Revisit of Group-based Unidirectional Proxy Re-encryption Scheme

Chunbo Ma and Jun Ao

School of Information and Communication,

Guilin University of Electronic and Technology, Guilin, Guangxi, 541004, P. R. China

machunbo@guet.edu.cn

Abstract. Currently, researchers have focused their attention on proxy re-encryption scheme deployed between two entities. Lots of bidirectional schemes have been proposed and this kind of scheme is suitable for the scenario in which the two entities have already established a relationship of trust. How to construct a unidirectional scheme is an open problem and receiving increasing attention. In this paper, we present a unidirectional proxy re-encryption scheme for group communication. In this scheme, a proxy is only allowed to convert ciphertext for Alice into ciphertext for Bob without revealing any information on plaintext or private key. It is suitable for the environment in which no mutual relationship exists and transitivity is not permitted. We prove the scheme secure against chosen ciphertext attack in standard model.

Keywords Unidirectional, Group-based, Proxy, Re-encryption, Standard model

1 Introduction

Mambo and Okamoto introduced the technique for delegating decryption right in [1]. Later, Blaze, Bleumer and Strauss [3] first present the concept of proxy re-encryption scheme, which allows a proxy to transform a ciphertext under Alice's public key into a ciphertext of the same message under Bob's private key. However, the proxy can't obtain anything about the plaintext or the private key used to decrypt the ciphertext.

From a functional point of view, proxy re-encryption schemes are divided into two categories: bidirectional and unidirectional. [2]. In a bidirectional scheme, the proxy secret key can be used to divert ciphertexts from Alice to Bob and vice versa. Obviously, a mutual trust relationship between Alice and Bob is needed, otherwise, some security problem will arise [4]. For example, one of the crucial issues in bidirectional scheme is how to deal with transitivity, i.e. proxy alone has ability to create delegation rights between two entities that have never agreed on this. In a unidirectional scheme, the proxy secret key is allowed to be used to divert ciphertexts from Alice to Bob, whereas from Bob to Alice is not permitted. Currently, how to construct an efficient unidirectional proxy re-encryption scheme has been an open and interesting problem.

The proxy re-encryption scheme has many applications. For example, in traditional storage system [12][13], the Server who housing information sometimes just semi-trusted and some added means should be used to ensure its security. In 2005, Ateniese et al. [4] designed an efficient and secure distributed storage system in which the proxy re-encryption scheme is employed. There are some other applications, such as secure email forwarding, and so on [3][6].

To date, most of the researches of proxy re-encryption emphasize two entities communication. For example, a proxy transforms a ciphertext computed under Alice's public key into one that can be opened by Bob's secret key. However, few literatures present approach to deal with proxy re-encryption for group communication. Group communication is a useful primitive for sharing message in a specifically group and has been widely used in unbalanced networks, for example, clusters of mobile devices [17]. Ma et al. [5] designed an encryption scheme to ensure the privacy of the messages shared in the group. In the scheme, anyone can encrypt a message and distribute it to a designated group and any member in the designated group can decrypt the ciphertext. There exists proxy re-encrypted problem in two different groups. For example, due to the change of duty, some work managed by group A has been assigned to group B such that some encrypted documents sent to group A should be decrypted by group B. In such scenario, proxy re-encryption technique can be used to realize this transformation.

Literature [18] proposed a group-based proxy re-encryption scheme, however it is bidirectional, i.e. the proxy using one secret key can divert ciphertext from group A to group B and vice versa. In this paper, as a natural extension of [18] we present a group-based unidirectional scheme which secure against chosen ciphertext attack in standard model. It is suitable for the scenario in which no mutual relationship exists and transitivity is not permitted.

The rest of paper consists of following sections. In section 2, we introduce some related works. In section 3, we give the security model and complexity assumptions. The proposed scheme is presented in section 4. In section 5, we discuss the security

of the proposed scheme in standard model. Finally, we draw the conclusions in section 6.

2 Related Works

The notion of "atomic proxy cryptography" was presented by Blaze et al. [3] in 1998. It provides securer and more efficient way than usual to deal with the scenario in which a proxy decrypts a ciphertext using Alice's private key and then encrypts the result using Bob's public key. They depict two examples: one for encryption, and another for signature. However, the two examples presented in this paper were proved to have low security guarantees. Their approach is only useful when the trust relationship between Alice and Bob is mutual and the transitivity is not harmful to the system. In addition, it is not suitable for group communication since the proxy has to preserve n re-encryption key for n group members.

In 2003, Ivan and Dodis [2] designed proxy encryption for ElGamal, RSA, and an IBE scheme using secret sharing technique. In their ElGamal based scheme, Public Key Generator (PKG) generates encrypt key EK and decrypt key DK for each user, and then DK is divided into two parts x_1 and x_2, which satisfy DK= $x_1 + x_2$. Moreover, they designed unidirectional and bidirectional proxy encryption scheme. These "secret-sharing" schemes don't change ciphertexts for Alice into ciphertext for Bob in the purest sense, the delegate decryption by requiring Bob to store additional secret that maybe difficult for him to manage.

Following the work of Ivan and Dodis, Ateniese et al. [4] presented an improved proxy re-encryption scheme, and employed it in distributed storage system. In their re-encryption scheme, the proxy only preserves a discrete value to prevent the collude attack. The advantage of the method presented in [2] is that it is feasible to design a unidirectional proxy encryption. Whereas it is very difficult to extend the scheme to group communication since overload stems from the secret sharing technology. Thus why the scheme proposed in [4] is not very practical.

Canetti and Hohenberger [6] proposed a bidirectional proxy re-encryption scheme secure against chosen ciphertext attack in standard model. In their paper the bilinear pairing technology is used to design proxy re-encryption scheme. Although their approach is just suitable for two entities, some method can be used to design group communication.

Libert and Vergnaud [19] proposed a proxy re-encryption scheme which comes from Canetti-Halevi-Katz's [20] scheme and can be seen as a natural extension of the Canetti-Hohenberger definition to the unidirectional case. Their scheme is unidirectional, i.e. only allows the proxy to divert ciphertexts form Alice to Bob. However, some messages on Alice such as public key have been preserved in the ciphertext generated in the phase of ReEnc. An attacker maybe uses these messages to recognize the original recipient of the ciphertext. Furthermore, the scheme may be menaced by malleability.

There are some other re-encryption schemes, such as Jakobsson's quorum controlled asymmetric proxy re-encryption [7], and the identity-based scheme presented by Green and Ateniese [8]. There are some investigations on proxy signature schemes [9][10].

3 Background

3.1 Preliminaries

Let G_1 be a cyclic multiplicative group generated by g, whose order is a prime q and G_2 be a cyclic multiplicative group of the same order q. Assume that the discrete logarithm in both G_1 and G_2 is intractable. A bilinear pairing is a map $e: G_1 \times G_1 \to G_2$ and satisfies the following properties:

1. Bilinear: $e(g^a, p^b) = e(g, p)^{ab}$. For all g, $p \in G_1$ and $a, b \in \mathbb{Z}_q^*$, the equation holds.
2. Non-degenerate: There exists $p \in G_1$, if $e(g, p) = 1$, then $g = O$.
3. Computable: For g, $p \in G_1$, there is an efficient algorithm to compute $e(g, p)$.

Typically, the map e will be derived from either the Weil or Tate pairing on an elliptic curve over a finite field. Pairings and other parameters should be selected in proactive for efficiency and security [11].

3.2 Complexity Assumptions

— **Computational Diffie-Hellman Assumption**

Given g^a and g^b for some $a, b \in \mathbb{Z}_q^*$, compute $g^{ab} \in G_1$. A (τ, ε)-CDH attacker in G_1 is a probabilistic machine Ω running in time τ such that

$$Succ_{G_1}^{cdh}(\Omega) = \Pr[\Omega(g, g^a, g^b) = g^{ab}] \geq \varepsilon$$

where the probability is taken over the random values a and b. The CDH problem is (τ, ε)-intractable if there is no (τ, ε)-attacker in G_1. The CDH assumption states that it is the case for all polynomial τ and any non-negligible ε.

— **Decisional Bilinear Diffie-Hellman Assumption [14]**

We say that an algorithm π that outputs $b \in \{0,1\}$ has advantage ε in solving the **Decisional Bilinear Diffie-Hellman** (**DBDH**) problem in G_1 if

$|\Pr[\pi(g, g^a, g^b, g^c, e(g,g)^{abc}) = 0] - \Pr[\pi(g, g^a, g^b, g^c, T) = 0]| \geq \varepsilon$

where the probability is over the random bit of π, the random choice of $a, b, c \in \mathbb{Z}_q^*$, and the random choice of $T \in \mathrm{G}_2$. The **DBDH** problem is intractable if there is no attacker in G_1 can solve the **DBDH** with non-negligible ε.

— **V-Decisional Diffie-Hellman Assumption**

An algorithm π that outputs $b \in \{0,1\}$ has advantage ε in solving the **V-Decisional Diffie-Hellman** (**V-DDH**) problem in G_1 if

$|\Pr[\pi(g, g^a, g^{ab}, g^{ac}, g^{bc}) = 0] - \Pr[\pi(g, g^a, g^{ab}, g^{ac}, T) = 0]| \geq \varepsilon$

where the probability is over the random bit of π, the random choice of $a, b, c \in \mathbb{Z}_q^*$, and the random choice of $T \in G_1$. The **V-DDH** problem is intractable if there is no attacker in G_1 can solve the **V-DDH** with non-negligible ε.

3.3 Security Notions

The proposed unidirectional re-encryption scheme consists of five algorithms, namely **KeyGen**, **ReKeyGen**, **Enc**, **ReEnc** and **Dec**.

— **KeyGen** (1^λ). On input the security parameter, outputs the public key P_{pub} of each group and the corresponding private key s_{ki} for each member.

— **ReKeyGen** (s_{k1}, s_{k2})**.** On input two private key s_{k1} and s_{k2}, outputs a unidirectional re-encryption key $r_{k(1\to 2)}$.

— **Enc** (P_{pub}, m)**.** On input message $m \in \{0,1\}^*$ and a public key P_{pub}, outputs a ciphertext C.

— **ReEnc** $(r_{k(1\to 2)}, C_1)$**.** On input ciphertext C_1 and the re-encryption key $r_{k(1\to 2)}$, outputs a ciphertext C_2 or an error symbol $\perp$.

— **Dec** (s_k, C)**.** On input ciphertext C and a private key s_k, outputs the corresponding message m.

The indistinguishable chosen ciphertext attack (IND-CCA) [15] presented by Goldwasser and Micali has been widely used to analyze the security of an encryption scheme. In this model, several queries are available to the attacker to model his capability. Subsequently, Rackhoff and Simon [16] enhanced it and proposed adaptively chosen ciphertext attack (IND-CCA2). Since this notion is stronger, it is becoming a prevalent model in analyzing encryption scheme. Green and Ateniese [8] enhanced the model and used it to discuss the security of proxy re-encryption scheme, then followed by Canetti and Hohenberger [6].

In this part, we define adaptively chosen ciphertext security of the group-based unidirectional proxy re-encryption scheme. Compared to the model mentioned in [6], we don't consider the case of group A or B's corruption due to the properties of our key generation. Security is defined using the following game between an Attacker and Challenger.

1. **Setup.** The Challenger initializes the system and gives the Attacker the resulting system parameters and the public key P_{pub}. It keeps private key to itself.
2. **Query phase 1.**
   - **Decrypt queries.** The Attacker issues a query (c_{i1}, c_{i2}, c_{i3}). The Challenger outputs **Decrypt** (c_{i1}, c_{i2}, c_{i3}), otherwise outputs error symbol $\perp$.
   - **Re-encrypt queries**. The Attacker issues a query (c_{i1}, c_{i2}, c_{i3}) encrypted using the public key of group A. The Challenger outputs **Re-encrypt** $(r_{k(\mathrm{A}\to\mathrm{B})}, c_{i1}, c_{i2}, c_{i3})$. Obviously, the output is a ciphertext encrypted using the public key of group B.

   The Attacker is allowed to perform the **Query phase 1** several times.
3. **Challenge.** Once the Attacker decides that **Query phase 1** is over, the Attacker outputs two equal length messages $\{M_0, M_1\}$ to the Challenger. Upon receiving the messages, the Challenger chooses a random bit $e \in \{0,1\}$, invokes **Encrypt** (P_{A}, M_e) and outputs (c_1^*, c_2^*, c_3^*) as the answer.
4. **Query phase 2.** The Attacker continues to adaptively issue **Decrypt** queries and **Re-encrypt** queries. The Challenger responds as in the phase 1. These queries may be asked adaptively as in **Query phase 1**, but the query on (c_1^*, c_2^*, c_3^*) is not permitted.
5. **Guess.** Finally, the Attacker outputs a guess $e' \in \{0,1\}$ for e and wins the game if $e' = e$.

The encryption scheme is secure against chosen ciphertext attack, if the Attacker has a negligible advantage $\varepsilon = \left|\Pr(e = e') - \frac{1}{2}\right|$ to win the game.

4 The proposed unidirectional proxy re-encryption scheme

We assume that there exist two groups in our scheme, namely A and B. The function of the Proxy is to transform ciphertext corresponding to the public key of group A into ciphertext for the public key of group B without revealing any information about

the secret decryption keys or the clear text. It means that our proxy re-encryption is a unidirectional scheme. The proposed scheme consists of following steps.

4.1 Initialize

Let G_1 be a cyclic multiplicative group generated by g, whose order is a prime q and G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map: $e: G_2 \times G_1 \to G_2$ that can be efficiently computed. PKG chooses $a, b \in \mathbb{Z}_q^*$ and $h \in G_1$ uniformly at random, and then computes $g_1 = g^a$ and $g_2 = g^b$. The master private keys are a and b, and the master public keys are g_1, g_2 and h.

4.2 Key Generation

PKG chooses $l, t \in \mathbb{Z}_q^*$ uniformly at random as the tag of the group B. Using $P_B = g^l$ as group B's public key. The private key of the member $p_i \in B$ can be generated as follows:

1. PKG chooses $r_i \in \mathbb{Z}_q^*$ uniformly at random.
2. compute and output $d_{i1} = h^{l \cdot r_i} g^{r_i}$, $d_{i2} = h^{(r_i - a \cdot t) \cdot b^{-1}} g^{r_i b^{-1}}$, and $d_{i3} = g^{a \cdot t} h^{l \cdot r_i}$.

The member p_i's private key is $d_i = \{d_{i1}, d_{i2}, d_{i3}\}$. This set of keys is used to decrypt re-encrypted ciphertext. In case p_i is demanded to directly decrypt a ciphertext that sends to him without converted by the proxy, PKG should generate following set of private keys for him to complete this mission.

$$d_{i1}^{'} = h^{t \cdot r_i} g^{r_i} \qquad d_{i2}^{'} = h^{(r_i - a \cdot l) \cdot b^{-1}} g^{r_i b^{-1}} \qquad d_{i3}^{'} = g^{a \cdot l} h^{t \cdot r_i}$$

We have $d_i^{'} = \{d_{i1}^{'}, d_{i2}^{'}, d_{i3}^{'}\}$. Similarly, PKG chooses $k, z \in \mathbb{Z}_q^*$ uniformly at random as the tag of the group A. Using $P_A = g^k$ as group A's public key. The member's private key can be generated as $p_i \in B$.

4.3 Encrypt

In order to encrypt a message $M \in \{0,1\}^l$ for the group A, the sender (S_{Enc}) first chooses $s \in \mathbb{Z}_q^*$ uniformly at random, and computes the ciphertext

$$c_1 = e(g_1, P_A)^s \cdot M \qquad c_2 = (hg)^s \qquad c_3 = g_2^s.$$

The ciphertext for message M is $c = (c_1, c_2, c_3)$. The sender S_{Enc} sends the ciphertext to all the members in the group A by broadcast over Internet.

4.4 Re-encrypt

In order to transform the ciphertext to group B whose public key is $P_B = g^l$, PKG picks a random number $n_1 \in \mathbb{Z}_q^*$ and computes n_2, such that $n_1 + n_2 = t$. Thereafter, PKG generates three Re-encrypt keys

$$rk_{A \to B}^1 = g^{(n_1 - k)ab^{-1}} \qquad rk_{A \to B}^2 = g^{n_2 a} \qquad rk_{A \to B}^3 = h^{b^{-1} a n_2}$$

and sends these keys to proxy in a secure way. Then using the Re-encrypt keys, the proxy performs the following computing

$$\begin{aligned}
\tilde{c}_1 &= \frac{e(g^a, g^k)^s \cdot M \cdot e(c_3, rk_{A \to B}^1) e(c_2, rk_{A \to B}^2)}{e(c_3, rk_{A \to B}^3)} \\
&= \frac{e(g,g)^{aks} \cdot M \cdot e(g^{bs}, g^{(n_1 - k)ab^{-1}}) \cdot e(h^s g^s, g^{an_2})}{e(g^{bs}, h^{ab^{-1} n_2})} \\
&= \frac{e(g,g)^{ask} \cdot M \cdot e(g,g)^{a(n_1 - k)s} \cdot e(h^s, g^{an_2}) e(g^s, g^{an_2})}{e(g,h)^{asn_2}} \\
&= e(g,g)^{ask} \cdot M \cdot e(g,g)^{a(n_1 - k)s} \cdot e(g,g)^{asn_2} \\
&= e(g,g)^{ask} \cdot M \cdot e(g,g)^{a(t-k)s} \\
&= e(g,g)^{ats} \cdot M \\
\tilde{c}_2 &= (h \cdot g)^s \\
\tilde{c}_3 &= g_2^s = g^{bs}
\end{aligned}$$

The proxy sends the Re-encrypted ciphertext $(\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$ to group B.

4.5 Decrypt

After receiving the re-encrypted message $c = (\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$, the member $p_i \in B$ decrypts the ciphertext as follows:

1. compute $T = e(\tilde{c}_2, d_{i3}) e(\tilde{c}_3, d_{i2}) / e(\tilde{c}_2, d_{i1})$.
2. compute $M = \tilde{c}_1 / T$.

In fact any member $p_i \in B$ can compute T correctly, since

$$T = \frac{e(\tilde{c}_2, d_{i3})e(\tilde{c}_3, d_{i2})}{e(\tilde{c}_2, d_{i1})}$$

$$= \frac{e(g^s h^s, h^{l\cdot r_i} g^{a\cdot t})e(g_2^s, h^{-ab^{-1}t} h^{r_i b^{-1}} g^{r_i b^{-1}})}{e(g^s h^s, g^{r_i} h^{l\cdot r_i})}$$

$$= \frac{e(h^s, h^{l\cdot r_i})e(h^s, g^{a\cdot t})e(g^s, h^{l\cdot r_i})e(g^s, g^{a\cdot t})}{e(h^s, h^{l\cdot r_i})e(h^s, g^{r_i})} \frac{e(g_2^s, h^{-ab^{-1}t})e(g_2^s, h^{r_i b^{-1}})e(g_2^s, g^{r_i b^{-1}})}{e(g^s, h^{l\cdot r_i})e(g^s, g^{r_i})}$$

$$= e(g^s, g^{at}) = e(g, g)^{ats}$$

So the member p_i can obtain the plaintext $M = \tilde{c}_1 / T$.

In case $p_i \in \mathrm{B}$ is demanded to directly decrypt a ciphertext that sender send to him, he should use private keys $\{d_{i1}^{'}, d_{i2}^{'}, d_{i3}^{'}\}$ to decrypt it as we have mentioned in section 4.2. To the ciphertext generated for group B, for example $c_1^{'} = e(g_1, P_{\mathrm{B}})^s \cdot M$, $c_2^{'} = (hg)^s$ and $c_3^{'} = g_2^s$, the users p_i decrypts the ciphertext as follows.

$$T^{'} = \frac{e(c_2^{'}, d_{i3}^{'})e(c_3^{'}, d_{i2}^{'})}{e(c_2^{'}, d_{i1}^{'})} = e(g, g)^{als}$$

Then we have $M = c_1^{'} / T^{'}$.

Note that the proxy with the re-encrypt keys ($rk_{A\to B}^1, rk_{A\to B}^2, rk_{A\to B}^3$) can only convert ciphertext for group A into ciphertext for B as we have described above. In other words, the proxy can transform $e(g^a, g^k)^s \cdot M$ into $e(g^a, g^t)^s \cdot M$ that can be decrypted by group B. Obviously, it is impossible to transform $e(g^a, g^l)^s \cdot M$ into $e(g^a, g^k)^s \cdot M$ with the re-encrypt keys ($rk_{A\to B}^1, rk_{A\to B}^2, rk_{A\to B}^3$). Therefore, we say this scheme is a unidirectional scheme.

5 Security

In this section, we will discuss the security of the proposed unidirectional proxy re-encryption scheme in standard model. The measure used to prove our scheme comes from the paper [6].

Lemma. Suppose the **CDH** assumption holds. Then given $g^a, g^{ab}, g^{ac} \in \mathrm{G}_1$, computing g^{bc} is intractable.

Proof. Assume that given $g^a, g^{ab}, g^{ac} \in \mathrm{G}_1$, the attack Alice has ability to compute another g^{bc}. Then we can design an algorithm to solve CDH problem. In other words, given $g^m, g^n \in \mathrm{G}_1$, the challenger Bob can compute $g^{m\cdot n}$ by running Alice as a subroutine.

To the given $g^m, g^n \in \mathrm{G}_1$, Bob chooses a random number $t \in \mathbb{Z}_q^*$, computes g^{mt} and g^{nt}, and then sends g^t, g^{mt} and g^{nt} to Alice. With the assumption, Alice can output $g^{m\cdot n}$, then Bob can solve CDH problem.

□

Theorem. Suppose that the **V-DDH** is intractable. Then our proxy re-encryption scheme is secure against adaptively chosen ciphertext attack.

Proof. Assume that if the attacker Alice has ability to break the proposed encryption scheme via chosen ciphertext attack with non-negligible probability ε, then we can prove that there exists challenger Bob that can solve **V-DDH** problems with the same probability. In other words, given $g^{a^*}, g^{a^* s^*}, g^{a^* k^*} \in \mathrm{G}_1$ and $T \in \mathrm{G}_1$, Bob can decide if T is equal to $g^{s^* k^*}$ with non-negligible probability by running Alice as a subroutine. The challenger Bob interacts with Alice by simulating **Decrypt**, **Re-encrypt** oracles.

Bob initializes the system, chooses random numbers $w, v \in \mathbb{Z}_q^*$. Let

$g_1 = g^{a^*}$ $\quad g_2 = g^{a^* \cdot k^* \cdot w}$ $\quad P_{\mathrm{A}} = g^{a^* k^*}$ $\quad h = g^{a^* \cdot k^* \cdot v - 1}$.

Then Bob chooses a random number $\alpha, \beta \in \mathbb{Z}_q^*$ and publishes $P_{\mathrm{A}} = g^{a^* k^*}$ and $P_{\mathrm{B}} = g^{a^* k^* \alpha}$.

Query phase 1.

- **Decrypt queries**. To every new query (c_1, c_2, c_3), Bob computes and outputs $M = c_1 / e(g_1, c_3^{1/w})$ as the answer.
- **Re-encrypt queries**. To every new query (c_1, c_2, c_3), Bob computes

$$\tilde{c}_1 = e(g_1, P_{\mathrm{A}})^s \cdot M \cdot e(c_3^{1/w}, g^{a^* \beta - a^*})$$
$$= e(g, g)^{(a^*)^2 k^* s + s(a^*)^2 k^* (\beta - 1)} \cdot M$$
$$= e(g, g)^{(a^*)^2 k^* s \beta} \cdot M$$

and sets $\tilde{c}_2 = c_2$ and $\tilde{c}_3 = c_3$, and then outputs $(\tilde{c}_1, \tilde{c}_2, \tilde{c}_3)$ as the answer.

Since $w, \alpha, \beta \in \mathbb{Z}_q^*$ are two random number, Alice can't distinguish the simulated answers from the actual results. Thereby, we say above simulation is perfect. Alice is allowed to perform **Decrypt** and **Re-encrypt** queries several times.

Challenge phase. When Alice decides Query phase 1 is over, she chooses two equal length messages M_1, M_0, and sends them to

Bob. Bob chooses a random bit $e \in \{0,1\}$, computes and outputs

$c_1^* = e(g_1, T) \cdot M_e = e(g^{a^*}, g^{a^* \cdot k^*})^{s^*/a^*} \cdot M_e$

$c_2^* = (T)^v = (g^{k^* s^*})^v = (g \cdot g^{a^* \cdot k^* \cdot v - 1})^{s^*/a^*}$

$c_3^* = (T)^w = (g^{k^* s^*})^w = (g^{a^* k^* w})^{s^*/a^*}$

as the answer. The **Challenge phase** can be performed only once.

Query phase 2. Alice continues to adaptively issue **Decrypt** and **Re-encrypt** queries. Bob responds as in the phase 1. However, the query on (c_1^*, c_2^*, c_3^*) is not permitted.

Guess. Finally, Alice outputs a guess $e' \in \{0,1\}$ for e. If $e' = e$, then Bob decides $T = g^{s^* k^*}$, otherwise Bob decides $T \neq g^{s^* k^*}$.

Obviously, above simulation is perfect. We say that Alice can break the proxy re-encryption scheme with non-negligible probability ε. It means that Alice can output correct e' with probability ε. Then Bob can solve the **V-DDH** with same probability ε by running Alice as a subroutine.

□

6 Conclusions

Many proxy re-encryption schemes have been presented in recent few years. However, unidirectional scheme is still an open problem which is attracting much attention. In this paper, we present a unidirectional proxy re-encryption scheme used for group communications. In our scheme, the proxy only has ability to divert the ciphertext for group A into ciphertext for group B. To the member in group A/B, he can independently decrypt the ciphertext for the group. Obviously, the performance of encryption in our proposed scheme is similarly to that of paper [6], and it is crucial to the group communication since lots of members are involved in. Decryption operation is independently completed by each group member.

References

1. M. Mambo and E. Okamoto. Proxy Cryptosystems: Delegation of the Power to Decrypt Ciphertexts. IEICE Trans. Fund. Electronics Communications and Computer Science, E80-A/1: 54-63, 1997.
2. A. Ivan, Y. Dodis. Proxy cryptography revisited. In Proceedings of the Tenth Network and Distributed System Security Symposium. February, 2003.
3. M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. In EUROCRYPT'98, LNCS 1403: 127-144.
4. G. Ateniese, K. Fu, M. Green, and S. Honhenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In Proceedings of NDSS, 2005, 29-43.
5. C. Ma, Q. Mei, and J. Li. "Broadcast Group-oriented Encryption for Group Communication". Journal of Computational Information Systems 3:1 (2007) 63-71.
6. R. Canetti, S. Hohenberger. Chosen-Ciphertext Secure Proxy Re-Encryption. Available at http://eprint.iacr.org/2007/171
7. M. Jakobsson. On quorum controlled asymmetric proxy re-encryption. In Proceedings of Public Key Cryptography, 1999, 112-121.
8. M. Green, G. Ateniese. Identity-based Proxy Re-encryption. In Proceedings of ACNS 2007, LNCS 4521: 288-306.
9. H. Kim, J. Baek, B. Lee, and K. Kim. Computing with secrets for mobile agent using one-time proxy signature. In Proceedings of SCIS 2001, Vol 2/2: 845-850.
10. P. MacKenzie and M. K. Reiter. Two-party generation of DSA signature. In Advances in Cryptology-CRYPTO2001, LNCS 2139: 137－154
11. D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. Advances in Cryptology -- Asiacrypt'2001, Gold Coast, Australia, Lecture Notes in Computer Science, 2248, Springer-Verlag (2001) 514-532.
12. M. Blaze. A Cryptographic File System for Unix. First ACM Conference on Communications and Computing Security, Fairfax, VA November, 1993.
13. W. Freeman and E. Miller. Design for a decentralized security system for network-attached storage. In Proceedings of the 17th IEEE Symposium on Mass Storage Systems and Technologies, pages 361–373, College Park, MD, March 2000.
14. D.Boneh and X. Boyen. Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles. Advances in Cryptology Eurocrypt 2004. Berlin:Springer-Verlag,2004: 223-238.
15. S. Goldwasser and S. Micali. Probabilistic Encryption. Journal of Computer and System Sciences, 1984, 28: 270-299.
16. C. Rackhoff and D. R. Simon. Non interactive zero-knowledge proof of knowledge and chosen ciphertext attack. In Advanced in Cryptology-CRYPTO'91. Springer-Verlag, 1992: 434-444.
17. T. Phan,., L. Huan, , C. Dulan,: Challenge: integrating mobile wireless devices into the computational grid. In Proceedings of MobiCom

(2002) 271-278.
18. C. Ma, J. Ao, and J. Li. Group-oriented encryption secure against collude attack. http://eprint.iacr.org/2007/371.
19. B. Libert and D. Vergnaud. Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption. In Proceedings of PKC 2008, LNCS 4939, pp. 360-379, 2008.
20. R. Canetti, S. Halevi, J. Katz. Chosen-Ciphertext Security from Identity-Based Encryption. In Proceedings of EUROCRYPTO 2004, LNCS 3027, pp. 207-222, 2004.