Comment on Security and Improvement of Partial Blind Signature Scheme and Revocable Certificateless Signature Scheme

Xiaoming Hu*, Fangshu Chen, Chuang Ma and Wenan Tan
College of Computer and Information Engineering, Shanghai Polytechnic University, Shanghai, 201209, China
*Corresponding author’s e-mail: xmhu@sspu.edu.cn

Abstract. Partial blind signature scheme (BLD-SS) can protect the specific content of the signed message by adding factor to blind the signed message and can also prevent the misuse of the signature by adding common information negotiated in advance. Revocable certificateless signature scheme (RCSS) can prevent the user’s privacy from leaking by adding time key in the signature process and signature verification process. BLD-SS and RCSS both have wide applications in electronic-voting, electronic-cash system and other fields. In this paper, it presents a security analysis on a partial blind signature scheme and a revocable signature scheme proposed recently. It points out that the BLD-SS does not satisfy the unforgeability. A malicious user can forge a partial blind signature on any message and any common information without known from PKG (Private Key Generation). It also shows that the RCSS does not satisfy the unforgeability. A malicious enemy can forge a signature on any message and on any user. The PKG also cannot update the time key immediately when a user’s key is leaked or his identity is expired. In order to overcome these problems, it proposes some simple improvement methods which are almost the same efficiency with the original signature scheme.

1. Introduction
In a blind signature scheme (BLD-SS) proposed first by Chaum [1], the signer signs a message without knowing the real message because it has been blinded by the signature requestor. When the signature is published, the signer cannot relate the signature to the original message which protects the real content of the signed message. By adding common information negotiated by the signer and the signature requestor in BLD-SS [2-7] which is called partial BLD-SS [8-11], it can prevent the misuse of the signature. Certificateless signature scheme (CSS) [12-16] is another signature with special properties. In a CSS, the private key of the signer consists of two parts from the PKG (Private Key Generation) and the signer itself which can prevent the PKG from generating the private key only itself. In a Revocable certificateless signature scheme (RCSS) [17-19] when a user’s key is leaked or his identity is expired, the PKG can revoke the time key immediately which can protect the user’s privacy.

Due to the excellent properties, many partial BLD-SS and RCSS have been proposed. In [20], He et al. proposes a partial BLD-SS but it is pointed out to be insecure. In [10], Liu et al. proposes a partial BLD-SS. However, Jiang and Deng [21] point out that Liu et al.’s scheme is also not secure because the attacker can tamper the common information. In this paper, we show that Jiang and Deng partial BLD-SS [21] yet is not secure. In [21], a malicious user can forge a blind signature on any
message and any common information. We also point out that Liu et al.’s RCSS [22] is also not secure and the attacker can forge a certificateless signature without being known by PKG. Thus, when a user’s key is leaked or his identity is expired, PKG cannot update the time key immediately. In order to overcome these problems, we also give some simple improved methods.

2. Review and the Security Of Jiang and Deng’s Partial Blind Signature Scheme (BLD-SS)

2.1. Review of Jiang and Deng’s Partial BLD-SS

Jiang and Deng’s partial BLD-SS [21] consists of the following parts.

- **System Initialization Part:** PKG (Private Key Generator) selects two cyclic groups $G_1$ and $G_2$ with prime order $q$, and $P \in G_1$ is the generator element for $G_1$. PKG sets $e : G_1 \times G_1 \rightarrow G_2$ and $E = e(P, P)$. PKG selects $s \in \mathbb{Z}_q^*$ and sets $pubP = sp$. The parameters are $\{q, e, G_1, G_2, P, pubP, H_1, H_2, H_3\}$ to be published publicly and $s$ is kept secretly, where $H_1, H_2 : \{0,1\}^* \rightarrow \mathbb{Z}_q^*$.

- **Partial Key Generation Part:** For the signer $A$, PKG checks its identity $AID$ and then computes its partial private key $AS = P_{IDH}A$ and sends secretly to $A$. $A$ sets $AP = pubP + P_{IDH}A$.

- **Personal Key Generation Part:** $A$ selects $Ax \in \mathbb{Z}_q^*$ and sets its personal public key $APK = e(x, P)$, and its private key is $(AS, Ax)$.

- **Blind Signature Part:** Assume $A$ is the signer with identity $ID_A$ and $B$ is the requester of the signature with identity $ID_B$. $m$ is the message to be signed and $c$ is the common information which is negotiated by $A$ and $B$ in advance. Then $A$ and $B$ performs the following interaction process.

  (1) **Promising:** The signer $A$ selects $k \in \mathbb{Z}_q^*$ and computes $K = e(P, P)e^{H_1(ID_A)}$. $A$ sends $K$ secretly to $B$.

  (2) **Blinding:** After $B$ gets $K$, $B$ selects $\alpha, \beta \in \mathbb{Z}_q^*$ and computes $R = K^{\alpha}PK_A^{\beta}, h = H_2(m, c, R)$, $U = (1 + \alpha^{-1}h + H_3^{\beta}(c))P$. $B$ sends to $A$.

  (3) **Signing:** After $A$ gets $U$, $A$ computes $V' = kS_A + H_3(c)x_AU$ and sends $V'$ to $B$.

  (4) **Unblinding:** After $B$ gets $V'$, $B$ computes $V = \alpha V'$. Then, $\delta = (V, h, R, c)$ is the partial blind signature on message $m$.

- **Signature Verification Part:** After the verifier gets $(\delta = (V, h, R, c), m)$, the verifier checks

  \[ R = e(V, pubP + H_1(ID_A))PK_A^{-H_3(c)}. \]  

2.2. Security Analysis of Jiang and Deng’s Partial BLD-SS

Here, we show the security analysis of Jiang and Deng’s partial BLD-SS [21].

2.2.1. Security Analysis

Here, we show that Jiang and Deng’s partial BLD-SS does not satisfy the unforgeability. A malicious user $A$ can forge a blind signature on any message and any common information. The main process is as following. Assume $m^*$ is the message to be signed and $c^*$ is the common information both selected by the malicious user $A$.

- The malicious user $A$ selects $r^* \in \mathbb{Z}_q^*$ and computes

  \[ R^* = e(r^*P, pubP + H_1(ID_A)) . \]
\[ h^* = H_2(m^*, c^*, R^*) , \]

\[ V^* = r^* P + h^* H_3(c^*) x_A P . \]

Then, \( \delta^* = (V^*, h^*, R^*, c^*) \) is the forged blind signature on message \( m^* \).

- The above forged signature \( (m^*, \delta^* = (V^*, h^*, R^*, c^*) ) \) is correct.

\[ e(V^*, P \text{pub} + H_1(ID_A) P) PK_A^{-k} H_3(c^*) \]

\[ = e(r^* P + h^* H_3(c^*) x_A P, P \text{pub} + H_1(ID_A) P) PK_A^{-k} H_3(c^*) \]

\[ = e(r^* P, P \text{pub} + H_1(ID_A) P)e(h^* H_3(c^*) x_A P, P \text{pub} + H_1(ID_A) P) PK_A^{-k} H_3(c^*) \]

\[ = R^* e(h^* H_3(c^*) x_A P, P \text{pub} + H_1(ID_A) P) PK_A^{-k} H_3(c^*) \]

\[ = R^* e(x_A P, P \text{pub} + H_1(ID_A) P) PK_A^{-k} H_3(c^*) \]

\[ = R^* PK_A^{-k} H_3(c^*) \]

\[ = R^* . \]

2.2.2. Simple Improvement. The key reason that the malicious user can forge a blind signature is because that the malicious user can modify \( V \). So, the key is to limit \( V \). The improved method refers to [23] which is secure and efficient blind signature. But, [23]’s BLD-SS is not partial blindness. Therefore, based on the [23]’s BLD-SS, it needs add common information \( c \) into their BLD-SS. The simple method is to add \( c \) into \( h = H(ID_A, y_A, m) \) of [23]’s BLD-SS. Namely it modifies \( h = H(ID_A, y_A, m) \) to become

\[ h = H(ID_A, y_A, m, c) . \]  

Thus, [23]’s BLD-SS becomes a partial blind signature scheme.

3. Review and the Security Of Liu et al.’s Revocable Certificateless Signature Scheme (RCSS)

Here, we show the security analysis of Liu et al.’s RCSS [22].

3.1. Review of Liu et al.’s RCSS

Liu et al.’s RCSS [22] consists of the following parts.

- Setup System Part: PKG selects one elliptic curve \( E \) with one base point \( G \), and \( P \) is the generator element of \( G \). PKG selects \( s \in R Z_q^* \) and sets \( P \text{pub} = sP \). The parameters are \{ \( q \), \( G \), \( P \), \( P \text{pub} \), \( H_1 \), \( H_2 \) \} to be published publicly and \( s \) is kept secretly, where \( H_1 : \{ 0,1 \}^* \times G^2 \rightarrow Z_q^* \) and \( H_2 : \{ 0,1 \}^* \times G^4 \rightarrow Z_q^* \).

- Secret-Public Key Generation Part: For the user \( ID_i \), \( ID_i \) selects its secret key \( x_i \in R Z_q^* \). \( ID_i \) sets \( PK_i = x_i P \) as its public key.


- **Partial Private Key Generation Part:** For the user $ID_i$, PKG selects $r_i \in_R Z^*_q$ and computes $R_i = r_iP$, $h_i = H_i(ID_i, R_i, P_{pub})$, $d_i = r_i + sh_i$. PKG sends $D_i = (d_i, R_i)$ secretly to $ID_i$ and $ID_i$ makes $D_i$ as its partial private key.
- **Time Key Generation Part:** PKG computes $R_i = r_iP$, $h_i = H_i(ID_i, R_i, P_{pub}, t)$, $s_i = r_i + sh_i$, where $t$ is the system initial time. PKG sends $(R_i, s_i)$ to the user $ID_i$. The user $ID_i$ makes $(R_i, s_i)$ as its time key.
- **Signature Generation Part:** The user $ID_i$ selects $r_i \in_R Z^*_q$ and computes $T_i = t_iP$, $k_i = H_2(ID_i, m, T_i, PK_i, R_i, P_{pub})$, and

$$\sigma_i = t_i + k_i x_i + d_i + s_i.$$  \hfill (3)

Then, $(R_i, T_i, \sigma_i)$ is the signature on message $m$.
- **Signature Verification Part:** After getting a signature $(R_i, T_i, \sigma_i)$ on message $m$, the verifier checks

$$\sigma_i P = T_i + k_i PK_i + 2R_i + h_i P_{pub} + h_i P_{pub}.$$  \hfill (4)



### 3.2. Security Analysis of Liu et al.’s RCSS

#### 3.2.1. Security Analysis

Here, we show that Liu et al.’s RCSS does not satisfy the unforgeability. A malicious enemy $A$ can forge a signature on any message and on any user. The PKG also cannot update the time key immediately when a user’s key is leaked or his identity is expired. The main process is as following. Assume $m^*$ is the message to be signed and $ID_i^*$ (where $PK_i^* = x_i^* P$) is the identity both selected by the malicious user $A$.

- The malicious user $A$ selects $R_i^* \in_R G$, $t_i^*$ and $x_i^* \in_R Z^*_q$. $A$ computes

$$h_i^* = H_i(ID_i^*, R_i^*, P_{pub})$$

$$PK_i^* = x_i^* P$$

$$h_i^* = H_i(ID_i^*, R_i^*, P_{pub}, t)$$

$$T_i^* = t_i^* P - 2R_i^* - h_i^* P_{pub} - h_i^* P_{pub}$$

$$k_i^* = H_2(ID_i^*, m^*, T_i^*, PK_i^*, R_i^*, P_{pub})$$

$$\sigma_i^* = t_i^* + k_i^* x_i^*.$$  \hfill (3)

Then, the malicious user $A$ forges a signature $(R_i^*, T_i^*, \sigma_i^*)$ on message $m^*$.
- $(m^*, (R_i^*, T_i^*, \sigma_i^*))$ is correct.

$$\sigma_i^* P$$

$$= (t_i^* + k_i^* x_i^*) P$$

$$= t_i^* P + k_i^* x_i^* P$$

$$= t_i^* P + k_i^* PK_i^* - 2R_i^* + 2R_i^* - h_i^* P_{pub} + h_i^* P_{pub} - h_i^* P_{pub} + h_i^* P_{pub}$$
\[ t^i_i P - 2R^i_i - h^i_i P^\text{pub} - h^i_i P^\text{pub} + k^i_i PK^\text{pub}_i + 2R^i_i + h^i_i P^\text{pub} + h^i_i P^\text{pub} \]

\[ - T^i_i + k^i_i PK^\text{pub}_i + 2R^i_i + h^i_i P^\text{pub} + h^i_i P^\text{pub}. \]

3.2.2. Simple Improvement. The key reason that the malicious user \( A \) can forge a signature is because that the malicious user \( A \) can replace the public key of the signer \( PK_i = x_i P \) and it can modify \( T_i \). So, the key of the improvement is to limit \( PK_i \). The main process is as following.

- In the improved scheme, Setup System Part, Secret-Public Key Generation Part, Partial Private Key Generation Part, and Time Key Generation Part are the same with the original scheme of Liu et al.’s RCSS [22].

- Signature Generation Part: The user \( ID_i \) selects \( t_i \in \mathbb{Z}_q^* \) and computes

\[
\begin{align*}
T^i_i &= t_i P, \\
k^i_i &= H_2(ID_i, m, T^i_i, PK_i, R^i_i, P^\text{pub}), \\
\sigma^i_i &= (h^i_i + h^i_i)_{T^i_i} + k^i_i x_i + d_i + s_i .
\end{align*}
\]

Then, \( (R^i_i, T^i_i, \sigma^i_i) \) is the signature on message \( m \), where

\[
(h^i_i + h^i_i)_{T^i_i} = H_1(ID_i, R^i_i, P^\text{pub}) , \quad h^i_i = H_1(ID_i, R^i_i, P^\text{pub}, t) .
\]

- Signature Verification Part: After getting a signature \( (R^i_i, T^i_i, \sigma^i_i) \) on message \( m \), the verifier checks

\[
\sigma^i_i P = (h^i_i + h^i_i)_{T^i_i} + k^i_i PK^\text{pub}_i + 2R^i_i + h^i_i P^\text{pub} + h^i_i P^\text{pub} .
\] (5)

- Security and efficiency Analysis. By adding two hash values \( h_i \) and \( h^i_i \) in the signature process \( \sigma^i_i = (h^i_i + h^i_i)_{T^i_i} + k^i_i x_i + d_i + s_i \) and also adding \( h_i \) and \( h^i_i \) in the signature verification process \( \sigma^i_i P = (h^i_i + h^i_i)_{T^i_i} + k^i_i PK^\text{pub}_i + 2R^i_i + h^i_i P^\text{pub} + h^i_i P^\text{pub} \) which makes the malicious user be unable to modify \( T_i \) and replace the public key \( PK^\text{pub}_i \).

The above improvement only adds \((h^i_i + h^i_i)_{T^i_i}\) and \((h^i_i + h^i_i)_{T^i_i}\) two operations. Therefore, the computational cost almost is the same with the original scheme of Liu et al.’s RCSS.

4. Conclusions

In this paper, a partial blind signature scheme that includes common information negotiated by the signer and the signature requester in advance which can prevent the misuse of the signature is analysed on the security. At the same, this paper also analyses the security of a revocable certificateless signature scheme that the time key can be revoked by PKG when the key is leaked or others. By the review and security analysis of their both schemes, this paper shows the two schemes do not satisfy the unforgeability and are not secure by both detail processes. And this paper also makes some simple analysis on the improvement and presents two simple improved methods which not only are efficient but also can overcome the security problems.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No.61103213, 61672022), the Innovation Program of Shanghai Municipal Education Commission (No.14ZZ167), the Key Disciplines of Computer Science and Technology of Shanghai Polytechnic University (No.XXKZD1604).
References

[1] Chaum, D. (1983) Blind Signatures for Untraceable Payments. In: Advances in Cryptology. Springer-Verlag. pp.199-203.

[2] Zhu, H., Tan, Y., Zhu, L., Wang, X., Zhang, Q., Li, Y. (2018) An identity-based anti-quantum privacy-preserving blind authentication in wireless sensor networks. Sensors, 18(5):1663.

[3] Nedal, T., Ashraf, T., Ramzi, A., Talal, E. (2020) Design of identity-based blind signature scheme upon chaotic maps. International Journal of Online and Biomedical Engineering, 16(5):104-118.

[4] Cheon, J.H., Jeong, J., Shin, J.S. (2019) Cryptoanalysis on á round-optimal lattice-based blind signature scheme for cloud services. Fut. Gener. Comput. Syst., 95:100-103.

[5] Girraj, K., Singh, B. (2018) Efficient identity-based blind message recovery signature scheme from pairings. IET Information Security, 12(2):150-156.

[6] Kong, W., Shen, J., Vijayakumar, P., Cho, Y., Chang, V. (2020) A practical group blind signature scheme for privacy protection in smart grid. Journal of Parallel and Distributed Computing, 136:29-39.

[7] Mao, Y., Deng, L. (2017) An identity-based blind signature scheme and its security proof. Computer and Modernization, 4:105-108.

[8] Papachristoudis, D., Hristu-Varsakelis, D., Baldimtsi, F., Stephanides, G. (2019) Leakage-resilient lattice-based partially blind signatures. IET Information Security, 13(6):670-684.

[9] Cao, S., Dai, W., Wang, C., Wang, X., Sun, H., Zuo, W. (2018) Analysis and improvement of an ID-based partially blind signature scheme. Computer Engineering and Science, 40(12):2193-2197.

[10] Liu, E., Zhou, H., Zuo, L., Wang, X. (2016) New in-based partially blind signature scheme without trusted private key generator. Computer Applications and Software, 33(5):285-288.

[11] Niu, S., Li, W., Wang, C. (2020) Partially blind Proxy re-signature scheme without bilinear pairing. Computer Engineering, 46(5):187-192.

[12] Karati, A., Islam, S., Karuppiah, M. (2018) Provably secure and lightweight certificateless signature scheme for IoT environments. IEEE Transactions on Industrial Informatics, 14(8):3701-3711.

[13] L. Ma, Q. Yang, and J. Lai, A certificateless-based aggregated signature scheme with designated verifier property. Henan Science and Technology, vol.717, no.17, pp.10-12, 2020.

[14] Zhang, Y., Deng, R., Zheng, D., et al. (2019) Efficient and robust certificateless signature for data crowd sensing in cloud-assisted industrial IoT. IEEE Transactions On Industrial Informatics, 15(9):5099-5108.

[15] Zuo, L., Chen, Z., Xia, P., et al. (2019) Improved efficient certificateless short signature Scheme. Computer science, 46(4):172-176.

[16] Zuo, L., Zhang, M., Hu, K., et al. (2020) Certificateless Short Signature Scheme with Double KGC. Application Research Of Computers, 37(5):1482-1487.

[17] Zhang, Y., Li, C., Zhou, D., et al. (2015) Efficient revocable certificateless signature scheme. Computer Engineering, 41(7):157-162.

[18] Sun, Y., Zhang, F., Shen, L. (2015) Efficient revocable certificateless signature against signing key exposure. Journal of Software, 26(12):3196-3203.

[19] Jia, X., He, D., Zeadally, S., et al. (2017) Efficient revocable ID based signature with cloud revocation server. IEEE Access, 5:2945-2954.

[20] He, J., Sun, F., Qi, C. (2013) Cryptanalysis and improvement of ID-based partially blind signature scheme. Journal of Computer Applications, 33(3):762-765.

[21] Jiang, Y., Deng, L. (2020) Analysis and improvement of a partial blind signature scheme. Journal of Guizhou Normal University (Natural Sciences), 38(2):85-91.

[22] Liu, Y., Wang, D., Wang, Z., Duan, R. (2020) Efficient revocable certificateless signature scheme for cloud computing. Computer Engineering and Design, 41(9):2442-2446.
[23] Zuo, L., Xia, P., Chen, Z. (2020) A provably secure short blind signature scheme. Computer Engineering, 45(2):114-118.