JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 27, 1153-1158 (2011)

Short Paper

Comments on Shao-Cao's Unidirectional Proxy Re-Encryption Scheme from PKC 2009*

MIN-RONG CHEN[1,2], XI ZHANG[3,+] AND XIA LI[2]
[1]*Management School*
Jinan University
Guangzhou, 510632 P.R. China
[2]*College of Information Engineering*
[3]*College of Computer and Software*
Shenzhen University
Shenzhen, 518060 P.R. China

Proxy re-encryption (PRE), introduced by Blaze, Bleumer and Strauss, allows a semi-rusted proxy to convert a ciphertext originally intended for Alice into an encryption of the same message intended for Bob. In PKC'09, Shao and Cao proposed a unidirectional PRE scheme without pairings, and compared their scheme with Libert-Vergnaud's pairing-based unidirectional PRE scheme from PKC'08. In this paper, we indicated that Shao-Cao's scheme is not secure against chosen-plaintext attack in Libert-Vergnaud's security model.

Keywords: proxy re-encryption, chosen-ciphertext attack, chosen-plaintext attack, bilinear pairing, transformed ciphertext

1. INTRODUCTION

In Eurocrypt'98, Bleumer and Strauss [1] introduced an innovative concept named proxy re-encryption (PRE). In a PRE system, a semi-trusted proxy, given a re-encryption key, is able to transform a ciphertext originally intended for Alice into an encryption of the same message intended for Bob. The proxy, however, cannot learn anything about the messages encrypted under either key. Since its advent, PRE has attracted great interest, and many PRE schemes as well as some variants (*e.g.*, [2-6]) have been proposed. According to the direction of transformations, PRE can be categorized into *bidirectional* PRE and *unidirectional* PRE. In bidirectional PRE, the proxy can transform from Alice to Bob and vice versa. In contrast, the proxy in unidirectional PRE cannot transform ciphertexts in the opposite direction. PRE can also be categorized into *multi-hop* PRE, in which the ciphertexts can be transformed from Alice to Bob and then to Charlie and so on, and *single-hop* PRE, in which the ciphertexts can only be transformed once.

Received October 1, 2009; revised January 22, 2010; accepted March 26, 2010.
Communicated by Wen-Guey Tzeng.
* This work was supported by the National Natural Science Foundation of China under grants No. 61005049 and 60772148, and the Specialized Research Fund for Ph.D. Program Foundation of Colleges and Universities of China under grant No. 200805900001.
+ Corresponding author.

Earlier PRE schemes (*e.g.* [1, 7-10]) either merely resist chosen-plaintext attack (CPA), or rely on bilinear pairings. However, applications often require security against chosen-ciphertext attacks (CCA), and bilinear parings are rather expensive compared with standard operations such as modular exponentiation in finite fields. In view of this, Canetti and Hohenberger [8] left an important open problem in ACM CCS'07, *i.e.*, how to construct a CCA-secure PRE scheme without pairings.

In CANS'08, Deng *et al.* [11] proposed the first CCA-secure single-hop bidirectional PRE scheme without pairings. Subsequently, in PKC'09 Shao and Cao [12] proposed a single-hop unidirectional PRE scheme without pairings, and claimed that their scheme is CCA-secure. However, by giving a concrete chosen-ciphertext attack, Chow *et al*. [13] recently pointed out that Shao-Cao's scheme is not CCA-secure, and proposed another more efficient CCA-secure unidirectional PRE scheme without pairings. We notice that Shao and Cao also compared their scheme with Libert-Vergnaud's single-hop unidirectional PRE scheme [9] from PKC'08. In this paper, we further indicate that Shao-Cao's scheme is even not CPA-secure in Libert-Vergnaud's security model.

2. REVIEW OF SHAO-CAO'S SCHEME

We here review Shao-Cao's PRE scheme [12] as below, only with minor notational differences.

- **Global-Setup:** Choose three hash functions H_1, H_2 and H_3 where H_1: $\{0, 1\} \to \{0, 1\}^{k_1}$, H_2: $\{0, 1\} \to \{0, 1\}^n$, and H_3: $\{0, 1\} \to \{0, 1\}^{k_2}$. Here k_1 and k_2 are security parameters, and n is the bit-length of messages to be encrypted. The public parameters are $param = (H_1, H_2, H_3, n, k_1, k_2)$.
- **KeyGen:** First choose a safe prime modulus $N = pq$, where $p = 2p' + 1$, $q = 2q' + 1$, p, p', q, q' are primes. Next, choose three random numbers $\alpha \in Z^*_{N^2}$, $a, b \in [1, pp', qq']$ and a hash function H such that H: $\{0, 1\}^* \to Z_{N^2}$. Furthermore, set $g_0 = \alpha^2 \bmod N^2$, $g_1 = g_0^a \bmod N^2$, and $g_2 = g_0^b \bmod N^2$. The public key for this user is $pk = (H, N, g_0, g_1, g_2)$, the "weak" secret key is $wsk = (a, b)$, and the long term secret key is $sk = (p, q, p', q')$.
- **ReKeyGen:** On input a public key $pk_Y = (H_Y, N_Y, g_{Y0}, g_{Y1}, g_{Y2})$, a "weak" secret key $wsk_X = a_X$, and a long term secret key $sk_X = (p_X, q_X, p'_X, q'_X)$, it outputs the re-encryption key $rk_{X\to Y} = (rk^{(1)}_{X\to Y}, rk^{(2)}_{X\to Y})$, where $rk^{(1)}_{X\to Y} = (\dot{A}, \dot{B}, \dot{C})$, as follows,

  1. Randomly pick $\dot{\sigma} \in Z_{N_Y}$ and $\dot{\beta} \in \{0, 1\}^{k_1}$. Compute $rk^{(2)}_{X\to Y} = a_X - \dot{\beta} \bmod (p_X q_X p'_X q'_X)$.
  2. Compute $r_{X\to Y} = H_Y(\dot{\sigma} \| \dot{\beta})$ and then

$$\dot{A} = (g_{Y0})^{r_{X\to Y}} \bmod (N_Y)^2,\ \dot{B} = (g_{Y2})^{r_{X\to Y}} \cdot (1 + \dot{\sigma} N_Y) \bmod (N_Y)^2,\ \dot{C} = H_1(\dot{\sigma}) \oplus \dot{\beta}.$$

- **Enc:** On input a public key $pk = (H, N, g_0, g_1, g_2)$ and a message $m \in \{0, 1\}^n$, the sender acts as follows,

  1. Randomly pick $\sigma \in Z_N$. Then compute $r = H(\sigma \| m)$, $A = (g_0)^r \bmod N^2$, $B = (g_1)^r \cdot (1 + \sigma N) \bmod N^2$, $C = H_2(\sigma) \oplus m$, and $D = (g_2)^r \bmod N^2$.
  2. Run$(c, s) \leftarrow$ SoK.Gen$(A, D, g_0, g_2, (B, C))$, where the underlying hash function is H_3.

Here SoK.Gen is a function defined in [12]. For detailed description, please refer to [12].

3. Output the original ciphertext CT = (A, B, C, D, c, s).

- **ReEnc:** On input a re-encryption key $rk_{X\to Y} = (rk^{(1)}_{X\to Y}, rk^{(2)}_{X\to Y})$ and an original ciphertext CT = (A, B, C, D, c, s) under key pk_X = (H_X, N_X, g_{X0}, g_{X1}, g_{X2}), this algorithms first checks whether $c = H_3(A\|D\|g_{X0}\|g_{X2}\|(g_{X0})^s A^C\|(g_{X2})^s D^c\|(B\|C))$ holds. If no, return $\perp$; otherwise, compute $A' = A^{rk^{(2)}_{X\to Y}} = (g_{X0})^{r(a_X-\beta)} \bmod (N_X)^2$, and output the transformed ciphertext $CT_Y = (pk_X, A, A', B, C, rk^{(1)}_{X\to Y}) = (pk_X, A, A', B, C, \dot{A}, \dot{B}, \dot{C})$.
- **Dec:** On input a private key and a ciphertext CT, this algorithm acts according to cases:

– If CT is an original ciphertext in the form CT = (A, B, C, D, c, s), it works as follows,

1. Check whether $c = H_3(A\|D\|g_0\|g_2\|(g_0)^s A^C\|(g_2)^s D^c\|(B\|C))$ holds. If not, return $\perp$, else,
   * if the secret key is the "weak" secret key a, compute $\sigma = \dfrac{B/(A^a) - 1 \bmod N^2}{N}$.
   * if the secret key is the long term secret key (p, q, p', q'), compute

$$\sigma = \frac{B/(g_0^{w_1})^{2p'q'} - 1 \bmod N^2}{N} \cdot \pi \bmod N,$$

   where w_1 is computed as that in [14], and π is the inverse of $2p'q' \bmod N$.
2. Compute $m = C \oplus H_2(\sigma)$. If $B = (g_1)^{H(\sigma\|m)} \cdot (1 + \sigma N) \bmod N^2$ holds, return m; else return $\perp$.

– If CT is a transformed ciphertext in the form CT = (pk_X, A, A', B, C, $\dot{A}$, $\dot{B}$, $\dot{C}$) re-encrypted from pk_X to pk_Y:

1. Compute $\dot{\sigma}$ according to the following situations:
   * if the secret key is the "weak" secret key b, compute

$$\dot{\sigma} = \frac{\dot{B}/(\dot{A}^b) - 1 \bmod (N_Y)^2}{N_Y}.$$

   * if sk is the long term secret key (p, q, p', q'), compute

$$\dot{\sigma} = \frac{\dot{B}/(g_{Y_0}^{w_1})^{2p'q'} - 1 \bmod (N_Y)^2}{N_Y} \cdot \pi \bmod N_Y$$

   where w_1 is computed as that in [14], and π is the inverse of $2p'q' \bmod N_Y$.
2. Compute $\dot{\beta} = \dot{C} \oplus H_1(\dot{\sigma})$, and check whether $B = (g_{Y1})^{H_Y(\dot{\sigma}\|\dot{\beta})} \cdot (1 + \dot{\sigma} N_Y) \bmod (N_Y)^2$ holds. If not, return $\perp$.
3. Compute $\sigma = \dfrac{B/(A' \cdot A^{\dot{\beta}}) - 1 \bmod (N_X)^2}{N_X}$, and $m = C \oplus H_2(\sigma)$. If $B = (g_{X1})^{H_X(\sigma\|m)} \cdot (1 + \sigma N_X) \bmod (N_X)^2$ holds, return m; else return $\perp$.

3. CRYPTANALYSIS OF SHAO-CAO'S SCHEME

Libert and Vergnaud [9] defined two types of security models for single-hop unidirectional PRE: one concerning original ciphertexts, the other concerning transformed ciphertexts. Shao-Cao's security model in fact corresponds to the one concerning original ciphertexts, except that it considers the CCA-security instead of the replayable CCA-security [15]. Chow *et al.*'s attack has indicated that Shao-Cao's scheme is not CCA-secure in the model concerning original ciphertexts. In this section, we shall indicate that Shao-Cao's scheme is not secure in Libert-Vergnaud's security model concerning transformed ciphertexts.

We first briefly explain some necessary facts about Libert-Vergnaud's security model concerning transformed ciphertexts (for more details, please refer to [9]). In this model, since the transformed ciphertexts cannot be further transformed, the adversary is allowed to corrupt *any* re-encryption keys. In addition, the adversary is allowed to corrupt any user except the target user.

Next, some properties about Shao-Cao's scheme should be explained: A collusion of a delegator X and his proxy enables the recover of the "weak" secret key of X. Any re-encryption of ciphertext for X still contains most part of the original one, which means that no matter who is the delegatee, it can still be decryptable by applying the "weak" secret key of X on the original components.

Now, we explain how an adversary can break Shao-Cao's scheme according to Libert-Vergnaud's security model concerning transformed ciphertexts. Given a challenge transformed ciphertext CT_{Y^*} under the target user Y^* transformed from the delegator X, the adversary can decrypt this challenge ciphertext in the following two ways:

- By corrupting another user Z's secret key and the re-encryption key from X to Z, the adversary can recover user X's "weak" secret key. Then the adversary can use this "weak" secret key to decrypt CT_{Y^*} and recover the underlying plaintext.
- Recall that the adversary is allowed to corrupt any user except the target user. So, the adversary can simply corrupt user X to obtain user X's "weak" secret key, and then uses it to decrypt CT_{Y^*} and recover the underlying plaintext.

Note that the above adversary does not issue any decryption query. This means that Shao-Cao's scheme is even not CPA secure in Libert-Vergnaud's security model concerning transformed ciphertexts.

Remark: Although our attack is the CPA attack and Chow *et al.*'s is the CCA attack, we stress that it would be misleading to say that Chow *et al.*'s CCA attack is overkill: Chow *et al.*'s attack is conformed to Shao-Cao's security model concerning original ciphertexts, and their attack is refuting the "proof" in [12] by making clever use of decryption oracle; while our attack is conformed to Libert-Vergnaud's security model for transformed ciphertexts which was not considered in [12].

4. CONCLUSIONS

We pointed out that Shao-Cao's comparisons between their unidirectional PRE scheme and Libert-Vergnaud's scheme is unfair, since Shao-Cao's scheme is even not CPA-secure in Libert-Vergnaud's security model.

REFERENCES

1. M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proceedings of EUROCRYPT*, LNCS 1403, 1998, pp. 127-144.
2. B. Libert and D. Vergnaud, "Tracing malicious proxies in proxy re-encryption," in *Proceedings of the 2nd International Conference on Pairing-based Cryptography*, LNCS 5209, 2008, pp. 332-353.
3. Q. Tang, "Type-based proxy re-encryption and its construction," in *Proceedings of the 9th International Conference on Cryptology in India*, LNCS 5365, 2008, pp. 130-144.
4. J. Weng, R. H. Deng, X. Ding, C. K. Chu, and J. Lai, "Conditional proxy re-encryption secure against chosen-ciphertext attack," in *Proceedings of ACM Symposium on Information, Computer and Communication Security*, 2009, pp. 322-332.
5. C. K. Chu, J. Weng, S. S. M. Chow, J. Zhou, and R. H. Deng, "Conditional proxy broadcast re-encryption," in *Proceedings of the 14th Australasian Conference on Information Security and Privacy*, LNCS 5594, 2009, pp. 327-342.
6. J. Weng, Y. Yang, Q. Tang, R. H. Deng, and F. Bao, "Efficient conditional proxy re-encryption with chosen-ciphertext security," in *Proceedings of the 12th International Information Security Conference*, LNCS 5735, 2009, pp. 151-166.
7. G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, 2005, pp. 29-43.
8. R. Canetti and S. Hohenberger, "Chosen-siphertext cecure proxy re-encryption," in *Proceedings of the 14th ACM Conference on Computer Communications and Society*, 2007, pp. 185-194.
9. B. Libert and D. Vergnaud, "Unidirectional chosen-ciphertext secure proxy re-encryption," in *Proceedings of the 11th International Workshop on Practice and Theory in Public Key Cryptography*, LNCS 4939, 2008, pp. 360-379.
10. J. Weng, M. Chen, Y. Yang, R. Deng, K. Chen, and F. Bao, "CCA-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles," *Science China Information Sciences*, Vol. 53, 2010, pp. 593-606.
11. R. H. Deng, J. Weng, S. Liu, and K. Chen, "Chosen-ciphertext secure proxy re-encryption without pairings," in *Proceedings of the 7th International Conference on Cryptology and Network Security*, LNCS 5339, 2008, pp. 1-17.
12. J. Shao and Z. Cao, "CCA-secure proxy re-encryption without pairings," in *Proceed- ings of the 12th International Conference on Practice and Theory in Public Key Cryptography*, LNCS 5443, 2009, pp. 357-376.
13. S. S. M. Chow, J. Weng, Y. Yang, and R. H. Deng, "Efficient unidirectional proxy re-encryption," in *Proceedings of the 3rd International Conference on Cryptology in*

Africa, LNCS 6055, 2009, pp. 316-322.
14. E. Bresson, D. Catalano, and D. Pointcheval, "A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications," in *Proceedings of the 9th International Conference on the Theory and Application of Cryptology and Information Security*, LNCS 2894, 2003, pp. 37-54.
15. R. Canetti, H. Krawczyk, and J. B. Nielsen, "Relaxing chosen-ciphertext security," in *Proceedings of the 23rd Annual International Cryptology Conference*, LNCS 2729, 2003, pp. 565-582.

Min-Rong Chen (陳泯融) is a Lecture in the College of Information Engineering, Shenzhen University, and she also works for the Management School in Jinan University, P.R. China. She received the B.S. degree, M.S. degree and Ph.D. degree in 2000, 2004 and 2008 respectively. Her research interests include information security and intelligent computation. Currently she focuses on the cryptanalysis and design of cryptosystems, mainly cooperated with Prof. Xi Zhang who is the initiator of this paper. She has published more than 20 papers in international journals and refereed conferences.

Xi Zhang (张席) received the B.S. degree from Xi'an Jiao Tong University in 1985. He got the M.S. degree in Computer Science, South China University of Technology in 1997. Currently, he is an Associate Professor in the College of Computer and Software, Shenzhen University. His current research area includes cryptography and information security.

Xia Li (李霞) received the B.S. and M.S. degrees both from Xidian University, Xi'an, P.R. China. She got the Ph.D. degree from the Division of Information Engineering, the Chinese University of Hong Kong, in 1997. She is currently a Professor in the College of Information Engineering, Shenzhen University, Shenzhen, P.R. China. Her research interests include information security, emergent optimization technology and intelligent signal processing.