Cryptanalysis of a Certificateless Ring Signcryption Scheme

Hongzhen Du¹ and Qiaoyan Wen²

¹ School of Mathematics and Information Science, Baoji University of Arts and Sciences, Baoji 721007, China
² School of Science, Beijing University of Posts and Telecommunications, Beijing 100876, China
hongzhendu@163.com

Abstract

Certificateless public key cryptography (CL-PKC) is an appealing paradigm with the advantages of both conventional public key cryptosystem and ID-based cryptosystem because it avoids using certificates and eliminates the key escrow problem. Ring signcryption is an attractive primitive which allows one user to send a message anonymously, confidentially and authentically. Recently, Qi et al. proposed a novel certificateless ring signcryption scheme with bilinear pairings, and claimed the scheme is provably-secure in the random oracle model. In this paper, we reveal that Qi et al.’s scheme is not secure against both a Type I adversary and a Type II adversary. By giving specific attacks, we found it is unable to meet the fundamental requirements of confidentiality and unforgeability.

Keywords: certificateless public key cryptography, ring signcryption, confidentiality, unforgeability

1. Introduction

Identity-based cryptography (IBC) was first put forward by Shamir [1] in 1984, which permits a user to utilize his identity information such as name, e-mail address, telephone number, etc. as his own public key. This public key is well-known and does not need a certificate to guarantee his authenticity. This greatly eliminates the certificate management problems in a conventional Public Key Cryptosystem (PKC). However, in an IBC, there innately exists a drawback named private key escrow because the cryptosystem needs a Private Key Generator (PKG), which is in charge of generating a user’s private key on the basis of his identity. Consequently, the PKG can literally decipher any ciphertext and fake any user’s signature on a message.

To solve the key escrow problem in IBC, Al-Riyami and Paterson [2] put forward Certificateless Public Key Cryptography (CL-PKC) in 2003. The CL-PKC is a medium between conventional PKC and IBC. In a CL-PKC, a user’s private key is not produced by the Key Generation Center (KGC). Instead, it is composed of a partial private key produced by the KGC and a secret value picked by the user. Therefore, the KGC is unable to gain the user’s private key. Thus, the key escrow problem in IBC can be solved. CL-PKC not only overcomes the key escrow problem in IBC, but also eliminates the usage of certificates in the conventional PKC. So, CL-PKC has attracted great attention, many certificateless cryptosystems have been designed, including many certificateless signature schemes and certificateless encryption schemes, e.g. [3-7].

The definition of signcryption was first proposed by Zheng [8]. Signcryption absorbed the functions of both public key encryption and signature synchronously, and outdoes the sign-then-encrypt method. Ring signcryption entitles a user to signcrypt one message along with identities of a group of potential senders, including the user himself, but does
not reveal which user in the group has produced the signcryption in fact. Ring signcryption is an effective method for leaking trustworthy secrets anonymously, authentically and confidentially. The first identity-based ring signcryption scheme was proposed by Huang et al. [9] in 2005. Subsequently, several identity-based ring signcryption schemes have been constructed, such as [10-12]. However, Sree Vivek S. et al. [13] showed that the scheme in [10] has the security weakness. Selvi et al. [14] pointed out that schemes in [11-12] are insecure against the chosen plaintext attacks. Zhu et al. [15] presented an efficient identity-based ring signcryption scheme from bilinear pairings. However, Deng et al. [16] show that the scheme is not secure and present an improved scheme.

Being a primitive in CL-PKC, certificateless ring signcryption (CLRSC) schemes are usually used in communication gaining anonymity, authentication and confidentiality. However, up to now, there are few research results on CLRSC. Recently, Qi et al. [17] constructed a CLRSC scheme based on bilinear pairings and claimed that the scheme is secure against both Type I and Type II adversaries, and satisfies the needs of confidentiality and unforgeability. Unfortunately, we found that Qi et al.’s CLRSC scheme cannot resist attacks from a Type I or a Type II adversary. In our attack, we show that a Type I or Type II adversary is able to decrypt any ring ciphertext generated for the receiver. Moreover, we point out that a Type I or Type II adversary can impersonate any sender to send a valid ring signcrypted message to a receiver.

The following sections are organized as below. In the next section, we review bilinear pairings and introduce the definition and the security notions for CLRSC scheme. In Section 3, we review Qi et al.’s CLRSC scheme. In Section 4, we give concrete attacks on Qi et al.’s CLRSC scheme. Conclusions are drawn in the last section.

2. Preliminaries

In this subsection, we briefly introduce bilinear pairings.

2.1. Bilinear Pairings

Let $G_1$ be a cyclic additive group of prime order $q$, and $G_2$ be a cyclic multiplicative group of the same order $q$. A bilinear pairing is a map $e: G_1 \times G_1 \rightarrow G_2$ which meets the following properties:

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$, where $P, Q \in G_1$, $a, b \in \mathbb{Z}_q^*$.
2. Non-degeneracy: There exist $P, Q \in G_1$ such that $e(P, Q) \neq 1$.
3. Computability: There exists a computable algorithm to obtain $e(P, Q)$ for all $P, Q \in G_1$.

2.2. Formal Definition of Certificateless Ring Signcryption

A CLRSC scheme consists of the following five polynomial time algorithms.

(i) Setup: This algorithm takes a security parameter $k$ as input and outputs the system parameters $\text{params}$ and the master secret key $s$.

(ii) Partial-Private-Key-Extract: Taking $\text{params}$ and a user’s identity $ID_i$ as input, it outputs the user $ID_i$’s partial private key $D_i$.

(iii) Key-Extract: Taking as input $\text{params}$, a user’s $ID_i$ and his partial private key $D_i$, and a randomly chosen secret value $t_i$, it returns the user’s public key $PK_i$ and the user’s (full) private key $SK_i$.

(iv) Signcrypt: To send a message $m$ to the receiver with the identity $ID_a$ and the public key $PK_a$, the sender with the identity $ID_i$ and the public key $PK_i$ chooses some other users to form a group $R=\{ID_{b_1}, ID_{b_2}, \ldots, ID_{b_r}, \ldots, ID_a\}$ (including himself) and runs the Signcrypt algorithm as below:
Taking as input \( \text{params}, m, R \) and the ring member’s public key \( PK_i \) (1 ≤ i ≤ n), and the actual sender’s private key \( SK_r \), the receiver’s identity \( ID_a \) and his public key \( PK_a \), the algorithm outputs a ring signcrypted ciphertext \( \sigma \).

(\text{V}) -\text{Unsigncrypt}: On providing \( \text{params}, \sigma, R, \) and \( PK_i \) (1 ≤ i ≤ n), the receiver’s identity \( ID_a \) and his private key \( SK_a \), the algorithm outputs the plaintext \( m \) if \( \sigma \) is a valid signcryption from \( R \) to \( ID_a \). Otherwise, it outputs an error symbol \( \perp \).

2.3. Security Requirements of Certificateless Ring Signcryption

As mentioned in [2], there exist two types of adversaries who have different capabilities in CL-PKC. Type I adversary imitates a dishonest user that does not have the knowledge of the master secret key but is able to replace a user’s public key arbitrarily, while Type II adversary models a malicious-but-passive KGC who knows the master secret key but is not capable of replace the public key of the target user.

The basic security requirements of a CLRSC scheme are “Message Confidentiality”, “Message Unforgeability” and “Message Anonymity”. Message Confidentiality means that only the receiver can retrieve the message from the signcrypted text. Message Unforgeability means only one of the ring members can generate a valid signcrypted text. Precise definitions of Message Confidentiality and Message Unforgeability are defined using security models. For the detail, please refer to [17].

3. Review of Qi et al.’s Certificateless Ring Signcryption Scheme

We review Qi et al.’s certificateless ring signcryption scheme [17], which is specified by the following five algorithms:

-Setup(\( k \)): Given a security parameter \( k \), the KGC chooses two groups \( G_1 \) and \( G_2 \) of the same prime order \( q \), a generator \( P \) in \( G_1 \) and a bilinear map \( e: G_1 \times G_1 \rightarrow G_2 \), and selects a random number \( s \in \mathbb{Z}_q^* \) as the master secret key and sets the public key \( p_{pub}=sP \). Then, the KGC chooses four cryptographic hash functions \( H_0: \{0, 1\}^* \rightarrow G_1 \), \( H_1: G_2 \rightarrow \{0, 1\}^l \times G_1 \), \( H_2: \{0, 1\}^l \times G_1 \times \{0, 1\}^* \times \{0, 1\}^* \times G_1 \rightarrow \mathbb{Z}_q^* \), \( H_3: \{0, 1\}^l \times \mathbb{Z}_q^* \rightarrow \mathbb{Z}_q^* \), and \( M=\{0, 1\}^l \), where \( l \in \mathbb{Z}^+ \) is an arbitrary fixed integer. The system parameters are \( \text{params} = <q, G_1, G_2, e, P, p_{pub}, H_0, H_1, H_2, H_3> \).

-Partial-Private-Key-Extract: Given a user’s identity \( ID_i \in \{0, 1\}^* \), the KGC computes \( Q_i=H_0(ID_i) \) and outputs the user \( ID_i \)’s partial private key \( D_i=sQ_i \).

-Key-Extract: The user with the identity \( ID_i \) chooses a random value \( t_i \in \mathbb{Z}_q^* \) and sets his full private key as \( SK_i=(t_i, S_i)=(t_i, t_1D_1) \) and sets his public key as \( PK_i=(t_iP+Q_i, t_1) \).

-Signcrypt: To send a message \( m \) to the receiver with identity \( ID_a \) and public key \( PK_a \), the sender with identity \( ID_i \) and public key \( PK_i \), uses his private key \( (t_i, S_i) \) to perform the following steps:

(i) Choose \( n \) potential senders and form a group \( R=(ID_1, ID_2, \ldots, ID_n, \ldots ID_n) \).
(ii) Randomly pick \( r \in \mathbb{Z}_q^* \) and compute \( \alpha = H_1(m, r), U = \alpha P, w = e(P_{pub}, PK_a)^\alpha \).
(iii) For \( i=1 \) to \( n \), \( i \neq r \), randomly choose \( x_i \in \mathbb{Z}_q^* \) and compute \( R_i=x_iP, h_i=H_2(m, R_i, w, R_i, ID_a, PK_a) \).
(iv) Randomly pick \( x_r \in \mathbb{Z}_q^* \) and compute \( R_r = x_rQ_r - \sum_{i=1, i \neq r}^n (R_i + h_iPK_i) \) and \( h_r=H_2(m, R_r, w, R_r, ID_a, PK_a) \).
(v) Compute \( Z=x_rD_r+h_r(t_rP_{pub}+S_i) \).
(vi) Set \( c = (m||Z) \oplus H_j(w) \).
(vii) Output the ciphertext \( \sigma = (c, U, R, R_i, \ldots, R_r) \) to the receiver \( ID_a \).
-Ring-Unsigncrypt: Upon receiving a ciphertext $\sigma=(c,U,R,R_i,\cdots,R_n)$, the receiver with identity $ID_A$ and public key $PK_A$ uses his private key $SK_A=(t_A, S_A)$ to decrypt the ciphertext as follows:

(i) Compute $w=e(U,t_A P_{pub}+S_A)$ and recover $m\|Z = c \oplus H_1(w)$.

(ii) For $i=1$ to $n$, compute $h_i=H_2(m, R_i, w, R, ID_A, PK_A)$ and check whether the following equation holds: $e\left(P_{pub}, \sum_{i=1}^{n}(R_i + h_i PK_i)\right) = e(P, Z)$.

(iii) Output $m$ if the equation holds. Otherwise, output an error symbol $\perp$.

About the correctness and the security analysis of the scheme, refer to [17].

4. Cryptanalysis of Qi et al.’s CLRSC Scheme

Qi et al. claimed that their scheme is both semantically secure against adaptive chosen ciphertext attacks and existentially unforgeable against adaptive chosen message attacks. However, in this section, we describe our attacks on Qi et al.’s scheme [17] to show its security vulnerabilities. We show that Qi et al.’s scheme does not achieve the requirements of message confidentiality and unforgeability under a Type I/II adversary’s attack.

4.1. Message Confidentiality Attack

In this subsection, we point out that Qi et al.’s scheme does not satisfy the property of message confidentiality.

4.1.1. The Type I Adversary $A_1$’s attack: A Type I adversary $A_1$ is able to unsigncrypt any ring ciphertext $\sigma=(c,U,R,R_i,\cdots,R_n)$ generated under the receiver $ID_A$’s public key chosen by $A_1$. The concrete attack is described in three stages.

Stage 1: $A_1$ picks a random value $t_A' \in Z_q^*$ and computes $PK_A'=t_A'P$, and replaces the receiver’s public key $PK_A$ with $PK_A'$.

Stage 2: Since no certificate is provided to bind a user and his public key, a sender with identity $ID_R$ cannot detect the receiver’s public key $PK_A$ is replaced by $A_1$. As a result, the sender will generate a ring signcrypted text with the public key $PK_A'$ of the receiver as follows:

(i) Choose $n$ potential senders and form a group $R:\{ID_1, ID_2, \cdots, ID_n, \cdots, ID_n\}$.

(ii) Randomly pick $r \in Z_q^*$ and compute $\alpha = H_2(m, r)$, $U = \alpha P$, $w = e(P_{pub}, PK_A')^\alpha$.

(iii) For $i=1$ to $n$, $i \neq r$, randomly choose $x_i \in Z_q^*$ and compute $R_i=x_i P$, $h_i=H_2(m, R_i, w, R, ID_A, PK_A')$.

(iv) Randomly pick $x \in Z_q^*$ and compute $R' = x_r P - \sum_{i=1, i \neq r}^{n}(R_i + h_i PK_i)$ and $h_i=H_2(m, R_i, w, R, ID_A, PK_A')$.

(v) Compute $Z=x, D_i+h_i(t_A' P_{pub}+S_i)$.

(vi) Set $c = (m\|Z) \oplus H_1(w)$.

(vii) Output the ciphertext $\sigma=(c,U,R,R_i,\cdots,R_n)$ to the receiver $ID_A$.

Stage 3: Upon receiving the ciphertext $\sigma=(c,U,R,R_i,\cdots,R_n)$, the Type I adversary $A_1$ decrypts the ciphertext as follows:

(i) Compute $w' = e(U,t_A' P_{pub}) = e(\alpha P,t_A' P_{pub}) = e(\alpha P_{pub},t_A' P) = e(P_{pub}, PK_A')^\alpha = w$, and recover $m\|Z = c \oplus H_1(w)$.
(ii) For $i=1$ to $n$, compute $h_i = H_2(m, R_i, w, R_i, ID_A, PK_A)$ and check whether the following equation holds: $e(Pr_{pub} \sum_{i=1}^n (R_i + h_i PK_i)) = e(P, Z)$. Thus, $A_1$ successfully obtains the message $m$.

4.1.2. The Type II Adversary $A_2$'s Attack: We also point out that Qi et al.‘s scheme is unable to resist attacks from a Type II adversary $A_2$ who knows the master secret key $s$ is able to unsigncrypt any ciphertext $\sigma = (c, U, R_i, \cdots, R_n)$ and get the corresponding plaintext $m$. The concrete attack is described in two stages.

Stage 1: $A_2$ computes $K_i = s \cdot PK_i$, where $PK_i = t_i (P + Q_\alpha)$ is the receiver’s public key.

Stage 2: Given a ciphertext $\sigma = (c, U, R, R_1, \cdots, R_n)$, $A_2$ uses $K_A$ to decrypt the ciphertext as follows:

(i) Compute $w = e(U, K_A) = e(U, s(t_A(P + Q_\alpha))) = e(U, t_A Pr_{pub} + S_\alpha)$.

(ii) Recover $(m \parallel Z) = c \oplus H_1(w)$.

As a result, $A_2$ gets the message $m$.

4.2. Unforgeability Attack

We show that Qi et al.‘s scheme is universally forgeable by a Type I adversary $A_1$ or a Type II adversary $A_2$. That is, Both $A_1$ and $A_2$ can arbitrarily forge a valid CLRSC ciphertext on any message with his choice on behalf of any sender.

4.2.1. The Type I Adversary $A_1$’s Attack: We indicate that a Type I adversary $A_1$ can successfully forge a valid ring signcryption ciphertext to cheat the receiver $ID_A$ by replacing the sender $ID_i$‘s public key $PK_i$ with $PK_i = PK_i' = l_iP$.

Stage 1. $A_1$ randomly picks $l_i \in Z_q^*$ and replaces the sender $ID_i$‘s public key $PK_i$ with $PK_i = PK_i' = l_iP$.

Stage 2. $A_1$ impersonate the sender $ID_i$ to generate a valid ciphertext as follows:

(i) Pick $n$ potential senders and form a group $R = \{ID_1, ID_2, \cdots, ID_n\}$.

(ii) Randomly pick $r \in Z_q^*$ and compute $\alpha = H_1(m, r)$, $U = \alpha P$, $w = e(P_{pub}, PK_A)^{\alpha}$.

(iii) For $i=1$ to $n$, $i \neq r$, randomly choose $x_i \in Z_q^*$ and compute $R_i = x_iP$, $h_i = H_2(m, R_i, w, R_i, ID_A, PK_A)$.

(iv) Randomly pick $x_i \in Z_q^*$ and compute $R_i = x_iP - \sum_{i=1, i \neq r}^n (R_i + h_i PK_i)$ and $h_i = H_2(m, R_i, w, R_i, ID_A, PK_A)$.

(v) Compute $Z = x_i P_{pub} + h_i P_{pub}$.

(vi) Set $c = (m \parallel Z) \oplus H_1(w)$.

(vii) Output the ciphertext $\sigma = (c, U, R, R_1, \cdots, R_n)$.

Stage 3. Given a ciphertext $\sigma = (c, U, R, R_1, \cdots, R_n)$ and all senders’ public keys $PK_1, PK_2, \cdots, PK_n$, the receiver $ID_A$ cannot detect that the sender $ID_i$‘s public key is replaced by $A_1$, he decrypts the ciphertext as follows:

(i) Compute $w = e(U, t_A P_{pub} + S_\alpha)$ and recover $(m \parallel Z) = c \oplus H_1(w)$.

(ii) For $i=1$ to $n$, compute $h_i = H_2(m, R_i, w, R_i, ID_A, PK_A)$ and check whether the equation $e(P_{pub} \sum_{i=1}^n (R_i + h_i PK_i)) = e(P, Z)$ holds:

(iii) Output $m$ if the equation holds. Otherwise, output an error symbol $\perp$.

The verification equation always holds. Since
\[ e \left( P_{pub}, \sum_{i=1}^{n} (R_i + h_i PK_i) \right) = e \left( P_{pub}, \sum_{i=1}^{n} (R_i + h_i PK_i) + R_i + h_i PK_i \right) = e \left( P_{pub}, x_i P + h_i PK_i \right) = e \left( P, x_i P_{pub} + h_i l P_{pub} \right) = e(P, Z). \]

It declares the forged ciphertext \( \sigma \) is valid. Therefore, we point out Qi et al.’s scheme is subject to universal forgery attack of a Type I adversary.

4.2.2 The Type II Adversary \( A_2 \)'s Attack: We indicate that a Type II adversary \( A_2 \) can successfully forge a valid ring signcrypted message to cheat the receiver \( ID_A \). \( A_2 \) performs as follows:

- **Signcrypt:** To signcrypt a message \( m' \) for the receiver with the identity \( ID_A \) and the public key \( PK_A \) on behalf of the sender with the identity \( ID_s \), and the public key \( PK_s \), \( A_2 \) computes \( D_i = sQ_i \) and \( K_r = s \cdot PK_r = s \cdot t_r(P + Q_r) = t_r P_{pub} + S_r \).

\( A_2 \) performs the following steps:

1. Choose \( n \) potential senders and form a group \( R = \{ID_1, ID_2, \cdots, ID_n, \cdots ID_A \} \).
2. Randomly pick \( r' \in Z_q^* \) and compute \( \alpha' = H_2(m', r') \), \( U' = \alpha' P \), \( w' = e(P_{pub}, PK_{\alpha'}) \).
3. For \( i=1 \) to \( n \), \( i \neq r \), randomly choose \( x_i' \in Z_q^* \) and compute \( R_i' = x_i' P \) and \( h_i' = H_2(m', R_i', w', R, ID_A, PK_A) \).
4. Randomly pick \( x_r' \in Z_q^* \) and compute \( R_r' = x_r' Q_r - \sum_{i=1, i \neq r}^{n} (R_i' + h_i' PK_i) \) and \( h_r' = H_2(m', R_r', w', R, ID_A, PK_A) \).
5. Compute \( Z' = x_r'D_r + h_r' K_r \).
6. Set \( c' = (m'\|Z') \oplus H_1(w') \).
7. Output the forged ciphertext \( \sigma' = (c', U', R', R_1', \cdots, R_n') \).

- **Unsigncrypt:** Upon receiving the ciphertext \( \sigma' = (c', U', R', R_1', \cdots, R_n') \), the receiver \( ID_A \) invokes the Unsigncrypt algorithm as follows:

\( A_2 \) performs the following steps:

1. Compute \( w' = e(U', t_{A_2} P_{pub} + S_{A_2}) \) and recover \( (m'\|Z') = c' \oplus H_1(w') \).
2. For \( i=1 \) to \( n \), compute \( h_i' = H_2(m', R_i', w', R, ID_A, PK_A) \) and check the validity of the ciphertext by verifying \( e \left( P_{pub}, \sum_{i=1}^{n} (R_i' + h_i' PK_i) \right) = e(P, Z') \).

Since we have
\[ w' = e(U', t_{A_2} P_{pub} + S_{A_2}) = e(\alpha' P, s \cdot t_{A_2} (P + Q_A)) = e(P_{pub}, t_{A_2} (P + Q_A)) = e(P_{pub}, PK_{A_2}) \]
and
\[ e \left( P_{pub}, \sum_{i=1}^{n} (R_i' + h_i' PK_i) \right) = e \left( P_{pub}, \sum_{i=1, i \neq r}^{n} (R_i' + h_i' PK_i) + R_r' + h_r' PK_r \right) = e \left( P_{pub}, x_r' Q_r + h_r' PK_r \right) = e \left( P, x_r' D_r + h_r' K_r \right) = e(P, Z'). \]

The verification equation always holds. It means the forged ciphertext \( \sigma' = (c', U', R', R_1', \cdots, R_n') \) is valid. So, we point out Qi et al.’s scheme is universally forgeable by a Type II adversary.
5. Conclusions

Ring signcryption can be used to protect privacy and authenticity of a collection of users who are connected through an ad-hoc network. In this paper, we analyze the security of a certificateless ring signcryption scheme proposed by Qi et al. and show that their scheme fails to satisfy the basic requirements of confidentiality and unforgeability for a secure certificateless ring signcryption scheme. Since no secure certificateless ring signcryption scheme is available in the literature, constructing an efficient and secure CLRSC scheme is our future work.

Acknowledgements

The work was supported by the National Natural Science Foundation of China (61402015) and Scientific Research Program of Baoji University of Arts and Sciences (ZK12042).

References

Authors

Hongzhen Du, she received the Ph.D. degree from Beijing University of Posts and Telecommunications in 2009. From 2011, she is an associate professor at Baoji University of Arts and Sciences. Her research interests include cryptography, digital signature.
E-mail: hongzhendu@163.com.

Qiaoyan Wen, she received the Ph.D. degree in cryptography from Xidian University in 1999. From 2003, she is a professor in school of science at Beijing University of Posts and Telecommunications. Her research interests include network security, cryptographic protocol and electronic commerce.
E-mail: wqy@bupt.edu.cn