LETTER

On the Security of Signcryption Scheme with Key Privacy

Chik-How TAN[†a)], *Affiliate Member*

SUMMARY In this paper, we analyse the signcryption scheme proposed by Libert and Quisquater in 2004 and show that their scheme does not meet the requirements as claimed in their paper in PKC'2004, such as, semantically secure against adaptive chosen ciphtertext attack, ciphertext anonymity and key invisibility.

key words: *cryptography, signcryption*

1. Introduction

The concept of a signcryption scheme is proposed by Zheng in 1997 [5]. Since then, there are many signcryption schemes proposed. It is only recently that a formal security proof model [1] is formalized providing security proof for Zheng's scheme [5] in the random oracle model. In 2003, Boyen [3] proposed a secured identity-based signcryption scheme with ciphertext anonymity and provable secure in the random oracle model. Their security proof model is slightly different from that of [1] which includes the ciphertext anonymity. In 2004, Libert and Quisquater [4] modified Boyen's security proof model to non-identity based signcryption scheme and proposed a signcryption scheme. They proved that their signcryption scheme is secure in the random oracle model with the following properties: semantically security against adaptive chosen ciphertext attacks, ciphertext anonymity and key invisibility. In this paper, we show that none of the above properties are achieved under their defined attacks games.

2. Libert-Quisquater Signcryption Scheme

A signcryption scheme normally involves three stages, that is, key generation, signcryption generation and unsigncryption. Now, we describe the Libert-Quisquater signcryption scheme [4] 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 $e : G_1 \times G_1 \rightarrow G_2$. Consider a user u, 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 $H_1 : \{0,1\}^{n+2l} \rightarrow G_1$, $H_2 : G_1 \times G_1 \times G_1 \rightarrow \{0,1\}^l$ and $H_3 : \{0,1\}^l \rightarrow \{0,1\}^{n+l}$, where n and l are some positive integer.

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

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

Then, the ciphertext is $C = (U, W, Z)$.

Unsigncrypt: Upon receipt of a ciphertext $C = (U, W, Z)$, the receiver r computes $V = W \oplus H_2(U, X_{\mathsf{r}}, x_{\mathsf{r}}U)$ and $(m \| X_{\mathsf{s}}) = Z \oplus H_3(V)$. If X_{s} is not a point on the curve on which G_1 is defined, then reject 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 does not hold, then reject the ciphertext.

3. Analysis

In this section, we describe the attack games in the security proof of the semantically secure against chosen ciphertext attacks, ciphertext anonymity and key invisibility which were defined in [4]. Although the authors proved all of three properties in the random oracle model, we show that none of them is achieved based on these attack games listed in [4]. Now, we describe these three attacks games as follows:

Definition 1 [4] (Semantically Security Against Chosen Ciphertext Attacks): A signcryption scheme is semantically secure against chosen ciphertext attacks if no probabilistic polynomial time adversaries have 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 unsigncryption. In signcryption queries, $\mathcal{A}$ chooses a message $m \in \mathcal{M}$ and an arbitrary public key pk_{r} and sends them to the challenger. The challenger runs the signcrypt oracle $\texttt{Signcrypt}(m, sk_{\mathsf{r}}^*, pk_{\mathsf{r}})$ and returns the result. In unsigncryption queries, $\mathcal{A}$ submits a ciphertext C to the challenger. The challenger runs the unsigncrypt oracle $\texttt{Unsigncrypt}(C, sk_{\mathsf{r}}^*)$. If the obtained signed-plaintext is valid for the recovered sender's public key, then returns the plaintext, otherwise returns the symbol $\perp$.

Manuscript received May 6, 2004.
Manuscript revised October 25, 2004.
Final manuscript received January 11, 2005.

[†]The author is with the School of Electrical & Electronic Engineering, Nanyang Technological University, Singapore 639798.
a) E-mail: echikhow@ntu.edu.sg

DOI: 10.1093/ietfec/e88–a.4.1093

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 $C^* = \mathtt{Signcrypt}(m_b, sk_{\mathsf{s}}, pk_{\mathsf{r}}^*)$ of m_b with the sender's private key sk_{s} and the under attacked receiver's public key pk_{r}^*. Then, C^* is sent to $\mathcal{A}$ as a challenge ciphertext.
4. $\mathcal{A}$ continually makes a number of queries to the signcryption and unsigncryption. $\mathcal{A}$ is not allowed to query the unsigncrypt oracle of the challenge ciphertext C^* with the private key sk_{r}^*.
5. At the end of the game, $\mathcal{A}$ outputs bits b' and wins if $b' = b$. The adversary $\mathcal{A}$'s advantage is defined to be $\mathrm{Adv}^{\mathtt{IND-CCA}}(\mathcal{A}) := 2\Pr[b' = b] - 1$.

Definition 2 [4] (Ciphertext Anonymity or Key Privacy): A signcryption scheme satisfies the ciphertext anonymity property if no probabilistic polynomial time distinguishers have 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 $\mathtt{Signcrypt}(m, sk_{\mathsf{r},c}, pk_{\mathsf{r}})$ for arbitrary recipient key pk_{r} and unsigncryption $\mathtt{Unsigncrypt}(C, sk_{\mathsf{r},c})$ for $c = 0$ or $c = 1$.
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 $C^* = \mathtt{Signcrypt}(m, sk_{\mathsf{s},b}, pk_{\mathsf{r},b'})$ which is sent to $\mathcal{D}$.
4. $\mathcal{D}$ continually queries the signcryption and unsigncryption with the restriction that it is not allowed to ask the unsigncryption of the challenge ciphertext C^* with the private keys $sk_{\mathsf{r},0}$ and $sk_{\mathsf{r},1}$.
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 $\mathrm{Adv}^{\mathtt{IND-CA}}(\mathcal{D}) := \Pr[(d, d') = (b, b')] - 1/4$.

Definition 3 [4] (Key Invisibility): A signcryption scheme satisfies the key invisibility if no probabilistic polynomial time distinguishers have a non-negligible advantage in the following game:
1. The challenger first generates a private/public key $(sk_{\mathsf{r}}^*, pk_{\mathsf{r}}^*)$ and gives pk_{r}^* to the distinguisher $\mathcal{D}$.
2. $\mathcal{D}$ adaptively makes a number of queries of signcryption $\mathtt{Signcrypt}(m, sk_{\mathsf{r}}^*, pk_{\mathsf{r}})$, for arbitrary recipient's public key pk_{r}, and unsigncryption $\mathtt{Unsigncrypt}(C, sk_{\mathsf{r}}^*)$.
3. $\mathcal{D}$ outputs a sender's private keys sk_{s} and a message $m \in \mathcal{M}$. The challenger then flips a coin $b \in \{0,1\}$. If $b = 0$ the challenger returns an actual ciphertext $C^* = \mathtt{Signcrypt}(m, sk_{\mathsf{s}}, pk_{\mathsf{r}}^*)$ to $\mathcal{D}$. Otherwise, the challenger returns a random C^* uniformly taken from the ciphertext space.
4. $\mathcal{D}$ continually queries the signcryption and unsigncryption with the restriction that it cannot query the unsigncryption of the challenge ciphertext C^* with the private keys sk_r^*.
5. At the end of the game, $\mathcal{D}$ outputs bits b' and wins if $b' = b$. The distinguisher $\mathcal{D}$'s advantage is defined to be $\mathrm{Adv}^{\mathtt{K-INV}}(\mathcal{D}) := 2\Pr[b' = b] - 1$.

Based on the above attack games for proving the security, we show that none of the above properties is achieved in the following three claims:

Claim 1: The Libert-Quisquater signcryption scheme is not semantically secure against chosen ciphertext attack.

Proof: Assume that given the receiver's public key X_{r} and the challenge ciphertext is $C^* = (U^*, W^*, Z^*)$ with the sender's secret key x_{s} and a message m_b which is one of m_0, m_1 (generated by the adversary $\mathcal{A}$), the adversary $\mathcal{A}$ computes $V_i = x_{\mathsf{s}} H_1(m_i, U^*, X_{\mathsf{r}})$ and $(m_i^* \| X_{\mathsf{s}}) = Z^* \oplus H_3(V_i)$ for $i = 0, 1$. Then, one of m_i^* must be equal to m_b, say $m_{b'}^*$ for some $b' \in \{0,1\}$. Hence the adversary $\mathcal{A}$ will make a correct guess b' which is equal to b. Therefore, we conclude that the Libert-Quisquater signcryption scheme is not semantically secure against chosen ciphertext attacks. □

Claim 2: The Libert-Quisquater signcryption scheme does not provide ciphertext anonymity.

Proof: Given the receiver's public key $X_{\mathsf{r},0}$ and $X_{\mathsf{r},1}$, the distinguisher $\mathcal{D}$ generates the sender's secret key $x_{\mathsf{s},0}$ and $x_{\mathsf{s},1}$ and a message m^*; and sends to the challenger. The challenger first chooses two randoms $b, b' \in \{0,1\}$ for the target sender's secret key $(x_{\mathsf{s},b})$ and the target receiver's public key $(X_{\mathsf{r},b'})$ respectively and produces the challenge ciphertext $C^* = (U^*, W^*, Z^*)$. Upon receipt of the challenge ciphertext, the distinguisher $\mathcal{D}$ computes $V_{i,j} = x_{\mathsf{s},i} H_1(m^*, U^*, X_{\mathsf{r},j})$ and $(m_{i,j} \| \bar{X}_{i,j}) = Z^* \oplus H_3(V_{i,j})$ for $i, j = 0, 1$. Then, one of $m_{i,j}$ must be equal to m^*, say $m_{d,d'}$ for some $d, d' \in \{0,1\}$. Note that $\bar{X}_{d,d'}$ must also be equal to $X_{\mathsf{s},b}$ (one of the sender's public key corresponding to the secret key $x_{\mathsf{s},b}$). Then the distinguisher $\mathcal{D}$ outputs the correct guess (d, d') which is equal to (b, b'). Hence, we conclude that the Libert-Quisquater signcryption scheme does not provide ciphertext anonymity. □

Claim 3: The Libert-Quisquater signcryption scheme does not provide key invisibility.

Proof: Given the receiver's public key X_{r}, the distinguisher $\mathcal{D}$ generates the sender's secret key x_{s} and a message m^*; and sends to the challenger to produce the challenge ciphertext $C^* = (U^*, W^*, Z^*)$. Upon receipt of the challenge ciphertext, the distinguisher $\mathcal{D}$ computes $V_t = x_{\mathsf{s}} H_1(m^*, U^*, X_{\mathsf{r}})$ and $(m_t \| X_t) = Z^* \oplus H_3(V_t)$. If $m_t = m^*$ and $X_t = X_{\mathsf{s}}$, then the distinguisher $\mathcal{D}$ outputs the guess $b' = 0$, otherwise outputs $b' = 1$. Hence, we conclude that the Libert-Quisquater signcryption scheme does not provide key invisibility. □

4. Conclusion

In this paper, we showed that the Libert-Quisquater signcryption scheme does not fulfill the claim as stated in the paper [4], that is, semantically security against chosen ciphertext attack, ciphertext anonymity and key invisibility. We demonstrate the attack methods for all the three properties and conclude that the Libert-Quisquater signcryption scheme is insecure in their attack games.

Acknowledgments

The author wishes to thank the reviewers for their insightful comments and invaluable suggestions for revision of this paper.

References

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

[2] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from Weil pairing," Advances in Cryptology—Asiacrypt'01, Lecture Notes in Computer Science, vol.2248, pp.514–532, Springer-Verlag, 2001.

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

[4] B. Libert and J.J. Quisquater, "Efficient signcryption with key privacy from gap Diffie-Hellman groups," Public Key Cryptography—PKC'04, Lecture Notes in Computer Science, vol.2947, pp.187–200, Springer-Verlag, 2004.

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