JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 27, 969-982 (2011)

Truly Non-Repudiation Certificateless Short Signature Scheme from Bilinear Pairings*

CHUN-I FAN, RUEI-HAU HSU AND PEI-HSIU HO
Department of Computer Science and Engineering
National Sun Yat-sen University
Kaohsiung, 804 Taiwan

Certificateless signature scheme is a practical solution to confront the drawback, Key Generation Center (KGC) being able to forge the signature of a user, of an identity based (ID-based) signature scheme. Lots of previous research results have shown the security models and the generic constructions for certificateless signatures. However, most of them did not satisfy Girault's level-3 security which the conventional public key infrastructure (PKI) can achieve. Until 2007, Hu *et al*. introduced a generic construction and security model that can fulfill the requirement of Girault's level-3 security. Recently, Du and Wen proposed a certificateless short signature scheme which is more computation efficient than the previous ones. But a flaw in security proofs and lack of Girault's level-3 security can be still found in their scheme. In this paper, a cryptanalysis on Du-Wen scheme and an improved scheme will be presented, and we also provide formal proofs to demonstrate the security of the proposed scheme.

Keywords: certificateless signature, ID-based cryptosystems, Girault's security, random oracles, non-repudiation

1. INTRODUCTION

1.1 Backgrounds

A conventional public key infrastructure (PKI) requires heavy management and communication cost to achieve authenticity of the public keys of users. Identity based (ID-based) cryptography was proposed by Shamir [17] to conquer the problem of public key certification. Each user is allowed to take her/his public identity information as her/his public key without being certified by any authority or trusted third party. To validate the public key and the corresponding private key of a user, the private key is issued by a Key Generation Center (KGC) to obtain the authorization. However, it has a serious drawback, *i.e*., KGC can also have the same ability as the user to perform public-key cryptographic operations, such as decryption and signing, by yielding the same key pair via the identity of the user and its master key. Consequently, confidentiality and non-repudiation cannot be satisfied in such ID-based public-key cryptosystems.

To solve the shortcoming of ID-based cryptosystems, a certificateless cryptosystem, which combines the advantages of PKI and ID-based cryptosystems, was proposed by

Received October 1, 2009; revised January 26, 2010; accepted May 19, 2010.
Communicated by Chin-Laung Lei.
* A partial result of this research was presented at the 4th Joint Workshop on Information Security (JWIS), Kaohsiung, Taiwan, August 6-7, 2009, which was sponsored by Japan Information and Communication System Security of the Institute of Electronics, Japan Information and Communication Engineers, Korea Institute for Information Security and Cryptology, Chinese Cryptology and Information Security Association, and Taiwan Information Security Center. This work was supported in part by the National Science Council of Taiwan, R.O.C. under grants No. NSC 98-2219-E-110-001 and NSC 96-2221-E-110-071-MY3.

Al-Riyami and Paterson [1]. In the key issuing phase of a certificateless signature scheme, both the secret of a user and the master key of KGC are required for the generation of the public key and private key of the user. It prevents KGC from producing the user's private key for signing or decrypting messages. Subsequently, several certificateless signature (CLS) schemes [6, 10, 13, 15, 19, 22] were proposed where [10, 15, 19] just provided informal security analyses and [6, 13, 22] proved the security of their schemes via a formal manner. Later, key replacement attacks [2, 5, 21] were proposed against the schemes [10, 15, 19]. In the development of CLS, some generic constructions [2, 11, 13] for CLS were introduced to provide versatile abilities, *e.g*., employing different kinds of signature schemes in the construction of CLS schemes. From the above studies, some proposed schemes [10, 15, 19] were demonstrated as being insecure under key replacement attacks and [1, 13, 15] were vulnerable to malicious-but-passive-KGC attacks [2]. Thus, [2, 14] presented two provably secure CLS schemes under the presence of some specified adversaries [12].

However, the security model of [2, 14] cannot reach the same security level as that of PKI-based signature schemes. The conventional PKI can meet Girault's level-3 security [8], that is, KGC or trusted third party (TTP) cannot find out all secret information of a user nor generate a contradictory public key, which is another public key indistinguishable from the real public key of the user. Therefore, Hu *et al*. [12] proposed an improved generic model to construct a CLS scheme to achieve Girault's level-3 security. After that, Tso *et al*. [18], and Du and Wen [7] proposed certificateless short signature schemes with provable security. Nevertheless, a user in Tso *et al*.'s scheme and Du-Wen scheme can change its public key without being certified again by KGC. Also, there is a flaw in the simulation of the security proofs in Du-Wen scheme. In this paper, we will show how a user can replace his public key without the help of KGC against Girault's level-3 security in Du-Wen scheme and point out a flaw in the security proofs. Finally, we propose a certificateless short signature scheme based on Boneh-Boyen short signature scheme [4] and prove that our scheme can achieve Girault's level-3 security.

The rest of this paper is organized as follows. In section 2, we introduce the security model of certificateless signature schemes. In section 3, we show a flaw in the simulation of the security proofs and how to perform the public-key replacement attack in Du-Wen scheme. In section 4, we briefly review Boneh-Boyen short signature scheme which is an underlying foundation of the proposed scheme. We then propose a provably secure certificateless short signature scheme with Girault's level-3 security and compare our scheme with others. Finally, a concluding remark is given in section 5.

2. SECURITY MODEL

In this section, we introduce a definition of certificateless signatures, and then define three types of adversaries and simulation games along with the oracles which will be queried in the games to demonstrate the security of certificateless signatures.

2.1 Generic Construction of Certificateless Signature Scheme

A certificateless signature scheme consists of five polynomial-time algorithms, **Master-Key-Gen**, **User-Key-Gen**, **Partial-Private-Key-Gen**, **CL-Sign**, and **CL-Verify**.

- **Master-Key-Gen:** On inputting k being a security parameter, it produces a master public-secret key pair (mpk, msk).
- **User-Key-Gen:** On inputting mpk and a user's identity ID, it produces the user's public key and secret key (upk, usk).
- **Partial-Private-Key-Gen:** On inputting upk, msk, and a user's identity ID, it produces the user's partial private key $partial\_key$, which is a part of the user's private key.
- **CL-Sign:** On inputting a user's private key, which consists of the user's secret key usk and partial private key $partial\_key$, and message $m \in \{0, 1\}^*$, it outputs a signature σ.
- **CL-Verify:** On inputting mpk, upk, message m, and signature σ, it returns *true* if the signature passes the verification. Otherwise, it returns *false*.

2.2 Types of Adversaries

To achieve Girault's level-3 security, in a certificateless signature scheme, we define three types of adversaries to simulate various kinds of attacks and the games for corresponding adversaries to capture the notion of existential unforgeability against chosen message attacks [9]. There are three types of adversaries, $\mathcal{A}_I$, $\mathcal{A}_{II}$, and $\mathcal{A}_{III}$, were proposed in [12]. $\mathcal{A}_I$ is able to compromise the user's secret key or replace the user's public key, but is unable to gain KGC's master secret key nor the user's partial private key issued by KGC. $\mathcal{A}_{II}$ can obtain KGC's master secret key and the user's partial private key, but cannot compromise the user's secret key nor replace her/his public key. Additional type III adversary $\mathcal{A}_{III}$ is to simulate the environments for the proof of that the partial private key, corresponding to a specific identity ID, issued by KGC, cannot be produced without KGC's master key.

Before defining the games for simulating different kinds of adversary environments, we define five oracles which can be accessed by the adversaries according to the game criteria. The oracles are described as follows,

1. **CreateUser:** Input identity $ID \in \{0, 1\}^*$ and check if the identity has been created. If not, the oracle generates the upk and the private key which includes usk and $partial\_key$. After that, the oracle returns usk, upk, and $partial\_key$.
2. **RevealPartialKey:** Input an identity ID and check if ID has been created or not. If true, return $partial\_key$ of ID. Otherwise, a symbol $\perp$ meaning invalid is returned.
3. **RevealSecretKey:** Input an identity ID and check if ID has been created or not. If yes, return usk of ID. Otherwise, a symbol $\perp$ meaning invalid is returned.
4. **ReplaceKey:** Input an identity ID and a user public-secret key pair (upk', usk'), which is used to replace the original public-secret key pair (upk, usk), of the user with identity ID. If ID has not been created, ignore this request.
5. **Sign:** A signature is requested for an identity ID and a message $m \in \{0, 1\}^*$. If ID has been created, the oracle returns a valid signature, σ, signed by the current private key of the user with identity ID. Otherwise, a symbol $\perp$ is returned.

The following three games with three kinds of adversaries will be defined for certificateless signatures.

Game I: Let $\mathcal{S}_I$ be the game simulator and k be a security parameter for Game I. An adversary $\mathcal{A}_I$, which is a probabilistic polynomial-time Turing machine, interacts with $\mathcal{S}_I$.

1. $\mathcal{S}_I$ sets up a master public-secret key pair.
2. $\mathcal{A}_I$ can issue queries to the oracles, **CreateUser**, **RevealPartialKey**, **RevealSecretKey**, **ReplaceKey**, and **Sign**.
3. After querying the oracles, $\mathcal{A}_I$ outputs (ID^*, m^*, σ^*).

$\mathcal{A}_I$ wins this game if (ID^*, m^*, σ^*) can pass the verification and the oracle **Sign** has never been queried with (ID^*, m^*) where one additional restriction is that $\mathcal{A}_I$ cannot issue any query to **RevealPartialKey** with ID^*.

A certificateless signature scheme is secure in Game I if $\mathcal{A}_I$ wins the game with negligible probability.

Game II: Let $\mathcal{S}_{II}$ be the game simulator and $\mathcal{A}_{II}$ be the attacker interacting with $\mathcal{S}_{II}$.

1. $\mathcal{S}_{II}$ sets up a master public-secret key pair and gives the master secret key to $\mathcal{A}_{II}$.
2. $\mathcal{A}_{II}$ can issue queries to all of the oracles defined above with the restriction that **RevealSecretKey** and **ReplaceKey** cannot be queried by $\mathcal{A}_{II}$ with a target identity ID^*.
3. Finally, $\mathcal{A}_{II}$ outputs a message-signature triple (ID^*, m^*, σ^*).

$\mathcal{A}_{II}$ wins the game if (ID^*, m^*, σ^*) passes the verification and **Sign** has never been queried with (ID^*, m^*) by $\mathcal{A}_{II}$.

Game III: This game is simulated to demonstrate that a certificateless signature scheme meets Girault's level-3 security. $\mathcal{S}_{III}$ is the simulator and $\mathcal{A}_{III}$ is the adversary in this game. The setting of the simulation of this game is the same as Game I and $\mathcal{A}_{III}$ can also issue queries to all oracles defined above.

1. $\mathcal{S}_{III}$ firstly sets up a master public-secret key pair.
2. $\mathcal{A}_{III}$ issues queries to all oracles.
3. Eventually, $\mathcal{A}_{III}$ outputs a user key pair which includes the public key and private key of the user with identity ID^*.

$\mathcal{A}_{III}$ wins this game if the oracle **CreateUser** with ID^* has been queried by $\mathcal{A}_{III}$ and $\mathcal{A}_{III}$ can output user ID^*'s key pair where the public key of the key pair outputted from $\mathcal{A}_{III}$ is different from the public keys created by **CreateUser** and **ReplaceKey** queries.

Definition 1 A certificateless signature scheme is with existential unforgeability against chosen message attacks if no probabilistic polynomial-time adversary has non-negligible probability to win Game I and Game II.

Definition 2 A certificateless signature scheme meets Girault's level-3 security if no probabilistic polynomial-time adversary has non-negligible probability to win Game III.

3. CRYPTANALYSIS ON DU-WEN CERTIFICATELESS SHORT SIGNATURE SCHEME

In this section, we will review Du-Wen certificateless short signature scheme from bilinear pairings.

3.1 Bilinear Pairings

Let G_1 be a cyclic additive group and G_2 be a cyclic multiplicative group of the same prime order q. There exists a bilinear mapping e: $G_1 \times G_1 \rightarrow G_2$ which satisfies the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$, where $P, Q \in G_1$, $a, b \in Z_q^*$.
2. Non-Degeneracy: There exists $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3. Computability: There is an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

The modified Tate pairing [3] on a supersingular elliptic curve is such a bilinear pairing.

3.2 Du-Wen Certificateless Short Signature Scheme

Du-Wen scheme consists of seven algorithms defined as follows,

- **Setup:** Let k be the system security parameter. Then KGC selects two groups G_1 and G_2 of prime order $q \leq 2^k$, a bilinear mapping e: $G_1 \times G_1 \rightarrow G_2$, a generator P of group G_1. Leg $g = e(P, P)$. KGC also selects two distinct cryptographic hash functions H_1: $\{0, 1\}^* \rightarrow Z_q^*$, H_2: $\{0, 1\}^* \times G_1 \rightarrow Z_q^*$, and chooses a random number $s \in Z_q^*$ as its master key, and then generates its public key $P_{pub} = sP \in G_1$. Thereafter, KGC publishes the system parameters, $params = \{k, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$, and keeps s secretly.
- **Partial-Private-Key-Extract:** Given a user identity $ID \in \{0, 1\}^*$, KGC computes $Q_{ID} = H_1(ID)$ and $d_{ID} = \frac{1}{s + Q_{ID}} P$. Then, KGC sends d_{ID} to the user with identity ID as her/his partial private key via a secure channel. The partial private key can be verified by checking if $e(d_{ID}, P_{pub} + Q_{ID}P) = g$. Besides, let $T = P_{pub} + Q_{ID}P$.
- **Set-Secret-Value:** The user randomly selects $r \in Z_q^*$ and sets it as her/his secret value.
- **Set-Private-Key:** The user sets (d_{ID}, r) as her/his private key.
- **Set-Public-Key:** Take $params$ and the user's secret value r as inputs, and then generate the user's public key $pk_{ID} = r(P_{pub} + Q_{ID}P) = rT$.
- **CL-Sign:** To produce the signature of message $m \in \{0, 1\}^*$, the user performs the following steps:
  1. set $h = H_2(m, pk_{ID})$;
  2. compute $S = \frac{1}{r + h} d_{ID} = \frac{1}{(r + h)(s + Q_{ID})} P$. ($S$ is the signature on m of the user.)
- **CL-Verify:** Given $params$, m, pk_{ID}, and the signature S on m of the user with identity ID, the signature can be verified by the followings,

1. calculate $h = H_2(m, pk_{ID})$;
2. check if $e(S, pk_{ID} + hT) = g$.

3.3 Comments on Du-Wen Scheme

There is a flaw in the security proofs of Du-Wen scheme. In the proofs of Lemmas 1 and 2 in [7], when attacker $\mathcal{A}_1$ makes a **Signing Query** (ID_i, m_j) where $ID_i = ID_t$ is the target ID and m_j is not the target message m^*, simulator C cannot generate ID_i's signature on m_j for $\mathcal{A}_1$. It means that the security model is weaker than that in one-more forgery [16].

Moreover, a certificateless signature scheme should be as secure as a traditional digital signature scheme based on PKI. However, Du-Wen scheme is not as secure as PKI-based ones since it cannot achieve Girault's level-3 security [8]. Girault who proposed an aspect of the trust levels of an authority where he classifies the trust of an authority into three levels. Higher level means that users need less trust in their authority. Also, truly non-repudiation can be achieved only when the authority can impersonate no user. There are three different trust levels for certificateless signatures as follows.

Level 1 KGC knows users' secrets and can impersonate any user without being detected.

Level 2 KGC does not know users' secrets but it can still impersonate a user by generating a false private key, which is different from the original one, without being detected.

Level 3 KGC does not know users' secrets and cannot impersonate any user by generating any private key since the impersonation of any user can be detected.

To achieve Girault's level-3 security, a certificateless signature scheme should restrict that every user cannot produce any false private key which is different from the original one. It leads that only KGC can produce a false private key for impersonating the corresponding user. In this case, if KGC produces a false private key corresponding to the public key of a specific user and it is different from the original one, the user can sign a message by the original private key to show that her/his private key is legal.

According to the above definitions, we find that Du-Wen scheme cannot meet the requirement of Girault's level-3 security since the public key and the private key, which includes the partial private key, of a user can be replaced without the help of KGC. Thus, KGC can produce a false private key and its corresponding public key such that the user cannot convince the others that the false one is not produced by her/him. A user with identity ID can replace its public key and the corresponding private key through the following steps. First, the user randomly selects a new secret value r' and sets its private key as (d_{ID}, r'). The user then computes the corresponding public key $pk'_{ID} = r'(P_{pub} + Q_{ID}P) = r'T$ to replace its original public key pk_{ID}. After generating the new public and private keys, the user can produce a signature $S' = \frac{1}{r' + h'} d_{ID} = \frac{1}{(r' + h')(s + Q_{ID})} P$ on m, where $h' = H_2(m, pk'_{ID})$. The signature can pass the verification due to $e(S', pk'_{ID} + h'T) = e = (\frac{1}{r' + h'} d_{ID}, (r' + h')T) = e(P, P) = g$.

4. THE PROPOSED CERTIFICATELESS SIGNATURE SCHEME BASED ON BONEH-BOYEN SHORT SIGNATURE SCHEME

4.1 Boneh-Boyen Short Signature Scheme

Boneh-Boyen short signature scheme [4] is briefly described as follows. Let G_1, G_2, and G_T be three cyclic additive groups of prime order $q \leq 2^k$ where k is a security parameter, and e be an efficiently computable bilinear pairing e: $G_1 \times G_2 \rightarrow G_T$, which satisfies the properties of bilinearity and non-degeneracy. Suppose that a message m which will be signed is an element in Z_q^*.

- **Key Generation:** Select two random generators $P_1 \in G_1$ and $P_2 \in G_2$, and a random integer $s \in Z_q^*$. Then compute $P_{pub} = sP_2 \in G_2$ and $g = e(P_1, P_2) \in G_T$. The public key is (P_1, P_2, P_{pub}, g) and the secret key is (P_1, s).
- **Signing:** Given the secret key (P_1, s) and a message $m \in Z_q^*$, compute the signature $\sigma = \frac{1}{s+m} P_1 \in G_1$.
- **Verification:** Given the public key (P_1, P_2, P_{pub}, g), a message m, and a signature σ, the signature can be verified by checking if $e(\sigma, P_{pub} + mP_2) = g$.

Boneh-Boyen short signature scheme has been proved being secure.

4.2 The Proposed Scheme

In order to achieve Girault's level-3 security, we propose an enhanced Du-Wen scheme without increasing much computation cost. The details of the proposed scheme are shown below.

Setup: KGC generates G_1, G_2, G_T, q, k, e, P_1, P_2, g, s, and P_{pub} which are the same as those in Boneh-Boyen signature scheme (section 4.1). It then selects two distinct cryptographic hash functions H_1: $\{0, 1\}^* \rightarrow Z_q^*$ and H_2: $\{0, 1\}^* \times G_2 \rightarrow Z_q^*$. KGC publishes the system parameters, $params = \{k, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$, and keeps its master key s secretly.

- **User-Key-Gen:** A user with identity ID randomly chooses $r \in Z_q^*$ and then computes $pk_{ID} = rP_2$ and $pk'_{ID} = r(P_{pub} + Q_{ID}P_2)$ where $Q_{ID} = H_1(ID)$. The user keeps r secretly and sets (pk_{ID}, pk'_{ID}) as its public key.
- **Partial-Private-Key-Gen:** KGC takes $params$, the user's partial public information (Q_{ID}, pk_{ID}) as inputs, and then generates the user's partial private key $d_{ID} = 1/(s + Q_{ID} + H_1(ID \| pk_{ID}))P_1$. Then KGC returns d_{ID} to the user via a secure manner. After receiving d_{ID}, the user checks the correctness of d_{ID} by examining if $e(d_{ID}, P_{pub} + Q_{ID}P_2 + H_1(ID \| pk_{ID})P_2) = g$. The private key of the user is (d_{ID}, r).
- **CL-Sign:** To produce the signature on message $m \in \{0, 1\}^*$, the user with identity ID performs the following steps:
  1. set $h = H_2(m, pk_{ID})$;
  2. compute $S = \frac{1}{r+h} d_{ID}$, where S is the signature on message m of the user.

- **CL-Verify:** Given *params*, message m, pk_{ID}, pk'_{ID}, and the signature S on message m of the user with identity ID, the signature can be verified as follows,
  1. let $h = H_2(m, pk_{ID})$;
  2. if the following formula holds, the signature S is valid.

$$e(S, pk'_{ID} + H_1(ID \| pk_{ID})pk_{ID} + h(P_{pub} + Q_{ID}P_2 + H_1(ID \| pk_{ID})P_2)) = g$$

4.3 Security Proofs

We will prove that the proposed certificateless signature scheme is with unforgeability and Girault's level-3 security.

Theorem 1 If Boneh-Boyen short signature scheme is secure against existential forgery under a chosen message attack, the proposed signature scheme is with existential unforgeability against a chosen message attack.

We exploit two lemmas to prove this theorem, where one is for the proof of that the proposed scheme is secure in Game I and the other is for Game II.

Lemma 1 Suppose that Boneh-Boyen short signature is secure against existential forgery under a chosen message attack. Then the proposed signature scheme is secure against the attacker in Game I under the random oracle model.

Proof: Let **BB-SO** be the signing oracle of Boneh-Boyen signature scheme. In the following game, we construct algorithm $\mathcal{A}_S$ interacts with $\mathcal{A}_C$, which is an adversary in the proposed scheme, and then breaks Boneh-Boyen signature scheme. The simulation is shown as follows,

- **Setup:** $\mathcal{A}_S$ selects q_h, which is the possibly maximal number of H_1 queries, random messages $m_1', \ldots, m'_{q_h}$ and sends them to **BB-SO**. **BB-SO** responds q_h signatures $\sigma_1', \ldots, \sigma'_{q_h}$ on $m_1', \ldots, m'_{q_h}$, respectively, and the corresponding public key $PK = (P_1, P_2, \lambda, e(P_1, P_2))$ to $\mathcal{A}_S$, where $\sigma_i' = \frac{1}{s + m_i'} P_1$, $i = 1, \ldots, q_h$, $\lambda = sP_2$, P_1 is a generator of G_1, P_2 is a generator of G_2, and $g = e(P_1, P_2) \in G_T$. Let s be the master secret key, $P_{pub} = \lambda$ be the master public key, and q be the prime order of G_1, G_2, and G_T. $\mathcal{A}_S$ gives these public parameters $\{k, G_1, G_2, e, q, P_2, g, P_{pub}\}$ to $\mathcal{A}_C$, where k is the security parameter.
- **Queries:** $\mathcal{A}_S$ simulates all oracles which can be queried by $\mathcal{A}_C$ as follows,
  – Hash queries: For each H_1 query, $\mathcal{A}_S$ returns a random string consistently by maintaining a hash list, H_1-list. If $\mathcal{A}_C$ queries H_1 with $ID_i \| pk_{ID_i}$ for some identity ID_i at the first time and H_1 has never been queried with ID_i, $\mathcal{A}_S$ randomly chooses δ_i as the output value of $H_1(ID_i \| pk_{ID_i})$ and computes $H_1(ID_i) = Q_{ID_i} = m_i' - \delta_i$. $\mathcal{A}_S$ then stores these two values δ_i and Q_{ID_i} with corresponding inputs of H_1 oracle in H_1-list. If $\mathcal{A}_C$ queries H_1 with ID_i at the first time and H_1 has never been queried with $ID_i \| pk_{ID_i}$, $\mathcal{A}_S$ generates the output of $H_1(ID_i \| pk_{ID_i})$ and then generates the output $H_1(ID_i)$ by the above manner. Otherwise, $\mathcal{A}_S$ returns the generated corresponding hashed value from H_1-list. $\mathcal{A}_S$ responds H_2 oracle queries by returning random values consistently where the hash list, H_2-list, of H_2 is maintained.

– CreateUser: On the input of identity ID_i, if no user with ID_i has been created, $\mathcal{A}_S$ randomly selects $r_i \in Z_q^*$ as the secret key of the user with identity ID_i, and computes the corresponding public key $pk_{ID_i} = r_iP_2$, $pk'_{ID_i} = r_i(P_{pub} + Q_{ID_i}P_2)$ and partial private key $d_{ID_i} = \sigma_i' = \frac{1}{s+m_i'} P_1 (= \frac{1}{s+Q_{ID_i} H_1(ID_i \| pk_{ID_i})} P_1)$, where $H_1(ID_i \| pk_{ID_i}) = m_i' - Q_{ID_i}$. $\mathcal{A}_S$ then stores the public key and the private key. If the user with ID_i has been created, this request will be ignored.
– RevealPartialKey: On the input of identity ID_i, if the user with ID_i has been created, $\mathcal{A}_S$ returns d_{ID_i} as the partial private key of the user. Otherwise, $\mathcal{A}_S$ returns the symbol $\perp$.
– RevealSecretKey: On the input of identity ID_i, if the user with ID_i has been created, $\mathcal{A}_S$ returns the corresponding secret key r_i which has been chosen in the simulation of **CreateUser** oracle. Otherwise, $\mathcal{A}_S$ creates the user with ID_i by querying **CreateUser** and then returns the corresponding secret key.
– ReplaceKey: On the input of identity ID_i, $\tilde{pk}_{ID_i}$, $\tilde{pk}'_{ID_i}$, and the corresponding secret key $\tilde{r}_i$, if the user with ID_i has been created, $\mathcal{A}_S$ replaces the original public key tuple with $(\tilde{pk}_{ID_i}, \tilde{pk}'_{ID_i})$ and then stores the corresponding secret key $\tilde{r}_i$ and partial private key which is corresponding to $\tilde{r}_i$. Otherwise, $\mathcal{A}_S$ ignores this request.
– Sign: On the input of identity ID_i and message m, if the user with ID_i has been created, $\mathcal{A}_S$ computes $S = \frac{1}{r_i + h} d_{ID_i}$ where $h = H_2(m, pk_{ID})$. Otherwise, $\mathcal{A}_S$ creates the user with ID_i and then generates S via the above step. Finally, $\mathcal{A}_S$ returns $\sigma = (S, pk_{ID_i}, pk'_{ID_i})$, where S is the signature on m.

• **Output:** After finishing the oracle queries, $\mathcal{A}_C$ outputs a forgery, (ID^*, m^*, σ^*), where $\sigma^* = (S^*, pk_{ID^*}, pk'_{ID^*})$. $\mathcal{A}_S$ can return the forgery, $(\tilde{m^*} = Q_{ID^*} + H_1(ID^* \| pk_{ID^*}), \tilde{\sigma^*} = (r^* + h^*)S^*)$, where r^* is the secret key of the user with ID^* and $h^* = H_2(m^*, pk_{ID^*})$, of Boneh-Boyen signature scheme due to $\tilde{\sigma^*} = (s + \tilde{m^*})^{-1}P_1$. Therefore, if $\mathcal{A}_C$ successfully outputs a forgery of the proposed certificateless signature scheme with non-negligible probability, $\mathcal{A}_S$ also has non-negligible probability to break Boneh-Boyen signature scheme. ❑

Lemma 2 If Boney-Boyen short signature scheme is secure against existential forgery under a chosen message attack, the proposed signature scheme is secure against the attacker in Game II under the random oracle model.

Proof: The simulation environment of Game II, which is similar to Game I, is shown as follows,

• **Setup:** $\mathcal{A}_S$ selects q_h, which is the possibly maximal number of H_2 queries, random messages $m_1', \ldots, m'_{q_h}$ and sends them to **BB-SO**. **BB-SO** responds q_h signatures $\sigma_1', \ldots, \sigma'_{q_h}$ on $m_1', \ldots, m'_{q_h}$, respectively, and the corresponding public key $PK = (P_1, P_2, \lambda, e(P_1, P_2))$ to $\mathcal{A}_S$, where $\lambda = rP_2$, and $\sigma_i' = \frac{1}{r+m_i'} P_1$, $i = 1, \ldots, q_h$. Let r be the secret key of the user with target identity ID' and $pk_{ID'} = \lambda$ $(= rP_2)$ be a part of the public key of the user. $\mathcal{A}_S$ then randomly selects s, which is the master secret key of KGC, and computes $Q_{ID'}$ and $H_1(ID' \| pk_{ID'})$. $\mathcal{A}_S$ computes $d_{ID'} = \frac{1}{s+Q_{ID'} + H_1(ID' \| pk_{ID'})} P_1$ as the partial private key

of the user, and $pk'_{ID'} = (s + Q_{ID'})\lambda = r(P_{pub} + Q_{ID'}P_2)$ as the other part of the public key of the user, where $P_{pub} = sP_2$. After that, $\mathcal{A}_S$ gives public parameters $\{k, G_1, G_2, e, q, P_2, g, P_{pub}\}$ and s to $\mathcal{A}_C$.

- **Queries:** $\mathcal{A}_S$ simulates all oracles, which can be queried by $\mathcal{A}_C$, as follows,
  - Hash queries: If $\mathcal{A}_C$ issues a hash query with $(m_i, pk_{ID'})$ to H_2 oracle, $\mathcal{A}_S$ returns m_i', which is the message of signature σ_i' in Boneh-Boyen signature scheme. Otherwise, $\mathcal{A}_S$ outputs a random value as the result of H_2 query.
  - CreateUser: On the input of identity ID_i, if no user with ID_i has been created, $\mathcal{A}_S$ randomly selects $r_i \in Z_q^*$ as the secret key of the user with identity ID_i, and computes the corresponding public key $pk_{ID_i} = r_iP_2$, $pk'_{ID_i} = r_i(P_{pub} + Q_{ID_i}P_2)$ and partial private key $d_{ID_i} = \frac{1}{s + Q_{ID_i} + H_1(ID_i \| pk_{ID_i})} P_1$. $\mathcal{A}_S$ then stores the public key and the private key of the user. If the user has been created, this request will be ignored.
  - RevealPartialKey: On the input of identity ID_i, if the user with ID_i has been created, $\mathcal{A}_S$ returns d_{ID_i} as the partial private key of the user. Otherwise, $\mathcal{A}_S$ returns the symbol $\perp$.
  - RevealSecretKey: On the input of identity ID_i except the target identity ID_i, if the user with ID_i has been created, $\mathcal{A}_S$ returns the corresponding secret key r_i of the user with ID_i.
  - ReplaceKey: On the input of identity ID_i, $pk_{ID_i}^{\sim}$, $pk'^{\sim}_{ID_i}$, and the corresponding secret key $r_i^{\sim}$, if the user with ID_i has been created and $ID_i \neq ID'$, $\mathcal{A}_S$ replaces the original public key tuple with $(pk_{ID_i}^{\sim}, pk'^{\sim}_{ID_i})$ and then stores the corresponding secret key $r_i^{\sim}$ and partial private key which is corresponding to $r_i^{\sim}$. Otherwise, $\mathcal{A}_S$ ignores this request.
  - Sign: On the input of identity ID_i and message m, if the user with ID_i has been created and $ID_i \neq ID'$, $\mathcal{A}_S$ computes $S = \frac{1}{r_i + h} d_{ID_i}$ where $h = H_2(m, pk_{ID})$, and returns $\sigma = (S, pk_{ID_i}, pk'_{ID_i})$ where S is the signature of m. If $ID_i = ID'$, $\mathcal{A}_S$ computes $S = 1/(s + Q_{ID'} + H_1(ID' \| pk_{ID'}))\sigma_i'$, where $\sigma_i' = \frac{1}{r + m_i'} P_1$ and $H_2(m, pk_{ID'}) = m_i'$, and then returns $\sigma = (S, pk_{ID_i}, pk'_{ID_i})$.
- **Output:** Finally, $\mathcal{A}_C$ outputs a forgery, (ID^*, m^*, σ^*), where $\sigma^* = (s^*, pk_{ID^*}, pk'_{ID^*})$. If $ID^* = ID'$, $\mathcal{A}_S$ can return the forgery, $(\tilde{m^*} = h^* = H_2(m^*, pk_{ID^*})$, $\tilde{\sigma^*} = (s + Q_{ID'} + H_1(ID' \| pk_{ID'}))s^*)$, of Boneh-Boyen signature scheme. Otherwise, $\mathcal{A}_S$ outputs "failure" and aborts. If $\mathcal{A}_C$ outputs a forgery of the proposed certificateless signature scheme with non-negligible probability, $\mathcal{A}_S$ also has non-negligible probability to break Boneh-Boyen signature scheme. ❑

By Lemmas 1 and 2, the proposed signature scheme is secure against existential forgery under a chosen message attack, *i.e.*, Theorem 1 holds. Then we will demonstrate that the proposed scheme also meets Girault's level-3 security.

Theorem 2 Suppose that Boneh-Boyen short signature scheme is secure against existential forgery under a chosen message attack. Then the proposed signature scheme is with Girault's level-3 security.

Proof: The simulation for Game III is shown as follows,

- **Setup:** $\mathcal{A}_S$ selects q_c, which is the possibly maximal number of **CreateUser** queries, random messages m_1', …, m'_{q_c} and sends them to **BB-SO**. **BB-SO** responds q_c signatures σ_1', …, σ'_{q_c} on m_1', …, m'_{q_c}, respectively, and the corresponding public key $PK = (P_1, P_2, \lambda, e(P_1, P_2))$ to $\mathcal{A}_S$, where $\lambda = sP_2$, and $\sigma_i' = \frac{1}{s + m_i'} P_1$, $i = 1, \ldots, q_c$. Let s be the master secret of KGC. After that, $\mathcal{A}_S$ gives public parameters $\{k, G_1, G_2, e, q, P_2, g, P_{pub} (= \lambda)\}$ to $\mathcal{A}_C$.
- **Queries:** The simulations of the oracles, H_1, H_2, **CreateUser**, **RevealPartialKey**, **RevealSecretKey**, **ReplaceKey**, and **Sign**, are similar to those in Game I, except that $\mathcal{A}_C$ can issue a query to **CreateUser** with every ID_i only once.
- **Output:** $\mathcal{A}_C$ outputs an additional private key (d_{ID^*}, r^*) and public key (pk_{ID^*}, pk'_{ID^*}) with identity ID^* which has been created. If $\mathcal{A}_C$ outputs the public-private keys with non-negligible probability and the public key (pk_{ID^*}, pk'_{ID^*}) is different from the public keys created by **CreateUser** and **ReplaceKey** queries, $\mathcal{A}_S$ also has non-negligible probability to break Boneh-Boyen signature scheme by outputting the forgery $(\tilde{m^*} = Q_{ID^*} + H_1(ID^* \| pk_{ID^*}), \tilde{\sigma^*} = d_{ID^*}$. ❑

4.4 Comparisons

In this section, we will provide the comparisons between our scheme and other related pairing-based certificateless signature schemes [1, 7, 10, 15, 18, 19]. The comparisons for the computation costs of signing and verification operations, the space cost of the user's public key and signature, and the conditions of possessing or lacking Girault's level-3 security are summarized in Table 1.

From Table 1, the computation cost of our scheme is less than that of the other schemes except Du-Wen scheme. The total space cost of public key and signature of our scheme is less than [1, 15] and equal to [10, 18, 19], except Du-Wen scheme. The space cost of private key of our scheme is equal to [7, 18] and larger than [1, 10, 19]. Nevertheless, our scheme is able to achieve Girault's level-3 security but the other schemes cannot. (Except that [15] mentioned their scheme can achieve Girault's level-3 security by changing the partial private key issuing step. However the scheme does not be proven secure.) It turns out that our scheme is an efficient certificateless short signature scheme with truly non-repudiation.

Table 1. The comparison of certificateless signature schemes.

	[1]	[15]	[19]	[10]	[7]	[18]	Ours
Sign	2*s* + 1*e* + 1*p*	2*s*	2*s*	2*s*	1*s*	1*e*	1*s*
Verify	4*p*	2*s* + 4*p*	2*s* + 2*p*	1*s* + 3*p*	1*s* + 1*p*	1*e* + 4*p*	4*s* + 1*p*
PK-S	320*b*	320*b*	160*b*	160*b*	160*b*	320*b*	320*b*
PR-S	160*b*	160*b*	160*b*	160*b*	320*b*	320*b*	320*b*
S-S	320*b*	320*b*	320*b*	320*b*	160*b*	160*b*	160*b*
G-level-3	NO	NO	NO	YES[#]	NO	NO	YES

s: a scalar multiplication in G_1 or G_2; *e*: an exponentiation computation; *p*: a pairing computation; *b*: bits;
PK-S: the size of the public key; **PR-S:** the size of the private key; **S-S:** the size of the signature;
G-level-3: Girault's level-3 security.
[#] It has not been proved.

5. CONCLUSIONS

In this paper, we have reviewed the security proof of Du-Wen scheme and found that it does not cover complete one-more forgery. Moreover, the scheme is insufficient for Girault's level-3 security. Certificateless signatures with Girault's level-3 security are urgently desired since the improved generic model of certificateless signatures proposed by [12] has already included the security property. Certificateless signature schemes cannot fulfill non-repudiation without Girault's level-3 security. Therefore, we have also proposed an efficient certificateless short signature scheme to achieve Girault's level-3 security. We make use of the short signature scheme [4], which was proved being secure, to design our certificateless short signature scheme. Finally, the formal proofs have been provided to demonstrate the security of our scheme.

ACKNOWLEDGEMENT

We would like to thank the anonymous reviewers of this paper for their valuable comments.

REFERENCES

1. S. Al-Riyami and K. G. Paterson, "Certificateless public key cryptography," in *Proceedings of ASIACRYPT*, LNCS 2894, 2003, pp. 452-473.
2. M. H. Au, J. Chen, J. K. Liu, Y. Mu, D. S. Wong, and G. Yang, "Malicious KGC attacks in certificateless cryptography," in *Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security*, 2007, pp. 302-311.
3. I. Blake, G. Seroussi, and N. Smart, "Advances in elliptic curve cryptography," *London Mathematical Society Lecture Notes Series*, Cambridge University Press, 2005.
4. D. Boneh and X. Boyen, "Short signatures without random oracles and the SDH assumption in bilinear groups," *Journal of Cryptology*, Vol. 21, 2008, pp. 149-177.
5. X. Cao, K. G. Paterson, and W. Kou, "An attack on a certificateless signature scheme," Cryptology ePrint Archive: Report 2006/367.
6. K. Y. Choi, J. H. Park, J. Y. Hwang, and D. H. Lee, "Efficient certificateless signature schemes," in *Proceedings of the 5th International Conference on Applied Cryptography and Network Security*, LNCS 4521, 2007, pp. 443-458.
7. H. Du and Q. Wen, "Efficient and provably-secure certificateless short signature scheme from bilinear pairings," *Computer Standards and Interfaces*, Vol. 31, 2009, pp. 390-394.
8. M. Girault, "Self-certified public keys," in *Proceedings of Eurocrypto*, LNCS 547, 1991, pp. 490-497.
9. S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen-message attack," *SIAM Journal on Computing*, Vol. 17, 1998, pp. 281-308.
10. M. C. Gorantla and A. Saxena, "An efficient certificateless signature scheme," in *Proceedings of International Conference on Computational Intelligence and Security*, LNCS 3802, 2005, pp. 110-116.

11. B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Key replacement attack against a generic construction of certificateless signature," in *Proceedings of the 11th Australasian Conference on Information Security and Privacy*, LNCS 4058, 2006, pp. 235-246.
12. B. C. Hu, D. S. Wong, Z. Zhang, and X. Deng, "Certificateless signature: A new security model and an improved generic construction," *Designs, Codes and Cryptography*, Vol. 42, 2007, pp. 109-126.
13. X. Huang, W. Susilo, Y. Mu, and F. Zhang, "On the security of certificateless signature schemes from AsiaCrypt 2003," in *Proceedings of the 4th International Conference Cryptology and Network Security*, LNCS 3810, 2005, pp. 13-25.
14. X. Huang, Y. Mu, W. Susilo, D. S. Wong, and W. Wu, "Certificateless signature revisited," in *Proceedings of the 12th Australasian Conference on Information Security and Privacy*, LNCS 4586, 2007, pp. 308-322.
15. X. Li, K. Chen, and L. Sun, "Certificateless signature and proxy signature schemes from bilinear pairings," *Lithuanian Mathematical Journal*, Vol. 45, 2005, pp. 76-83.
16. D. Pointcheval and J. Stern, "Provably secure blind signature schemes," in *Proceedings of International Conference on the Theory and Applications of Cryptology and Information Security: Advances in Cryptology*, LNCS 1163, 1996, pp. 252-265.
17. A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proceedings of CRYPTO*, LNCS 196, 1985, pp. 47-53.
18. R. Tso, X. Yi, and X. Huang, "Efficient and short certificateless signature," in *Proceedings of the 7th International Conference on Cryptology and Network Security*, LNCS 5339, 2008, pp. 64-79.
19. W. S. Yap, S. H. Heng, and B. M. Goi, "An efficient certificateless signature scheme," in *Proceedings of EUC Workshops on Emerging Directions in Embedded and Ubiquitous Computing*, LNCS 4097, 2006, pp. 322-331.
20. D. H. Yum and P. J. Lee, "Generic construction of certificateless signature," in *Proceedings of the 9th Australasian Conference on Information Security and Privacy*, LNCS 3108, 2004, pp. 200-211.
21. Z. Zhang and D. Feng, "Key replacement attack on a certificateless signature scheme," Cryptology ePrint Archive: Report 2006/453.
22. Z. Zhang, D. Wong, J. Xu, and D. Feng, "Certificateless public-key signature: Security model and efficient construction," in *Proceedings of the 4th International Conference on Applied Cryptography and Network Security*, LNCS 3989, 2006, pp. 293-308.

Chun-I Fan (范俊逸) was born in Tainan, Taiwan. He received his M.S. degree in Computer Science and Information Engineering from National Chiao Tung University, Taiwan, in 1993, and the Ph.D. degree in Electrical Engineering at National Taiwan University in 1998. From 1999 to 2003, he was an associate researcher and project leader of Telecommunication Laboratories, Chunghwa Telecom Co., Ltd., Taiwan. In 2003, he joined the faculty of the Department of Computer Science and Engineering, National Sun Yat-sen University, Kaohsiung, Taiwan to be an Assistant Professor. He had been an Associate Professor from 2006 and

has been a full Professor from 2010. He won the Dragon Thesis Award from Acer Foundation and Best Thesis Award from Institute of Information and Computing Machinery in 1999, Best Student Paper Awards in National Conference on Information Security 1998 and 2007. He also was the editor-in-chief of InforZation Security Newsletter, Chinese Cryptology and Information Security Association. He was a program co-chair of ACM International Workshop on Cross Layer Design 2008, an international advisor of the International Congress on Pervasive Computing and Management 2008, and program committee members of IEEE International Conference on Communications 2007, IEEE International Conference on Wireless and Mobile Computing, Networking and Communications 2008, the 2008 International Workshop of Information Security, 2008 International Conference on Computational Intelligence and Security, the 3rd Joint Workshop on Information Security, Information Security Conference 2008, the fourth International Symposium on Smart Home, and the 4th Joint Workshop on Information Security. His current research interests include information security, cryptographic protocols, wireless security, and electronic commerce, and he has published over 80 papers in journals, books, and conference proceedings.

Ruei-Hau Hsu (徐瑞壕) was born in Kaohsiung, Taiwan on July 11, 1979. He received his B.S. and M.S. degrees in Computer Science and Information Engineering from Tunghai University, Taiwan, in 2002 and 2004, respectively. He is toward to his Ph.D. degree in Computer Science and Engineering at National Sun Yat-sen University from 2005 until now. From 2004 to 2005, he was a Technical Engineer of the Computer Center of Hsiuping Institute of Technology, Dali, Taiwan. From August to December 2007, he joined the International Collaboration for Advancing Security Technology (iCAST) program to be a visiting researcher in Carnegie Mellon University, America. His current research interests include information security, information privacy, and cryptographic primitives of wireless authentication protocols and signature schemes.

Pei-Hsiu Ho (何佩修) was born in Taichung, Taiwan on Apr. 30, 1976. She received her M.S. degree in Information Management from Southern Taiwan University of Technology, Taiwan, in 2003. From 2003 to 2005, she was a software engineer in Asia Pacific Telecom Co., Ltd., Taiwan. She is now a Ph.D. candidate of Computer Science and Engineering at National Sun Yat-sen University. Her current research interests include information security and cryptographic protocols for electronic cash and digital signatures.