Identity-Based Parallel Key-Insulated Proxy Signature Without Random Oracles

Jianhong Chen*
1 Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huaian 223003, China
* 1395996433@qq.com

Abstract. Exposure of private keys is the dangerous attack in the public key cryptosystems. We put forward an identity-based parallel key-insulated proxy signature (IBPKIPS) scheme to deal with the problem of key exposure in the identity-based proxy signature system. Our IBPKIPS scheme is secure without random oracles. In the IBPKIPS scheme, we use two different helper keys to renew the temporary private keys. Our IBPKIPS scheme is more flexible than the identity-based proxy signature scheme.

1. Introduction
Security is harmed by inadvertent loss of private keys. The key insulation mechanism [2] was put forward in 2002. The key insulation mechanism is a key-evolving protocol and protects private keys in public key cryptosystems. Parallel key-insulation [3] was given in 2006. Parallel key-insulation in which two distinct helpers are used is the variant of key insulation. The proxy signature system [4] where the original signer delegates the signing right to the proxy signer was proposed in 1996. The identity-based key-insulated proxy signature (IBKIPS) [1] scheme where the key-insulated mechanism is used to protect the private keys was given in 2011. However, The IBKIPS scheme has some pitfalls and is not secure in some scenarios because only one helper is used. In these scenarios, two helpers can be used to enhance the security. To deal with the the problem of key exposure when at least two helpers are needed to evolve the secret keys, we put forward an identity-based parallel key-insulated proxy signature (IBPKIPS) scheme. The IBPKIPS scheme is secure without random oracles.

2. Model of IBPKIPS
2.1. Definition of IBPKIPS
In our paper, $\mathbb{Z}_p^*$, $x \in \mathbb{R}$, bilinear pairings, CDH assumption and PRF[1] are used. The definition can be seen in Chen et al.’s paper [1]. Our IBPKIPS scheme includes the following algorithms:

I. Generation of master secret key and public parameters: this algorithm is used by the private key generator; the input is the security parameter; the output is a master secret key and the public parameters.

II. Extracton of initial private key and helper keys: this algorithm is used by the private key generator; the input is the user’s identity; the output is an initial private key and and the two helper keys of the user.
III. Renewal of key-update information: this algorithm is used by the i-th helper of the user where i = t mod 2; the input is a period index t, the user's identity and the i-th helper key; the output is the update key of the user and period index.

IV. Renewal of temporary private keys: this algorithm is used by the user; the input is the period index, the user’s identity, the temporary private key of i-1 and the update key of the user and period index t; the output is the temporary private key.

V. Delegation of signature: this algorithm is used by the original signer; the input is the period index, the temporary private key of the original signer and the period index, and the warrant which means the delegation relation; the output is the period index and the proxy certificate which make a tuple.

VI. Verification of the proxy certificate: this algorithm is used by the verifier; the input is the original signer’s identity and the proxy certificate tuple; the output is “continues” or “terminates the protocol”.

VII. Renewal of temporal proxy private keys: this algorithm is used by the proxy signer; the input is the proxy certificate tuple and the period index; the output is the temporal proxy private key of the proxy signer.

VIII. Generation of proxy signature: this algorithm is used by the proxy signer in the time period; the input is the message, the warrant and the temporary private key; the output is the period index, the proxy certificate and the proxy signature which make a tuple.

IX. Verification of the proxy signature: this algorithm is used by the verifier; the input is the original signer’s identity and the proxy signer’s identity, the warrant w, the message and the candidate proxy signature tuple; the output is 1 or 0.

2.2. Security notions for IBPKIPS
We omit the security notions of our proposed identity-based parallel key-insulated proxy signature since the security notions can be gotten according to the proof of the identity-based key-insulated proxy signature [1] and the parallel key-insulated public key encryption [3].

3. Our Proposed IBPKIPS Scheme
I. Generation of master secret key and public parameters:
(1) Group G_1 and group G_2 are both groups of prime order p of size κ. e: G_1 × G_1 → G_2 is a bilinear pairing.
(2) F is a pseudo-random function of a κ-bit seed s and a κ-bit argument and outputs a κ-bit string F_s(s).
(3) H_{κ}: {0,1}^∗ → {0,1}^κ is a collision-resistant hash function with n_{κ} ∈ Z_κ.
(4) Get α ∈ R Z_p^∗; let g_1 = g^α; get g_2 ∈ R G_1.
(5) Get u', v', m' ∈ R G_1; let U = (u_i) of length n_u; let V = (v_i) length n_v; let M = (m_i) of length n_m; u_i, v_i and v_i are all random elements of G_1.
(6) The public parameters are (G_1, G_2, e, g, g_1, g_2, u', U, v', V, m', M).
(7) The master secret is g_2^α are the master secret.

II. Extractor of initial private key and helper keys:
(1) u is an identity and a bitstring of length n_u; u[i] is the i-th bit of the identity.
(2) U_u = {1,2, ... , n_u} is the set of indices k and u[k] = 1.
(3) u_0 is the output of H_0(u,0).
(4) u_0[i] is the i-th bit of u_0.
(5) U_{u,0} = {1,2, ... , n_u} is the set of indices k and u_0[i] = 1.
(6) u_1 is the output of H_0(u,1) and let u_1[i] is the i-th bit of u_1.
(7) U_{u,1} = {1,2, ... , n_u} is the set of indices k such that u_1[i] = 1.
(8) $hk_{u,0}, hk_{u,1} \in \mathbb{R}\{0,1\}^k$, $k_{u,1} = F_{hk_{u,1}}(-1||u)$, $k_{u,0} = F_{hk_{u,0}}(0||u)$. $r_u \in \mathbb{R}Z_p$, let the initial private key, $d_{u,0}$, of the identity $u$ be

$$d_{u,0} = (d_{u,0}^{(1)}, d_{u,0}^{(2)}, d_{u,0}^{(3)}, d_{u,0}^{(4)})$$

$$= (g_u^a (u \prod_{i \in \lambda_u} u_i)^k, (u' \prod_{i \in \lambda_{u,1}} u_i)^k, g_{k_{u,1}}, g_{k_{u,0}}, g_{r_u})$$

$hk_o$ is the helper key of the original signer. Let the initial private key $d_{o,0}$ of the original signer be

$$d_{o,0} = (d_{o,0}^{(1)}, d_{o,0}^{(2)}, d_{o,0}^{(3)}, d_{o,0}^{(4)})$$

$$= (g_o^a (u' \prod_{i \in \lambda_o} u_i)^g, (u' \prod_{i \in \lambda_{o,1}} u_i)^g, g_{k_{o,1}}, g_{k_{o,0}}, g_{r_o})$$

$hk_p$ is the helper key of the proxy signer. Let the initial private key $d_{p,0}$ of the proxy signer be

$$d_{p,0} = (d_{p,0}^{(1)}, d_{p,0}^{(2)}, d_{p,0}^{(3)}, d_{p,0}^{(4)})$$

$$= (g_p^a (u' \prod_{i \in \lambda_p} u_i)^g, (u' \prod_{i \in \lambda_{p,1}} u_i)^g, g_{k_{p,1}}, g_{k_{p,0}}, g_{r_o})$$

III. Renewal of key-update information:

1. The output of $H_o(u,t)$ is $u_t$: the $i$th bit of $u_t$ is $u_t[i]$.
2. The set of indices $i$ ($u_t[i] = 1$) is $\mathcal{U}_{u,t} \subseteq \{1, 2, \ldots, n_u\}$.
3. The output of $H_o(u,t')$ is $u_{t'}$: the $i$th bit of $u_{t'}$ is $u_{t'}[i]$.
4. The set of indices $i$ ($u_{t'}[i] = 1$) is $\mathcal{U}_{u,t'} \subseteq \{1, 2, \ldots, n_u\}$.
5. $k_{u,t} = F_{hk_{u,1}}(t-2||u)$, $k_{u,t} = F_{hk_{u,1}}(t||u)$
6. $u_{i,t}$ is the key-update information for identity $u$ from and period $t$ where

$$u_{i,t} = (u_{i,t}^{(1)}, u_{i,t}^{(2)}) = (u' \prod_{i \in \lambda_{u,t}} u_i)^{k_{u,t}} / (u' \prod_{i \in \lambda_{u,t}} u_i)^{k_{u,t}}$$

Here $u_{i,t}$ is the original signer’s key-update information for $t$ and $u_{i,p,t}$ is the proxy signer’s key-update information for $t$.

IV. Renewal of temporary private keys:

1. Let the temporary private key of time period $t-1$ be

$$(d_{u,t-1}^{(1)}, d_{u,t-1}^{(2)}, d_{u,t-1}^{(3)}, d_{u,t-1}^{(4)})$$

2. Let the temporary private key of time period $t$ be

$$(d_{u,t}^{(1)}, d_{u,t}^{(2)}, d_{u,t}^{(3)}, d_{u,t}^{(4)})$$

$$= (d_{u,t-1}^{(1)}, u_{i,t}^{(1)}, d_{u,t}^{(2)}, d_{u,t-1}^{(4)})$$

$$= (d_{u,t}^{(1)}, d_{u,t}^{(2)}, d_{u,t}^{(3)}, d_{u,t}^{(4)})$$

Here $d_{o,t}$ is the original signer’s temporary private key for $t$ and $d_{p,t}$ is the proxy signer’s temporary private key for $t$.

V. Delegation of signature:

1. The warrant that means the delegation is $w$ and a bit string of length $n_r$.
2. The $j$th bit of $w$ is $w[j]$.
3. The set of indices $j$ ($w[j] = 1$) is $V_w \subseteq \{1, 2, \ldots, n_r\}$.
4. The warrant $w$ is used by the original signer in time period $t$.
5. Get $r_{t-1}, r_t \in \mathbb{R}Z_p$. t
(6) \((t, W) = (t, (w, \sigma_5))\) is the proxy certificate tuple where
\[
\sigma_5 = (\sigma_{n_1}, \sigma_{n_2}, \sigma_{n_3}, \sigma_{n_4}, \sigma_{n_5})
\]
\[
= (d_{g_{p}, i}^{(l)} (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, d_{g_{p}, i}^{(l)} (v' \prod_{j=1}^{n-1} v_j)^{v_{j}}),
\]
\[
= (g_2^a (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}).
\]

VI. Verification of the proxy certificate:
If \(e(g, \sigma_{n_1}) = e(g, g_2) e(\sigma_{n_2}, u' \prod_{i=1}^{n-1} u_i) e(\sigma_{n_3}, u' \prod_{i=1}^{n-1} u_i) e(\sigma_{n_5}, v' \prod_{j=1}^{n-1} v_j)\), the proxy certificate tuple will be valid and the proxy signer will say “accept and go on”. Else, the proxy signer will say “terminate”.

VII. Renewal of temporary proxy private keys:
(1) \(r'_1, r'_2, r'_3 \in \mathbb{Z}_p\).
(2) Let the temporary proxy private key of \(t, \text{tskp}_t\) be
\[
\text{tskp}_t^{(1)}, \text{tskp}_t^{(2)}, \text{tskp}_t^{(3)}, \text{tskp}_t^{(4)}, \text{tskp}_t^{(5)}, \text{tskp}_t^{(6)}, \text{tskp}_t^{(7)}, \text{tskp}_t^{(8)}
\]
\[
= (\sigma_{n_1} d_{g_{p}, i}^{(l)} (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, d_{g_{p}, i}^{(l)} (v' \prod_{j=1}^{n-1} v_j)^{v_{j}}, \sigma_{n_2}, \sigma_{n_3}, d_{g_{p}, i}^{(l)} g^{v_{j}}, d_{g_{p}, i}^{(l)} g^{v_{j}}, \sigma_{n_4}, d_{g_{p}, i}^{(l)} \sigma_{n_5} g^{v_{j}}
\]
\[
= (g_2^a (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}).
\]

VIII. Generation of proxy signature:
(1) The message is \(m\) and a bit string of length \(n_m\).
(2) The \(k\)th bit of \(m\) is \(m[k]\).
(3) The \(k\) is \(1 \leq k \leq n_m\).
(4) Let \(\text{tksp}_t\) be \(\text{tskp}_t^{(1)}, \text{tskp}_t^{(2)}, \text{tskp}_t^{(3)}, \text{tskp}_t^{(4)}, \text{tskp}_t^{(5)}, \text{tskp}_t^{(6)}, \text{tskp}_t^{(7)}, \text{tskp}_t^{(8)}\).
(5) \(r_m, r'_1, r'_2, r'_3 \in \mathbb{Z}_p\).
(6) \(r'_1 = k_{a_1}, r'_2 = r'_3 = r'_4, r'_5 = r'_6 = r'_7 = k_{a_2}, r'_8 = r'_9 = r'_10 = k_{a_3}\).
(7) Let \(\sigma_p\) be
\[
\sigma_p = \text{tskp}_t^{(1)} (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}, (u' \prod_{i=1}^{n-1} u_i)^{v_{j}}.
\]
(8) \(t, w\) and \(\sigma_p\) make the proxy signature tuple \((t, w, \sigma_p)\).

IX. Verification of the proxy signature:
(1) If the message \(m\) is the required quality of the warrant, go on. Else, terminate.
(2) If the proxy signer is permitted by the original signer in the warrant, go on. Else, terminate.

(3) Let \( \sigma_p \) be \( (\sigma_{p1}, \sigma_{p2}, \sigma_{p3}, \sigma_{p4}, \sigma_{p5}, \sigma_{p6}, \sigma_{p7}, \sigma_{p8}, \sigma_{p9}) \)

(4) The verifier will say “accept” and output 1 when

\[
 e(\sigma_{p1}, g) = e(g_1, g_2)^{e(u' \prod_{i \in \mathcal{I}_u} u_i \cdot \sigma_{p4})} e(u' \prod_{i \in \mathcal{I}_p} u_i \cdot \sigma_{p2}) e(u' \prod_{i \in \mathcal{I}_{u+1}} u_i \cdot \sigma_{p3}) e(u' \prod_{i \in \mathcal{I}_{p+1}} u_i \cdot \sigma_{p4})
\]

Else, the verifier will say “reject” and output 0.

4. Security
We omit the proof of our proposed identity-based parallel key-insulated proxy signature because the proof can be gotten according to the proof of the identity-based key-insulated proxy signature [1] and the parallel key-insulated public key encryption [3].

5. Conclusion
We devised the first identity-based parallel key-insulated proxy signature scheme, a novel identity-based proxy signature scheme. In our identity-based parallel key-insulated proxy signature scheme, the private key is protected by the mechanism of parallel key insulation.

References
[1] Chen, J., Chen, K., Wang, Y. (2011) Identity-Based Key-Insulated Proxy Signature Without Random Oracles. Journal of Shanghai Jiaotong University (Science), 5: 557–566.
[2] Dodis, Y., Katz J., Xu, S., Yung, M. (2002) Key-Insulated Public-Key Cryptosystem. In: Knudsen, R. (Eds.), Eurocrypt 2002. Springer, Heidelberg. pp. 65-82.
[3] Hanaoka, G., Hanaoka Y., Imai, H. (2006) Parallel key-insulated public key encryption. In: Yung, M., Dodis, Y., Kiayias, A., Malkin T. (Eds.), PKC 2006. Springer, Heidelberg. pp. 105-122.
[4] Manbo, M., Usuda, K., Okamoto, E. (1996) Proxy Signature: Delegation of the power to sign message. IEICE Transactions on Fundamentals of Electronic Communications and Computer Science, E79-A (9): 1338-1354.