Identity-Based Proxy Signing Key Insulated Signature in the Standard Model

Jianhong Chen* 1

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

Abstract. The first signer arranges for an agent to generate a proxy private key using an identity based proxy signature (IBPS) scheme. The agent outputs the proxy signature for the first signer can generate the signature for the original signer using the proxy private key. Because the potential problem of information security must be taken into account with the development of network technology, the proxy private key needed to be protected. We propose an identity-based proxy signing key-insulated proxy signature (IBPSKIPS) scheme to prevent the proxy private key from being exposed.

1. Introduction
Loss of proxy secret keys is harmful to information security. A method to revoke users from the system is important to PKI or Identity-based setting if their secret keys are in danger. The revocation of identity based encryption was studied by Boldyreva et al. [1] in 2006. Key exposures cannot be avoided with the growth of mobile devices. If private keys are in danger, all security will not be guaranteed. A mechanism of key insulation was put forward by Dodis et al. [2] to solve the problem of the exposure of private keys. The owners of private keys can use insulation mechanism to protect their keys. In Dodis et al.’s secure system, there are long-lived keys and short-lived keys. Long-lived keys are used by the owner. Short-lived keys are saved in an ancillary container. The mechanism of parallel key insulation [3, 4] was put forward in the scenario in which many ancillary containers were used to refresh the short-lived keys. The mechanism of threshold key insulation [5] was put forward in the scenario in which the threshold of the number of the ancillary containers needed to reached to refresh the short-lived keys.

The first signer arranges for an agent to output a proxy private key using an identity based proxy signature (IBPS) scheme [6, 7]. The agent generates the proxy signature for the first signer can generate the signature for the original signer using the proxy private key. Some researchers [8-9] used the mechanism of key insulation and put forward proxy signature schemes in the identity-based scenario. In their proxy signature scheme, both the first signer’ secret key and the agent’s secret key are refreshed. Then Chen [10] modified their proxy signature scheme to make them secure in the scenario in which many ancillary devices were used to refresh the provisional keys. Chen’s scheme [9] is less efficient because both the original signing keys and the proxy signing keys are updated. However, only proxy signing keys must be updated in some scenarios. We put forward an IBPSKIPS scheme to prevent the proxy private key from being framed. In our proposed IBPSKIPS scheme, only proxy signing keys are updated. Our IBPSKIPS scheme is more efficient and useful for practical use.
2. Definitions

- Setup: similar to that of the IBKIPS [9].
  - Extraction: The creator of secret keys creates the key of the first signer, the earliest short-lived key of the agent and an ancillary key. The first signer saves his key in his private device. The agent saves his earliest short-lived key in his private device. The ancillary key is stored in the subsidiary container.
  - HelperUpdate: The subsidiary container creates the refreshing data from \( t' \) and \( t \) for the agent. The refreshing data is saved in the ancillary container.
  - UserUpdate: The agent creates the short-lived keys for himself using the refreshing data from \( t' \) and \( t \) for the agent in the subsidiary container. The agent saves his new short-lived key in his private device.
  - Delegation: The first signer creates the proxy proof for the agent. The agent saves the proxy proof in his private device.
  - DVerification: The agent verifies the proxy proof so that he can know whether the proxy proof is generated by the first signer.
  - PGeneration: similar to that of the IBKIPS [9].
  - PSigning: similar to that of the IBKIPS [9].
  - PVerification: similar to that of the IBKIPS [9].

The definition of security is similar to that of the IBKIPS [9].

3. The proposed scheme

- There are nine parts in the scheme.

  1. Setup: \( \mathcal{O}1 \) and \( \mathcal{O}2 \) are groups. Both their prime orders are \( b \) of size \( k \). \( BP \) is a bilinear pairing of \( \mathcal{O}1 \) and \( \mathcal{O}2 \). \( PRF \) is a pseudo-random function. \( HFU : \{0,1\}^* \rightarrow \{0,1\}^{w*} \) is a collision-resistant hash function. Vectors \( X=x_i \), \( Y=y_i \), \( Z=z_i \) are of length \( nx \), \( ny \), \( nz \), respectively. \( a \) is a random element of \( Z^* \). Let \( g_i=g^a \). Let \( x,y,z \in \mathbb{Z} \) and \( g_i=g^a \). Public data is \( pd=(\mathcal{O}1, \mathcal{O}2, BP, g, g_1, g_2, x, X, y, Y, z, Z) \) and secret data is \( g^2 \).

  2. Extraction: \( x \) is a bitstring of length \( nx \), and \( p \) stands for an index. \( X_p \) is a subset of \( \{ 1, 2, \ldots, n_x \} \) and \( X_p \) is a set in which \( x_i = 1 \). \( hkp_0 \) is a random element of \( \{ 0,1 \}^k \). The creator of secret keys creates \( K_0 \rightarrow F_{hkp} \). \( g, rp \) are random elements of \( Z_b \). The agent’s ancillary key is \( hkp_0 \) and his earliest short-lived key is as follows.

\[
\begin{align*}
d_{p,0} & = (d_{p,1,0}, d_{p,2,0}, d_{p,3,0}) \\
& = (g_{2,0}^{(x' \prod_{i \in X_p} x_i)} g_{2,0}^{x' \prod_{i \in X_p} x_{i_2}}, g_{2,0}^{x' \prod_{i \in X_p} x_{i_2}}, g_{2,0}^{x' \prod_{i \in X_p} x_{i_2}}).
\end{align*}
\]

  3. HelperUpdate: \( p_i \) is the output of \( HFU (p, t') \). \( p_i[i] \) is the ith bit of \( p \). \( U_i \subset \{ 1, 2, \ldots, n_x \} \) is the set of indices \( i \) \( ( p_i[i] = 1 ) \). \( p_i \) is the output of \( HFU (p, t') \). \( pr[i] \) is the ith bit of \( pr \). \( U_p \subset \{ 1, 2, \ldots, n_w \} \) is the set of indices \( i ( p_r[i] = 1 ) \). The auxiliary device of the agent first generates \( kpt=PRF ( t' || p ) \) and \( kpt=PRF ( t' || p ) \). Then the auxiliary device generates the refreshing data from \( t' \) and \( t \) for the agent as follows.

\[
\begin{align*}
u_{p, t'} & = (u_{p, t', u_{p, t', x}}, u_{p, t', x}) \\
& = (u' \prod_{i \in X_p} u_{i_2}, u' \prod_{i \in X_p} u_{i_2}, u' \prod_{i \in X_p} u_{i_2}).
\end{align*}
\]

  4. UserUpdate: \( d_{p, t} \) is \( (d_{p,1,t}, d_{p,2,t}, d_{p,3,t}) \). \( d_{p,t} \) is \( (d_{p,1,t}, d_{p,2,t}, d_{p,3,t}) = (d_{p,1,t}, u_{p, t' u_{p, t', x}}, u_{p, t' u_{p, t', x}}, d_{p,3,t}) \).

During the time period \( t \),

\[
\begin{align*}
d_{p, t} &= (d_{p,1,t}, d_{p,2,t}, d_{p,3,t}) = (g_{2,0}^{x' \prod_{i \in X_p} u_{i_2}}, g_{2,0}^{x' \prod_{i \in X_p} u_{i_2}}, g_{2,0}^{x' \prod_{i \in X_p} u_{i_2}}).
\end{align*}
\]

  5. Delegation: \( y \) is a bit string of length \( ny \) and \( y \) is the warrant. There is a clear proof of the delegation relationship between the first signer and the agent. \( y[j] \) is the \( j \)th bit of \( y \). \( w \) is a subset of \( \{ 1, 2, \ldots, n_y \} \). \( y[j] = 1 \). During the time period \( t \), the first signer generates a warrant \( w, r, r_y \) are random elements of \( Z_b \). The first signer generates the proxy proof as follows.
\[ \sigma_v = (\sigma_{v1}, \sigma_{v2}, \sigma_{v3}) = (d_{v1} (x' \prod_{i \in I_{v1}} x_i)^{x}, d_{v2}, g^{\sigma}) \]

\[ = (g_{v}^{2a} (x' \prod_{i \in I_{v1}} x_i)^{x}, (y' \prod_{j \in I_{v2}} y_j)^{y}, g^{\sigma}, g^{\sigma}) \]

The first signer gives the proof tuple \((t, Y) = (t(w, \sigma_v))\) to the agent.

(6) DVerification: The agent will think that proxy proof is valid if the following equation makes sense. The agent will not accept the proof if the following equation doesn’t make sense.

\[ BP(g_{v}, \sigma_v) = BP(g_{1}, g_{2}) BP(\sigma_{v2}, x' \prod_{i \in I_{v1}} x_i) BP(\sigma_{v3}, y' \prod_{j \in I_{v2}} y_j). \]

(7) PGeneration: \(r_v, r_v'\) are random elements of \(Z_b\). The agent generates the short-lived key as follows.

\[ Tskp_r = \{ tskp^{(1)}, tskp^{(2)}, tskp^{(3)}, tskp^{(4)}, tskp^{(5)}, tskp^{(6)} \} \]

\[ = (\sigma_{01} d_{p1} (x' \prod_{i \in I_{p1}} u_i)^{\sigma_1}, \sigma_{02}, d_{p2}, g^{\sigma_2}, \sigma_{03}, d_{p3}, \sigma_{04} g^{\sigma_3}) \]

\[ = (g_{2a}^{2a} (x' \prod_{i \in I_{p1}} x_i)^{x}, (y' \prod_{j \in I_{p2}} x_i)^{y}, g^{\sigma_2}, g^{\sigma_3}). \]

(8) PSign: \(z\) be a bit string of length \(n_z\). \(z\) stands for the message. \(z[k]\) be the \(k\)th bit of \(z\). \(Z_e\) is the subset of \(\{1, 2, \ldots, n_z\}\). \(r_z, r_z'\) are random elements of \(Z_{p}^{e}\). The agent generates the signature as follows.

\[ \sigma_{0} = (\sigma_{p1}, \sigma_{p2}, \sigma_{p3}, \sigma_{p4}, \sigma_{p5}, \sigma_{p6}) \]

\[ = (tskp^{(1)}(x' \prod_{i \in I_{p1}} x_i)^{x}, tskp^{(2)}, tskp^{(3)}, g^{\sigma_1}, g^{\sigma_2}, \sigma_{p3}, \sigma_{p4}, \sigma_{p5}, \sigma_{p6}) \]

\[ = (g_{2a}^{2a} (x' \prod_{i \in I_{p1}} x_i)^{x}, (y' \prod_{j \in I_{p2}} x_i)^{y}, g^{\sigma_1}, g^{\sigma_2}, g^{\sigma_3}, g^{\sigma_4}, g^{\sigma_5}, g^{\sigma_6}). \]

In the above signature, \(T_{t} = k_{p1} r_z + r_z'\) and \(T_{v} = r_v + r_v'. \)

(9) PVerification: The verifier will think that signature is valid if the following equation makes sense. The verifier will not accept the signature if the following equation doesn’t make sense.

\[ BP(\sigma_{p1}, g) \]

\[ = BP(g_{1}, g_{2}) BP(x' \prod_{i \in I_{p1}} x_i, \sigma_{p3}) BP(x' \prod_{i \in I_{p1}} x_i, \sigma_{p4}) BP(x' \prod_{i \in I_{p1}} x_i, \sigma_{p5}) BP((y' \prod_{j \in I_{p2}} y_j)^{y}, \sigma_{p6}) \]

\[ BP(z' \prod_{k \in I_z} z_k, \sigma_{p6}) \]

The correctness of the scheme is as follows.

\[ BP(\sigma_{p1}, g) \]

\[ = BP(g_{2a}^{2a} (x' \prod_{i \in I_{p1}} x_i)^{x}, (y' \prod_{j \in I_{p2}} x_i)^{y}, g^{\sigma_1}, g^{\sigma_2}, g^{\sigma_3}, g^{\sigma_4}, g^{\sigma_5}, g^{\sigma_6}) \]

\[ = BP(g_{2a}^{2a} g) BP(((x' \prod_{i \in I_{p1}} x_i)^{x}, g) BP((x' \prod_{i \in I_{p1}} x_i)^{x}, g) BP((y' \prod_{j \in I_{p2}} y_j)^{y}, g) \]

\[ BP((z' \prod_{k \in I_z} z_k)^{x}, g) \]
There is a performance comparison between the proposed scheme and other schemes in TABLE I.

**TABLE I. A PERFORMANCE COMPARISON WITH OTHER IBPKIS SCHEMES**

| Scheme                | Proxy signature length | Proxy signature issuing | Verification of proxy signature |
|-----------------------|------------------------|-------------------------|---------------------------------|
| Proposed Scheme       | $1|t|+8|=G_1$            | $4t_p$                  | $9t_p$                          |
| The scheme in [9]     | $1|t|+9|=G_1$            | $5t_p$                  | $10t_p$                         |

4. Conclusion

An identity-based proxy signing key insulated proxy signature scheme in the standard model is put forward in this paper. In the proposed scheme, the short-lived secret keys of the agent are refreshed periodically.

Acknowledgments

We are particularly grateful to the reviewers for their important commentary.

References

[1] A. Boldyreva, V. Goyal, and B. Waters., “Identity-based encryption with efficient revocation,” in CCS 2008, P. F. Syverson and S. Jha, Eds. ACM, 2008, pp. 417–426.
[2] Y. Dodis, J. Katz, S. Xu, and M. Yung, “Key-Insulated Public-Key Cryptosystem,” in Eurocrypt 2002, R. Knudsen, Eds. Springer, Heidelberg, 2002, pp. 65–82.
[3] G. Hanaoka, Y. Hanaoka, and H. Imai, “Parallel key-insulated public key encryption,” in PKC 2006, M. Yung, Y. Dodis, A. Kiayias and T. Malkin, Eds. Springer, Heidelberg, 2006, pp. 105-122.
[4] J. Weng, S. Liu, K. Chen and X. Li, “Identity-Based Parallel Key-Insulated Signature: Framework and Construction,” Journal of Research and Practice in Information Technology, vol. 40(1), pp. 55-68, 2008.
[5] J. Weng, S. Liu, K. Chen, D. Zheng, W. Qiu, “Key-Insulated Public-Key Cryptosystem,” in CT-RSA 2008, T. Malkin, Ed. Springer, Heidelberg, 2008, pp. 203-220.
[6] M. Manbo, K. Usuda, and E. Okamoto, “Proxy Signature: Delegation of the power to sign message,” IEICE Transactions on Fundamentals of Electronic Communications and Computer Science, E79-A (9), pp. 1338-1354, 1996.
[7] F. Zhang and F. Kim, “Efficient ID-Based Blind Signature and Proxy Signature from Bilinear Pairings,” in ACISP 2003, S. Safavi-Naini and J. Seberry Eds. Springer, Heidelberg, 2003, pp. 312-323.
[8] Z. Wan, X. Lai, J. Weng, S. Liu and X. Hong, “Identity-Based Key-Insulated Proxy Signature,” Journal of Electronics (China), vol. 26(6), pp. 853-858, 2009.
[9] J. Chen, K. Chen, and Y. Wang, “Identity-Based Key-Insulated Proxy Signature Without Random Oracles,” Journal of Shanghai Jiaotong University (Science), vol. 16(5), pp. 1–9, 2011.
[10] J. Chen, “Identity-Based Parallel Key-Insulated Proxy Signature Without Random Oracles,” Journal of Physics: Conference Series, Series 1325 012111, pp. 1–6, December 2019.