CCA secure type-based proxy re-encryption in the adaptive corruption model without random oracle

Yanni Chang[a,b]
[a]School of Mathematics and Computer Engineering
XiHua University
ChengDu 610039, China
Changyanni82@gmail.com

Mingxing He[a]
[b]School of Mathematics and Statistics
NanYang Normal University
473000, China
Hemingxing64@gmail.com

***Abstract*—Type-based proxy re-encryption can solve the fine-grained delegation perfectly, and being more and more important in applications. However, as we know, there is still a problem come up with type-based proxy re-encryption in adaptive corruption model. In this paper, we propose a typed-based proxy re-encryption in the adaptive corruption model without random oracle; the scheme is CCA secure and proxy-invisible. Compared with the type-based proxy re-encryption proposed by J.S.D in 2013, this scheme has advantages in both security and efficiency.**

Keywords- adaptive corruption model; CCA secure; type-based proxy re-encryption; proxy-invisible

I. INTRODUCTION

In order to delegate the decryption right from one part (the delegator) to another part (the delegatee), the concept of proxy re-encryption (PRE) was proposed by M. Blaze, G. Bleumer, and M. Strauss [1] in 1998. In a PRE scheme, the semi-trusted proxy with the re-encryption key generated by delegator transforms the cipher text under the public key of delegator into the cipher text of another one (we call it delegatee), and the proxy cannot obtain any information about the plaintext under any public key. PRE schemes turn to be a useful primitive, especially in following fields, distributed file system, encrypted emails forwarding and access of the encrypted files in cloud storage.

A. Related Work

In the document [1], based on E1Gamal's public key encryption scheme, Blaze and others presented a specific PRE scheme. In this scheme, proxy can transform the ciphertext under Alice's public key to the ciphertext of Bob's and vice versa. Thus, this scheme is bidirectional (the PRE scheme which can only support one-way transformation is unidirectional). But, unfortunately, Alice (Bob) can plot together with proxy to obtain the private key of Bob (Alice). We call this scheme *non–master- key secure*. This problem is quite serious, as users generally use the same secret keys for both their encryption schemes and signature schemes and thus the success of plotting together can get rid of the non-repudiation ensured by signature schemes. Later, Jakobsson [2] and Zhou and others [3] proposed a method to solve the problem of master key insecurity in [1], in which more than one proxy is used. But, in essence, the problem of master key insecurity is not resolved by dong this. In documents [4], based on secret key sharing technology, the delegator's secret key is divided into two parts, one part given to the proxy and the other part given to the delegatee. Using this technology, Ivan and Dodis put forward a general method to construct unidirectional PRE scheme in [4]. Although this way of construction shows great improvements compared with previous methods, it suffers from the following disadvantages: i. besides a personal secret key, the delegatee has to store another secret message from the delegator. ii. though it is impossible for the delegator and proxy to plot together to obtain the secret key of the delegatee, the delegatee and proxy are able to plot together to get the secret key of the delegator, which causes the loss of the security of master key.

However, as mentioned in many documents [5], the schemes discussed previously can only achieve chosen plaintext attacks (CPA) security, while, in actual use, the schemes are often required to achieve chosen ciphertext attack (CCA) security. Lately, based on another secret key sharing technology, Green and Ateniese respectively proposed the first CPA secure and CCA-secure identity-based unidirectional PRE scheme in [6]. The key factor that distinguishes this new secret key sharing technology from the one of Ivan and Dodis is that the second part of the secret key is not sent to the delegatee directly by the delegator. Instead, it is sent to the proxy after encrypted by public key of delegatee's. Finally, the proxy sends it to the delegatee. In this way, it is unnecessary for the delegatee to store extra secret message. But their scheme can't satisfy master key security.

All the above-mentioned schemes are proved secure under random oracle model, but it does not mean that they are also secure in real life. In the 2007 ACM CCS conference, Canettiand and Hohenberger proposed the first bidirectional PRE scheme that is proved CCA-secure under standard model [5]. They had excellent results. To achieve CCA secure, Canetti used the technology of Canetti, Halevi and Katz mentioned in documents [7], by which any chosen-ID secure identity-based encryption scheme is transformed into a CCA-secure public key encryption scheme. In 2010, J. weng [8] proposed a CCA-secure unidirectional proxy re-encryption in the adaptive

corruption model, in which the adversary can choose the corrupted users adaptively.

To deal with fine-grain delegation, Tang [9] proposed a new definition, named type-based proxy re-encryption (TB-PRE) and give the first proxy-invisible TBPRE scheme. However, Tang's scheme is only CPA-secure. Weng [10] proposed another definition, called conditional proxy re-encryption (CPRE) almost at the same time. The two definitions are identical in essence (we call type-based proxy re-encryption in the following text). TBPRE scheme only allows proxy to re-encrypt files of some types set by delegator, so TBPRE realizes the selective delegation. The definition and secure model of CPRE were formalized by Weng and Yang in [11], and a CCA-secure CPRE scheme was proposed in random oracle model. Jun Shao [12] proposed the definition of identity-based conditional proxy re-encryption (IBCPRE) in 2011, and proposed the first CCA-secure IBCPRE scheme in random oracle model. In 2012, Jae woo seo et al. [13] proposed a proxy-invisible TBPRE scheme, that is RCCA-secure (the cipher text will tolerance a harmless damage) without random oracle. But the scheme is not CCA-secure in the adaptive corruption model.

B. Organization

We organize our paper as follow. Some preliminaries are given in Section II. In section III, we give the definition and secure model of type-based proxy re-encryption. Our concrete construction of type-based proxy re-encryption and the efficiency analysis is given in section IV. In the last section V, we conclude our paper.

II. PRELIMINARIES

A. Notations

If I is a finite set, then $x \in_R I$ denotes the operation of selecting an element x of I uniformly at random; $[x]_\tau$ denotes its first τ bits, and $[x]^\tau$ denotes its last τ bits.

B. Complexity Assuption

The security of our scheme is based on 3-Quotient Decision Bilinear Diffie-Hellman (3-QDBDH) assumption [14], which has been used by Jian Weng to construct CCA-secure PRE schemes in adaptive corruption model.

Definition 1. The 3-QDBDH problem [14]:

In groups (G, G_T), given a tuple $(g, g^a, g^{a^2}, g^{a^3}, g^b, Q) \in G^5 \times G_T$ with unknown $a, b \in_R Z_p$, to estimate whether $Q = e(g,g)^{b/a}$.

Definition 2. The 3-QDBDH assumption [14]:

For a probabilistic polynomial-time adversary B, we define his advantage in solving the 3-QDBDH problem in group (G, G_T) as

$$Adv_{\mathrm{B}}^{3-QDBDH} = \left| \Pr[B(g, g^a, g^{a^2}, g^{a^3}, g^b, Q = e(g,g)^{b/a}) = 1] - \Pr[B(g, g^a, g^{a^2}, g^{a^3}, g^b, Q = e(g,g)^c) = 1] \right|$$

Where the probability is taken over the randomly choices of a, b and the random coins consumed by adversary B.

We say the a 3-QDBDH assumption holds in groups (G, G_T), if there is no adversary B can solve the 3-QDBDH problem with non-negligible probability.

III. UNIDIRECTIONAL TBPRE

A. Model of unidirectional TBPRE

Definition 3. A type-based proxy re-encryption comprises following algorithms:

1) Setup: This is a probabilistic algorithm. On input security parameter λ, this algorithm outputs system parameters, which are used in the rest algorithms.

2) KeyGen: This algorithm outputs the public/private key pair $KeyGen(\lambda) \rightarrow (pk_i, sk_i)$ for an user U_i.

3) ReKeyGen: On input user U_i private key sk_i, user U_j public key pk_j and the type value t, this algorithm outputs a re-encryption key $\mathrm{Re}KeyGen(sk_i, t, pk_j) \rightarrow rk_{i \rightarrow j,t}$.

4) Enc₂: On input user public key pk_i, message $m \in M$ and the type value t, this algorithm outputs a second level ciphertext (which can be re-encrypted) $Enc_2(pk_i, m, t) \rightarrow C_i$.

5) Enc₁: On input user public key pk_i, message $m \in M$, this algorithm outputs a first level cipher text $Enc_1(pk_i, m) \rightarrow C_i'$.

6) ReEnc: On input a second level cipher text C_i with the type value t and the re-encryption key $rk_{i \rightarrow j,t}$ from U_i to U_j, this algorithm outputs a first level ciphertext $\mathrm{Re}Enc(C_i, rk_{i \rightarrow j,t}) \rightarrow C_j'$.

7) Dec₂: On input a second level cipher text C_i with the type value t and a private key sk_i, this algorithm outputs the message $Dec_2(C_i, sk_i, t) \rightarrow m$ or an error symbol $\perp$.

8) Dec₁: On input a first level ciphertext C_i' and a private key sk_i, this algorithm outputs the message $Dec_1(C_i', sk_i) \rightarrow m$ or an error symbol $\perp$.

For any type value t, any message m and any public/private key pair (pk_i, sk_i), (pk_j, sk_j), the correctness of type-based proxy re-encryption scheme is as follows:

$$Dec_2(Enc_2(pk_i, m, t), sk_i, t) = m,$$

$$Dec_1(Enc_1(pk_i, m), sk_i) = m,$$

$Dec_1(\mathrm{Re}\,Enc(Enc_2(pk_i, m, t), \mathrm{Re}\,KeyGen(sk_i, t, pk_j)), sk_j) = m$.

B. Secutity Model of TBPRE

The difference between the security model of adaptive corruption model and that of non-adaptive corruption model is that challenger can generate the challenge cipher text successfully for the adversary in the former case, even if the adversary is allowed to adaptively corrupt users; but the adversary must commit ahead of time the target user that he wants to attack in the later case.

The security of TBPRE in adaptive corruption model is similar to the security of unidirectional single-hop PRE in Weng [8]. Here we omitted the definition of the security model.

IV. CONCRETE SCHEME

We construct a proxy-invisible TB-PRE scheme that is CCA-secure under adaptive corruption model without random oracle.

A. Construction

1) Setup (λ): Given a secure parameter λ, the setup algorithm choose groups G_1 and G_2 of order $p(>2^{\lambda})$ with the bilinear map $e: G_1 \times G_1 \to G_2$, it picks generators $g, \eta, u, v, w \in_R G_1$, sets $K = e(g,g)$. Choose a collision-resistant hash function $H_0: G_1 \times \{0,1\}^{k_1+k_2} \to Z_p^*$. Choose a pseudorandom function F [15]: $G_2 \times G_1 \to \{0,1\}^{k_1} \square \{0,1\}^{k_2}$, here k_1 and k_2 are secure parameters, $t \in Z_p^*$ is the type value of files. The public parameter is $param = (p, G_1, G_2, g, \eta, u, v, w, K, H_0, F, k_1, k_2)$.

2) KeyGen(λ): User i picks $x_i \in_R Z_p^*$, and sets $sk_i = x_i$ as his pravite key and $pk_i = g^{x_i}$ as his public key.

3) ReKeyGen(sk_i, pk_j, t): On input user i's pravite key $sk_i = x_i$, user j's public key $pk_j = g^{x_j}$ and the type value t, this algrithm generates the re-encryption key $rk_{i\to j,t} = pk_j^{1/(x_i - t)} = g^{x_j/(x_i - t)}$.

4) Enc2(pk_i, m, t): Given a message $m \in \{0,1\}^{k_2}$ with type value t and the public key pk_i, the sender proceeds as follows:

a) Pick $r \in_R Z_p^*$, and compute $A = \eta^r$, and $B = pk_i^r \cdot g^{-rt}$.

b) Compute $Z = K^r = e(g,g)^r$ and set $C = [F(Z,A)]_{k_1} \square ([F(Z,A)]^{k_2} \oplus m)$.

c) Pick $s \in_R Z_p^*$ and compute $h = H_0(A,C)$ and $D = (u^h v^s w)^r$, output the second cipher text $CT_i = (s, A, B, C, D)$.

5) Enc1(pk_j, m): Pick $r \in_R Z_p^*$, and compute $A = \eta^r$ and $B' = e(g, pk_j)^r = e(g,g)^{x_j \cdot r}$. Compute $K = Z^r = e(g,g)^r$ and set $C = [F(Z,A)]_{k_1} \square ([F(Z,A)]^{k_2} \oplus m)$. Pick $s \in_R Z_p^*$, and compute $h = H_0(A,C)$ and $D = (u^h v^s w)^r$, output the first level cipher text $CT_j = (s, A, B', C, D)$.

6) ReEnc($rk_{i\to j,t}, CT_i$): On input a re-encryption key $rk_{i\to j,t}$ and a second level cipher text $CT_i = (s, A, B, C, D)$ under public key pk_i with type value t, compute $h = H_0(A,C)$ and check the validity of the cipher text CT_i by testing whether the following equalitions hold:

$$e(D, \eta) = e(u^h v^s w, A) \quad (1)$$

$$e(B, \eta) = e(pk_i \cdot g^{-t}, A) \quad (2)$$

If not, output $\perp$. Otherwise, compute $B' = e(B, rk_{i\to j,t}) = e(g^{r(x_i - t)}, g^{x_j/(x_i - t)}) = e(g,g)^{x_j \cdot r}$, then output the first level cipher text under public key pk_j as $CT_j = (s, A, B', C, D)$.

7) Dec2: Given a second level cipher text $CT_i = (s, A, B, C, D)$ with type value t, user i proceed as following with his private key as another input: First checks the validity of CT_i as in eq.(1)(2). If the verification fails, out $\perp$. Compute $Z = e(B,g)^{1/(x_i - t)}$, if $[F(Z,A)]_{k_1} = [C]_{k_1}$ holds, output $m = [F(Z,A)]^{k_2} \oplus [C]^{k_2}$; else output $\perp$.

8) Dec1: To decrypt a first level cipher text $CT_j = (s, A, B', C, D)$ under public key pk_j, user j with private key sk_j proceeds as following: First checks the validity of CT_j as in eq.(1). If the verification fails, out $\perp$; otherwise, compute $Z = (B')^{1/x_j}$, if $[F(Z,A)]_{k_1} = [C]_{k_1}$ holds, output $m = [F(Z,A)]^{k_2} \oplus [C]^{k_2}$, else output $\perp$.

B. Analysis of Security and Efficiency

1) The security of our scheme is as followings:

Theorem 1

Under the assumptions of that the hash function H_0 is collision resistant and F is a pseudorandom function family [15], our scheme is chosen-cipher text attack secure at second level cipher text while the 3-QDBDH assumption holds in groups (G_1, G_2). The proof of theorem 1 is similar to that of theorem 1 in Weng [8], we omit it here.

Theorem 2

Our scheme is IND-TBPRE-CCA secure at the first level cipher text, assuming the hash function H is collision resistant, F is a pseudorandom function family and the 3-QDBDH assumption holds in groups (G_1, G_2). The proof of theorem 2 is similar to that of theorem 2 in Weng [8], we omit it here.

Lemma 1

If there is an adversary A who can break the MSS-PRE security [8] of a single-hop unidirectional PRE scheme, then there also exists an adversary B who can

break the IND-1PRE-CCA security of the same PRE scheme.

Obviously, our scheme is IND-1PRE-CCA secure as the illustration about the first level cipher text in theorem 2, our scheme is master key secure, which is vital to a PRE scheme. And the proof of lemma 1 is forthright, here omitted that.

Our scheme is proxy-invisible, because the form of the cipher text from the Enc_1 is same as the form of the re-encrypted cipher text. Furthermore, our scheme satisfies the property of non-transitive (Non-transitive property: the proxy alone cannot generate $rk_{i\to j,t}$ from $rk_{i\to k,t}$ *and* $rk_{k\to j,t}$).

2) Compare

We compare our scheme to the scheme in J.D.P [13] in table I. We first give the explanation of the notations in table I. $|Z_p|, |G_1|, |G_2|$ denotes the length of an element in Z_p, G_1, G_2 respectively, $l = k_1 + k_2$ is the length of the output of the pseudorandom function F. Here t_{me}, t_e, t_p, t_s, t_v present the computation time of a multi-exponentiation, an exponentiation, a bilinear pairing, one signing and one verifying a one-time signature, respectively.

TABLE I.

		Our Scheme	**J.D.P[13] scheme**
cipher text(CT) length	2-level CT	$\|Z_p\|+3\|G_1\|+l$	$2\|G_1\|+\|G_2\|+\|Z_p\|$
	1- level CT	$\|Z_p\|+2\|G_1\|+\|G_2\|+l$	$4\|G_1\|+\|G_2\|$
computational cost	Enc_2	$t_{me}+3t_e$	$t_{me}+3t_e+t_s$
	Enc_1	$t_{me}+3t_e$	$t_{me}+4t_e+t_s$
	ReEnc	$3t_p+2t_{me}$	$t_{me}+3t_e+2t_p+t_v$
	Dec_2	$3t_p+2t_{me}+t_e$	$t_{me}+t_e+3t_p+t_v$
	Dec_1	$2t_p+2t_{me}+t_e$	$t_{me}+t_e+4t_p+t_v$
Standard model?		yes	yes
Security		CCA	RCCA
Corruptive Model		Adaptive	Non-Adaptive

V. CONCLUSION

In this paper, we construct a proxy-invisible TBPRE scheme, that is CCA-secure in adaptive corruption model, and give the compare to the scheme in J.D.P [13] in table I. Our scheme has advantages in both efficiency and security.

ACKNOWLEDGMENT

This work is supported by following projects: Innovation Fund of Postgraduate of XiHua University under the contract number 201315; National Key Technology R&D Program of the Ministry of Science and Technology, the number is 2011BAH26B00; Project of International Cooperation of Sichuan Province, the number of the project is 2009HH0009; Sichuan Province Key Discipline Construction Project, the number of the project is SZD0802-09-1; Sichuan Province Information Security Innovation Team Building Project, the number of the project is 13TD0005.

REFERENCES

[1] M. Blaze, G. Bleumer and M. Strauss. Divertible protocols and atomic proxy cryptography. In EUROCRYPT 1998, LNCS 1403, PP.127—144, 1998.

[2] M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In PKC 1999, LNCS 1560, PP.1 12-121,1999.

[3] L. Zhou, M. A. Marsh, EB. Schneider and A. Redz. Distributed blinding for distributed elgamal re-encryption. In Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS 2005) Volume 00, PP.824-834,2005.

[4] A.Ivan and Y. Dodis. Proxy cryptography revisited. In Internet Society(ISOC)：NDSS 2003, 2003.

[5] R. Canetti and S. Hohenberger. Chosen-ciphertext secure proxy re-encryption. In ACM CCS 2007. Full version: Cryptology ePrint Archieve: Report 2007／17 1.

[6] M. Green and G. Ateniese. Identity based proxy re-encryption. In ACNS 2007, LNCS 452 1, PP.288 306, 2007. Full version: Cryptology ePrint Archieve: Report 2006／473.

[7] R. Canetti, S. Halevi and J. Katz. Chosen-ciphertext security from identity-based encryption. In EUROCRYPT 2004, LNCS 3027, PP.207-222, 2004.

[8] J. Weng, M. R. Chen, Y. J. Yang, et al. CCA-secure unidirectional proxy re-encryption in the adaptive corruption model without random oracles. Science China Information Sciences 53.3 (2010): 593-606.

[9] Q. Tang. Type-based proxy re-encryption and its construction. INDOCRYPT 2008.LNCS, vol.5365.Springer, Heidelberg, 2008.130-144.

[10] J. Weng, R. Deng, C. Chu, X. Ding, J. Lai. Conditional proxy re-encryption secure against chosen-ciphertext attack, in: Proc. of the 4th International Symposium on ACM Symposium on Information, Computer and Communications Security, ASIACCS 2009, 2009, pp. 322-332.

[11] J. Weng, S.S. Chow, Y. Yang and R.H. Deng. Efficient unidirectional proxy re-encryption. Cryptology ePrint Archive, Report 2009/189 (2009),http://eprint.iacr.org/.

[12] J. Shao and G.Y. Wei. Identity-based Conditional Proxy Re-encryption. IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings.

[13] Jae.W.S, Dea. H. Y and Pil. J. L . Proxy-invisible CCA-secure type-based proxy re-encryption without random oracles. Theoretial Computer Science. Volume 491, 17 June 2013, Page 83-93.

[14] Libert B, Vergnaud D. Unidirectional chosen-ciphertext secure proxy re-encryption. In Cramer R, ed. Public Key Cryptography.Lecture Notes in Computer Science, Vol 4939. Berlin: Springer-Verlag, 2008, 360-379.

[15] Goldreich O, Goldwasser S,Micali S. How to construct random functions. J. ACM, 1986, 33(4): 792-807.