IEICE TRANS. FUNDAMENTALS, VOL.E89–A, NO.1 JANUARY 2006

LETTER *Special Section on Cryptography and Information Security*

Security Analysis of Signcryption Scheme from q-Diffie-Hellman Problems*

Chik-How TAN[†a)], ***Affiliate Member***

SUMMARY In this paper, we analyse the Libert-Quisquater's q-DH signcryption scheme proposed in SCN'2004. Although the paper proved that their scheme is secure against adaptive chosen ciphertext attacks in the random oracle model, we disprove their claim and show that their scheme is not even secure against non-adaptive chosen ciphtertext attacks, which is the weaker security than the adaptive chosen ciphertext attacks. We further show that the semantically secure symmetric encryption scheme defined in their paper is not sufficient to guarantee their signcryption scheme to be secure against adaptive chosen ciphertext attacks.

key words: *cryptography, signcryption*

1. Introduction

The basic concept of a signcryption scheme is to provide confidentiality and authenticity simultaneously and was first proposed by Zheng in 1997 [10]. Since then, many signcryption schemes were proposed. It was only recent that a formal security proof model [2] was formalized by Baek, Steinfeld and Zheng in 2002. They also gave a security proof of Zheng's scheme [10] in the random oracle model. In 2003, Boyen [5] 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 [2] which included the ciphertext anonymity. In 2004, Libert and Quisquater [7] 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: semantically security against adaptive chosen ciphertext attacks, ciphertext anonymity and key invisibility. In 2005, Tan [9] showed that none of the above properties were achieved under their defined attacks games. In 2004, Libert and Quisquater [8] also proposed an improved signcryption from q-Diffie-Hellman problems and proved that their scheme was secure against adaptive chosen ciphertext attack in the random oracle model. In this paper, we disprove their claim and show that their scheme is not even secure against non-adaptive chosen ciphertext attacks. We also show that the semantically secure symmetric encryption scheme defined in their paper [8] is not sufficient to guarantee their signcryption scheme to be secure against adaptive chosen ciphertext attacks.

Manuscript received March 18, 2005.
Manuscript revised June 27, 2005.
Final manuscript received August 8, 2005.

[†]The author is with NISlab, Department of Computer Science and Media Technology, Gjøvik University College, Norway.

[*]This work was carried out while the author was at Nanyang Technological University, Singapore.

a) E-mail: chik.tan@hig.no

DOI: 10.1093/ietfec/e89–a.1.206

2. Libert-Quisquater's q-DH Signcryption

A signcryption scheme normally involves three stages, that is, key generation, signcryption generation and de-signcryption. Now, we describe the Libert-Quisquater's q-DH signcryption scheme [8] as follows:

Key Generation: Let p be a prime number and k be a positive integer such that $2^{k-1} < p < 2^k$ and G_1 and G_2 be two groups of the same prime order p. Let g be a generator of G_1 and e be a bilinear map such that $e : G_1 \times G_1 \to G_2$. Let H_1, H_2 and H_3 be hash functions such that $H_1 : \{0,1\}^* \to Z_p$, $H_2 : G_1 \times G_1 \times G_1 \to \{0,1\}^k$ and $H_3 : \{0,1\}^k \to \{0,1\}^\lambda$, where λ is a positive integer. Also assume a pseudo-random function $H' : \{0,1\}^* \to \{0,1\}$. Let $(\mathcal{E}, \mathcal{D})$ be a semantically secure symmetric encryption scheme** of key length λ. Consider a user u, first chooses a random $x_\mathsf{u}, \in Z_p$ and computes $X_\mathsf{u} = g^{x_\mathsf{u}}$. Then, the public key of user u is X_u and the private key is x_u. We denote the sender and the receiver as 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.

Signcrypt: To signcrypt a message $m \in \{0,1\}^n$, where n is a positive integer, for the intended user r, the sender s first chooses a random $w \in Z_p^*$ and computes

$$b_m = H'(x_\mathsf{s}, m), \quad v = \frac{w}{H_1(b_m \| m) + x_\mathsf{s}},$$
$$c_1 = g^v \in G_1, \quad c_2 = w \oplus H_2(c_1, X_\mathsf{r}, X_\mathsf{r}^v),$$
$$c_3 = \mathcal{E}_k(m \| X_\mathsf{s}) \in \{0,1\}^{n+\lambda},$$

where $k = H_3(w) \in \{0,1\}^\lambda$. Then, the ciphertext is $C = (b_m, c_1, c_2, c_3)$.

De-signcrypt: Upon receipt of a ciphertext $C = (b_m, c_1, c_2, c_3)$, the receiver r computes $w = c_2 \oplus H_2(c_1, X_\mathsf{r}, c_1^{x_\mathsf{r}})$. If $w \notin Z_p^*$, then return $\perp$, otherwise computes the following:

$$k = H_3(w), \quad m \| X_\mathsf{s} = \mathcal{D}_k(c_3), \quad \sigma = c_1^{w^{-1}}.$$

The receiver accepts the message m if and only if $e(\sigma, X_\mathsf{s} g^{H_1(b_m \| m)}) = e(g, g)$.

**An adversary against such a symmetric encryption is unable to decide which one of two chosen messages matches a challenge ciphertext without having access to encryption or decryption oracles.

3. Analysis

In this section, we describe the attacks game in the security against adaptive chosen ciphertext attacks which was defined in [8]. Although the authors [8] proved their scheme was secure in the random oracle model, we will show that the scheme is in fact not secure based on their defined attacks game listed in [8]. Now, we describe the attacks game as follows:

Definition 1: [8] (Security Against Chosen Ciphertext Attacks) A signcryption scheme is 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 de-signcryption. 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 $\mathtt{Signcrypt}(m, sk_{\mathsf{r}}^*, pk_{\mathsf{r}})$ and returns the result. In de-signcryption queries, $\mathcal{A}$ submits a ciphertext C to the challenger. The challenger runs the de-signcrypt oracle $\mathtt{De-signcrypt}(C, sk_{\mathsf{r}}^*)$. 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 ciphertext $C^* = \mathtt{Signcrypt}(m_b, sk_{\mathsf{s}}, pk_{\mathsf{r}}^*)$ 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 de-signcryption. $\mathcal{A}$ is not allowed to query the de-signcrypt 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 $\mathrm{Adv}^{\mathtt{IND-CCA}}(\mathcal{A}) := 2\Pr[b' = b] - 1$.

Based on the above attacks game for proving the security against adaptive chosen ciphertext attacks, we show that the Libert-Quisquater's q-DH signcryption scheme is not secure against non-adaptive chosen ciphertext attacks as follows:

Claim 1: The Libert-Quisquater's q-DH signcryption scheme is not secure against non-adaptive chosen ciphertext attacks.

Proof: Assume that given the receiver's public key X_{r} and the adversary $\mathcal{A}$ first chooses a sender secret key x_{s} and two equal length messages m_0 and m_1 such that $b_{m_0} = H'(x_{\mathsf{s}}, m_0) = 0$ and $b_{m_1} = H'(x_{\mathsf{s}}, m_1) = 1$ and send x_{s}, m_0 and m_1 to the challenger. The challenger then compute the challenge ciphertext $C^* = (b_{m_b}^*, c_1^*, c_2^*, c_3^*)$ where $b \in \{0, 1\}$. Upon receipt of the challenge ciphertext $C^* = (b_{m_b}^*, c_1^*, c_2^*, c_3^*)$, then b_{m_b} must be equal to either b_{m_0} or b_{m_1}. Hence the adversary $\mathcal{A}$ can make a correct guess b' which is equal to b. Therefore, we conclude that the Libert-Quisquater q-DH signcryption scheme is not secure against non-adaptive chosen ciphertext attacks. □

As mentioned in the paper [8], the introduction of $b_m = H'(x_{\mathsf{s}}, m)$ is to achieve tight security reduction without a random salt. We showed in claim 1 that this leads to insecurity of signcryption scheme against non-adaptive chosen ciphertext attacks. In the following, we further show that even ignoring b_m, the signcryption is also not secure against adaptive chosen ciphertext attacks with the assumption of the semantically secure symmetric encryption scheme $(\mathcal{E}, \mathcal{D})$ defined in [8]. In [6], Goldreich gave a construction of a semantically secure symmetric encryption scheme (Construction 5.3.9 or Construction 5.3.12 and proved in Proposition 5.4.12, [6]) which was briefly described as follows: Let the semantically secure symmetric encryption scheme be $(\bar{\mathcal{E}}, \bar{\mathcal{D}})$ such that $\bar{\mathcal{E}}_k(z, m) = f_k(z) \oplus m$ where f_k is a pseudorandom function using secret key k, random string z and message m. One of the example is a block cipher encryption in the counter mode. This example also shows to be semantically secure in [3].

Claim 2: The semantically secure symmetric encryption scheme $(\mathcal{E}, \mathcal{D})$ in the Libert-Quisquater's q-DH signcryption scheme does not sufficiently guarantee their signcryption to be secure against adaptive chosen ciphertext attacks.

Proof: Let the semantically secure symmetric encryption scheme be $(\bar{\mathcal{E}}, \bar{\mathcal{D}})$ constructed as above. Assume that given the receiver's public key X_{r}, the adversary $\mathcal{A}$ first chooses a sender secret key x_{s} and two equal length messages m_0 and m_1 and send these to the challenger. The challenger then computes the challenge ciphertext $\bar{C} = (\bar{b}_{m_b}, \bar{c}_1, \bar{c}_2, \bar{c}_3)$ where $b \in \{0, 1\}$. Upon receipt of the challenge ciphertext $\bar{C} = (\bar{b}_{m_b}, \bar{c}_1, \bar{c}_2, \bar{c}_3)^{\dagger}$, the adversary first makes a "wild guess" that b to be 0 and constructs a new ciphertext by choosing a random message $\hat{m}$ whose length is equal to that of m_0 and computing the following:

$$\hat{X}_{\mathsf{s}} = X_s g^{H_1(\bar{b}_{m_b} \| |m_0) - H_1(0 \| |\hat{m})},$$
$$\hat{c}_3 = \bar{c}_3 \oplus (m_0 \oplus \hat{m}) \| (X_{\mathsf{s}} \oplus \hat{X}_{\mathsf{s}}).$$

Then, the adversary $\mathcal{A}$ sent the ciphertext $\hat{C} = (0, \bar{c}_1, \bar{c}_2, \hat{c}_3)$ to the challenger for de-signcryption. Upon receipt the query, the challenger computes $\hat{w} = \bar{c}_2 \oplus H_2(\bar{c}_1, X_{\mathsf{r}}, \bar{c}_1^{x_{\mathsf{r}}})^{\dagger\dagger}$. If $\hat{w} \notin Z_p^*$, then returns $\perp$, otherwise computes the following:

$$k = H_3(\hat{w}), \quad m' \| X'_{\mathsf{s}} = \bar{\mathcal{D}}_k(\hat{c}_3), \quad \hat{\sigma} = \bar{c}_1^{\hat{w}^{-1}}.$$

[†]Here, we ignore the attack on $\bar{b}_{m_b}$ as in Claim 1.

[††]It is noted that $\hat{w}$ is the same as that computed in the challenge ciphertext.

If $e(\hat{\sigma}, X'_s g^{H_1(0\|m')}) = e(g,g)^{\dagger}$, then the challenger returns the message m', otherwise rejects the message. If the response from the challenger is message m' (which is equal to $\hat{m}$), then the adversary will know that m_0 is the plaintext for the challenge ciphertext (as the adversary $\mathcal{A}$ uses m_0 to compute the new ciphertext $\hat{C}$). If the response is rejected, then m_1 is the plaintext for the challenge ciphertext. Hence, the adversary will make a correct guess of b. Therefore, the Libert-Quisquater's q-DH signcryption scheme is not secure against adaptive chosen ciphertext attacks. □

It is noted that an attacker does not make use of the signer's secret key in the proof of the claim 2. So, the Libert-Quisquater's q-DH signcryption scheme is also not secure in the sense of the outsider security defined by An, Dodis and Rabin [1] in 2002. The outsider security is defined as the same as that of definition 1 except that an attacker is given the sender's public key instead of the sender's secret key.

4. Conclusion

In this paper, we showed that the Libert-Quisquater's q-DH signcryption scheme is not secure against non-adaptive chosen ciphertext attacks which is the weaker security than the adaptive chosen ciphertext attack as claimed in the paper [8]. We further demonstrated that the semantically secure symmetric encryption scheme is not sufficient to guarantee the Libert-Quisquater's q-DH signcryption scheme to be secure against adaptive chosen ciphertext attacks.

Acknowledgments

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

[†]It is noted that the challenger first checks whether $X'_s \in G_1$. If $X'_s \notin G_1$, then it is not necessary to check the signature verification equation, otherwise it checks the signature verification equation. This is not mentioned in paper [8].

References

[1] J.-H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," Advances in Cryptology—Eurocrypt'02, Lect. Notes Comput. Sci., vol.2332, pp.83–107, Springer-Verlag, 2002.

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

[3] M. Bellare, A. Desai, E. Jopkipii, and P. Rogaway, "A concrete security treatment of symmetric encryption: Analysis of the DES modes of operation," The 38th IEEE Annual Symposium on Foundations of Computer Science, pp.394–403, IEEE, 1997.

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

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

[6] O. Goldreich, Foundations of Cryptography: Basic Applications, vol.2, Cambridge University Press, 2004.

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

[8] B. Libert and J.J. Quisquater, "Improved signcryption from q-Diffie-Hellman problems," Security Communication Networks—SCN'04, Lect. Notes Comput. Sci., vol.3352, pp.220–234, Springer-Verlag, 2005.

[9] C.H. Tan, "On the security of signcryption scheme with key privacy," IEICE Trans. Fundamentals, vol.E88-A, no.4, pp.1093–1095, April 2005.

[10] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) ≪ cost(signature) + cost(encryption)," Advances in Cryptology—Crypto'97, Lect. Notes Comput. Sci., vol.1294, pp.165–179, Springer-Verlag, 1997.