On security of a certificateless signcryption scheme

Songqin Miao
Nanjing Normal University, miaosongqin@163.com

Futai Zhang
Nanjing Normal University, futai@uow.edu.au

Sujuan Li
Nanjing Normal University

Yi Mu
University of Wollongong, ymu@uow.edu.au

On security of a certificateless signcryption scheme

Abstract

It would be interesting if a signcryption scheme in the standard model could be made certificateless. One of the interesting attempts is due to Liu et al. [Z. Liu, Y. Hu, X. Zhang, H. Ma, Certificateless signcryption scheme in the standard model, Information Sciences 180 (3) (2010) 452-464]. In this paper, we provide a cryptanalysis on this scheme by depicting two kinds of subtle public key replacement attacks against it. Our analysis reveals that it does not meet the basic requirements of confidentiality and non-repudiation.

Keywords

security, certificateless, scheme, signcryption

Disciplines

Engineering | Science and Technology Studies

Publication Details

Miao, S., Zhang, F., Li, S. & Mu, Y. (2013). On security of a certificateless signcryption scheme. Information Sciences, 232 475-481.

On Security of A Certificateless Signcryption Scheme

Songqin Miao[a], Futai Zhang[a,b], Sujuan Li[a], Yi Mu[c]

[a]School of Computer Science and Technology, Nanjing Normal University, P.R. China
[b]Jiangsu Engineering Research Center on Information Security and Privacy Protection Technology, Nanjing, P.R. China
[c]Centre for Computer and Information Security Research,
School of Computer Science and Software engineering, University of Wollongong, Australia.

Abstract

It would be interesting if a signcryption scheme in the standard model could be made *certificateless*. One of interesting attempts is due to Liu, Hu, Zhang and Ma, who published a certificateless signcryption scheme in the standard model in Volume 180 (3), Information Science, in 2010. In this paper, we provide a cryptanalysis on this scheme and show that it is insecure under two kinds of subtle public key replacement attacks. We show that it does not meet the basic requirements of confidentiality and non-repudoation.

Keywords: certificateless cryptography, signcryption, public key replacement attack

1. Introduction

In traditional public key cryptography, a trusted third party called certification authority (CA) is employed to issue public key certificates to users. Public-key certification poses some problems in certificate management, including certificate generation, storage, distribution and revocation. To avoid the costly certificate management, Shamir [17] introduced the identity-based public key cryptography (ID-PKC). In ID-PKC, digital identities of users such as email address, phone number, etc. can be utilized as public keys. However, a trusted third party is required to compute private keys of users. This unfortunately introduces the key escrow problem.

Certificateless cryptography (CLC) was introduced by Al-Ryiami and Paterson [1] in order to overcome the problem of key escrow in ID-PKC and maintain certificate freeness. In CLC, a third party called Key Generation Center (KGC) is also employed to help users generate their private keys. However, the KGC only produces a partial private key for a user. To generate the full private key, the user uses the partial private key and a secret value chosen by himself. As the

Email addresses: `miaosongqin@163.com` (Songqin Miao), `zhangfutai@njnu.edu.cn` (Futai Zhang), `lisujuan1978@126.com` (Sujuan Li), `ymu@uow.edu.au` (Yi Mu)

secret value is known to the user only, the KGC cannot compute the full private key of the user. Therefore, the key escrow problem in ID-PKC is eliminated. Many certificateless cryptosystems have been proposed, including encryption schemes [1, 10, 24, 25], signature schemes [1, 11, 28, 29], key agreement protocols [1, 31], threshold cryptosystems [8, 14, 23, 26], and signcryption schemes [3, 4, 5, 12, 13, 21, 22]. As the adversary models in CLC are more complex, the security proofs in CLC are more challenging. We notice that some existing certificateless cryptosystems have been broken [16, 18, 19, 20].

Signcryption, introduced by Zheng [32], is a cryptographic primitive, which captures the encryption and signature simultaneously, and is more efficient than the sign-then-encrypt method. Many secure signcryption schemes have been proposed in traditional public key cryptosystem (e.g., [33, 2]). The signcryption in ID-PKC was first investigated by Malone-Lee [15]. Later, Boyen [6] defined the formal security model for identity-based signcryption schemes and proposed a provably secure scheme in the model. A more efficient ID-based signcryption scheme proven secure in Boyen's model [6] was given in [9].

As a primitive in CLC, certificateless signcryption (CLSC) schemes can be used in communication capturing both confidentiality and non-repudiation. The first CLSC scheme was introduced by Barbosa and Farshim [4] with a formal security analysis in the random oracle model. Later, some efficient CLSC schemes were proposed [3, 21, 22]. Unfortunately, as shown in [16, 18], all the above schemes [4, 21, 3] have security flaws. Li *et al.* commented on the certificateless hybrid signcryption in [12]. The security of the above mentioned schemes are proven in the random oracle model which can only be considered as a heuristic argument [7]. We notice that, Barreto *et al.* [5] depicted a method to construct efficient CLSC schemes. However, they only gave the assessment of the security implications of their proposal without a formal security proof. Very recently, Liu *et al.* [13] introduced an efficient certificateless signcryption scheme with the security proof in the standard model. They claimed that their scheme was provably secure under the decisional Bilinear Diffie-Hellman assumption and the computational Diffie-Hellman assumption. Unfortunately, their Security proof is not sound [16, 20] and is in fact insecure.

In this paper, we show that the CLSC scheme in [13] is flawed by demonstrating two kinds of subtle public key replacement attacks against it. In our first attack, we show that a Type I Adversary who replaces a receiver's public key can decrypt any signcrypted message generated under the replaced public key. This means the scheme in [13] is not a secure one-way encryption. In the other attack, we show that a Type I Adversary who uses public key replacement attack may impersonate any sender to send valid signcrypted message to a receiver. Therefore, the scheme [13] is subject to the universal forgery of Type I attackers. Thus, the original CLSC scheme of Liu *et al.* [13] fails to achieve any of the security goals for a signcryption scheme.

The rest of this paper is organized as follows. Section 2 gives some preliminaries. Section 3 introduces the definition and the security notions for certificateless signcryption schemes. Section 4 reviews the certificateless signcryption (CLSC) scheme of Liu *et al.* [13]. Section 5 presents the attacks on Liu *et al.*'s scheme. Section 6 concludes this paper.

2. Preliminaries

This section revisits some basic concepts and necessary complexity assumptions.

2.1. Bilinear Maps

Let G_1 and G_2 be two multiplicative cyclic groups with prime order p, g a generator of G_1. A map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ is called a bilinear map if it satisfies the following properties:

- Bilinearity: $\hat{e}(g^a, h^b) = \hat{e}(g, h)^{ab}$, for all $a, b \in Z_p^*$, and $g, h \in G_1$.
- Non-degeneracy: There exit $g, h \in G_1$ such that $\hat{e}(g, h) \neq I_{G_2}$, where I_{G_2} is the identity element of G_2.
- Computability: There exits an efficient algorithm to compute $\hat{e}(g, h)$ for all $g, h \in G_1$.

2.2. Complexity Assumptions

Computational Diffie-Hellman (CDH) problem in G_1: Given a randomly chosen $g \in G_1$, as well as g^a, g^b, compute g^{ab} for unknown a and b.

The CDH problem in G_2 can be defined similarly. The CDH assumption means that there is no polynomial time algorithm to solve the CDH problems in both G_1 and G_2 with non-negligible probability.

Decisional Bilinear Diffie-Hellman (DBDH) Problem in $(G_1, G_2, \hat{e})$: Given a randomly chosen $g \in G_1$, as well as g^a, g^b, g^c and $h \in G_2$, decide whether $h = \hat{e}(g, g)^{abc}$ for unknown a, b and c.

The DBDH assumption means that there is no polynomial time algorithm to solve the DBDH problem in $(G_1, G_2, \hat{e})$ with non-negligible probability.

3. Certificateless Signcryption

3.1. Formal Definition of Certificateless Signcryption Schemes

A certificateless signcryption scheme is defined by a six-tuple of probabilistic polynomial-time algorithms [13]:

- Setup: This algorithm is run by the KGC. It takes as input a security parameter k and returns the system parameters *params* and the system master secret key *msk*. After running this algorithm, the KGC publishes the *params* and keeps the *msk* secret.
- Partial-Private-Key-Extract: This algorithm is run by the KGC, after verifying the user's identity. It takes as input *params*, *msk* and an identity $u \in \{0, 1\}^*$ of a user and returns a partial private key d_u.

- User-Key-Generate: This algorithm takes as input $params$, msk, and a user's identity u, and returns a randomly chosen secret value x_u and the public key pk_u of the user. Then the user distributes pk_u without being certificated.

- Set-Private-Key: This algorithm takes as input $params$, the partial private key d_u and the secret value x_u and returns the user's full private key sk_u.

- Signcrypt: This algorithm takes as input $params$, the plaintext M, the sender's private key sk_S, the sender's public key pk_S, the receiver's identity u_R and its public key pk_R and returns a signcrypted text σ or an error symbol $\perp$.

- Unsigncrypt: This algorithm takes as input a signcrypted text σ, the receiver's private key sk_R, the sender's identity u_S and public key pk_S, and returns a plain text M or an error symbol $\perp$.

3.2. Security Requirements of Certificateless Signcryption

The basic security requirements for a signcryption scheme are '*Message Confidentiality*' and'*Non-repudiation*'. Intuitively, *Message Confidentiality* means that no adversary can learn the message in the signcrypted text. We say that a signcryption scheme offers *Non-repudiation* if it prevents the sender of a signcrypted text from repudiating his signature. In other words, without the possession of the full private key of a sender, nobody can generate valid signcrypted texts on behalf of the sender. Precise definitions of *Message Confidentiality* and *Non-repudiation* are defined using security models. For the detail, please refer to [9].

For a cryptographic scheme to be secure in CLC, it requires that the scheme should resist the attacks of both Type I Adversaries and Type II Adversaries. A Type I Adversary does not have access to the master key of the KGC, but he has the ability to replace the public key of any user with a value of his choice. While a Type II Adversary has access to the master key of the KGC but is not allowed to perform public key replacement. The research on CLC reveals that it is challenging to design a scheme secure against a Type I Adversary. In fact, many existing cryptographic schemes in CLC are vulnerable to public key replacement attacks of a Type I Adversary [3, 16, 18, 19, 21]. The main reason is, in CLC, no certificate is used to provide the binding between a user and his public key. Thus, a Type I Adversary can choose any value in the public key space as a target user's public key. As a signcryption scheme aiming to provide both functionalities of public key encryption and signature, for a signcryption scheme in CLC to be secure against a Type I Adversary, it should satisfy: 1) even if a sender uses a replaced public key (chosen by the adversary) of a receiver to generate a signcrypted text, a Type I Adversary still cannot extract the plaintext from the signcrypted text. 2) a Type I Adversary who replaces the public key of the sender cannot impersonate the sender to generate a valid signcrypted text on behalf of the sender.

4. Revisiting the Certificateless Signcryption (CLSC) Scheme of Liu *et al.*

The scheme includes three parties: a KGC, a sender with identity u_S, and a receiver with identity u_R. It consists of the following 6 algorithms.

- Setup: Let G_1 and G_2 be two multiplicative cyclic groups with prime order p, g a generator of G_1. Given a bilinear map $\hat{e} : G_1 \times G_1 \to G_2$ and a collision resistant hash function $H : \{0,1\}^n \to \{0,1\}^m$, the KGC randomly chooses a value $\alpha \in Z_p$ and then computes $g_1 = g^\alpha$. The KGC chooses three random values g_2, u', v' in G_1 and two vectors $U = (u_i)_n$ and $V = (v_j)_m$ whose coordinates are selected from G_1 as well. It keeps the system master secret key $msk = g_2^\alpha$ secret and publishes the system parameters

$$params = \{G_1, G_2, \hat{e}, g, g_1, g_2, u', v', U, V, H\}.$$

- Partial-Private-Key-Extract: Denote by $u[i]$ the ith bit of an identity $u \in \{0,1\}^*$, and $\mathcal{U} = \{i|u[i] = 1, i = 1, 2...n\}$. To generate the partial private key for 19 a user with identity u, the KGC chooses $r_u \in Z_p$ uniformly at random and computes

$$d_u = (d_{u1}, d_{u2}) = (g_2^\alpha (u' \prod_{i \in \mathcal{U}} u_i)^{r_u}, g^{r_u}).$$

  Respectively, we denote the sender's and receiver's partial private keys as

$$d_S = (d_{S1}, d_{S2}) = (g_2^\alpha (u' \prod_{i \in \mathcal{U}_S} u_i)^{r_S}, g^{r_S})$$

  and

$$d_R = (d_{R1}, d_{R2}) = g_2^\alpha (u' \prod_{i \in \mathcal{U}_R} u_i)^{r_R}, g^{r_R}).$$

- User-Key-Generate: An user with identity u randomly chooses a value $x_u \in Z_p$ and outputs his secret value x_u and public key $pk_u = \hat{e}(g_1, g_2)^{x_u}$.

- Set-Private-Key: The user with 20 identity u randomly chooses $r' \in Z_p$. Then he computes

$$sk_u = (sk_{u1}, sk_{u2}) = (d_{u1}^{x_u} (u' \prod_{i \in \mathcal{U}} u_i)^{r'}, d_{u2}^{x_u} g^{r'}) = (g_2^{\alpha x_u} (u' \prod_{i \in \mathcal{U}} u_i)^t, g^t)$$

  where $t = r_u x_u + r'$.

- Signcrypt: The sender chooses a random r'', then sends the message $M \in G_2$ to a receiver with public key $pk_R = \hat{e}(g_1, g_2)^{x_R}$ as follows:

  1. Compute $\sigma_1 = M \cdot pk_R^{r''} = M \cdot \hat{e}(g_1, g_2)^{x_R r''}$.

2. Compute $\sigma_2 = g^{r''}$.
3. Compute $\sigma_3 = (u' \prod\limits_{i \in \mathcal{U}_R} u_i)^{r''}$.
4. Set $\sigma_4 = sk_{s2}$.
5. Compute $h = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_R, pk_R) \in \{0,1\}^m$, where $h[j]$ is the jth bit of h and $\mathcal{M} = \{j | h[j] = 1, j = 1, 2...m\}$.
6. Compute $\sigma_5 = sk_{s1} \cdot (v' \prod\limits_{j \in \mathcal{M}} v_j)^{r''}$.
7. Output the signcrypted text $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

- Unsigncrypt: On receiving the signcrypted text $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, the receiver decrypts the signcrypted text as follows.

  1. Compute $h = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4, u_R, pk_R) \in \{0,1\}^m$, and $\mathcal{M} = \{j | h[j] = 1, \ j = 1, 2...m\}$, where $h[j]$ is the jth bit of h.
  2. If the equality

  $$\hat{e}(\sigma_5, g) = pk_S \cdot \hat{e}(u' \prod_{i \in \mathcal{U}_S} u_i, \sigma_4) \cdot \hat{e}(v' \prod_{j \in \mathcal{M}} v_j, \sigma_2)$$

  holds, compute and output

  $$M = \sigma_1 \cdot \hat{e}(\sigma_3, sk_{R2}) / \hat{e}(\sigma_2, sk_{R1}).$$

  Otherwise, output an error symbol $\perp$.

5. Analysis of the CLSC Scheme by Liu *et al.*

In this section, we describe our attacks on Liu *et al.*'s scheme [13] to show its security vulnerabilities.

5.1. Analysis of message confidentiality

We show that Liu *et al.*'s scheme [13] does not satisfy the message confidentiality property in this section. In particular, a Type I Adversary $\mathcal{A}$ who uses a public key replacement attack can unsigncrypt any signcrypted text generated under the replaced public key of a receiver. The concrete attack is described in three stages.

Stage 1: In this stage, $\mathcal{A}$ randomly picks $x'_R \in Z_p$, computes $pk'_R = \hat{e}(g, g)^{x'_R}$, and replaces the receiver's public key pk_R with pk'_R.

Stage 2: In CL-PKC, since no certificate is provided to bind a user and his public key, a sender who receives the replaced public key pk'_R cannot detect that the public key of the receiver is replaced by $\mathcal{A}$. Thus, the sender will generate a signcrypted text with the replaced public key of the receiver as follows.

1. Choose a random $r'' \in Z_p$, compute $\sigma_1^* = M \cdot {pk'_R}^{r''} = M \cdot \hat{e}(g, g)^{x'_R r''}$.
2. Compute $\sigma_2 = g^{r''}$.

3. Compute $\sigma_3 = (u' \prod_{i \in \mathcal{U}_R} u_i)^{r''}$.
4. Set $\sigma_4 = sk_{s2}$.
5. Compute $m^* = H(\sigma_1^*, \sigma_2, \sigma_3, \sigma_4, u_R, pk'_R) \in \{0,1\}^m$, where $m[j]$ is the jth bit of m^* and $\mathcal{M} = \{j | m[j] = 1, j = 1, 2...m\}$.
6. Compute $\sigma_5 = sk_{s1} \cdot (v' \prod_{j \in \mathcal{M}} v_j)^{r''}$.
7. Output the signcrypted text $\sigma^* = (\sigma_1^*, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$.

Stage 3: On receiving the signcrypted text $\sigma^* = (\sigma_1^*, \sigma_2, \sigma_3, \sigma_4, \sigma_5)$, $\mathcal{A}$ can extract the plain text by using the following algorithm.

1. Compute
$$m^* = H(\sigma_1^*, \sigma_2, \sigma_3, \sigma_4, u_R, pk'_R) \in \{0,1\}^m,$$
$\mathcal{M} = \{j | m[j] = 1, j = 1, 2...m\}$, where $m[j]$ is the jth bit of m^*.
2. If the equality $\hat{e}(\sigma_5, g) = pk_S \cdot \hat{e}(u' \prod_{i \in \mathcal{U}_S} u_i, \sigma_4) \cdot \hat{e}(v' \prod_{j \in \mathcal{M}} v_j, \sigma_2)$ holds, the adversary obtains the message M by computing $M = \sigma_1^* \cdot \hat{e}(\sigma_2, g)^{-x'_R}$.

The correctness can be verified by the following equalities.

$$\begin{aligned}
\hat{e}(\sigma_5, g) &= \hat{e}(sk_{s1}(v' \prod_{j \in \mathcal{M}} v_j)^{r''}, g) \\
&= \hat{e}(g_2^{\alpha x_s}, g) \cdot \hat{e}((u' \prod_{i \in \mathcal{U}_S} u_i)^t_s, g) \cdot \hat{e}((v' \prod_{j \in \mathcal{M}} v_j)^{r''}, g) \\
&= \hat{e}(g_2, g^{\alpha})^{x_s} \cdot \hat{e}(u' \prod_{i \in \mathcal{U}_S} u_i, \sigma_4) \cdot \hat{e}(v' \prod_{j \in \mathcal{M}} v_j, \sigma_2) \\
&= pk_S \cdot \hat{e}(u' \prod_{i \in \mathcal{U}_S} u_i, \sigma_4) \cdot \hat{e}(v' \prod_{j \in \mathcal{M}} v_j, \sigma_2)
\end{aligned}$$

where $t = r_S x_s + r'$.

$$\begin{aligned}
\sigma_1^* \cdot \hat{e}(\sigma_2, g)^{-x'_R} &= \sigma_1^* \cdot \hat{e}(g^{r''}, g)^{-x'_R} \\
&= \sigma_1^* \cdot \hat{e}(g, g)^{-x'_R r''} \\
&= \sigma_1^* \cdot {pk'_R}^{-r''} \\
&= M
\end{aligned}$$

Thus, the scheme fails to satisfy the requirement of message confidentiality.

5.2. Analysis of non-repudiation

A secure CLSC scheme should have the property that a sender cannot deny that he has performed a valid signcryption and has sent the signcrypted text to a receiver. Furthermore, it requires that, without knowing the full private key of a sender, any adversary cannot impersonate the sender to generate valid signcrypted texts. In the following, we show that a Type I Adversary $\mathcal{A}$ can successfully forge a valid signcrypted text to cheat the receiver by replacing the sender's public key. The attack consists of the following three stages:

Stage 1. In this stage, $\mathcal{A}$ randomly picks $x'_S \in Z_p$ and replaces the sender's public key with $pk'_S = \hat{e}(g,g)^{x'_S}$.

Stage 2. In this stage, $\mathcal{A}$ impersonates the sender to generate a signcrypted text under the replaced public key. $\mathcal{A}$ 21 proceeds as follows.

1. Choose a random $r'' \in Z_p$, compute $\sigma_1 = M \cdot pk_R^{r''} = M \cdot \hat{e}(g_1, g_2)^{x_R r''}$.
2. Compute $\sigma_2 = g^{r''}$.
3. Compute $\sigma_3 = (u' \prod_{i \in \mathcal{U}_R} u_i)^{r''}$.
4. Randomly choose $a \in Z_p$, and compute $\sigma_4^* = g^a$.
5. Compute
$$h = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4^*, u_R, pk_R) \in \{0,1\}^m,$$
and $\mathcal{M} = \{j | h[j] = 1, j = 1, 2...m\}$, where $h[j]$ is the jth bit of h.
6. Compute $\sigma_5^* = g^{x'_S} \cdot (u' \prod_{i \in \mathcal{U}_S} u_i)^a \cdot (v' \prod_{j \in \mathcal{M}} v_j)^{r''}$.
7. Output the signcrypted text $\sigma^* = (\sigma_1, \sigma_2, \sigma_3, \sigma_4^*, \sigma_5^*)$.

Finally, $\mathcal{A}$ sends the signcrypted text $\sigma^* = (\sigma_1, \sigma_2, \sigma_3, \sigma_4^*, \sigma_5^*)$ together with the sender's identity and the replaced public key to the receiver.

Stage 3. We notice that, since there is no binding between a user's identity and his public key, the receiver cannot detect that the sender's public key is replaced by $\mathcal{A}$. In this stage, upon receiving the signcrypted text, the receiver invokes the Unsigncrypt algorithm as follows.

1. Compute
$$h = H(\sigma_1, \sigma_2, \sigma_3, \sigma_4^*, u_R, pk_R) \in \{0,1\}^m,$$
and $\mathcal{M} = \{j | h[j] = 1, j = 1, 2...m\}$, where $h[j]$ is the jth bit of h.
2. Check the validity of the signcrypted text by verifying
$$\hat{e}(\sigma_5^*, g) = pk'_S \cdot \hat{e}(u' \prod_{i \in \mathcal{U}_S} u_i, \sigma_4^*) \cdot \hat{e}(v' \prod_{j \in \mathcal{M}} v_j, \sigma_2).$$
If the equation holds, he computes and outputs
$$M = \sigma_1 \cdot \hat{e}(\sigma_3, sk_{R2}) / \hat{e}(\sigma_2, sk_{R1}).$$
Otherwise, he outputs an error symbol $\perp$.

Since we have

$$\begin{aligned}
\hat{e}(\sigma_5^*, g) &= \hat{e}(g^{x'_S} \cdot (u' \prod_{i \in \mathcal{U}_S} u_i)^a \cdot (v' \prod_{j \in \mathcal{M}} v_j)^{r''}, g) \\
&= \hat{e}(g,g)^{x'_S} \cdot \hat{e}(u' \prod_{i \in \mathcal{U}_S} u_i, g^a) \cdot \hat{e}(v' \prod_{j \in \mathcal{M}} v_j, g^{r''}) \\
&= pk'_S \cdot \hat{e}(u' \prod_{i \in \mathcal{U}_S} u_i, \sigma_4^*) \cdot \hat{e}(v' \prod_{j \in \mathcal{M}} v_j, \sigma_2),
\end{aligned}$$

the verification equation always holds. This declares that the forged signcrypted text $(\sigma_1, \sigma_2, \sigma_3, \sigma_4^*, \sigma_5^*)$ is valid. Therefore, the scheme is subject to universal forgery with respect to a Type I Adversary $\mathcal{A}$ who replaces the sender's public key.

6. Conclusion

In this paper, we demonstrated two kinds of subtle public key replacement attacks against the recently proposed certificateless signcryption scheme by Liu *et al.*. In our attacks, an adversary can replace the receiver's public key to decrypt the sender's signcrypted text and obtain the message easily, and a Type I Adversary can forge a valid signcrypted text by replacing the public key of a sender. Thus, the certificateless signcryption scheme of Liu *et al.* fails to meet the requirements of confidentiality and non-repudiation for a secure signcryption scheme.

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments and suggestions. This research is supported by the Nature Science Foundation of China (No. 60673070).

References

[1] S.S. Al-Riyami, K.G. Paterson, Certificateless public key cryptography, in: Proceedings of the Asiacrypt 2003, Taipei, Taiwan, 2003, pp.452-473.

[2] J.H. An, Y. Dodis, T. Rabin, On the security of joint signature and encryption, in: Advances in Cryptology - EUROCRYPT 2002, Amsterdam, 2002, pp.83-107.

[3] D. Aranha, R. Castro, J. Lopez, *et al.*, Efficient certificateless signcryption, http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03 01resumo.pdf.

[4] M. Barbosa, P. Farshim, Certificateless signcryption, in: in: M. Abe, V. Gligor(Eds.), Proceedings of the 2008 ACM Symposium on Information, Computer and Communications Security(ASIACCS08), ACM, NewYork, 2008, pp.369-372.

[5] P. Barreto, A.M. Deusajute, E.D.S Cruz, *et al.*, Toward efficient certificateless signcryption from (and without) bilinear pairings, http://sbseg2008.inf.ufrgs.br/anais/data/pdf/st03 03 artigo.pdf.

[6] X. Boyen, Multipurpose identity-based signcryption: A swiss army knife for identity-based cryptography, in: Proceedings of 23rd Annual International Cryptology Conference, Santa Barbara, CA, USA(CRYPTO '03), 2003, pp.383-399.

[7] R. Canetti, O. Goldreich, S. Halevi, The random oracle methodology, revisited, Journal of the ACM 51(4) (2004) 557-594.

[8] S. Chang, D.S. Wong, Y. Mu, Z. Zhang, Certificateless threshold ring signature, Information Sciences 179 (20) (2009) 3685-3696.

[9] L. Chen, J. Malone-Lee, Improved identity-based signcryption, in: Proceedings of Public Key Cryptography - PKC 2005, Les Diablerets, Switzerland, 2005, pp.362-379.

[10] Y. Chen, F. Zhang, A new certificateless public key encryption scheme, Wuhan University Journal of Natural Sciences 13 (6) (2008) 721-726.

[11] K.Y. Choi, J.H. Park, D.H. Lee, A new provably secure Certificateless short signature scheme, Computers and Mathematics with Applications 61 (7) (2011) 1760-1768.

[12] F. Li, M. Shirase, T. Takagi, Certificateless Hybrid Signcryption, in: Proceedings of The 5th Information Security Practice and Experience Conference (ISPEC 2009), LNCS 5451, 2009, pp. 112-123.

[13] Z. Liu, Y. Hu, X. Zhang, H. Ma, Certificateless signcryption scheme in the standard model, Information Sciences 180 (3) (2010) 452-464.

[14] Y. Long, K. Chen, Efficient chosen-ciphertext secure certificateless threshold key encapsulation mechanism, Information Sciences 180 (7) (2010) 1167-1181.

[15] J. Malone-Lee, Identity-Based Signcryption, in: Cryptology ePrint Archive, Report 2002/098, 2002.

[16] S.S.D. Selvi, S.S. Vivek, C.P. Rangan, Security Weaknesses in Two Certificateless Signcryption schemes, in: Cryptology ePrint Archive, Report 2010/92, 2010.

[17] A. Shamir, Identity-based cryptosystems and signature schemes, in: Proceedings of 4th Annual International Cryptology Conference, Santa Barbara, CA, USA, 1984, pp.47-53.

[18] S. Sharmila, S.S.D. Selvi, S.S. Vivek, *et al.*, On the Security of Certificateless Signcryption Schemes, in: Cryptology ePrint Archive, Report 2009/298, 2009.

[19] K.A. Shim, Breaking the short certificateless signature scheme, Information Sciences 179 (2009) 303-306.

[20] J. Weng, G. Yao, R. H. Deng, M.R. Chen, X. Li, Cryptanalysis of a Certificateless signcryption scheme in the standard model, Information Sciences 181 (3) (2011) 661-667.

[21] C. Wu, Z. Chen, A new efficient certificateless signcryption scheme, in: Proceedings of IEEE International Symposium on Information Science and Engieering, Shanghai, China, 2008, pp.661-664.

[22] W. Xie, Z. Zhang, Efficient and Provably Secure Certificateless Signcryption from Bilinear Maps, in: Cryptology ePrint Archive, Report 2009/578, 2009.

[23] H. Xiong, F. Li, Z. Qin, Certificateless threshold signature secure in the standard model, Information Sciences (2010), doi:10.1016/j.ins.2010.06.010.

[24] G. Yang, C.H. Tan, Certificateless public key encryption: A new generic construction and two pairing-free schemes, Theoretical Computer Science 412 (8-10) (2011) 662-674.

[25] G. Yang, C.H. Tan, Certificateless cryptography with KGC trust level 3, Theoretical Computer Science, In Press, Corrected Proof, Available online 17 June 2011.

[26] H. Yuan, F. Zhang, X. Huang, Y Mu, W Susilo, L Zhang, Certificateless threshold signature scheme from bilinear maps, Information Sciences 180 (23) (2010) 4714-4728.

[27] L. Zhang, B. Qin, Q. Wu, F. Zhang, Efficient many-to-one authentication with Certificateless aggregate signatures, Computer Networks 54 (14) (2010) 2482-2491.

[28] L. Zhang, F. Zhang, A new provably secure certificateless signature scheme, in: Proceedings of IEEE International Conference on Communications, Beijing, China, 2008, pp.1685-1689.

[29] L. Zhang, F. Zhang, A new certificateless aggregate signature scheme, Computer Communications 32 (2009) 1079-1085.

[30] L. Zhang, F. Zhang, B. Qin, S. Liu, Provably-secure electronic cash based on Certificateless partially-blind signatures, Electronic Commerce Research and Applications, doi:10.1016/j.elerap.2011.01.004.

[31] L. Zhang, F. Zhang, Q. Wu, J. Domingo-Ferrer, Simulatable certificateless two-party authenticated key agreement protocol,Information Sciences 180 (6) (2010) 1020-1030.

[32] Y. Zheng, Digital signcryption or how to achieve cost (signature and encryption) << cost (signature) + cost(encryption), in: Advances in Cryptology-CRYPTO'97, Springer Berlin, 1997, 291-312.

[33] Y. Zheng, H. Imai, How to construct efficient signcryption schemes on elliptic curves, Information Processing Letters 68 (1998) 227-233.