = 1$ if $\chi(S_{i,2}) = 1$ and $X_i = 0$ if $\chi(S_{i,2}) = 0$ for ith signature $\sigma_i = (S_{i,1}, S_{i,2}, S_{i,3})$. We know that $\{X_i\}$ are mutually independent since a signature is generated for a random identity ID_i and a random message M_i. From the above analysis, we have that there is a difference between two games such as $\Pr[X_i = 1] = \frac{1}{2}$ in the game $\mathbf{G}_0$ and $\Pr[X_i = 1] = \frac{1}{2} + \frac{1}{4q_k}$ in the simulated game $\mathbf{G}_1$. To distinguish two games, $\mathcal{D}$ estimates the probability of $X_i = 1$ by sampling L signatures and guess that it is the real game $\mathbf{G}_0$ if the estimated value is less than the middle value $\frac{1}{2} + \frac{1}{8q_k}$. However, this guess cannot be always correct since there could be an error. To increase the confidence of this guessing, we can calculate the minimum number of signature samples by using the Chernoff bound [10]. Let δ be an error of guessing. From the Chernoff bound, we have $\delta = e^{-L(1/8q_k)^2/2}$. Thus we have $L = O(\log(\delta^{-1}) \cdot q_k^2)$.

Therefore, $\mathcal{D}$ can correctly guess the game with $1 - \delta$ probability if it makes at most $O(\log(\delta^{-1}) \cdot q_k^2)$ number of signature queries. For instance, if $\delta = \frac{1}{4}$, then it can guess the game with probability $\frac{3}{4}$ just making $O(q_k^2)$ number of signature queries. This completes our proof. □

Next, we show that if there is an adversary algorithm for the IBS scheme of Kwon, then there exists another algorithm such that the simulator of Kwon cannot extract the CDH value from the forged signature.

Lemma 3.2. *If there is a PPT algorithm $\mathcal{A}$ that can forge the IBS scheme of Kwon with probability ε, then there is another PPT algorithm $\mathcal{F}$ can forge a signature with almost the same probability ε, but the simulator of Kwon in the simulated game $\mathbf{G}_1$ cannot extract the CDH value from the forged signature of $\mathcal{F}$.*

Proof. The basic idea is that an adversary easily can check the condition of the simulator that leads to extract the CDH value. Let $\mathcal{A}$ be an adversary for the IBE scheme of Kwon with ε probability. Let λ be the security parameter of the IBS scheme. A modified adversary $\mathcal{F}$ that uses $\mathcal{A}$ is described as follows:

1. $\mathcal{F}$ is first given PP, and it runs $\mathcal{A}$ by giving PP. $\mathcal{F}$ handles the query of $\mathcal{A}$ as follows: If this a private key query for ID, then it uses its own oracle to response the query. If this is a signature query for ID and M, then it uses its own oracle to response the query.

2. $\mathcal{A}$ finally outputs a forged signature $\sigma^* = (S_1^*, S_2^*, S_3^*)$ on a message M^* for an identity ID^*.

3. $\mathcal{F}$ additionally requests signatures on random messages $M_1, \ldots, M_\lambda$ for the identity ID^*, and then it receives signatures $\sigma_1, \ldots, \sigma_\lambda$ where λ is a security parameter.

4. If there is at least one signature $\sigma_i = (S_{i,1}, S_{i,2}, S_{i,3})$ such that $\chi(S_{i,2}) = 0$, then $\mathcal{F}$ outputs the forged signature $\sigma^* = (S_1^*, S_2^*, S_3^*)$ of $\mathcal{A}$ on the message M^* for the identity ID^*. Otherwise, it just stops without outputting the signature.

Note that $\mathcal{F}$ is a valid adversary since the additional signature queries for the identity ID^* are allowed in the security model of IBS.

We first analyze the success probability of $\mathcal{F}$. Suppose that $\mathcal{A}$ can forge a signature for the identity ID^* with ε probability. In the game $\mathbf{G}_0$, $\mathcal{F}$ can forge a signature with probability $(1-\frac{1}{2^\lambda})\cdot\varepsilon$ since the probability of at least one signature has $\chi(S_2)=0$ is $1-\frac{1}{2^\lambda}$. In the simulated game $\mathbf{G}_1$ of Kwon, we consider two cases. If $F(ID^*)\not\equiv 0 \mod p$, then $\mathcal{F}$ outputs a forged signature with $(1-\frac{1}{2^\lambda})\cdot\varepsilon$ probability since the simulator $\mathcal{B}$ of Kwon can create a signature regardless of $\chi(S_2)$. If $F(ID^*)\equiv 0 \mod p$, then $\mathcal{F}$ does not output a forged signature since $\mathcal{B}$ cannot create a signature with $\chi(S_2)=0$. Thus, $\mathcal{F}$ outputs a forged signature with at least the probability of $(1-\frac{1}{2q_k})\cdot(1-\frac{1}{2^\lambda})\cdot\varepsilon$ in the game $\mathbf{G}_1$ since $\Pr[F(ID^*)\equiv 0]=\frac{1}{2q_k}$.

We finally show that $\mathcal{B}$ cannot extract a CDH value from σ^* of $\mathcal{F}$. From the description of $\mathcal{B}$, we know that $\mathcal{B}$ can extract a CDH value if $F(ID^*)\equiv 0 \mod p$ and $\chi(S_2^*)=0$ are satisfied. However, $\mathcal{B}$ never outputs σ^* with $F(ID^*)\equiv 0 \mod p$ since it can check this condition by requesting additional signature queries. This completes our proof. □

3.3 Discussions

From the above two lemmas, we showed that a PPT algorithm can distinguish two games and the security in $\mathbf{G}_1$ is not related with the hardness of the CDH assumption. Thus the security in $\mathbf{G}_0$ that directly corresponds to the security of the IBS scheme of Kwon is not related with the hardness of the CDH assumption. The main reason of the errors that falsify the argument of Kwon is that an adversary can easily obtain the information $F(ID)$ that is set by a simulator if it interacts with a simulated game by requesting additional signature queries. To hide the information $F(ID)$ from the adversary, we may use the PKS scheme of Waters [11] for message signing instead of using the weak modified PKS scheme of Boneh and Boyen [2], but this IBS scheme without strong unforgeability is similar to previous IBS schemes in [3, 7].

4 Conclusion

In this paper, we analyzed the security argument of the Kwon's IBS scheme. Although we didn't present a forgery attack, we showed that the security argument of Kwon is seriously flawed. The flaws of Kwon are that the distribution of signatures in the simulated game is easily distinguished from that of the real game, and the simulator of Kwon cannot extract the solution of the CDH assumption from the forged signature of an adversary. Therefore, the security of the Kwon's IBS scheme is not related with the hardness of the CDH assumption.

References

[1] Mihir Bellare, Chanathip Namprempre, and Gregory Neven. Security proofs for identity-based identification and signature schemes. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 268–286. Springer, 2004.

[2] Dan Boneh and Xavier Boyen. Efficient selective-id secure identity-based encryption without random oracles. In Christian Cachin and Jan Camenisch, editors, *EUROCRYPT 2004*, volume 3027 of *Lecture Notes in Computer Science*, pages 223–238. Springer, 2004.

[3] Sanjit Chatterjee and Palash Sarkar. Hibe with short public parameters without random oracle. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 145–160. Springer, 2006.

[4] David Galindo, Javier Herranz, and Eike Kiltz. On the generic construction of identity-based signatures with additional properties. In Xuejia Lai and Kefei Chen, editors, *ASIACRYPT 2006*, volume 4284 of *Lecture Notes in Computer Science*, pages 178–193. Springer, 2006.

[5] Craig Gentry and Alice Silverberg. Hierarchical id-based cryptography. In Yuliang Zheng, editor, *ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 548–566. Springer, 2002.

[6] Saeran Kwon. An identity-based strongly unforgeable signature without random oracles from bilinear pairings. *Inf. Sci.*, 2014. `http://dx.doi.org/10.1016/j.ins.2014.02.041`.

[7] Kenneth G. Paterson and Jacob C. N. Schuldt. Efficient identity-based signatures secure in the standard model. In Lynn Margaret Batten and Reihaneh Safavi-Naini, editors, *ACISP 2006*, volume 4058 of *Lecture Notes in Computer Science*, pages 207–222. Springer, 2006.

[8] Adi Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and David Chaum, editors, *CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.

[9] Victor Shoup. Sequences of games: A tool for taming complexity in security proofs. Cryptology ePrint Archive, Report 2004/332, 2004. `http://eprint.iacr.org/2004/332`.

[10] Victor Shoup. *A Computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2009.

[11] Brent Waters. Efficient identity-based encryption without random oracles. In Ronald Cramer, editor, *EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 114–127. Springer, 2005.