Available online at www.sciencedirect.com
SCIENCE DIRECT®
Information Processing Letters 99 (2006) 135–138
Information Processing Letters
www.elsevier.com/locate/ipl

Analysis of improved signcryption scheme with key privacy

Chik How Tan

NISlab, Department of Computer Science and Media Technology, Gjøvik University College, Norway

Received 14 September 2005; received in revised form 24 January 2006; accepted 26 January 2006

Available online 15 May 2006

Communicated by Y. Desmedt

Abstract

In this paper, we analyse the Yang–Wong–Deng signcryption scheme [G. Yang, D.S. Wong, X. Deng, Analysis and improvement of a signcryption scheme with key privacy, in: Information Security Conference—ISC'05, in: Lecture Notes in Comput. Sci., vol. 3650, Springer-Verlag, Berlin, 2005, pp. 218–232] proposed in ISC'05, which is the improvement and enhancement of the security of Libert–Quisquater signcryption scheme [B. Libert, J.J. Quisquater, Efficient signcryption with key privacy from gap Diffie–Hellman groups, in: Public Key Cryptography—PKC'04, in: Lecture Notes in Comput. Sci., vol. 2947, Springer-Verlag, Berlin, 2004, pp. 187–200]. Although Yang et al. [G. Yang, D.S. Wong, X. Deng, Analysis and improvement of a signcryption scheme with key privacy, in: Information Security Conference—ISC'05, in: Lecture Notes in Comput. Sci., vol. 3650, Springer-Verlag, Berlin, 2005, pp. 218–232] proved that their scheme is secure against adaptive chosen ciphertext attacks and achieves ciphertext anonymity (which is also called key privacy) in the random oracle model; we disprove all their claims and show that their scheme is not semantically secure and does not achieve ciphertext anonymity.

Keywords: Cryptography; Signcryption

1. Introduction

Since the concept of a signcryption scheme was introduced by Zheng [8] in 1997, many signcryption schemes were proposed. But, it was only recent that a formal security proof model [1] was formalized by Baek et al. in 2002. They also gave a security proof of Zheng's scheme [8] in the random oracle model. In 2003, Boyen [2] proposed a secure identity-based signcryption scheme with ciphertext anonymity, which was provably secure in the random oracle model. Their security proof model was slightly different from that of [1] which included the ciphertext anonymity (which is also called key privacy). In 2004, Libert and Quisquater [3] modified Boyen's security proof model to non-identity based signcryption scheme and proposed a signcryption scheme. They proved that their signcryption scheme was secure in the random oracle model with the following properties: semantic security against adaptive chosen ciphertext attacks, ciphertext anonymity and key invisibility. In 2005, Tan [5] showed that none of the above properties were achieved under their defined attacks games. Tan [6] showed further that the signcryption scheme [4] was also insecure against chosen ciphertext attacks. In Information Security Conference 2005, Yang et al. [7] also independently showed that the signcryption scheme [3] were insecure and further improved the signcryption scheme. They proved that

E-mail address: chik.tan@hig.no (C.H. Tan).

0020-0190/$ – see front matter
doi:10.1016/j.ipl.2006.01.015

their improved signcryption scheme was secure against adaptive chosen ciphertext attacks and achieved ciphertext anonymity in the random oracle model. In this paper, we show that none of the above two properties were achieved under their defined attacks games. That is, the improved signcryption scheme proposed by Yang et al. [7] is also not secure against adaptive chosen ciphertext attacks and does not achieve ciphertext anonymity.

2. Yang–Wong–Deng signcryption scheme

A signcryption scheme normally involves three stages, that is, key generation, signcryption generation and de-signcryption. Now, we describe the Yang–Wong–Deng signcryption scheme [7] as follows:

Key generation. Let q be a prime number and G_1 and G_2 be groups of the same prime order q. Let P be a generator of G_1 and e be a bilinear map such that $e: G_1 \times G_1 \to G_2$. Consider a user u, he first chooses a random $x_\mathsf{u} \in Z_q$ and computes $X_\mathsf{u} = x_\mathsf{u} P$. Then, the public key of a user u is X_u and the private key is x_u. We denote the sender and the receiver by s and r, respectively, and their private and public key pairs are $(x_\mathsf{s}, X_\mathsf{s})$ and $(x_\mathsf{r}, X_\mathsf{r})$, respectively. Let H_1, H_2 and H_3 be cryptographic hash functions such that $H_1: \{0,1\}^{n+2l} \to G_1$, $H_2: G_1 \times G_1 \times G_1 \to \{0,1\}^l$ and $H_3: G_1 \times G_1 \times G_1 \to \{0,1\}^{n+l}$, where n and l are some positive integers such that elements in G_1 takes l-bits to represent.

Signcrypt. To signcrypt a message $m \in \{0,1\}^n$ for the intended user r, the sender s first chooses a random $w \in Z_q$ and computes

$$U = wP, \qquad V = x_\mathsf{s} H_1(m, U, X_\mathsf{r}),$$
$$W = V \oplus H_2(U, X_\mathsf{r}, wX_\mathsf{r}) \quad \text{and}$$
$$Z = (m \| X_\mathsf{s}) \oplus H_3(U, X_\mathsf{r}, wX_\mathsf{r}).$$

Then, the ciphertext is $\mathcal{C} = (U, W, Z)$.

De-signcrypt. Upon receipt of a ciphertext $\mathcal{C} = (U, W, Z)$, the receiver r computes $V = W \oplus H_2(U, X_\mathsf{r}, x_\mathsf{r} U)$ and $(m \| X_\mathsf{s}) = Z \oplus H_3(U, X_\mathsf{r}, x_\mathsf{r} U)$. If $X_\mathsf{s} \notin G_1$, then reject $\mathcal{C}$, otherwise compute $H = H_1(m, U, X_\mathsf{r})$ and check $e(X_\mathsf{s}, H) = e(P, V)$. If the above condition holds, then output m, otherwise reject the ciphertext.

It is noted that the signature V is encrypted by $H_2(U, X_\mathsf{r}, wX_\mathsf{r})$, while the message m is encrypted by $H_3(U, X_\mathsf{r}, wX_\mathsf{r})$.

3. Security analysis

In this section, we describe the attacks games used in the security proof to show the semantic security against chosen ciphertext attacks and ciphertext anonymity, which were listed in [7] and similar to those defined in [3]. Although Yang et al. proved that their signcryption scheme was secure for the above two properties in the random oracle model, we show that none of these are achieved based on the attacks games listed in [7]. Now, we describe the two attacks games as follows:

Definition 1 *(Semantic security against chosen ciphertext attacks).* ([7]) A signcryption scheme is semantically secure against chosen ciphertext attacks if no probabilistic polynomial time adversary has a non-negligible advantage in the following game:

1. The challenger runs the key generation algorithm to generate a private/public key pair $(sk_{\mathsf{r}^*}, pk_{\mathsf{r}^*})$ and gives pk_{r^*} to the adversary $\mathcal{A}$.
2. $\mathcal{A}$ submits a number of queries to the signcryption and de-signcryption. In signcryption queries, $\mathcal{A}$ chooses a message $m \in \mathcal{M}$ (message space) and an arbitrary recipient public key pk_r and sends them to the challenger. The challenger runs the signcrypt oracle $\texttt{Signcrypt}(m, sk_\mathsf{s}, pk_\mathsf{r})$ with a sender's private key sk_s (sk_s can be chosen to be sk_{r^*} provided $pk_\mathsf{r} \neq pk_{\mathsf{r}^*}$) and returns the result. In de-signcryption queries, $\mathcal{A}$ submits a ciphertext $\mathcal{C}$ to the challenger. The challenger runs the de-signcrypt oracle $\texttt{De-signcrypt}(\mathcal{C}, sk_\mathsf{r})$. If the obtained signed-plaintext is valid for the recovered sender's public key, then returns the plaintext, otherwise returns the symbol $\perp$.
3. $\mathcal{A}$ chooses two equal-length messages $m_0, m_1 \in \mathcal{M}$ and an arbitrary private key sk_s and sends them to the challenger. The challenger then flips a coin $b \in \{0,1\}$ to compute a signcryption $\mathcal{C}^* = \texttt{Signcrypt}(m_b, sk_\mathsf{s}, pk_{\mathsf{r}^*})$ of m_b with the sender's private key sk_s and the under attacked receiver's public key pk_{r^*}. Then, $\mathcal{C}^*$ is sent to $\mathcal{A}$ as a challenge ciphertext.
4. $\mathcal{A}$ continues to make queries to the signcryption and de-signcryption. $\mathcal{A}$ is not allowed to query the de-signcrypt oracle of the challenge ciphertext $\mathcal{C}^*$.
5. At the end of the game, $\mathcal{A}$ outputs bit b' and wins if $b' = b$. The adversary $\mathcal{A}$'s advantage is defined to be $\text{Adv}^{\text{IND-CCA}}(\mathcal{A}) := \Pr[b' = b] - 1/2$.

Definition 2 *(Ciphertext anonymity).* ([7]) A signcryption scheme satisfies the ciphertext anonymity property

if no probabilistic polynomial time distinguisher has a non-negligible advantage in the following game:

1. The challenger generates two keys $(sk_{\mathsf{r}^*,0}, pk_{\mathsf{r}^*,0})$ and $(sk_{\mathsf{r}^*,1}, pk_{\mathsf{r}^*,1})$, and gives $pk_{\mathsf{r}^*,0}$ and $pk_{\mathsf{r}^*,1}$ to the distinguisher $\mathcal{D}$.
2. $\mathcal{D}$ adaptively makes a number of queries of signcryption $\texttt{Signcrypt}(m, sk_{\mathsf{s}}, pk_{\mathsf{r}})$ with a sender's private key sk_{s} (sk_{s} can be chosen to be $sk_{\mathsf{r}^*,c}$ provided $pk_{\mathsf{r}} \neq pk_{\mathsf{r}^*,c}$ for $c = 0$ or $c = 1$) for arbitrary recipient key pk_{r} and de-signcryption $\texttt{De-signcrypt}(\mathcal{C}, sk_{\mathsf{r}})$.
3. $\mathcal{D}$ outputs two senders' private keys $sk_{\mathsf{s}^*,0}$ and $sk_{\mathsf{s}^*,1}$ and a message $m \in \mathcal{M}$. The challenger then flips two coins $b, b' \in \{0, 1\}$ and computes a challenge ciphertext $\mathcal{C}^* = \texttt{Signcrypt}(m, sk_{\mathsf{s}^*,b}, pk_{\mathsf{r}^*,b'})$ which is sent to $\mathcal{D}$.
4. $\mathcal{D}$ continues to make queries to the signcryption and de-signcryption with the restriction that it is not allowed to ask the de-signcryption of the challenge ciphertext $\mathcal{C}^*$.
5. At the end of the game, $\mathcal{D}$ outputs bits d, d' and wins if $(d, d') = (b, b')$. The distinguisher $\mathcal{D}$'s advantage is defined to be $\mathrm{Adv}^{\text{IND-CA}}(\mathcal{D}) := \Pr[(d, d') = (b, b')] - 1/4$.

Based on the above attacks games for proving the security, we show two attacks on Yang–Wong–Deng signcryption scheme as follows:

3.1. Attack against adaptive chosen ciphertext attacks

Assume that given the receiver's public key X_{r}, the adversary $\mathcal{A}$ first chooses a sender's private key x_{s} and two equal length messages m_0 and m_1 and sends these to the challenger. The challenger then chooses a random $b \in \{0, 1\}$ and computes the challenge ciphertext of the message m_b as $\mathcal{C}^* = (U^*, W^*, Z^*)$. Upon receipt of the challenge ciphertext $\mathcal{C}^* = (U^*, W^*, Z^*)$, the adversary first makes a "wild guess" of b to be 0 and constructs a new ciphertext by choosing a random message $\bar{m}$ whose length is equal to that of m_0 and a random $\bar{x}_{\mathsf{s}} \in Z_q^*$. Then, the adversary computes the following:

$$\bar{X}_{\mathsf{s}} = \bar{x}_{\mathsf{s}} P, \qquad V^* = x_{\mathsf{s}} H_1(m_0, U^*, X_{\mathsf{r}}),$$
$$\bar{V} = \bar{x}_{\mathsf{s}} H_1(\bar{m}, U^*, X_{\mathsf{r}}),$$
$$\bar{W} = (\bar{V} \oplus V^*) \oplus W^*,$$
$$\bar{Z} = \big((m_0 \oplus \bar{m}) \| (\bar{X}_{\mathsf{s}} \oplus X_{\mathsf{s}})\big) \oplus Z^*.$$

Finally, the adversary $\mathcal{A}$ sends the ciphertext $\bar{\mathcal{C}} = (U^*, \bar{W}, \bar{Z})$ to the challenger for de-signcryption. Upon receipt of the query, the challenger runs the de-signcrypt oracle which computes $\hat{m} \| \hat{X}_{\mathsf{s}} = \bar{Z} \oplus H_3(U^*, X_{\mathsf{r}}, x_{\mathsf{r}} U^*)$ (then $\hat{X}_{\mathsf{s}} = \bar{X}_{\mathsf{s}}$) and the following:

$$\hat{V} = \bar{W} \oplus H_2(U^*, X_{\mathsf{r}}, x_{\mathsf{r}} U^*),$$
$$H = H_1(\hat{m}, U^*, X_{\mathsf{r}}).$$

If $e(\hat{X}_{\mathsf{s}}, H) = e(P, \hat{V})$, then the challenger returns the message $\hat{m}$, otherwise rejects the message. If the response message $\hat{m}$ from the challenger is equal to $\bar{m}$, then the adversary will know that m_0 is the plaintext for the challenge ciphertext (as the adversary $\mathcal{A}$ used m_0 to compute the new ciphertext $\bar{\mathcal{C}}$). If the response is rejected or $\hat{m}$ is not equal to $\bar{m}$, then m_1 is the plaintext for the challenge ciphertext. Therefore, we conclude that the Yang–Wong–Deng signcryption scheme is not secure against adaptive chosen ciphertext attacks.

3.2. Attack against ciphertext anonymity

Given the receiver's public key $X_{\mathsf{r},0}$ and $X_{\mathsf{r},1}$, the distinguisher $\mathcal{D}$ generates the senders' private key $x_{\mathsf{s},0}$ and $x_{\mathsf{s},1}$ and a message m^*; and sends these to the challenger. The challenger first chooses two randoms $b, b' \in \{0, 1\}$ for the target sender's private key $x_{\mathsf{s},b}$ and the target receiver's public key $X_{\mathsf{r},b'}$, respectively, and produces the challenge ciphertext $\mathcal{C}^* = (U^*, W^*, Z^*)$. Upon receipt of the challenge ciphertext $\mathcal{C}^* = (U^*, W^*, Z^*)$, the distinguisher $\mathcal{D}$ first constructs four new ciphertexts $\bar{\mathcal{C}}_{i,j} = (U^*, \bar{W}_{i,j}, \bar{Z}_i)$ for $i, j = 0, 1$ by choosing a random message $\bar{m}$ whose length is equal to that of m^* and a random $\bar{x}_{\mathsf{s}} \in Z_q^*$ as follows:

$$\bar{X}_{\mathsf{s}} = \bar{x}_{\mathsf{s}} P, \qquad V^*_{i,j} = x_{\mathsf{s},i} H_1(m^*, U^*, X_{\mathsf{r},j}),$$
$$\bar{V}_j = \bar{x}_{\mathsf{s}} H_1(\bar{m}, U^*, X_{\mathsf{r},j}),$$
$$\bar{W}_{i,j} = (\bar{V}_j \oplus V^*_{i,j}) \oplus W^*,$$
$$\bar{Z}_i = \big((m^* \oplus \bar{m}) \| (\bar{X}_{\mathsf{s}} \oplus X_{\mathsf{s},i})\big) \oplus Z^*.$$

Then, the distinguisher $\mathcal{D}$ sends the ciphertexts $\bar{\mathcal{C}}_{i,j} = (U^*, \bar{W}_{i,j}, \bar{Z}_i)$ to the challenger one by one for de-signcryption. Upon receipt of the query, the challenger runs the de-signcrypt oracle which computes $\hat{m}_{i,j} \| \hat{X}_{i,j} = \bar{Z}_i \oplus H_3(U^*, X_{\mathsf{r}}, x_{\mathsf{r},j} U^*)$ for $i, j = 0, 1$. If $\hat{X}_{i,j} \notin G_1$, then returns $\perp$, otherwise computes the following:

$$\hat{V}_{i,j} = \bar{W}_{i,j} \oplus H_2(U^*, X_{\mathsf{r},j}, x_{\mathsf{r},j} U^*),$$
$$H_{i,j} = H_1(\hat{m}_{i,j}, U^*, X_{\mathsf{r},j}).$$

For $i, j = 0, 1$, if $e(\hat{X}_{i,j}, H_{i,j}) = e(P, \hat{V}_{i,j})$, then it returns the message $\hat{m}_{i,j}$, otherwise rejects the message. Then, one of the returned message $\hat{m}_{i,j}$ must be equal to $\bar{m}$, say $m_{d,d'}$ for some $d, d' \in \{0, 1\}$. Therefore, the

distinguisher $\mathcal{D}$ outputs the correct guess (d, d') which is equal to (b, b'). Hence, we conclude that the Yang–Wong–Deng signcryption scheme does not provide ciphertext anonymity.

4. Conclusion

In this paper, we showed that the Yang–Wong–Deng signcryption scheme does not fulfill the claims as stated in the paper [7], that is, semantic security against chosen ciphertext attacks and ciphertext anonymity. We demonstrate the attack methods for the two properties and conclude that the Yang–Wong–Deng signcryption scheme is insecure under their attacks games.

Acknowledgements

The author wishes to thank the anonymous referees for their useful comments and invaluable suggestions for improving this paper.

References

[1] J. Baek, R. Steinfeld, Y. Zheng, Formal proofs for the security of signcryption, in: Public Key Cryptography—PKC'02, in: Lecture Notes in Comput. Sci., vol. 2274, Springer-Verlag, Berlin, 2002, pp. 80–98.

[2] X. Boyen, Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography, in: Advances in Cryptology—Crypto'03, in: Lecture Notes in Comput. Sci., vol. 2729, Springer-Verlag, Berlin, 2003, pp. 383–399.

[3] B. Libert, J.J. Quisquater, Efficient signcryption with key privacy from gap Diffie–Hellman groups, in: Public Key Cryptography—PKC'04, in: Lecture Notes in Comput. Sci., vol. 2947, Springer-Verlag, Berlin, 2004, pp. 187–200.

[4] B. Libert, J.J. Quisquater, Improved signcryption from q-Diffie–Hellman problems, in: Security Communication Networks—SCN'04, in: Lecture Notes in Comput. Sci., vol. 3352, Springer-Verlag, Berlin, 2005, pp. 220–234.

[5] C.H. Tan, On the security of signcryption scheme with key privacy, IEICE Trans. on Fundamentals E88-A(4) (2005) 1093–1095.

[6] C.H. Tan, Security analysis of signcryption scheme from q-Diffie–Hellman problems, IEICE Trans. on Fundamentals E89-A(1) (2006) 206–208.

[7] G. Yang, D.S. Wong, X. Deng, Analysis and improvement of a signcryption scheme with key privacy, in: Information Security Conference—ISC'05, in: Lecture Notes in Comput. Sci., vol. 3650, Springer-Verlag, Berlin, 2005, pp. 218–232.

[8] Y. Zheng, Digital signcryption or how to achieve cost(signature & encryption) $\ll$ cost(signature) + cost(encryption), in: Advances in Cryptology—Crypto'97, in: Lecture Notes in Comput. Sci., vol. 1294, Springer-Verlag, Berlin, 1997, pp. 165–179.