A New Certificateless Signcryption scheme without Bilinear Pairing

Li Cui
College of Information and Communication
National University of Defense Technology
Xi'an, China
lcsy0304@126.com

Bai Yun
College of Information and Communication
National University of Defense Technology
Xi'an, China

Shi Lin
Department of Electronic Technology
Engineer University of CAPF
Xi'an, China
slshilin@126.com

Bai Wenhua
College of Information and Communication
National University of Defense Technology
Xi'an, China

***Abstract*—The certificateless signcryption schemes have been explored in depth by many scholars because of minor calculation, do not require complicated certificate management and inexistence of key escrow problem. In recent years, many scholars promoted a large number of certificateless signcryption schemes, in which some schemes are insecure under the attack of replace several public keys. On this background, a new certificateless signcryption scheme was proposed, and the computation and security of our scheme was analyzed. The results show that our scheme is not only more secure than former schemes, but also has a lower calculation.**

Keywords—Bilinear Pairing; Certificateless Public Key Cryptography; Signcryption Scheme;

I. INTRODUCTION

In the traditional public key cryptosystem, user's public key is bound to the identity of the user through a certificate issued by a credible Certification Authority (CA)[1], but this wastes a lot of storage space and computing time on the certificate management, which has greatly limited the application of PKI (Public Key Infrastructure) technology in real-time and bandwidth-constrained environments[2]. In order to simplify certificate management, Shamir proposed an identity-based public key cryptosystem in 1984[3]. In this system, user's identity information (such as ID number, student number, and mailbox) is the user's public key. This naturally achieves the binding of the user's public key and its identity, but because the user's private key is generated by the PKG (Private Key Generator), the PKG knows the private key of every user, so the identity-based cryptosystem brought new problems with key escrow. In view of the complex certificate management in PKI and the unavoidable key escrow in identity-based cryptosystem, Al-Riyami and Paterson proposed the concept of Certificateless Public Key Cryptography (CL-PKC) in 2003[4]. In certificateless public key cryptosystem, a PKG is also required to generate user's partial private key. However, this partial private key does not need to be kept confidential, nor does it require a secure channel to transmit to the target user. The user selects a secret value that only he himself knows, and at the same time combines the partial private key to generate his complete private key. Since the certificateless cryptosystem not only avoids the problem of certificate management in the traditional public key cryptosystem, but also solves the problem of private key leakage in the identity-based cryptosystem. It builds a good balance between the traditional public key cryptosystem and the identity-based cryptosystem, which has caused widespread concern of relevant scholars.

Digital signature and encryption are two important functions of cryptography. Signature and encryption functions were used separately before. As applications continue to expand, more and more applications are required to provide both authentication and confidentiality.The traditional practice to achieve this goal is to "first sign and then encrypt", the amount of computation and communication of this approach is the sum of the signature and encryption, and thus is less efficient. On this background, Zheng proposed a new cryptographic primitive "Signcryption" in 1997 to accomplish both goals simultaneously[5].Since certificateless public key cryptography was proposed, the certificateless signcryption scheme has been extensively studied by scholars.

In the protocol design process, security and efficiency have always been the core concerns of people. From the theoretical analysis[6] and the experimental results[7][8], it is found that the bilinear pairing computation is about 20 times higher than point multiplication of the elliptic curve under the same safety intensity. Therefore, the certificateless signcryption scheme without bilinear pairing is more efficient and has greater research value. Since Barreto[9] proposed the first certificateless signcryption scheme without bilinear pairing in 2008, many researchers have done a lot of efforts on the security and efficiency of the certificateless signcryption scheme without bilinear pairing. Jing[10] designed an efficient certificateless signcryption scheme without bilinear pairing, but Wang[11]demonstrated that Jing's scheme neither satisfies unforgeability nor satisfies confidentiality through specific attacks; Liu[12]proposed another efficient signcryption scheme, but He[13] pointed out that it does not have its claimed security. The certificateless signcryption scheme without bilinear pairing proposed by Zhu[14] was later proved to be insecure. Zhao[15] and Zhou[16] pointed out that Zhu's scheme could be forged and given a specific method of forgery. Based on previous schemes ,Wang[11], Zhao[15], and Zhou[16] designed a new certificateless signcryption scheme respectively and gave the scheme's security prove. Through in-depth analysis of these improved solutions, this paper finds that their solutions can resist the attack of the attacker replacing a single public key, but cannot resist the attack of replacing

978-1-5386-5495-8/18/$31.00 ©2018 IEEE

multiple public keys at the same time. In addition, the plans of Zhou [16] and Wang[17] did not meet the forward security. This article conducts an in-depth study of the schemes of Wang[11] and zhou[15]. By increasing the restrictions of the association between public keys, a new certificateless signcryption scheme without bilinear pairing is designed. The new scheme has unforgeability, confidentiality, public verifiability, and forward security. The computational cost is lower and the efficiency is higher. It is suitable for resource-constrained network environment.

II. SAFETY ANALYSIS OF ZHAO'S SCHEME

This section constructs concrete attack algorithms to prove that the schemes of Wang and Zhao cannot meet their claimed unforgeability and confidentiality. Since Wang and Zhao's plan have the same security risks, this section uses Zhao's plan[15] as an example to give specific attack steps. Zhao's plan is detailed in [15].

Let users A and B be the sender and receiver respectively, A's private key is $SK_A=(t_A,z_A)$, public key is $PK_A=(w_A,u_A)$. B's private key is $SK_B=(t_B,z_B)$, public key is $PK_B=(w_B,u_B)$. Let Q be an attacker of type 1 (that is, the role of an ordinary user in a simulated system, who does not know the system's master key, but can replace the public key of a legitimate user).

A. Unforgeablity Attack

The following attack can illustrate that Zhao's scheme does not satisfy unforgeability:

1) The attacker Q chooses random numbers $a,b,c\in Z^*_q$, computes $u_A'=g^a$, $w_A'=g^b$, $y'=g^c$, and replaces u_A,w_A,y respectively.

2) Q randomly selects r, Q calculates as (1):

$$R=g^r,\quad k_A'=H_2\left(ID_A,u_A',w_A',y'\right)$$

$$h_A'=H_1\left(ID_A,w_A',y'\right),\quad k_B'=H_2\left(ID_B,u_B,w_B,y'\right)$$

$$h_B=H_1\left(ID_B,w_B,y\right),\quad T=\left(u_B^{k_B'}w_B y^{h_B}\right)^r \tag{1}$$

$$c=H_4(T)\oplus m,\quad h=H_3(m,R,T)$$

$$s=\frac{r+h}{k_A'a+b+ch_A'}$$

3) Q sends message $\sigma=\{R,s,c\}$ to B.

Theorem 1 Q's signcrypted text produced by the above method are legal.

Proof: After receiving the signcrypted text $\sigma=\{R,s,c\}$, B performs the unsigncryption algorithm. We only need to prove that the signcrypted text can be verified through the unsigncryption algorithm.

Because the attacker Q replaced the public key, the public key of user A used by B is $PK_A=\left(w_A',u_A'\right)$, the system public parameters is $y=y'$, where $u_A'=g^a$, $w_A'=g^b$, $y'=g^c$.

B's verification process is as follows:

1) B computes as (2):

$$k_B'=H_2\left(ID_B,u_B,w_B,y'\right)$$

$$T'=R^{k_B'z_B+t_B}=\left(u_B^{k_B'}w_B y^{h_B}\right)^r=T \tag{2}$$

$$m=H_4(T)\oplus c$$

2) B computes and verifies as (3):

$$h=H_3(m,R,T),\quad h_A'=H_1\left(ID_A,w_A',y'\right)$$

$$k_A'=H_2\left(ID_A,u_A',w_A',y'\right) \tag{3}$$

$$\left(u_A'^{k_A'}w_A'y'^{hA'}\right)^s=\left(g^{ak_A'}g^b g^{ch_A'}\right)^s=g^{\left(ak_A'+b+ch_A'\right)\frac{r+h}{ak_A'+b+ch_A'}}=Rg^h$$

Since $\left(u_A'^{k_A'}w_A'y'^{hA'}\right)^s$ is equal to Rg^h, B accepts the message m. Therefore, Zhao's improvement plan does not satisfy unforgeability under such attack.

B. Confidentiality Attack

The following attack can illustrate that Zhao's scheme does not satisfy confidentiality:

1) The attacker Q chooses random numbers $a,b,c\in Z^*_q$, computes $u_A'=g^a$, $w_A'=g^b$, $y'=g^c$, and replaces u_A,w_A,y respectively.

2) Q randomly selects r, Q calculates as (4):

$$R=g^r,k_A'=H_2\left(ID_A,u_A',w_A',y'\right)$$

$$h_A'=H_1\left(ID_A,w_A',y'\right),k_B'=H_2\left(ID_B,u_B,w_B,y'\right)$$

$$h_B=H_1\left(ID_B,w_B,y\right),T=\left(u_B^{k_B'}w_B y^{h_B}\right)^r \tag{4}$$

$$c=H_4(T)\oplus m,\quad h=H_3(m,R,T)$$

$$s=\frac{r+h}{k_A'a+b+ch_A'}$$

3) Q sends message $\sigma=\{R,s,c\}$ to B.

Theorem 1 Q's signcrypted text produced by the above method are legal.

Proof: After receiving the signcrypted text $\sigma=\{R,s,c\}$, B performs the unsigncryption algorithm. We only need to prove that the signcrypted text can be verified through the unsigncryption algorithm.

Because the attacker Q replaced the public key, the public key of user A used by B is $PK_A = \left(w_A^{'}, u_A^{'}\right)$, the system public parameters is $y = y^{'}$, where $u_A^{'} = g^a$, $w_A^{'} = g^b$, $y' = g^c$.

B's verification process is as follows:

1) B computes as (5):

$$k_B^{'} = H_2\left(ID_B, u_B, w_B, y'\right)$$

$$T^{'} = R^{k_B^{'} z_B + t_B} = \left(u_B^{k_B^{'}} w_B y^{h_B}\right)^r = T \tag{5}$$

$$m = H_4(T) \oplus c$$

2) B computes and verifies as (6):

$$h = H_3(m, R, T),\ h_A^{'} = H_1\left(ID_A, w_A^{'}, y^{'}\right)$$

$$k_A^{'} = H_2\left(ID_A, u_A^{'}, w_A^{'}, y^{'}\right) \tag{6}$$

$$\left(u_A^{'k_A^{'}} w_A^{'} y^{'hA'}\right)^s = \left(g^{ak_A^{'}} g^b g^{ch_A^{'}}\right)^s = g^{\left(ak_A^{'} + b + ch_A^{'}\right)\frac{r+h}{ak_A^{'} + b + ch_A^{'}}} = Rg^h$$

Since $\left(u_A^{'k_A^{'}} w_A^{'} y^{'hA'}\right)^s$ is equal to Rg^h, B accepts the message m. Therefore, Zhao's improvement plan does not satisfy unforgeability under such attack.

III. THE NEW SIGNCRYPTION SCHEME

For the schemes in [10][12][14], by controlling u_A/u_B, the attacker uses a simple linear relationship to eliminate the influence of t_A / t_B on the signcrypted text and to achieves the purpose of forgery. On this basis, the schemes in [11][13][15] improve their plans. Although replace single public key attack is avoided, after analyzing in the previous section, simply destroying this linear relationship can resist the attacker replacing the single public key Attacks, but if an attacker replaces multiple public keys at the same time, replacing multiple public keys with irrelevant numbers, the improved solution is also insecure. Therefore, in order to improve the defects of the existing schemes, this section designs a new certificateless signcryption scheme without bilinear pairing, and analyzes the correctness of the scheme.

A. Scheme Description

This scheme is composed of system parameter setup algorithm, partial key generation algorithm, private key generation algorithm, public key generation algorithm, signcryption algorithm and unsigncryption algorithm.

1) system parameter setup algorithm

The KGC takes k as the input security parameter and produces two large primes p, q, $q \mid p$-1. G is a cyclic additive group on the elliptic curve, p is a random generator of this group. Select several safe hash functions. H_1: $\{0,1\}^{L_1} \times G \times G \to G$; H_2: $\{0,1\}^{L_1} \times G \times G \times G \to G$; H_3: $G \times \{0,1\}^{L_2} \to G$; H_4: $G \to \{0,1\}^{L_2}$, where L_1 is the length of the user ID, L_2 is the length of the plaintext message.

The KGC randomly selects $x \in Z_q^*$ as the master key, calculates $y = xp$, secrets the master key x and exposes system parameters $(p, q, y, H_1, H_2, H_3, H_4)$。

2) partial key generation algorithm

Given the user's identity ID_i, KGC randomly selects $s_i \in Z_q^*$ and calculates $w_i = s_i p$, $t_i = s_i + xH_1\left(ID_i, w_i, y\right)$, t_i is user's partial private key, w_i is user's partial public key. KGC sends the partial private key to user over a secure channel.

When user receives the partial private key from the KGC, it needs to verify whether equation $t_i p = w_i + yH_1\left(ID_i, w_i, y\right)$ is established. If established, it accepts the partial private key generated from the KGC and saves y at the same time. If not, it discards the partial private key sent by the KGC.

3) private key generation algorithm

Given the user's identity ID_i and partial private key t_i, the user randomly selects $z_i \in Z_q^*$ as a secret value. The user's private key is $SK_i = (t_i, z_i)$.

4) public key generation algorithm

Given the user's identity ID_i and partial public key w_i, user calculates $u_i = z_i p$. The user's public key is $PK_i = (w_i, u_i)$.

5) signcryption algorithm

When user A wants to send a message m to user B, A chooses a random number $r \in Z_q^*$, and calculates *as the following:*

$$R = rp,\ k_B = H_2\left(ID_B, w_B, u_B, y\right)$$

$$h_B = H_1\left(ID_B, w_B, y\right),\ T = r\left(k_B u_B + w_B + h_B y\right) \tag{7}$$

$$C = H_4(T) \oplus m,\ h = H_3(T, C),\ s = \frac{r}{k_A z_A + t_A + h}$$

A sends message $\sigma = \{R, s, C\}$ to B.

6) unsigncryption algorithm

After B receives the signcrypted text, B performs the following operations:

B calculates and recovers the plaintext as (8):

$$k_B = H_2\left(ID_B, w_B, u_B, y\right),\ T^{'} = R\left(k_B z_B + t_B\right)$$

$$m = H_4\left(T^{'}\right) \oplus C,\ h^{'} = H_3\left(T^{'}, C\right) \tag{8}$$

$$h_A = H_1\left(ID_A, w_A, y\right),\ R^{'} = s\left(k_A u_A + w_A + y h_A + h^{'} p\right)$$

B compare whether $R^{'}$ and R (sent from A) are equal. If they are equal, B accepts the message m. If it is not equal, it discards.

B. Correctness Analysis of The New Scheme

According to the unsigncryption algorithm:

$$\begin{aligned} T' &= R\left(k_B z_B + t_B\right) \\ &= rp\left(k_B z_B + t_B\right) \\ &= r\left(k_B z_B p + t_B p\right) \\ &= r\left(k_B u_B + w_B + y h_B\right) \\ &= T \end{aligned} \tag{9}$$

According to (9), B can recover the plaintext.

Since $T' = T$, then B calculates $h' = H_3\left(T', c\right) = h$

$$\begin{aligned} R' &= s\left(k_A u_A + w_A + y h_A + hp\right) \\ &= \frac{r}{k_A z_A + t_A + h}\left(k_A u_A + w_A + y h_A + hp\right) \\ &= \frac{r}{k_A z_A + t_A + h}\left(k_A z_A + t_A + h\right) p \\ &= rp \\ &= R \end{aligned} \tag{10}$$

As R' is equal to R , B accepts the message m.

As a result, the correctness of the proposed scheme can be proved.

IV. Analysis of New Construction Scheme

A. security analysis

1) Unforgeability and Confidentiality Analysis

This scheme is improved based on the previous schemes, so the new construction scheme can resist the replacement of a single public key attack. For attacks that replace multiple public keys, the user needs to verify whether $t_i p = w_i + y H_1\left(ID_i, w_i, y\right)$ is true when he receives KGC's partial private key in the new construction scheme. If it is, user can uses the partial private key and saves y at the same time. The attacker must replace y before user obtains the partial private key, because user will save y after obtaining the correct partial private key. At the same time, because the attacker does not know partial private key, if the attacker wants to replace y and w_i, the sum $w_i + y H_1\left(ID_i, w_i, y\right)$ before and after the replacement must be equal. Let $w_i + y H_1\left(ID_i, w_i, y\right)$ is equal to M, that is $w_i + y H_1\left(ID_i, w_i, y\right) = M$, and M is a fixed value.

Assuming that the attacker randomly selects a number a , replaces w_i with $w_i' = ap$. If the attacker wants to replace y with $y' = cP$, in that way, $y' H_1\left(ID_i, w_i, y\right) = cp H_1\left(ID_i, w_i, y\right) = M - w_i$. it is very difficult for an attacker to solve for c from equations $cp H_1\left(ID_i, w_i, y\right) = M - ap$ (M, a, $H_1\left(ID_i, w_i, y\right)$ and p are known), because it is a discrete logarithm problem on the elliptic curve.

By increasing the user's verification step when receiving partial private key, it is ensured that the system parameter y user stored is true, thus making it impossible for the attacker to replace w_i , u_i and y as irrelevant values. Therefore, the proposed scheme can resist attacks that replace multiple public keys. That is, the improved signcryption scheme in this paper can provide unforgeability and confidentiality.

2) Forward Security Analysis

In the new scheme, even if the sender's partial private key and secret value are both accidentally leaked, the person who has obtained the private key cannot calculates the random number r selected for each signcryption, cannot calculates T , and thus the plaintext cannot be recovered.

3) Public Verification Analysis

In the new construction scheme, when a dispute is encountered, the receiver only needs to submit the signcrypted text $\{h, s, R\}$ to the arbitrator, which can verify the authenticity of the signcrypted text. The entire verification process does not require the plaintext and the recipient's private key. In the case of known $\{h, s, R\}$, the verifier can not calculate the relevant information in plaintext. Therefore, the scheme of this article satisfies public verifiability.

Compare each scheme with the scheme of this article as follows, the results are shown in Table 1.

TABLE I. Security contrast of several schemes

scheme	Unforgeablity	Confidentiality	Forward Security	public verifiability
Scheme In [14]	×	×	×	×
Scheme In [15]	×	×	√	×
Scheme In [16]	√	√	×	×
Our scheme	√	√	√	√

Note: √ Satisfied, × Not satisfied

From the above table, we can see that in the case of attackers replacing multiple public keys, the improved scheme can still provide unforgeability and confidentiality. At the same time, the scheme has forward security and is publicly verifiable. In summary, the improved scheme proposed in this article is safer than the previous scheme.

B. Performance Analysis

This section compares the signcryption scheme proposed in this article with other certificateless signcryption schemes. For the elliptic curve-based scheme, we use the Koblitz curve $y^2 = x^3 + ax^2 + b$ defined on $F_{2^{163}}$, where $a = 1$ and b is a 163-bit prime number. The operating time for different operations is shown in Table 2[7]. Among them, ME represents the modular exponentiation operation, and SM represents the point multiplication on elliptic curve.

TABLE II. Running time of different operation

ME	SM
11.20ms	6.38ms

Here we compare the performance of the new scheme in this paper with the previous three schemes. Compared with the running time of the modular exponentiation operation and the elliptic curve point multiplication operation, the impact of the hash function and the exclusive OR operation on the overall performance is negligible. Here only the operation of the

elliptic curve point multiplication operation and the modular exponentiation operation are counted, as shown in Table 3.

TABLE III. CONTRAST OF COMPUTATION COST OF SEVERAL SCHEMES

Scheme	Signcryption	Unsigncryption
Scheme in [14]	3ME	4ME
Scheme in [15]	4ME	5ME
Scheme in [16]	2ME	6ME
Our scheme	3SM	5SM

From Table 3, it can be seen that the improved scheme in this paper also has an improvement in performance, which has advantages over those of Zhu, Zhao and Zhou. Therefore, the improved certificateless signcryption scheme has lower computational complexity and higher efficiency.

V. CONLUSION

This paper analyzes and summarizes the existing certificateless signcryption schemes without bilinear pairing. It finds that the existing scheme is insecure and cannot provide unforgeability and confidentiality when the attacker replaces multiple public keys at the same time, and gives the attack process. On this basis, this paper designs a new certificateless signcryption scheme without bilinear pairing. The new scheme resists the attacker's replacement of multiple public keys by increasing the correlation between public keys. After analysis, our scheme can not only meet the requirements of unforgeability, confidentiality, forward security, and public verification, but also reduce the amount of computation compared with previous scheme. By comparison, the scheme of this paper has higher security and operating efficiency.

REFERENCES

[1] CHI I Hsu and YU Ching Tung, The benefits of PKI application and competitive advantage [J]. WSEAS Transactions on communications, 2008, 7(9): 758-767.

[2] C. Ellison and B. Schneier, Ten risk of PKI: What you are not being told about public key infrastructure [J]. Computer Security Journal, 2000, 16(1): 1-7.

[3] ADI Shamir, Identity–based cryptosystems and signature schemes [C]. Advances in Cryptology –Crypto'84, Berlin: Springer-Verlag, 1984: 47-53.

[4] SS. AL-Riyami and KG. Paterson, Certificateless public key cryptography [C]. Advances in Cryptology-Asiacrypt'03, Berlin: Springer-Verlag, 2003: 452-473.

[5] YL. Zheng. Digital signcryption or how to achieve cost (signature & encryption « cost (signature) + cost (encryption) [C]. Advances in Cryptology-Crypto'97, Berlin: Springer-Verlag, 1997: 165—179.

[6] L. Chen, Z. Cheng and NP. Smart, Identity-based key agreement protocols from pairings[J]. Interational Journal of Information Security, 2007, 6(2): 213-241.

[7] X. Cao and W. Kou, A pairing-free identity-based authenticated key agreement scheme with minimal message exchanges[J].Information Sciences, 2010, 180(6): 2895-2903.

[8] D. He, J. Chen and J. Hu, An ID-based proxy signature schemes without bilinear pairings[J]. Annals of Telecommunications, 2011, 66(11-12): 657-662.

[9] P. Barreto, A. Deusajute, E. Cruz and et al, Toward efficient certificateless signcryption from (and without)bilinear pairing[EB/OL]. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_03_artigo.pdf.

[10] XF. Jing, Provably secure certificateless signcryption scheme without pairing[C]. 2011 International Conference on Electronic and Mechanical Engineering and Information Technology. China: IEEE, 2011: 4753-4756.

[11] DG. Wang, XF. Ding and K. Huang, Security analysis and improvement of strongly secure certificateless key agreement protocol[J]. Computer Science, 2013, 40(11A): 203-223.

[12] WH. Liu and C. Xu, Certificateless signcryption scheme without bilinear pairing[J]. Journal of software, 2011, 22(8):1918-1926.

[13] DB. He, Security analysis of a certificateless signcryption scheme[J]. Journal of software, 2013, 24(3): 618-622.

[14] H. Zhu, H. Li and YM. Wang, Certificateless signcryption scheme without pairing[J]. Journal of Computer Research and Development, 2010, 47(9): 1587-1594.

[15] ZG. Zhao, Security analysis and improvement of a certificateless signcryption scheme[J]. Journal of Commuication, 2015, 36(3): 2015060_1-2015060_6.

[16] YW. Zhou, B. Yang and WZ. Zhang, Security analysis and improvement of certificateless signcryption scheme without bilinear pairing[J], CHINESE JOURNAL OF COMPUTER, 2016, 39(6), 1257-1266.

[17] X. Wang, ZH. Qi and H. Huang, A certificateless signcryption scheme without bilinear pairing[J]. COMPUTER TECHNOLOGY AND DEVELOPMENT, 2017, 27(7): 106-110.