Truly Non-Repudiation Certificateless Short Signature Scheme from Bilinear Pairing

Authors: Chun-I Fan, Ruei-Hau Hsu, and Pei-Hsiu Ho
Speaker: Richard Ruei-Hau Hsu
National Sun Yat-sen University, Taiwan

JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 27, 969-982 (2011)
Truly Non-Repudiation Certificateless Short Signature Scheme from Bilinear Pairing

Outline

- Certificateless Signature
- Security Model
- Cryptanalysis on Du-Wen Certificateless Short Signature Scheme
- The Proposed Certificateless Signature Scheme Based on Boneh-Boyen Short Signature Scheme
- Conclusion
Certificateless signature scheme is an improvement of ID-based signature scheme.

The user can keep its signing secret without being known by KGC.
Generic Construction of Certificateless Signature Scheme

A certificateless signature scheme consists of the following five polynomial-time algorithms

- **Master-Key-Gen**: It produces a master public-secret key pair \((mpk, msk)\).

- **User-Key-Gen**: Input \(mpk\) and \(ID\), it produces the user’s public key and secret key \((upk, usk)\).

- **Partial-Private-Key-Gen**: Input \(upk, msk, ID\), it produces the user’s partial private key \(partial\_key\).
Generic Construction of Certificateless Signature Scheme (cont.)

- **CL-Sign**: Input a user’s private key, $usk$ and partial key, and message $m \in \{0, 1\}^*$, it outputs a signature $\sigma$.

- **CL-Verify**: Input $mpk$, $upk$, message $m$, and signature $\sigma$, it returns *true* if the signature passes the verification. Otherwise, it returns *false*.
Game I

\[ (ID^*, m^*, \sigma^*) \]

**Restriction**
- Sign has never been queried with \((ID^*, m^*)\)
- Adversary cannot issue any query to RevealPartialKey with \(ID^*\)
Game II

\[ (ID^*, m^*, \sigma^*) \]

**Restriction**
- Sign has never been queried with \((ID^*, m^*)\)
- RevealSecretKey and ReplaceKey cannot be queried by adversary with \(ID^*\)
Game III

**Setup master public-secret key pair**

- ** CreateUser**
- **RevealPartialKey**
- **RevealSecretKey**
- **ReplaceKey**
- **Sign**

Restriction:
- $ID^*$ has been created
- $upk_{ID^*}$ is different from the public key created by **CreateUser** and **ReplaceKey**
Bilinear Pairings

- $(G_1, +)$ and $(G_2, \cdot)$ are two cyclic groups of prime order $q$, the bilinear pairing is given as $e$:
  \[ G_1 \times G_1 \rightarrow G_2. \]

- Bilinearity: For all $P, Q, R \in G_1$,
  \[ e(P + Q, R) = e(P, R)e(Q, R), \]
  \[ e(P, Q + R) = e(P, Q)e(P, R). \]

- Non-degeneracy: There exists $P, Q \in G_1$ such that
  \[ e(P, Q) \neq 1. \]

- Computability: It is efficient to compute $e(P, Q)$ for all $P, Q \in G_1$. 
Setup

- $G_1$ and $G_2$ of the same prime order $q > 2^l$, and $e : G_1 \times G_1 \rightarrow G_2$.
- $P$ is a generator of group $G_1$.
- Let $g = e(P, P)$.
- KGC selects $H_1 : \{0, 1\}^* \rightarrow Z_q^*$, $H_2 : \{0, 1\}^* \times G_1 \rightarrow Z_q^*$.
- KGC chooses $s \in Z_q^*$ as system master key and computes $P_{pub} = sP \in G_1$.
- The public system parameters $\text{params} = \{l, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$. 
△ Partial-Private-Key-Extract

▷ Given an identity $ID \in \{0, 1\}^*$, KGC computes

$$Q_{ID} = H_1(ID) \quad \text{and} \quad d_{ID} = \frac{1}{s+Q_{ID}}P$$

▷ The partial key can be verified by checking if

$$e(d_{ID}, P_{pub} + Q_{ID}P) = g$$

▷ Let $T = P_{pub} + Q_{ID}P$
Set-Secret-Value

- The user selects $r \in_R \mathbb{Z}_q^*$ and sets it as her/his secret key

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 generate the user’s public key

$$pk_{ID} = r(P_{pub} + Q_{ID}P) = rT$$
CL-Sign : In order to generate a signature of an identity ID on a message $m \in \{0, 1\}^*$

- Set $h = H_2(m, pk_{ID})$.
- $S = \frac{1}{r+h}d_{ID} = \frac{1}{(r+h)(s+Q_{ID})}P$.
- The signature of identity ID on the message $m$ is $S$.

CL-Verify: Given $(\text{params}, m, pk_{ID}, S)$

- Compute $h = H_2(m, pk_{ID})$.
- $e(S, H(pk_{ID})P + hT) = g$?
Comment on Security Proof

Simulator $C$ cannot generate the signature of the target $ID_I$. The security model of Du-Wen Scheme cannot be as strong as one-more forgery.
Du-Wen signature scheme is not as secure as PKI-based signature scheme since it cannot achieve Girault’s level-3 security.

Three trust level of Girault’s security

- **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 impersonate a user by generating a false private key
- **Level 3.** KGC does not know users’ secrets and cannot impersonate any user by generating any false private key since the impersonation of any user can be detected
Girault’s Level-1 and Level-2 Security

Level-1 Security

KGC → User

Level-2 Security

KGC → User

: User Identity
: Signing Key
: KGC Master Secret Key
: Signature
: User Public Key
: User Secret Key
Girault’s Level-3 Security

Level-3 Security

KGC

User

Message

: User Identity

: Signing Key

: KGC Master Secret Key

: Signature

: User Public Key

: User Secret Key
A user with identity $ID$ can change its public key by itself by the following steps:

- The user first selects a new secret $r'$ 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 $pk_{ID}$

The user can produce a signature

$S' = \frac{1}{r' + h'} d_{ID} = \frac{1}{(r' + h')(s + Q_{ID})} P$ on $m$, where

$h' = H_2(m, pk'_{ID})$ with new private key.
The Proposed Scheme

- **Setup:**
  - $G_1$ and $G_2$ of the same prime order $q > 2^l$, and $e : G_1 \times G_1 \rightarrow G_2$.
  - $P$ is a generator of group $G_1$.
  - Let $g = e(P, P)$.
  - KGC selects $H_1 : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$, $H_2 : \{0, 1\}^* \times G_1 \rightarrow \mathbb{Z}_q^*$.
  - KGC chooses $s \in \mathbb{Z}_q^*$ as system master key and computes $P_{pub} = sP \in G_1$.
  - The public system parameters $\text{params} = \{l, G_1, G_2, e, q, P, g, P_{pub}, H_1, H_2\}$. 

The Proposed Certificateless Short Signature Scheme from Bilinear Pairing
The Proposed Certificateless Signature Scheme Based on Boneh-Boyen Signature Scheme

The Proposed Scheme

User-Key-Gen:

- A user with identity $ID$ selects $r \in_R Z_q^*$ and then computes $pk_{ID} = rP$ and $pk'_{ID} = r(P_{pub} + Q_{ID}P)$ where $Q_{ID} = H_1(ID)$.
- The user keeps $r$ secretly and sets $(pk_{ID}, pk'_{ID})$ as its public key.
The Proposed Scheme

- **Partial-Private-Key-Gen:**
  - Take the user’s partial public information \((Q_{ID}, pk_{ID})\) as inputs, and generates the her/his partial private key \(d_{ID} = \frac{1}{(s + Q_{ID} + H_1(pk_{ID}))}P\).
  - KGC returns \(d_{ID}\) to the user. The private key of the user is \((r, d_{ID})\).
The Proposed Certificateless Signature Scheme Based on Boneh-Boyen Signature Scheme

The Proposed Scheme

\textbf{CL-Sign:}

\begin{itemize}
  \item To produce the signature on message \( m \in \{0, 1\}^* \), the user with identity \( ID \) first sets \( h = H_2(m, pk_{ID}) \)
  \item Compute \( S = \frac{1}{r+h} d_{ID}(= \frac{1}{(r+h)(s+Q_{ID}+H_1(pk_{ID})))P}) \), where \( S \) is the signature on message \( m \) of the user
\end{itemize}

\textbf{CL-Verify:}

\begin{itemize}
  \item Given \textit{params}, \( m \), \( pk_{ID} \), \( pk'_{ID} \), the signature \( S \) on message \( m \), compute \( h = H_2(m, pk_{ID}) \).
  \item Then check whether the signature \( S \) is valid by the equation, \( e(S, pk'_{ID} + H_1(pk_{ID})pk_{ID} + h(P_{pub} + Q_{ID}P + H_1(pk_{ID})P)) = g \)
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.
Lemma 1

Lemma

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 of Lemma 1

- **BB-SO**: The signing oracle of Boneh-Boyen
- **$A_S$**: The adversary in Boneh-Boyen short signature scheme
- **$A_C$**: The adversary of the proposed certificateless short signature scheme
Proof of Lemma 1 (cont.)

\[ \mathcal{A}_C \rightarrow \mathcal{A}_S \]

\[ \begin{align*}
    m_1', \ldots, m_q' \\
    \sigma_1', \ldots, \sigma_q' \\
    PK = (P_1, P_2, \lambda, e(P_1, P_2)) \\
    \sigma_i' = \frac{1}{s + m_i'} P_1
\end{align*} \]

- \( s \) be the master secret key of KGC
- \( P_{pub} = \lambda = (sP_2) \) be the master public key
Proof of Lemma 1 (cont.)

\[ \mathcal{A}_C \quad \mathcal{A}_S \]

If \( \alpha = ID_i \parallel pk_{ID_i} \) and \( ID_i \) appears at the 1st time and \( ID_i \) has never been queried

\[ H_1(ID_i \parallel pk_{ID_i}) = \delta_i \in \mathbb{Z}_q^* \]

\[ H_1(ID_i) = Q_{ID_i} = m'_i - \delta_i \]

store \( Q_{ID_i} \) and \( \delta_i \) in \( H1 \)-list

Else If \( \alpha = ID_i \)

The same as the first condition

\[ H_2(\alpha) \in \mathbb{Z}_q^* \]

store the hash value in \( H2 \)-list
Proof of Lemma 1 (cont.)

Select \( r_i \in \mathbb{Z}_q^* \) as the secret key.

Compute

\[
pk_{id_i} = r_i P_2, \quad pk_{id_i}' = r_i (P_{pub} + Q_{id_i} P_2)
\]

\[
d_{id_i} = \sigma_i' = \frac{1}{s + m_i'} P_1 (= \frac{1}{s + Q_{id_i} + H_1(ID_i || pk_{id_i})} P_1)
\]

where \( H_1(ID_i || pk_{id_i}) = m_i' - Q_{id_i} \)
Proof of Lemma 1 (cont.)

If $\mathcal{ID}_i$ has been created
Replace the original public key tuple with
$(\tilde{p}k_{\mathcal{ID}_i}, \tilde{p}k_{\mathcal{ID}_i}^{'})$
Store the corresponding secret key $\tilde{r}_i$
and partial private key

$S = \frac{1}{r_i + h}d_{\mathcal{ID}_i}$, where $h = H_2(m, pk_{\mathcal{ID}_i})$
Proof of Lemma 1 (cont.)

Given $(ID^*, m^*, \sigma^* = S^*, pk_{ID^*}, pk_{ID^*}')$:

\[ m^* = Q_{ID^*} + H_1(ID^* || pk_{ID^*} \) \]

\[ \tilde{\sigma}^* = (r^* + h^*) S^* \]

where \( h^* = H_2(m^*, pk_{ID^*}) \)

Output

\[ (m^*, \sigma^*) \]
Lemma 2

Lemma

If Boneh-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 of Lemma 2

\[ \sigma_i' = \frac{1}{r + m_i} P_1 \]

\( r \) be the secret key of ID'

\[ pk_{ID} \cdot \lambda = (rP_2) \]

Select \( s \) as the master secret key of KGC

\( \{ k, G_1, G_2, e, q, P_2, g, P_{pub}(=sP_2) \} \)

\[ d_{ID} = \frac{1}{s + Q_{ID} + H_1(ID' \parallel pk_{ID}')} P_1 \]

\[ pk'_{ID} = (s + Q_{ID}) \lambda = r(P_{pub} + Q_{ID}, P_2) \]
Proof of Lemma 2 (cont.)

\[ H_1(\alpha) \in \mathbb{Z}_q^* \]
store the hash value in \( H1 \)-list

\[ H_2(m_i, pk_{ID}) = m_i' \]
and store \( H_2(m_i, pk_{ID}) \) in \( H2 \)-list
Proof of Lemma 2 (cont.)

\[ \mathcal{A}_C \]

Select \( r_i \in \mathbb{Z}_q^* \) as the secret key

Compute \( \text{pk}_{ID_i} = r_i P_2, \text{pk}_{ID_i}' = r_i (P_{pub} + Q_{ID_i} P_2) \)

\[ d_{ID_i} = \frac{1}{s + Q_{ID_i} + H_1(ID_i || \text{pk}_{ID_i})} P_1 \]

\[ \text{RevealPartialKey} \]

\[ \text{RevealSecretKey} \]

If \( ID_i = ID_i' \) ignore
Proof of Lemma 2 (cont.)

If $ID_i \neq ID'$

\[
S = \frac{1}{r_i + h} d_{id_i}
\]

where $h = H_2(m, pk_{id_i})$

If $ID_i = ID'$

\[
S = \frac{1}{s + Q_{id'} + H_1(ID' || p_{id_i})} \sigma_i'
\]

where $\sigma_i' = \frac{1}{r + m_i'} P_1$

$H_2(m, pk_{id_i}) = m_i'$
Proof of Lemma 2 (cont.)

\[ (ID^*, m^*, \sigma^* (= S^*, pk_{ID^*}, pk_{ID^*}')) \]

\[ m^* = Q_{ID^*} + H_1 (ID^* \parallel pk_{ID^*}) \]
\[ \tilde{\sigma}^* = (s + Q_{ID^*} + H_1 (ID' \parallel pk_{ID^*})) S^* \]
where \( h^* = H_2 (m^*, pk_{ID^*}) \)

\[ (m^*, \tilde{\sigma}^*) \]
Theorem 2

Theorem

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 of Theorem 2

\[ \mathcal{A}_C \]

\[ \mathcal{A}_S \]

\[ \text{Boneh-Boyen Signature} \]

\[ \sigma'_1, \ldots, \sigma'_q \]

\[ PK = (P_1, P_2, \lambda, e(P_1, P_2)) \]

\[ \sigma'_i = \frac{1}{s + m_i} P_1 \]

\[ s \] be the master secret key of KGC

\[ \lambda = sP_2 \]

\[ \{ k, G_1, G_2, e, q, P_2, g, P_{pub}(=\lambda) \} \]
Proof of Theorem 2 (cont.)

$A_C$  

$ID_i$  

$A_S$  

CreatUser  

Each $ID$ only once  

Hash Oracles  

RevealPartialKey  

RevealSecretKey  

ReplaceKey  

Sign  

The same as Game I
Proof of Theorem 2 (cont.)

If $ID^*$ has been created and $(pk_{ID^*}, pk_{ID^*}')$ is different from the public keys created by CreateUser and ReplaceKey queries

$$\tilde{m}^* = Q_{ID^*} + H_1(ID^* || pk_{ID^*})$$

$$\tilde{\sigma}^* = d_{ID^*}$$

$$\textbf{Output}$$

$(d_{ID^*}, r^*), (pk_{ID^*}, pk_{ID^*}')$
The weakness of the security proof of Du-Wen scheme and its security flaw has been discussed.

An improved certificateless signature scheme based on Boneh-Boyen signature scheme are proposed to achieve Girault’s level-3 security.

The security proofs to demonstrate Girault’s level-3 security are proposed.
Thank You!!