Some Certificateless Short Signature Schemes of Security Analysis and Simple Improvement

Xiaoming Hu*, Fangshu Chen, Wenan Tan and Chuang Ma

College of Computer and Information Engineering, Shanghai Polytechnic University, 2360 Jinhai Road, Pudong New Area, Shanghai, 201209, China
*Corresponding Author Email: xmhu@sspu.edu.cn

Abstract. Certificateless signature (CLS) scheme as an important filed of cryptography has a wide range of applications, such as information security, network security and so on. But, in the CLS scheme, the public key of the signer is generated directly by the signer itself without the verification of the trusted third part, so the public key easily is replaced by the malicious users which lead to the forgeability of the signature. In this paper, we show three CLS schemes proposed recently which have high efficient with short signature are not secure and the malicious user can forge a signature by replacing the public key of the signer. In the same, we also present three improved CLS schemes with simple modifying based on the original CLS schemes respectively. We also make a simple security analysis and efficiency analysis on the three improved CLS schemes. The analysis shows that the improved schemes not only can overcome the security problem but also almost have the same efficiency with the original CLS schemes.

1. Introduction
Certificateless signature (CLS) system has an important role in the security field. CLS which is a research hot recently [1-5] has extensive applications in many scenes, such as electronic pay, ad hoc network and so on. In CLS scheme, there exist two types of attacks. One is the malicious user who does not the master key of the system and the partial private key, but it can replace the public key of the user. Second is the malicious KGC (Key Generation Center) who knows the master key and the partial private key, but it cannot replace the public key of the user. Generally, a security CLS scheme ought to can resist to the attack from the above two types of enemy. Till now, many CLS schemes have been proposed [6-9]. However, [10,11] is proved to be insecure and cannot resist to the first type of attack. [12] is proved to cannot resist to the second type of attack.

Recently, Zuo et al. propose two CLS schemes [13,14] with short signature and high efficient. And they also prove the security of their CLS scheme in the random oracle. In 2020, Zuo et al. propose a certificateless signature scheme with short signature and double KGCs [15] which can reduce the harm from the simple KGC and also can solve the efficiency bottleneck of simple KGC. However, in this paper, we point out that their three CLS schemes are not secure. The malicious user can forge the signature by replacing the public key of the user, namely, the three CLS scheme does not satisfy the first type of attack. We also give three simple improvements and some security and efficiency analysis for these schemes.

2. Review And Security Analysis Of The FR-CLS- Zuo Scheme
Here, we first look back the Zuo et al.’s CLS scheme [13] and then show that the security analysis of Zuo et al.’s CLS scheme, finally we give a simple improved method.
2.1. Review of FR-CLS-ZUO Scheme

Zuo et al.’s CLS (FR-CLS-ZUO) scheme [13] includes the following algorithms.

- System Parameter Setup: Assume that $e$ is a bilinear map $G_1 \times G_1 \rightarrow G_T$ and $g$ is a generator of $G_1$. And define $H_1 : \{0,1\}^* \rightarrow Z_q^*$ and $H_2 : \{0,1\} \times G_1 \rightarrow Z_q^*$ to be two one-way hash functions. KGC (Key Generator Center) computes $y_{kgc} = x_{kgc}g$ where $x_{kgc} \in_R Z_q^*$ is the master key. The algorithm outputs the system public parameters $\{G_1, k, G_T, e, g, y_{kgc}, H_1, H_2\}$.

- Secret Value Setup: A user $A$ with the identity $ID_A$ computes $y_A = x_A g$ with $x_A \in_R Z_q^*$.

- Partial Private Setup: KGC computes $K_A = H_i(ID_A, y_A), d_A = \frac{K_A}{x_{kgc} + K_A} g$. And KGC sends secretly $d_A$ to $A$.

- Public-Private Key Setup: $A$ computes $T = y_{kgc} + K_A g$, $Y = x_A T$, Then $(x_A, d_A)$ and $(y_A, Y)$ are the private and public key for $A$.

- Signature Setup: Given a message $m \in \{0,1\}^*$, $A$ computes the signature $S$ for $m$.

$$h = H_2(m, ID_A, Y), \quad S = \frac{1}{x_A + h} d_A.$$  

- Verification Setup: The verifier computes $K_A = H_i(ID_A, y_A), h = H_2(m, ID_A, Y)$, and verifies if

$$e(S, K_A^{-1}(Y + hT)) = e(g, g).$$

2.2. Security Analysis and Simple Improvement of The FR-CLS-ZUO Scheme

We first give a security analysis on the FR-CLS-ZUO scheme, and then give a simple improvement.

2.2.1. Security analysis. Here, we show that FR-CLS-ZUO scheme is not secure and cannot resist the first type of forge attack. In other words, the enemy can forge a signature when it does not the master of KGC but it can replace the public key of the user. Assume that the identity which the enemy wants to attack is $ID_A$ and the message which the enemy wants to forge signature on is $m'$. Then the enemy does as follows.

- Choose $x_A^* \in_R Z_q^*$ and $x_B^* \in_R Z_q^*$, then the enemy computes

$$Y^* = x_A^* g, T^* = x_B^* g, h^* = H_2(m', ID_A, Y^*),$$

$$K_A^* = H_i(ID_A, y_A), S^* = K_A^*(x_A^* + h^* x_B^*)^{-1} g.$$  

Then, $S^*$ is the forged signature on message $m'$.

- $(m^*, S^*)$ is a valid signature because

$$e(S^*, K_A^{-1}(Y^* + h^* T^*)) = e(K_A^*(x_A^* + h^* x_B^*)^{-1} g, K_A^{-1}(Y^* + h^* T^*))$$

$$= e(K_A^*(x_A^* + h^* x_B^*)^{-1} g, K_A^{-1}(x_A^* g + h^* x_B^* g))$$

$$= e(K_A^*(x_A^* + h^* x_B^*)^{-1} g, K_A^{-1}(x_A^* + h^* x_B^* g)) = e(g, g).$$

2.2.2. Simple improvement. From the above security analysis, it can find that the main reason that the enemy can forge successfully is because $T$ can be modified by the enemy and does not any verify on $T$. Therefore, the improved method is to make $T$ be unmodified in the process of verification setup. In fact, it can find from the FR-CLS-ZUO scheme $T = y_{kgc} + K_A g$ which is more suitable to appear in the verification equal. So, the improved scheme is as follows.
Verification Setup: The verifier computes
\[ K_A = H_1(ID_A, y_A), h = H_2(m, ID_A, Y), \]
and verifies if
\[ e(S, K_A^{-1}(Y + h(y_{kgc} + K_A g))) = e(g, g). \] (1)
The other parts are the same with the original FR-CLS-ZUO scheme.

- Security and efficiency Analysis. In new verification equal (1), if the enemy wants to replace the \( Y^* \), then the enemy must know the master key \( x_{kgc} \) to construct the \( S \) which satisfies the verification equal (1). In other hand, if the enemy knows the master key \( x_{kgc} \) but cannot replace the public key. In this situation, \( Y \) must hold the construction \( x_g \) where \( x \in R Z_q^* \) but it is unable because \( Y (Y = x_A T) \) cannot be replaced. Therefore, the improved scheme can overcome the above attack.

On the efficiency, the improved scheme only adds a point add \( y_{kgc} + K_A g \) in Verification Setup. And it does not add any computation in signature setup. So, the improved scheme almost is the same efficiency with the original FR-CLS-ZUO scheme.

3. Review and Security Analysis of the Se-CLS- Zuo Scheme

Here, we present the second ZUO et al.’s CLS scheme [14] on its review, security analysis and simple improvement.

3.1. Review of FR-CLS-ZUO Scheme
The Zuo et al.’s CLS (SE-CLS-ZUO) scheme [14] includes the following algorithms.

- System Parameter Setup: Assume that \( P \) is a generator of \( G_1 \). Set \( g = e(P, P), y_{pub} = sP \) where \( s \in R Z_q^* \) is the master key. The algorithm outputs the system public parameters \( \{ G_1, k, G_F, e, g, P, y_{pub}, H_1, H_2 \} \).
- Secret Value Setup: A user \( ID \) computes \( y_{ID} = x_{ID} g \) with \( x_{ID} \in R Z_q^* \).
- Partial Private Setup: KGC computes \( Q_{ID} = H_1(ID, y_{ID}), k = H_1(ID, timestamp), K = kP, d_{ID} = \frac{k}{s + Q_{ID}} P \). And KGC sends secretely \( (d_{ID}, K) \) to \( ID \).
- Public-Private Key Setup: \( ID \) computes \( pk_{ID} = y_{ID} y_{pub} + Q_{ID} y_{ID} \). Then \( (x_{ID}, d_{ID}) \) and \( (y_{ID}, pk_{ID}, K) \) are the private and public key for \( ID \).
- Signature Setup: Given a message \( m \in \{0,1\}^* \), \( ID \) computes the signature \( S \) for \( m \).
\[ h_{ID} = H_2(ID, m, pk_{ID}), S = \frac{1}{x_{ID} + h_{ID}} d_{ID}. \]
- Verification Setup: The verifier computes \( Q_{ID} = H_1(ID, y_{ID}), h_{ID} = H_2(ID, m, pk_{ID}) \), and verifies if
\[ e(S, pk_{ID} + h_{ID}(y_{pub} + Q_{ID} P)) = e(K, P). \]

3.2. Security Analysis and Simple Improvement of The SE-CLS- ZUO Scheme

3.2.1. Security analysis. Here, we show that SE-CLS-ZUO scheme as above cannot resist the first type of forge attack. Assume that the identity which the enemy wants to attack is \( ID^* \) and the message which the enemy wants to forge signature on is \( m^* \). Then the enemy does as follows.
• Choose $a^* \in R \ Z^*_q$, then the enemy computes

$$Q_{ID}^* = H_1(ID^*, y_{ID}), h_{ID}^* = H_2(ID, m^*, pk_{ID}), S^* = a^*P, K^* = a^*(pk_{ID} + h_{ID}^*(y_{pub} + Q_{ID}^*P)).$$

Then, $S^*$ is the forged signature on message $m^*$.

• $(m^*, S^*)$ is a valid signature because

$$e(S^*, pk_{ID} + h_{ID}^*(y_{pub} + Q_{ID}^*P)) = e(a^*P, pk_{ID} + h_{ID}^*(y_{pub} + Q_{ID}^*P)) = e(P, a^*(pk_{ID} + h_{ID}^*(y_{pub} + Q_{ID}^*P))) = e(P, K).$$

3.2.2. Simple improvement. From the above security analysis, it can find that the main reason that the enemy can forge successfully is because $K$ can be modified by the enemy and does not any verify on $K$. Therefore, the improved method is to make $K$ be unmodified in the all parts of the full scheme. The improved method is as follows.

• Modify the computation of $Q_{ID}$ and $h_{ID}$ as follows $Q_{ID} = H_1(ID, y_{ID}, K), h_{ID} = H_2(ID, m, pk_{ID}),$ The other parts are the same with the original SE-CLS-ZUO scheme.

• Security and efficiency Analysis. By modifying $Q_{ID}$ from $Q_{ID} = H_1(ID, y_{ID})$ to $Q_{ID} = H_1(ID, y_{ID}, K)$ and $h_{ID}$ from $H_2(ID, m, pk_{ID})$ to $H_2(ID, m, pk_{ID}, K)$, it makes the enemy be unable to modify $K$. Because if the enemy wants to modify $K$, it must can compute the inputs of $H_1$ and $H_2$ which is contradictory to the one-way of $H_1$ and $H_2$ defined. Therefore, the improved scheme can overcome the above attack.

On the efficiency, the improved scheme only adds an input of $H_1$ and $H_2$. And it does not add any other computational cost. So, the improved scheme almost is the same efficiency with the original SE-CLS-ZUO scheme.

4. Review and Security Analysis of the TH-CLS-Zuo Scheme

Here, we present the second Zuo et al.’s CLS scheme [15] on its review, security analysis and simple improvement.

4.1. Review of TH-CLS-Zuo Scheme

The Zuo et al.’s CLS (TH-CLS-ZUO) scheme [15] includes the following algorithms.

• System Parameter Setup: Assume that $P$ is a generator of $G_1$. KGCA Computes $y_A = x_A P$, and KGCB computes $y_B = x_B P$, $T = x_B y_A = x_B x_A P$ where $x_A, x_B \in R \ Z^*_q$ is the master key for KGC1 and KGC2 respectively. The algorithm outputs the system public parameters \{$G_1, G_2, e, P, T, H_1, H_2, y_A, y_B$\}.

• Partial Private Setup: Given the user $ID$, KGCA computes $Q_{ID} = H_1(ID)$, $d_A = \frac{1}{x_A + Q_{ID}}P$. And KGCA sends secretly $d_A$ to KGCB. KGCB computes $Q_{ID} = H_1(ID)$, $d_{ID} = \frac{1}{x_B + Q_{ID}}d_A$. And KGCB sends secretly $d_{ID}$ to $ID$.

• Secret Value Setup: A user $ID$ chooses $x_{ID} \in R \ Z^*_q$, and $(x_{ID}, d_{ID})$ is secret value.

• Public Key Setup: $ID$ computes $Q_{ID} = H_1(ID), R = T + Q_{ID} y_A + Q_{ID} y_B + Q_{ID}^2 P$, $pk_{ID} = x_{ID} R$. Then $y_{ID}$ is the public key for $ID$.\n
4
4.2. Security Analysis and Simple Improvement of The TH-CLS- ZUO Scheme

4.2.1. Security analysis. Here, we show that TH-CLS-ZUO scheme has the same security problem as the above FR-CLS-ZUO scheme. Assume that the identity which the enemy wants to attack is ID* and the message which the enemy wants to forge signature on is m*. Then the enemy does as follows.

- Choose \( r_1^*, r_2^* \in R \) \( Z_q \), then the enemy computes
  \[
  R' = r_1^* P, \quad pk_{ID}^* = r_2^* P.
  \]
  \[
  h^* = H_2(m^*, pk_{ID}^*), \quad S^* = (h^* r_1^* + r_2^*)^{-1} P.
  \]

Then, \( S^* \) is the forged signature on message \( m^* \).

- \( (m^*, S^*) \) is a valid signature because
  \[
  e(S^*, h^* R' + pk_{ID}^*) = e((h^* r_1^* + r_2^*)^{-1} P, h^* r_1^* P + r_2^* P) = e((h^* r_1^* + r_2^*)^{-1} P, (h^* r_1^* + r_2^*) P) = e(P, P).
  \]

4.2.2. Simple improvement. From the above security analysis, it can find that the main reason that the enemy can forge successfully is similar to the FR-CLS-ZUO’s. Therefore, the improved method is to make \( R = T + Q_{ID} y_A + Q_{ID} y_B + Q_{ID}^2 P \) appear in the verification equal directly. So, the improved scheme is as follows.

- Verification Setup: The verifier computes \( h = H_2(m, pk_{ID}) \), and verifies if
  \[
  e(S, h(T + Q_{ID} y_A + Q_{ID} y_B + Q_{ID}^2 P) + pk_{ID}) = e(P, P)
  \]
  (2)

The other parts are the same with the original TH-CLS-ZUO scheme.

- Security and efficiency Analysis. The security analysis is similar to the FR-CLS-ZUO’s, if the enemy wants to replace the \( pk_{ID} \), then the enemy must know the input of \( H_2(m, pk_{ID}) \) which is contradictory to the one-way of \( H_2 \). In other hand, if the enemy knows the master keys \( x_A, x_B \) but cannot replace the public key. In this situation, \( pk_{ID} \) must hold the construction \( xP \) where \( x \in R \) \( Z_q \) but it is unable because \( pk_{ID} = x_{ID} R \) cannot be replaced. Therefore, the improved scheme can overcome the above attack.

On the efficiency, the improved CLS scheme only adds three point additions \( T + Q_{ID} y_A + Q_{ID} y_B + Q_{ID}^2 P \) in Verification Setup. And it does not add any computation in the signature setup. So, the improved CLS scheme almost is the same efficiency with the original TH-CLS-ZUO scheme.

5. Conclusions

In this paper, three CLS schemes are been looked back. Some security analyses on these CLS schemes also are showed. By security analysis, it can see that the three CLS schemes all are not secure and they
can be forged by the malicious user. Some simple improvement on these CLS schemes also are been given. At the same, this paper also gives a simple security analysis and efficiency analysis on the improved CLS schemes. The analysis shows that the improved CLS schemes can overcome the existed security drawbacks with almost the same efficiency.

6. Acknowledgments
This work is 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).

7. References
[1] Horng S., Tzeng S., Huang P., et al., An Efficient Certificateless Aggregate Signature with Conditional Privacy-Preserving for Vehicular Sensor Networks, Journal: INFORMATION SCIENCES, Year: 2015 Volume:317 Issue: C Pages:48-66
[2] Karati A., Islam S., Karuppiah M., Provably Secure and Lightweight Certificateless Signature Scheme for Iot Environments, Journal: IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, Year:2018 Volume:14 Issue:8 Pages:3701-3711
[3] Li J., Yuan H., Zhang Y., Cryptanalysis and Improvement for Certificateless Aggregate Signature, Journal: FUNDAMENTA INFORMATICAE, Year: 2018 Volume:157 Issue:1-2 Pages:111-123
[4] Bhatia T., Verma A., Cryptanalysis and Improvement Of Certificateless Proxy Signcryption Scheme for Eprescription System in Mobile Cloud Computing, Journal: ANNALS OF TELECOMMUNICATIONS, Year:2017 Volume:72 Pages:563-576
[5] Zhang Y., Lu W., Tang C., Research on an Efficient and Practical Cloud-Based Digital Signature Scheme, Journal: NETINFO SECURITY, Year:2016 Volume:2016 Issue:7 Pages:1-6
[6] Wang D., Wang P., Two Birds with One Stone: Two-Factor Authentication with Security Beyond Conventional Bound, Journal: IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, Year:2016 Volume:15 Issue:4 Pages:708–722
[7] Jia X., He D., Liu Q., et al., An Efficient Provably-Secure Certificateless Signature Scheme for Internet-of-Things Deployment, Journal: AD HOC NETWORKS, Year:2018 Volume:71 Pages:78-87
[8] Wang D., Wang P., Wang C., Efficient Multi-Factor User Authentication Protocol with Forward Secrecy for Real-Time Data Access in Wsns, Journal: ACM TRANSACTIONS ON CYBER-PHYSICAL SYSTEMS, Year:2020 Volume:4 Issue:3 Pages:1-26
[9] Zhang Y., Deng R., Zheng D., et al., Efficient and Robust Certificateless Signature for Data Crowd Sensing in Cloud-Assisted Industrial Iot, Journal:IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, Year:2019 Volume:15 Issue:9 Pages:5099-5108
[10] Yu Y., Mu Y., Wang G., et al., Improved Certificateless Signature Scheme Provably Secure in the Standard Model, Journal: IET INFORMATION SECURITY, Year: 2012 Volume:6 Issue:2 Pages:102-110
[11] Yeh K., Su C., Choo K., et al., A Novel Certificateless Signature Scheme for Smart Objects in the Internet-of-Things, Journal: Sensors, Year: 2017 Volume:17 Issue:5 Pages:1001
[12] Zhang Y., Zhou D., Li C., et al., Certificateless-based Efficient Agreggate Signature Scheme with Universal Designated Verifier, Journal: JOURNAL ON COMMUNICATION, Year:2015 Volume:36 Issue:2 Pages:52-59
[13] Zuo L., Chen Z., Xia P., et al., Improved Efficient Certificateless Short Signature Scheme, Journal: COMPUTER SCIENCE, Year:2019 Volume:46 Issue:4 Pages:172-176
[14] Zuo L., Zhou Q., Chen L., A Provably Security and Efficient Certificateless Short Signature Scheme, Journal:COMPUTER ENGINEERING, Year:2019Volume:45Issue:6Pages:193-198
[15] Zuo L., Zhang M., Hu K., et al., Certificateless Short Signature Scheme with Double KGC, Journal: APPLICATION RESEARCH OF COMPUTERS, Year: 2020 Volume:37 Issue:5 Pages:1482-1487