On the Security of a Certificateless Proxy Signature Scheme in the Standard Model

Caixue Zhou, Xiwei Dong, Lihua Wang, and Tao Li
(Corresponding author: Caixue Zhou)

School of Information Science and Technology, Jiujiang University
551 Qianjin Donglu, Jiujiang 332005, China
(Email: charlesjjjx@126.com)

(Received Dec. 10, 2017; Revised and Accepted Apr. 12, 2018; First Online Mar. 2, 2019)

Abstract

Certificateless cryptosystem can overcome the costly certificate management in the traditional public key cryptosystem, and meanwhile it does not have the private key escrow problem in the identity-based cryptosystem. Proxy signature can allow a proxy signer authorized by an original signer to sign messages on behalf of the latter. In this paper, we show that a recently proposed certificateless proxy signature scheme in the standard model is vulnerable to the public key replacement attack. Through this kind of attack, a malicious original signer or proxy signer can forge a valid proxy signature. We analyse the reasons for the success of the attack and point out the flaw in the proof of the original scheme.

Keywords: Bilinear Pairing; Certificateless Proxy Signature; Public Key Replacement Attack; Standard Model

1 Introduction

Certificateless cryptosystem [17] can simplify the costly certificate management in the traditional public key cryptosystem, and meanwhile to eliminate the private key escrow problem in the identity-based cryptosystem [16]. It has attracted a lot of attention since its introduction.

Proxy signature allows an original signer to delegate his/her signing power to a proxy signer [4,8–12,14,18,23,24]. Then the latter can sign messages on behalf of the former when the former is absent. It has been widely used in practice since its introduction.

By combining the certificateless cryptosystem and proxy signature, Li *et al.* [15] proposed the first certificateless proxy signature scheme by using bilinear pairings in 2005. But unfortunately, Yap *et al.* [25] pointed out that Li *et al.*'s scheme is vulnerable to the public key replacement attack in 2007. In the same year, Lu *et al.* [19] and Choi *et al.* [3] further gave an improvement to Li *et al.*'s scheme, respectively. However, neither of them gave the security proof of their schemes. In the aspects of provably secure certificateless proxy signature schemes, Chen *et al.* [2] gave a security model of certificateless proxy signature for the first time and a concrete provably secure scheme in 2009. Later, many provably secure certificateless proxy signature schemes [7,13,22] were proposed.

Considering the random oracle model [6] and the standard model [21], Canetti *et al.* [1] showed that security in the random oracle model cannot guarantee the security in the real world. Thus, it is very important to work out schemes that are secure in the standard model. Eslami *et al.* [5] took the first step in this respect. They proposed a certificateless proxy signature scheme in the standard model for the first time in 2012. But unfortunately, Lu *et al.* [20] pointed out that Eslami *et al.*'s scheme is vulnerable to the public key replacement attack and malicious KGC (Key Generation Center) attack in 2016. Lu *et al.* further proposed a new scheme and proved their scheme to be secure under the Squ-CDH assumption in the standard model. To the best of the authors' knowledge, only the above two certificateless proxy signature schemes have been proposed in the standard model till now. In this paper, we point out that Lu *et al.*'s scheme is still insecure. We give two public key replacement attacks to their scheme. We analyse the reasons for the success of this kind of attack and point out the flaw in the proof of the original scheme. Thus, designing a provably secure certificateless proxy signature scheme in the standard model is still an open problem.

The rest of the paper is organized as follows. In Section 2, we review Lu *et al.*'s scheme. In Section 3, we give two public key replacement attacks to their scheme. Then we analyse the reasons for the success of the attack and point out the flaw in the proof of the original scheme. We conclude the paper in Section 4.

2 Lu *et al.*'s Scheme

Setup: Given a security parameter 1^k, the KGC chooses two cyclic groups G_1 and G_2 of prime order q, a random generator g of G_1, a bilinear map $e : G_1 \times G_1 \rightarrow$

G_2 and three hash functions $H_0 : \{0,1\}^* \to \{0,1\}^n$, $H_1, H_2 : \{0,1\}^* \to Z_q^*$. He/she randomly selects $\alpha \in Z_q^*$ and $g_2, u', u_1, \cdots, u_n, v_0, v_1, m_0, m_1 \in G_1$, and sets $g_1 = g^\alpha$. He/she defines a function: $F_u(id) = u' \prod_{j=1}^{n} u_j^{i_j}$, where $id = i_1 i_2 \cdots i_n$ is a bit string. Let $Q \in G_1$, and he/she also defines another function $f(Q)$. If the x-coordinate of Q is odd, then $f(Q) = 1$; else $f(Q) = 0$. The public parameters are

$$\begin{aligned} Params &= \{G_1, G_2, e, q, g_1, g_2, u', u_1, \cdots, u_n, v_0, v_1, \\ &\quad m_0, m_1, H_0, H_1, H_2, F_u, f\}, \end{aligned}$$

and the master private key is $msk = g_1^\alpha$.

Partial-Private-Key-Gen: Given a user U's identity ID_U, the KGC randomly selects $r_U \in Z_q^*$, and computes the user's partial private key as

$$psk_U = (psk_{U,1}, psk_{U,2}) = (g_1^\alpha \cdot F_u(id_U)^{r_U}, g^{r_U}),$$

where $id_U = H_0(ID_U)$.

Set-Secret-Value: The user U randomly selects $x_U \in Z_q^*$ as his/her secret value.

Set-Public-Key: The user U computes his/her public key as

$$\begin{aligned} PK_U &= (PK_{U,1}, PK_{U,2}, PK_{U,3}) \\ &= (g_1^{x_U}, g_2^{1/x_U}, e(g_1, g_1)^{x_U^2}). \end{aligned}$$

The public key can be verified by checking the following equations:

$$\begin{aligned} e(PK_{U,1}, PK_{U,2}) &= e(g_1, g_2) \text{ and } e(PK_{U,1}, PK_{U,1}) \\ &= PK_{U,3}. \end{aligned}$$

Set-Private-Key: The user U randomly selects $r'_U \in Z_q^*$, and computes his/her private key as

$$\begin{aligned} SK_U &= (SK_{U,1}, SK_{U,2}) \\ &= (psk_{U,1}^{x_U^2} \cdot F_u(id_U)^{r'_U}, psk_{U,2}^{x_U^2} \cdot g^{r'_U}), \end{aligned}$$

where $id_U = H_0(ID_U)$.

Delegation-Gen: The original signer O produces a warrant m_w. Then he/she randomly selects $s \in Z_q^*$ and computes the delegation as

$$\begin{aligned} DC_{OP} &= (DC_{OP,1}, DC_{OP,2}, DC_{OP,3}) \\ &= (g^s, SK_{O,2}, SK_{O,1} \cdot (PK_{O,2}^\gamma \cdot v_\lambda)^s), \end{aligned}$$

where

$$\begin{aligned} \lambda &= f(DC_{OP,2}), \\ \gamma &= H_1(DC_{OP,1}, DC_{OP,2}, ID_O, PK_O, m_w, v_\lambda). \end{aligned}$$

Delegation-Verify: The proxy signer P computes

$$\begin{aligned} id_O &= H_0(ID_O), \\ \lambda &= f(DC_{OP,2}) \end{aligned}$$

and

$$\gamma = H_1(DC_{OP,1}, DC_{OP,2}, ID_O, PK_O, m_w, v_\lambda),$$

and checks whether

$$\begin{aligned} e(DC_{OP,3}, g) &= e(PK_{O,1}, PK_{O,1}) \cdot \\ &\quad e(F_u(id_O), DC_{OP,2}) \cdot \\ &\quad e(PK_{O,2}^\gamma \cdot v_\lambda, DC_{OP,1}) \end{aligned}$$

holds. If it does, he/she accepts the delegation. Otherwise, the proxy signer asks the original signer to produce the delegation again.

Proxy-Sign: Let $M \in \{0,1\}^*$. The proxy signer P randomly selects $s', t \in Z_q^*$, and computes the proxy signature as

$$\begin{aligned} \sigma &= (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5) \\ &= (g^t, SK_{P,2}, DC_{OP,1} \cdot g^{s'}, DC_{OP,2}, DC_{OP,3} \cdot \\ &\quad (PK_{O,2}^\gamma \cdot v_\lambda)^{s'} \cdot SK_{P,1} \cdot (PK_{P,2}^\eta \cdot m_\mu)^t), \end{aligned}$$

where

$$\begin{aligned} \lambda &= f(\sigma_4), \\ \gamma &= H_1(DC_{OP,1}, \sigma_4, ID_O, PK_O, m_w, v_\lambda), \\ \mu &= f(\sigma_2) \end{aligned}$$

and

$$\eta = H_2(\sigma_1, \sigma_2, \sigma_3, \sigma_4, ID_O, PK_O, ID_P, PK_P, M, m_\mu).$$

Proxy-Verify: Given a proxy signature

$$\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$$

on (M, m_w), a verifier first checks whether m is suitable for the warrant m_w. If it does, he/she computes

$$\begin{aligned} id_O &= H_0(ID_O), \\ id_P &= H_0(ID_P), \\ \lambda &= f(\sigma_4), \\ \gamma &= H_1(DC_{OP,1}, \sigma_4, ID_O, PK_O, m_w, v_\lambda), \\ \mu &= f(\sigma_2) \end{aligned}$$

and

$$\eta = H_2(\sigma_1, \sigma_2, \sigma_3, \sigma_4, ID_O, PK_O, ID_P, PK_P, M, m_\mu),$$

and checks whether the following equation holds:

$$\begin{aligned} e(\sigma_5, g) &= PK_{O,3} \cdot PK_{P,3} \cdot e(F_u(id_O), \sigma_4) \cdot e(PK_{O,2}^\gamma \cdot \\ &\quad v_\lambda, \sigma_3) \cdot e(F_u(id_P), \sigma_2) \cdot e(PK_{P,2}^\eta \cdot m_\mu, \sigma_1). \end{aligned}$$

If it does, he/she accepts the proxy signature.

Note: There is a clerical error in Lu *et al.*'s scheme. In order to verify the proxy signature, the verifier must know the value of $DC_{OP,1}$ to compute $\gamma = H_1(DC_{OP,1}, \sigma_4, ID_O, PK_O, m_w, v_\lambda)$ correctly. Thus, the proxy signer must transmit it with the proxy signature, which makes the proxy signature longer than the original scheme. In fact, we can replace $DC_{OP,1}$ with σ_3 in the computation of γ, and the length of proxy signature will not be added.

3 The Weakness of Lu *et al.*'s Scheme

In this section, we will show that Lu *et al.*'s scheme is vulnerable to the public key replacement attack of Type-I adversary. Then we point out the flaw in Lu *et al.*'s security proof. The formal definition and security model of certificateless proxy signature can be found in Lu *et al.*'s paper.

3.1 Public Key Replacement Attack

1) A malicious original signer O can forge a valid proxy signature without the private key of the proxy signer P.

According to the game of Definition 2 in Lu *et al.*'s paper, in the Queries stage, the malicious original signer O first randomly chooses $x'_P \in Z_q^*$ and computes

$$\begin{aligned} PK'_P &= (PK'_{P,1}, PK'_{P,2}, PK'_{P,3}) \\ &= (g_1^{x'_P}, g_2^{1/x'_P}, e(g_1, g_1)^{(x'_P)^2}). \end{aligned}$$

Subsequently, he/she makes a ReplacePublicKey oracle query to replace the public key of the proxy signer P with the new value PK'_P. In the Forgery stage, he/she randomly chooses $t, s, s', r_P \in Z_q^*$, an arbitrary message M and a warrant m_w. Then he/she computes

$$\begin{aligned} \sigma_1 &= g^t, \sigma_2 = g^{r_P}, \sigma_3 = g^{s+s'}, \sigma_4 = psk_{O,2}^{x_O^2+(x'_P)^2}, \\ \lambda &= f(\sigma_4), \\ \mu &= f(\sigma_2), \\ \gamma &= H_1(g^s, \sigma_4, ID_O, PK_O, m_w, v_\lambda), \\ \eta &= H_2(\sigma_1, \sigma_2, \sigma_3, \sigma_4, ID_O, PK_O, ID_P, \\ &\qquad PK'_P, M, m_\mu), \\ id_P &= H_0(ID_P), \\ id_O &= H_0(ID_O), \\ \sigma_5 &= (psk_{O,1})^{x_O^2} \cdot (psk_{O,1})^{(x'_P)^2} \cdot (PK_{O,2}^\gamma \cdot v_\lambda)^{s+s'} \cdot \\ &\quad F_u(id_P)^{r_P} \cdot ((PK'_{P,2})^\eta \cdot m_\mu)^t. \end{aligned}$$

It can be verified that $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ is a valid proxy signature.

$$\begin{aligned} & e(\sigma_5, g) \\ = \; & e((psk_{O,1})^{x_O^2} \cdot (psk_{O,1})^{(x'_P)^2} \cdot (PK_{O,2}^\gamma \cdot v_\lambda)^{s+s'} \\ & \cdot F_u(id_P)^{r_P} \cdot ((PK'_{P,2})^\eta \cdot m_\mu)^t, g) \\ = \; & e((psk_{O,1})^{x_O^2}, g) \cdot e((psk_{O,1})^{(x'_P)^2}, g) \cdot \\ & e((PK_{O,2}^\gamma \cdot v_\lambda)^{s+s'}, g) \cdot e(F_u(id_P)^{r_P}, g) \\ & \cdot e(((PK'_{P,2})^\eta \cdot m_\mu)^t, g) \\ = \; & e((g_1^\alpha \cdot F_u(id_O)^{r_O})^{x_O^2}, g) \cdot \\ & e((g_1^\alpha \cdot F_u(id_O)^{r_O})^{(x'_P)^2}, g) \\ & \cdot e((PK_{O,2}^\gamma \cdot v_\lambda)^{s+s'}, g) \cdot \\ & e(F_u(id_P)^{r_P}, g) \cdot e(((PK'_{P,2})^\eta \cdot m_\mu)^t, g) \\ = \; & PK_{O,3} \cdot PK'_{P,3} \cdot e(F_u(id_O), g^{r_O(x_O^2+(x'_P)^2)}) \cdot \\ & e((PK_{O,2}^\gamma \cdot v_\lambda)^{s+s'}, g) \cdot \\ & e(F_u(id_P)^{r_P}, g) \cdot e(((PK'_{P,2})^\eta \cdot m_\mu)^t, g) \\ = \; & PK_{O,3} \cdot PK'_{P,3} \cdot e(F_u(id_O), psk_{O,2}^{(x_O^2+(x'_P)^2)}) \cdot \\ & e((PK_{O,2}^\gamma \cdot v_\lambda)^{s+s'}, g) \cdot \\ & e(F_u(id_P)^{r_P}, g) \cdot e(((PK'_{P,2})^\eta \cdot m_\mu)^t, g) \\ = \; & PK_{O,3} \cdot PK'_{P,3} \cdot e(F_u(id_O), \sigma_4) \cdot \\ & e(PK_{O,2}^\gamma \cdot v_\lambda, \sigma_3) \cdot e(F_u(id_P), \sigma_2) \cdot \\ & e((PK'_{P,2})^\eta \cdot m_\mu), \sigma_1). \end{aligned}$$

Therefore, the malicious original signer O wins the game with probability 1.

2) A malicious proxy signer P can forge a valid proxy signature without the authorization of the original signer O.

According to the game of Definition 2 in Lu *et al.*'s paper, in the Queries stage, the malicious proxy signer P first randomly chooses $x'_O \in Z_q^*$ and computes

$$\begin{aligned} PK'_O &= (PK'_{O,1}, PK'_{O,2}, PK'_{O,3}) \\ &= (g_1^{x'_O}, g_2^{1/x'_O}, e(g_1, g_1)^{(x'_O)^2}). \end{aligned}$$

Subsequently, he/she makes a ReplacePublicKey oracle query to replace the public key of the original signer O with the new value PK'_O. In the Forgery stage, he/she randomly chooses $t, s, s', r_O \in Z_q^*$, an arbitrary message M and a warrant m_w. Then he/she computes

$$\begin{aligned} \sigma_1 &= g^t, \sigma_2 = psk_{P,2}^{(x'_O)^2+x_P^2}, \sigma_3 = g^{s+s'}, \sigma_4 = g^{r_O}, \\ \lambda &= f(\sigma_4), \\ \mu &= f(\sigma_2), \\ \gamma &= H_1(g^s, \sigma_4, ID_O, PK'_O, m_w, v_\lambda), \\ \eta &= H_2(\sigma_1, \sigma_2, \sigma_3, \sigma_4, ID_O, PK'_O, ID_P, \\ &\qquad PK_P, M, m_\mu), \end{aligned}$$

$$
\begin{aligned}
id_P &= H_0(ID_P),\\
id_O &= H_0(ID_O),\\
\sigma_5 &= (psk_{P,1})^{(x'_O)^2}\cdot(psk_{P,1})^{x_P^2}\\
&\quad\cdot((PK'_{O,2})^{\gamma}\cdot v_\lambda)^{s+s'}\\
&\quad\cdot F_u(id_O)^{r_O}\cdot(PK^{\eta}_{P,2}\cdot m_\mu)^t.
\end{aligned}
$$

It can be verified that $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$ is a valid proxy signature.

$$
\begin{aligned}
& e(\sigma_5, g)\\
=\ & e((psk_{P,1})^{(x'_O)^2}\cdot(psk_{P,1})^{x_P^2}\cdot((PK'_{O,2})^{\gamma}\\
& \cdot v_\lambda)^{s+s'}\cdot F_u(id_O)^{r_O}\cdot(PK^{\eta}_{P,2}\cdot m_\mu)^t, g)\\
=\ & e((psk_{P,1})^{(x'_O)^2}, g)\cdot e((psk_{P,1})^{x_P^2}, g)\\
& \cdot e(((PK'_{O,2})^{\gamma}\cdot v_\lambda)^{s+s'}, g)\\
& \cdot e(F_u(id_O)^{r_O}, g)\cdot e((PK^{\eta}_{P,2}\cdot m_\mu)^t, g)\\
=\ & e((g_1^{\alpha}\cdot F_u(id_P)^{r_P})^{(x'_O)^2}, g)\\
& \cdot e((g_1^{\alpha}\cdot F_u(id_P)^{r_P})^{x_P^2}, g)\cdot e(((PK'_{O,2})^{\gamma}\\
& \cdot v_\lambda)^{s+s'}, g)\cdot e(F_u(id_O)^{r_O}, g)\\
& \cdot e((PK^{\eta}_{P,2}\cdot m_\mu)^t, g)\\
=\ & PK'_{O,3}\cdot PK_{P,3}\cdot e(F_u(id_P), g^{r_P((x'_O)^2+x_P^2)})\\
& \cdot e(((PK'_{O,2})^{\gamma}\cdot v_\lambda)^{s+s'}, g)\cdot e(F_u(id_O)^{r_O}, g)\\
& \cdot e((PK^{\eta}_{P,2}\cdot m_\mu)^t, g)\\
=\ & PK'_{O,3}\cdot PK_{P,3}\cdot e(F_u(id_P), psk_{P,2}^{((x'_O)^2+x_P^2)})\\
& \cdot e(((PK'_{O,2})^{\gamma}\cdot v_\lambda)^{s+s'}, g)\cdot e(F_u(id_O)^{r_O}, g)\\
& \cdot e((PK^{\eta}_{P,2}\cdot m_\mu)^t, g)\\
=\ & PK'_{O,3}\cdot PK_{P,3}\cdot e(F_u(id_P), \sigma_2)\\
& \cdot e((PK'_{O,2})^{\gamma}\cdot v_\lambda, \sigma_3)\cdot e(F_u(id_O), \sigma_4)\\
& \cdot e(PK^{\eta}_{P,2}\cdot m_\mu, \sigma_1).
\end{aligned}
$$

Therefore, the malicious proxy signer P wins the game with probability 1.

3.2 The Flaw in Lu *et al.*'s Security Proof

First, let's see the σ_5 in a proxy signature.

$$
\begin{aligned}
\sigma_5 &= DC_{OP,3}\cdot(PK^{\gamma}_{O,2}\cdot v_\lambda)^{s'}\cdot SK_{P,1}\cdot(PK^{\eta}_{P,2}\cdot m_\mu)^t\\
&= SK_{O,1}\cdot SK_{P,1}\cdot(PK^{\gamma}_{O,2}\cdot v_\lambda)^{s+s'}\cdot(PK^{\eta}_{P,2}\cdot m_\mu)^t\\
&= g_1^{\alpha(x_O^2+x_P^2)}\cdot F_u(id_O)^{(r_O x_O^2+r'_O)}\cdot F_u(id_P)^{(r_P x_P^2+r'_P)}\\
&\quad\cdot(PK^{\gamma}_{O,2}\cdot v_\lambda)^{s+s'}\cdot(PK^{\eta}_{P,2}\cdot m_\mu)^t.
\end{aligned}
$$

To the original signer O, all the ephemeral variables can be randomly chosen by himself/herself. Therefore, only the master private key g_1^{α} and the proxy signer's secret value x_P are unknown to him/her. In addition, σ_1, σ_2, σ_3 and σ_4 can also be computed by himself/herself by randomly choosing all the ephemeral variables. Therefore, to forge a proxy signature, he/she just needs to know $g_1^{\alpha(x_O^2+x_P^2)}$ and the proxy signer's secret value x_P.

Through public key replacement attack, O can choose x'_P as the secret value of proxy signer P. Therefore, he/she just needs to compute $g_1^{\alpha(x_O^2+x_P^2)}$ to forge a proxy signature.

Holding the partial private key $psk_{O,1}$, he/she can compute

$$
\begin{aligned}
& (psk_{O,1})^{x_O^2}\cdot(psk_{O,1})^{(x'_P)^2}\\
=\ & g_1^{\alpha(x_O^2+(x'_P)^2)}\cdot F_u(id_O)^{r_O(x_O^2+(x'_P)^2)},
\end{aligned}
$$

which includes the $g_1^{\alpha(x_O^2+(x'_P)^2)}$. Therefore, computing σ_5 now becomes very simple and he/she can compute

$$
\begin{aligned}
\sigma_5 &= (psk_{O,1})^{x_O^2}\cdot(psk_{O,1})^{(x'_P)^2}\cdot(PK^{\gamma}_{O,2}\cdot\\
&\quad v_\lambda)^{s+s'}\cdot F_u(id_P)^{r_P}\cdot((PK'_{P,2})^{\eta}\cdot m_\mu)^t\\
&= g_1^{\alpha(x_O^2+(x'_P)^2)}\cdot F_u(id_O)^{r_O(x_O^2+(x'_P)^2)}\\
&\quad\cdot(PK^{\gamma}_{O,2}\cdot v_\lambda)^{s+s'}\cdot F_u(id_P)^{r_P}\cdot((PK'_{P,2})^{\eta}\cdot m_\mu)^t
\end{aligned}
$$

by randomly choosing $t, s, s', r_P \in Z_q^*$.

By setting

$$
\begin{aligned}
\sigma_2 &= g^{r_P}\\
\sigma_4 &= psk_{O,2}^{(x_O^2+(x'_P)^2)}\\
&= g_1^{r_O(x_O^2+(x'_P)^2)}.
\end{aligned}
$$

The original signer O can forge a valid proxy signature successfully.

Now, let's look at the proof of Theorem 1 in Lu *et al.*'s scheme. In Case 2 and Case 3 of the Forgery stage, Lu *et al.* proved that if a malicious original signer can output a forgery of a valid proxy signature, Challenger will solve the Squ-CDH problem with a non-negligible advantage.

Note that there is a condition when the above Theorem holds − during the forging of a proxy signature, there must be an unknown part (which is generally a private key) in computing the forged proxy signature. While in our attack, all parts are known to the original signer O in forging a valid proxy signature. Therefore the condition is not held, the proof is certainly wrong.

4 Conclusions

In this paper, we give two public key replacement attacks to a recently proposed certificateless proxy signature scheme in the standard model. Then we analyze the reasons for the success of the attack and point out the flaw in the proof of the original scheme. Therefore, designing a provably secure certificateless proxy signature scheme in the standard model is still an open problem.

Acknowledgments

This work was supported by the National Natural Science Foundation of China [grant numbers 61462048, 61562047 and 61662039]. We would like to present our thanks to Ms. Yan Di, who checked our manuscript.

References

[1] R. Canetti, O. Goldreich, and S. Halevi, "The random oracle methodology, revisited," *Journal of the ACM*, vol. 51, no. 4, pp. 557–594, 2004.

[2] H. Chen, F. T. Zhang, and R. S. Song, "Certificateless proxy signature scheme with provable security," *Journal of Software*, vol. 20, no. 3, pp. 692–701, 2009.

[3] K. Choi and D. Lee, "Certificateless proxy signature scheme," in *Proceedings of the 3rd International Conference on Multimedia, Information Technology and its Applications (MITA'07)*, pp. 437–440, Aug. 2007.

[4] L. Z. Deng, H. W. Huang, and Y. Y. Qu, "Identity based proxy signature from rsa," *International Journal of Network Security*, vol. 19, no. 2, pp. 229–235, 2017.

[5] Z. Eslami and N. Pakniat, "A certificateless proxy signature scheme secure in standard model," in *Proceedings of 2012 International Conference on Latest Computational Technologies (ICLCT'12)*, pp. 81–84, Mar. 2012.

[6] M. Hassouna, B. Barry, and E. Bashier, "A new level 3 trust hierarchal certificateless public key cryptography scheme in the random oracle model," *International Journal of Network Security*, vol. 19, no. 4, pp. 551–558, 2017.

[7] D. B. He, Y. T. Chen, and J. H. Chen, "An efficient certificateless proxy signature scheme," *Mathematical and Computer Modelling*, vol. 57, no. 9-10, pp. 2510–2518, 2013.

[8] M. S. Hwang, C. C. Lee, S. F. Tzeng, "A new proxy signature scheme for a specified group of verifiers," *Information Sciences*, vol. 227, pp. 102–115, 2013.

[9] M. S. Hwang, I. C. Lin, E. J. L. Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers", *Informatica*, vol. 11, no. 2, pp. 1-8, Apr. 2000.

[10] M. S. Hwang, S. F. Tzeng and S. F. Chiou, "A nonrepudiable multi-proxy multi-signature scheme", *Innovative Computing, Information and Control Express Letters*, vol. 3, no. 3, pp. 259–264, 2009.

[11] M. S. Hwang, S. F. Tzeng, C. S. Tsai, "Generalization of proxy signature based on elliptic curves", *Computer Standards & Interfaces*, vol. 26, no. 2, pp. 73–84, 2004.

[12] C. C. Lee, T. C. Lin, S. F. Tzeng and M. S. Hwang, "Generalization of proxy signature based on factorization", *International Journal of Innovative Computing, Information and Control*, vol. 7, no. 3, pp. 1039–1054, 2011.

[13] J. G. Li, Y. Q. Li, and Y. C. Zhang, "Provably secure forward secure certificateless proxy signature scheme," *KSII Transactions on Internet and Information Systems*, vol. 7, no. 8, pp. 1972–1988, 2013.

[14] L. H. Li, S. F. Tzeng, M. S. Hwang, "Generalization of proxy signature based on discrete logarithms", *Computers & Security*, vol. 22, no. 3, pp. 245–255, 2003.

[15] X. Li, K. Chen, and L. Sun, "Certificateless signature and proxy signature schemes from bilinear pairings," *Lithuanian Mathematical Journal*, vol. 45, no. 1, pp. 76–83, 2005.

[16] D. Liu, S. Zhang, H. Zhong, R. H. Shi, and Y. M. Wang, "An efficient identity-based online/offline signature scheme without key escrow," *International Journal of Network Security*, vol. 19, no. 1, pp. 127–137, 2017.

[17] L. H. Liu, W. P. Kong, Z. J. Cao, and J. B. Wang, "Analysis of one certificateless encryption for secure data sharing in public clouds," *International Journal of Electronics and Information Engineering*, vol. 6, no. 2, pp. 110–115, 2017.

[18] E. J. L. Lu, M. S. Hwang, and C. J. Huang, "A new proxy signature scheme with revocation", *Applied Mathematics and Computation*, vol. 161, no. 3, PP. 799-806, Feb. 2005.

[19] R. B. Lu, D. K. He, and C. J. Wang, "Cryptanalysis and improvement of a certificateless proxy signature scheme from bilinear pairings," in *Proceedings of the 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD'07)*, pp. 285–290, July 2007.

[20] Y. Lu and J. G. Li, "Provably secure certificateless proxy signature scheme in the standard model," *Theoretical Computer Science*, vol. 639, pp. 42–59, 2016.

[21] Y. Ming and Y. M. Wang, "Cryptanalysis of an identity based signcryption scheme in the standard model," *International Journal of Network Security*, vol. 18, no. 1, pp. 165–171, 2016.

[22] S. Padhye and N. Tiwari, "Ecdlp-based certificateless proxy signature scheme with message recovery," *Transactions on Emerging Telecommunications Technologies*, vol. 26, no. 3, pp. 346–354, 2015.

[23] S. F. Tzeng, C. C. Lee, and M. S. Hwang, "A batch verification for multiple proxy signature", *Parallel Processing Letters*, vol. 21, no. 1, pp. 77–84, 2011.

[24] C. Y. Yang, S. F. Tzeng, M. S. Hwang, "On the efficiency of nonrepudiable threshold proxy signature scheme with known signers", Journal of Systems and Software, vol. 73, no. 3, pp. 507–514, 2004.

[25] W. S. Yap, S. H. Heng, and B. M. Goi, "Cryptanalysis of some proxy signature schemes without certificates," in *Proceedings of the 1st Workshop on Information Security Theory and Practices Smart Cards, Mobile and Ubiquitous Computing Systems (WISTP'07)*, pp. 115–126, May 2007.

Biography

Caixue Zhou received BS degree in Computer Science Department from Fudan University in 1988, Shanghai, China and MS degree in Space College of Beijing University of Aeronautics and Astronautics in 1991, Beijing, China. He is an Associate Professor in the School of Information Science and Technology, Jiujiang University,

Jiujiang, China since 2007. He is a member of the CCF (China Computer Federation) and a member of CACR(Chinese Association for Cryptologic Research). His research interests include applied cryptography, security of computer networks.

Xiwei Dong received BS degree in School of Computer Science and Technology from Shandong University of Technology in 2005, Zibo, China and MS degree in School of Computer Science and Technology from Dalian University of Technology in 2010, Dalian, China. He is currently a PhD candidate in the School of Computer Science and Technology at the Nanjing University of Posts and Telecommunications. He is a lecturer in the School of Information Science and Technology, Jiujiang University, Jiujiang, China since 2011. He is a member of the CCF (China Computer Federation). His research interests include applied cryptography, security of computer networks and pattern recognition.

Lihua Wang received BS degree in School of Computer and Control from Harbin University of Science and Technology in 2003, Harbin, China and MS degree in School of Computer Science and Technology from Huazhong University of Science and Technology in 2008, Wuhan, China. She is a lecturer in the School of Information Science and Technology, Jiujiang University, Jiujiang, China since 2009. Her research interests include applied cryptography and network security.

Tao Li received MS degree in School of Computer Science and Technology from Anhui University of Science and Technology in 2009, Anhui, China and PhD degree in School of Computer Science and Technology from Hohai University in 2016, Nanjing, China. Now he is a lecturer in the School of Information Science and Technology, Jiujiang University. Jiujiang, China. His research interests include cryptography, information security, wireless network security and vehicular network security.