一个高效的选择密文安全的分类代理重加密方案

赵 菁[1],冯登国[2],杨 林[1],马琳茹[1]
(1.中国电子系统设备工程公司研究所,北京 100141; 2.信息安全国家重点实验室,北京 100190)

摘 要: 分类代理重加密通过密码学手段为密文委托与分发提供了高效便捷的解决方案,同时使密文拥有者有能力实施更细粒度的委托控制.本文提出了一种新的分类代理重加密方案,方案在随机预言模型下可证明选择密文安全,相对于现有采用双线性对构造的分类代理重加密方案,我们的无双线性对方案拥有更好的效率,并具备主密钥安全性.

关键词: 代理重加密; 分类代理重加密; 选择密文安全
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2011) 11-2513-07

CCA-Secure Type-Based Proxy Re-Encryption Without Pairings

ZHAO Jing[1], FENG Deng-guo[2], YANG Lin[1], MA Lin-ru[1]
(1. *Institute of Electronic System Equipment Engineering Company*, *Beijing* 100141, *China*;
2. *State Key Laboratory of Information Security*, *Beijing* 100190, *China*)

Abstract: Type-based proxy re-encryption is an effective and efficient cryptographic solution to ciphertext delegation and distribution, which also enables the ciphertext owners to carry out fine-grained delegation control. In this paper, we propose a new type-based proxy re-encryption scheme without pairings and prove it against the chosen-ciphertext attack (CCA) in the random oracle model. Compared with the existing type-based proxy re-encryption schemes constructed with pairings, our scheme owns better efficiency as well as the master key security.

Key words: proxy re-encryption; type-based proxy re-encryption; CCA security

1 引言

在信任非集中的分布式网络环境中,数据安全越来越受到资源拥有者的重视,加密作为数据安全的基本保障机制之一,得到了日益普遍的应用,加密数据共享需求随之凸现.这一需求目前主要利用密文数据库等可信服务或用户在线操作来满足,前者需要在密钥管理、明文安全或访问控制方面对服务器赋予完全的信任,后者则要求用户在线对密文进行解密再加密,十分繁琐不便[1].针对这一问题,文献[2]提出了代理重加密(proxy re-encryption)这一密码学概念,在代理重加密方案中,用户 Alice 可以在一个半可信的代理服务器上设置她到共享用户 Bob 的重加密密钥,代理服务器通过重加密密钥将以 Alice 公钥 pk_a 加密的密文重加密成以 Bob 公钥 pk_b 加密的密文,在这一过程中,明文和 Alice 与 Bob 的私钥都不会暴露给代理服务器.这样就通过密码学手段降低了对服务器的信任程度,同时明文与用户秘密得到了安全的保护,密文的委托或重分配的过程也相对便捷.这个过程可以视作 Alice 将自己的密文解密权委托给了 Bob,因此一般称 Alice 为委托方(delegator),Bob 为受理方(delegatee).代理重加密可以有效地解决许多应用领域中的相应问题,如加密电子邮件转发[2]、垃圾邮件过滤[3]、分布式文件系统的安全管理[3~6]、数字版权管理[7]等.

以分布式文件系统的安全管理为例[3],用户 Alice 在不完全可信的服务器上存储了以 pk_a 加密的文件,允许她指定的用户访问,但无法在每次发生数据访问时都在线进行密文转换.采用代理重加密方案,Alice 可以根据自己的私钥及受理方的公钥计算一个重加密密钥,设置于代理服务器上,当受理方访问文件时,服务器用相应的重加密密钥将密文重加密成可由受理方私钥解密的密文,如图 1 所示.代理重加密方案的性质保证了代理服务器无法获得明文,也无法得知委托方与受理方的私钥.这就只需赋予服务器最小程度的信任:只需正确执行重加密算法,允许对明文与用户私钥好奇.

在这样的场景中,Alice 通过代理重加密便捷有效

收稿日期:2010-01-20;修回日期:2011-07-22
基金项目:国家自然科学基金(No.60803129);信息网络安全公安部重点实验室(公安部第三研究所)开放基金(No.C11604);下一代互联网业务试商用及设备产业化专项(No.CNGI-09-03-03)

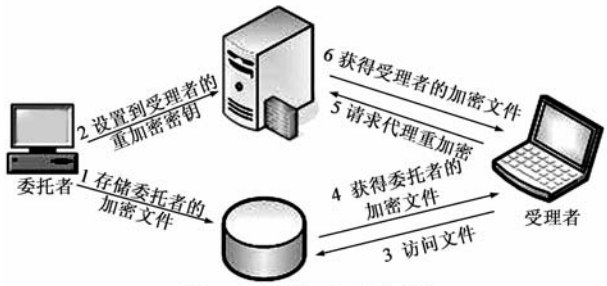

图1 代理重加密应用示例

地实现了对自己的密文文件的访问控制.然而,当 Alice 设置了一个到受理方 Bob 的重加密密钥时,Bob 可以访问 Alice 在该服务器上的所有文件,进一步地,Alice 会希望实现更细粒度的访问控制,比如允许 Bob 只能访问由她指定的一部分密文文件.直观对策是 Alice 采用不同的密钥来加密各类文件,但这需要 Alice 拥有多个密钥对,在实际应用中通常是难以管理或不可行的.依赖于不完全可信的文件服务器来执行细粒度访问控制也是不安全的.在代理重加密中加入分类重加密的属性,Alice 就可以通过对重加密密钥及密文的分类设定,让受理方只能获得 Alice 指定类型的重加密密文,从而实现对密文委托权的分类控制.

在现有分类代理重加密工作中,文献[8]首次提出了基于类型的代理重加密,并分别给出了选择明文安全和选择密文安全的具体构造;文献[9]提出了一个选择密文安全的条件代理重加密方案,尽管命名方式不同,实质上仍是一种分类代理重加密方案.这两种方案都是基于双线性对构造的.此外,文献[10]提出了基于属性的代理重加密,以基于属性的加密方案为基础,使委托方能对密文委托权实现属性粒度的控制,然而基于属性的加密方案要求委托方与受理方的密钥都是基于属性构造的,因此仅适用于存在属性权威的应用域,而文献[8,9]及本文中的方案主要针对使用一般公钥密码系统的应用环境.文献[11]介绍了如何应用文献[8]中的方案实现私人数据的访问控制.文献[4]讨论了基于身份与类型的代理重加密及其应用,其方案构造在基于身份的加密方案基础上.

本文提出了一种新的抗选择密文攻击的分类代理重加密方案,基于 ElGamal 加密系统和 Schnorr 签名方案构造,相对现有基于双线性对构造的分类代理重加密方案[8,9],具有更高的效率,同时具有主密钥安全性.方案的安全性基于可除计算 Diffie-Hellman(DCDH)问题的困难性,在随机预言模型下是可证明选择密文安全的.

2 预备知识

2.1 复杂性假设

我们方案的安全性基于 DCDH 假设,相关定义如下[12]:

定义 1 DCDH 问题

设 G 是以素数 q 为阶的循环乘法群,g 为 G 的生成元,$a, b_R \in Z_q^*$,已知 g^a, g^b,计算 $g^{a/b}$.

定义 2 DCDH 假设

一个概率多项式时间(简称 PPT)算法 A 解决 DCDH 问题的概率为 $\varepsilon > 0, \varepsilon = \Pr[g^{a/b} \leftarrow A(g, g^a, g^b)]$,若 ε 是可忽略的,则称 DCDH 问题是困难的.

2.2 分类代理重加密系统模型

分类代理重加密系统由系统建立、密钥生成、分类重加密密钥生成、加密、分类重加密、解密六个算法组成,形式化描述如下:

系统建立 $Setup(\kappa) \rightarrow params$

系统以 κ 为安全参数生成公开参数 $params$.

密钥生成 $KeyGen(params) \rightarrow (pk, sk)$

系统与用户根据 $params$ 生成用户的公私钥对(pk, sk).

分类重加密密钥生成 $ReKeyGen(sk_i, pk_j, t) \rightarrow rk_{i \xrightarrow{t} j}$

密文委托方 U_i 用私钥 sk_i、受理方 U_j 公钥 pk_j 及 U_i 指定的密文类型 t 生成从 U_i 到 U_j 的分类重加密密钥 $rk_{i \xrightarrow{t} j}$.

加密 $Enc(m, pk_i, t) \rightarrow C_i$

用 U_i 公钥 pk_i 和密文类型 t 加密消息 m,输出密文 C_i.

分类重加密 $ReEnc(rk_{i \xrightarrow{t} j}, C_i) \rightarrow C_j$

代理服务器用 $rk_{i \xrightarrow{t} j}$对类型为 t 的密文 C_i 运行分类重加密算法,输出以受理方 U_j 公钥 pk_j 加密的密文 C_j.

解密 $Dec_1(sk_i, C_i, t) \rightarrow m; Dec_2(sk_i, C_i) \rightarrow m$

用户 U_i 可根据密文类型使用相应的算法来解密用自己公钥加密的密文.

2.3 分类代理重加密安全模型

本方案建立于 *IND-PRE-CCA* 安全模型[8,13]之上,其中攻击者 A 具有问询密钥生成、重加密密钥生成与解密的权力,仅在直接获取解密目标明文的能力时给予限制(详见下文).安全模型描述如下:

(1)游戏建立:挑战者 B 以安全参数 κ 为输入,运行算法 setup 生成公开参数 $params$.

(2)阶段一:A 已知 $params$,可以以任何次序问询以下 Oracle: *KeyGen*, *ReKeyGen*, *ReEnc*, *Dec*. 其中 *KeyGen* 分为 *UKeyGen*(未攻破密钥生成,只返回用户公钥)与 *CKeyGen*(已攻破密钥生成,返回用户的公私钥对), *Dec* 分为 Dec_1 与 Dec_2. 要求当问询 Oracle *ReKeyGen*、*ReEnc* 与 *Dec* 时,问询的输入密钥是经由 *KeyGen* 问询生成的.

(3)挑战:A 结束阶段一,输出等长明文 $m_0, m_1 \in M$、目标密文类型 t^*、目标公钥 pk^*,要求 pk^* 由 *UKey-*

Gen 问询生成,且对于任何 pk_j,若 A 以(pk^*, pk_j, t^*)问询过 *ReKeyGen*,则不能以 pk_j 问询过 *CKeyGen*.若满足上述要求,B 选取随机比特$\delta\in\{0,1\}$,以 $c_\delta = Enc(m_\delta, t^*, pk^*)$为挑战密文返回给 A.

(4)阶段二:A 继续问询阶段一中的 Oracle,约束条件为:

(a)若 A 以(pk^*, pk_j, t^*)问询 *ReKeyGen*,则不能以 pk_j 问询过 *CKeyGen*.

(b)若 A 以(c_δ, t^*, pk^*, pk_j)问询 *ReEnc*,则不能以 pk_j 问询过 *CKeyGen*.

(c)A 不能以(c_δ, t^*, pk^*)问询 Dec_1.

(d)若 A 以(pk^*, pk_j, t^*)问询过 *ReKeyGen*,则不能以(c'_δ, pk_j)问询 Dec_2,其中 c'_δ 是 *ReEnc*(c_δ, t^*, pk^*, pk_j)的一个有效输出.

(5)猜测:A 输出对 δ 的猜测 $\delta'\in\{0,1\}$,攻击游戏结束.

定义 3　一个分类代理重加密方案是(t, q_u, q_c, q_{rk}, q_{re}, q_d, ε) – *IND* – *PRE* – *CCA* 安全的,若对任意 PPT 攻击者,在最多进行 q_u 次 *UKeyGen* 问询、q_c 次 *CKeyGen* 问询、q_{rk}次 *ReKeyGen* 问询、q_{re}次 *ReEnc* 问询、q_d 次 *Dec* 问询后,他在 *IND-PRE-CCA* 安全模型下的猜测优势 $|pr[\delta'=\delta]-1/2|\leqslant\varepsilon$ 是可忽略的.

3　方案构造

本方案基于 ElGamal 加密系统和 Schnorr 签名方案,借鉴了令牌控制的加密模式[14~17]技术来构造无双线性对的分类代理重加密方案.现有方案多基于双线性对构造的原因之一是重加密密钥构造的困难性,委托方既不能暴露私钥又不可获得受理方私钥.令牌模式下,密文可转换成与委托方已知令牌对应的密文形式,而非对应受理方私钥的密文形式,给构造的简洁性与灵活性留出了空间.方案构造如下:

系统建立　假定安全参数为 κ,选取 κ 比特长的素数 q,G 是 Z_q^* 的一个子群,g 是 G 的生成元.选择抗碰撞哈希函数 $H_i(i\in\{1,\cdots,4\})$,其中 $H_1:\{0,1\}^{k_1}\times\{0,1\}^{k_2}\to Z_q^*$,$H_2: G\to\{0,1\}^{k_1+k_2}$,$H_3:\{0,1\}^*\to Z_q^*$,$H_4: G\to Z_q^*$,$k_1$ 与 k_2 据 κ 确定;消息空间 $M=\{0,1\}^{k_1}$;密文类型 $t\in\{0,1\}^*$.系统的公开参数为(q, G, g, k_1, k_2, H_1, H_2, H_3, H_4).

密钥生成　为用户 U_i 生成公私钥对(pk_i, sk_i):

$a_i, b_{iR}\in Z_q^*$, $sk_i=(sk_{i,1}, sk_{i,2})=(a_i, b_i)$, $pk_i=(pk_{i,1}, pk_{i,2})=(g^{a_i}, g^{b_i})$.

分类重加密密钥生成　委托方 U_i 用私钥 $sk_i=(a_i, b_i)$、受理方 U_j 公钥 $pk_j=(pk_{j,1}, pk_{j,2})$、为 U_j 指定的可解密类型值 t,构造重加密密钥 $rk_i\xrightarrow{t}j$:

$\beta_R\in\{0,1\}^{k_1}$, $\gamma_R\in\{0,1\}^{k_2}$,计算:

$\sigma=H_1(\beta,\gamma)$, $\tilde{A}=g^\sigma$, $\tilde{B}=H_2(pk_{j,2}^\sigma)\oplus(\beta\parallel\gamma)$.

$$rk_i\xrightarrow{t}j=(rk_i^{(1)t}\xrightarrow{}j, rk_i^{(2)t}\xrightarrow{}j),$$

$$rk_i^{(1)t}\xrightarrow{}j=\frac{\beta}{(a_iH_4(pk_{i,2})+b_i)\cdot H_3(t\parallel 0)},$$

$$rk_i^{(2)t}\xrightarrow{}j=(\tilde{A},\tilde{B}).$$

加密　以 U_i 公钥($pk_{i,1}$, $pk_{i,2}$)加密类型为 t 的消息 $m\in M$:

$u_R\in Z_q^*$, $w_R\in\{0,1\}^{k_2}$,计算:

$D=(pk_{i,1}^{H_4(pk_{i,2})}pk_{i,2})^u$, $r=H_1(m,w)$,

$A=(pk_{i,1}^{H_4(pk_{i,2})}pk_{i,2})^{r\cdot H_3(t\parallel 0)}$, $B=H_2(g^r)\oplus(m\parallel w)$,

$s=u+r\cdot H_3(t\parallel 0)\cdot H_3(A,B,D)\bmod q$.

消息 m 的密文为:$C_i=(A,B,D,s)$.

分类重加密　重加密过程中,代理服务器拥有类型为 t 的密文 $C_i=(A,B,D,s)$,分类重加密密钥 $rk_i\xrightarrow{t}j$,通过分类重加密算法将用户 U_i 的 t 类密文 C_i 转换成用户 U_j 的无类型密文 C_j,过程如下:

检验$(pk_{i,1}^{H_4(pk_{i,2})}pk_{i,2})^s=D\cdot A^{H_3(A,B,D)}$是否成立,若不成立,输出⊥.若成立,计算 $A'=A^{rk_i^{(1)}\xrightarrow{t}j}$.

则 C_i 的重加密密文为:$C_j=(A',B,\tilde{A},\tilde{B})$.

其中,$A'=A^{rk_i^{(1)}\xrightarrow{t}j}$

$$=((pk_{i,1}^{H_4(pk_{i,2})}pk_{i,2})^{r\cdot H_3(t\parallel 0)})^{\frac{\beta}{(a_iH_4(pk_{i,2})+b_i)\cdot H_3(t\parallel 0)}}$$

$$=((g^{a_iH_4(pk_{i,2})+b_i})^{r\cdot H_3(t\parallel 0)})^{\frac{\beta}{(a_iH_4(pk_{i,2})+b_i)\cdot H_3(t\parallel 0)}}$$

$$=g^{r\cdot\beta}.$$

解密　以 U_i 私钥($sk_{i,1}$, $sk_{i,2}$)解密密文 C_i:

(1)当密文格式为 $C_i=(A,B,D,s)$时,

检验$(pk_{i,1}^{H_4(pk_{i,2})}pk_{i,2})^s=D\cdot A^{H_3(A,B,D)}$是否成立,若不成立,输出⊥.若成立,计算

$$(m\parallel w)=B\oplus H_2(A^{\frac{1}{(a_iH_4(pk_{i,2})+b_i)\cdot H_3(t\parallel 0)}}).$$

检查 $A=(pk_{i,1}^{H_4(pk_{i,2})}pk_{i,2})^{H_1(m,w)\cdot H_3(t\parallel 0)}$是否成立,若不成立,输出⊥.若成立,输出消息 m.

(2)当密文格式为 $C_j=(A',B,\tilde{A},\tilde{B})$时,

计算$(\beta\parallel\gamma)=\tilde{B}\oplus H_2(\tilde{A}^{b_i})$,$(m\parallel w)=B\oplus H_2(A'^{\frac{1}{\beta}})$,

检查 $\tilde{A}=g^{H_1(\beta,\gamma)}$, $A'=g^{H_1(m,w)\cdot\beta}$是否成立,若其一不成立,输出⊥.若两式均成立,输出消息 m.

4　安全性证明

定理 1　假定 DCDH 假设在群 G 上成立,且 Schnorr 签名是 *EUR* – *CMA* 安全的[18],则本方案在随机预言模型下是 *IND-PRE-CCA* 安全的.亦即,若存在一个敌手 A,最多对 $H_i(i\in\{1,\cdots,4\})$分别进行 q_{H_1}、q_{H_2}、$q_{H_{31}}$、$q_{H_{32}}$、

q_{H_4}次随机 oracle 问询,且攻破了本方案的$(t, q_u, q_c, q_{rk}, q_{re}, q_d, \varepsilon)$ – *IND-PRE-CCA* 安全性,则对于任意$0 < v < \varepsilon$:

要么存在算法 B,可以在时间 t'内以优势ε'攻破群 G 上的 DCDH 假设,其中

$$t' \leqslant t + (q_{H_1} + q_{H_2} + q_{H_{31}} + q_{H_{32}} + q_{H_4} + q_u + q_c + q_{rk} + q_{re} + q_d)O(1) + (2q_u + 2q_c + 2q_{rk} + 5q_{re} + 2q_d + (q_{H_1} + q_{H_{32}})q_{re} + (2q_{H_2} + 2q_{H_1} + 2q_{H_{32}})q_d)t_{\exp}$$

$$\varepsilon' \leqslant \frac{1}{q_{H_2}}\left(\frac{\varepsilon - v}{e(1 + q_{rk})} - \frac{q_{H_1}}{2^{k_1 + k_2}} - \frac{q_{H_{31}} \cdot q_{H_{32}} \cdot (q_d + 1)}{2^{2(k_1 + k_2)}} - \frac{q_{re} + (q_{H_{32}} + q_{H_1} + 2) \cdot q_{H_2} \cdot q_d}{q^2} - \frac{2(q_{H_1} + q_{H_{32}}) \cdot q_d}{2^{k_1 + k_2} \cdot q} - \frac{3q_d}{q}\right)$$

其中 $t_{\exp}$为群 G 上一次幂运算的运行时间.

要么存在一个攻击者可以在时间 t'内以优势 v 攻破 Schnorr 签名的 EUR-CMA 安全性.

证明 假设 Schnorr 签名的(t', v) – *EUF-CMA* 安全性中,优势 v 的范围为$0 < v < \varepsilon$.若存在敌手 A 在时间t 内以优势 $\varepsilon - v$ 攻破本方案的 *IND-PRE-CCA* 安全性,则可以构造一个算法 B,当输入为 DCDH 的挑战项$(g, g^{\frac{1}{a}}, g^b)$时,可以在时间 t'内以优势ε'输出g^{ab},攻破 G 上的 DCDH 假设.

以算法 B 为挑战者,与敌手 A 的 *IND-PRE-CCA* 攻击游戏进行如下:

系统建立 B 将系统公开参数$(q, G, g, k_1, k_2, H_1, H_2, H_3, H_4)$发送给 A,其中 B 控制随机 Oracle H_1, H_2, H_3, H_4 并维护初始为空的哈希列表 $H_i^{list}(i \in \{1, \cdots, 4\})$,对 A 的哈希 Oracle 问询响应如下:

对于 $H_1(m, w)$、$H_2(R)$、$H_3^1(A, B, D)$、$H_3^2(t \| 0)$、$H_4(pk)$,若列表 $H_i^{list}(i \in \{1, \cdots, 4\})$中分别存在对应项$(m, w, \alpha)$、$(R, \eta)$、$(A, B, D, \mu)$、$(T, t, \tau)$、$(pk, \pi)$,则分别响应以预定义的输出值 α、η、μ、τ、π,否则分别选取 $\alpha_R \in Z_q^*$、$\eta_R \in \{0,1\}^{k_1 + k_2}$、$\mu_R \in Z_q^*$、$\tau_R \in Z_q^*$、$\pi_R \in Z_q^*$,将对应项加入列表 $H_i^{list}(i \in \{1, \cdots, 4\})$,并响应以该输出值.

阶段 1 A 发起一系列 Oracle 问询. B 维护初始为空的列表 K^{list}和 R^{list},响应如下:

(1)未攻破用户密钥问询. B 选取 $a_i, b_{iR} \in Z_q^*$,采用安全性证明技术[19],掷币 $c_i \in \{0,1\}$,假定 $c_i = 1$ 的概率为 θ. 若 $c_i = 1$, $pk_i = (g^{a_i}, g^{b_i})$,若 $c_i = 0$, $pk_i = ((g^{\frac{1}{a}})^{a_i}, (g^{\frac{1}{a}})^{b_i})$. 将$(pk_i, a_i, b_i, c_i)$加入 K^{list}并响应以 pk_i.

(2)已攻破用户密钥问询. B 选取 $a_i, b_{iR} \in Z_q^*$,令 $c_j = \varphi$, $pk_i = (g^{a_i}, g^{b_i})$,将$(pk_j, a_j, b_j, c_j)$加入 K^{list}并响应以(pk_j, a_j, b_j).

(3)重加密密钥问询. 当 A 以(pk_i, pk_j, T)问询时,执行过程 $P1$:若 R^{list}中存在对应项$(pk_i, pk_j, T, c_j, (rk_i^{(1)t \to j}, \tilde{A}, \tilde{B}), \beta, \pi)$,响应以预定义的值$(rk_i^{(1)t \to j}, \tilde{A}, \tilde{B})$,否则从 K^{list}中恢复出(pk_i, a_i, c_i)、(pk_j, a_j, c_j). 选取 $\beta_R \in \{0,1\}^{k_1}$, $\gamma_R \in \{0,1\}^{k_2}$,计算:$\sigma = H_1(\beta, \gamma)$, $\tilde{A} = g^\sigma$, $\tilde{B} = H_2(pk_{j,2}^\sigma) \oplus (\beta \| \gamma)$. $P1$ 结束.

(a)当 $c_i = 1 \vee c_i = \phi$, $rk_i^{(1)t \to j} = \frac{\beta}{(a_i H_4(pk_{i,2}) + b_i) \cdot H_3(t \| 0)}$,令 $\pi = 1$.

(b)当 $c_i = 0$,选取 $rk_i^{(1)t \to j_R} \in Z_q^*$,令 $\pi = 0$.

B 将$(pk_i, pk_j, T, c_j, (rk_i^{(1)t \to j}, \tilde{A}, \tilde{B}), \beta, \pi)$加入 R^{list},响应以$(rk_i^{(1)t \to j}, \tilde{A}, \tilde{B})$.

(4)重加密问询. 当 A 以(pk_i, pk_j, C_i)问询时,若$(pk_{i,1}^{H_4(pk_{i,2})} pk_{i,2})^s = D \cdot A^{H_3(A,B,D)}$不成立,$B$ 响应以 $\perp$. 若成立, B 以(pk_i, pk_j, T)发起重加密密钥问询,获得 $rk_i \xrightarrow{t} j$,计算 $A' = A^{rk_i^{(1)t \to j}}$,并响应以 $C_j = (A', B, \tilde{A}, \tilde{B})$.

(5)解密问询. 当 A 以(pk_i, C_i)问询时, B 从 K^{list}中恢复出(pk_i, a_i, b_i, c_i),若 $c_i = 1$ 或 $c_i = \phi$,运行 Decrypt $((a_i, b_i), C_i)$,响应以解密结果. 否则,B 运行如下:

(a)当密文格式为 $C_i = (A, B, D, s)$,检验$(pk_{i,1}^{H_4(pk_{i,2})} pk_{i,2})^s = D \cdot A^{H_3(A,B,D)}$是否成立,若不成立,响应以 $\perp$. 若成立,执行过程 $P3$:从 H_1^{list} 中搜索(m, w, α),从 H_2^{list} 中搜索(R, η),从 H_3^{list} 中搜索(T, t, τ). 若 $P3$ 结果无法满足$(pk_{i,1}^{H_4(pk_{i,2})} pk_{i,2})^{\alpha \cdot \tau} = A$, $(m \| w) \oplus \eta = B$, $R = g^\alpha$,响应以 $\perp$,否则响应以 m.

(b)当密文格式为 $C_j = (A', B, \tilde{A}, \tilde{B})$,执行过程 $P3$,若某项不存在响应以 $\perp$,否则:若 R^{list}中存在对应项$(pk_i, pk_j, T, c_j, (rk_i^{(1)t \to j}, \tilde{A}, \tilde{B}), \beta, \pi)$,则计算 $A' = A'^{\frac{1}{rk_i^{(1)t \to j}}}$,使得$(pk_{i,1}^{H_4(pk_{i,2})} pk_{i,2})^{\alpha \cdot \tau} = A$, $(m \| w) \oplus \eta = B$, $R = g^\alpha$,响应以 m. 否则从 H_1^{list} 中搜索(β, γ, σ),从 H_2^{list} 中搜索(R', η'),使得 $g^\sigma = \tilde{A}$, $\eta' \oplus (\beta \| \gamma) = \tilde{B}$, $g^{\sigma \cdot \beta} = A'$, $(m \| w) \oplus \eta = B$, $R = g^\alpha$, $R' = pk_{j,2}^\sigma$,响应以 m.

挑战 A 结束阶段 1,输出目标公钥 pk_{i^*}、目标类型 T^* 与等长消息 $m_0, m_1 \in \{0,1\}^{k_1}$. B 响应如下:

从 K^{list}中恢复出$(pk_{i^*}, a_{i^*}, b_{i^*}, c_{i^*})$,若 $c_{i^*} = 1$,响应以事件 Fail. 若 $c_{i^*} = \phi$,响应 $\perp$. 否则, B 搜索 R^{list},若存在项$(pk_{i^*}, pk_j, T^*, c_j, (rk_{i^*}^{(1)t^* \to j}, \tilde{A}, \tilde{B}), \beta, \pi)$,且其中 $c_j = \phi$,响应以 $\perp$. 否则, B 选取 $e^*, s_R^* \in Z_q^*$,计算 $D^* = (g^b)^{-(a_{i^*} H_4(pk_{i^*,2}) + b_{i^*})e^*} (g^{\frac{1}{a}})^{(a_{i^*} H_4(pk_{i^*,2}) + b_{i^*})s^*}$, $A^* = (g^b)^{(a_{i^*} H_4(pk_{i^*,2}) + b_{i^*}) H_3(t^* \| 0)}$. 选取 $B_R^* \in (0,1)^{k_1 + k_2}$,使得 $H_3(t^* \| 0) \cdot H_3(A^*, B^*, D^*) = e^*$. 选取 $\delta_R \in (0,1)$,

$w_R^* \in (0,1)^{k_2}$,计算 $H_2(g^{ab}) = (m_\delta \parallel w^*) \oplus B^*$, $H_1(m_\delta, w^*) = ab$,响应以挑战密文 $C^* = (A^*, B^*, D^*, s^*)$.

阶段 2　A、B 继续阶段 1 中的问询与响应,遵循阶段 2 的约束条件,仅在重加密密钥问询和重加密问询处响应方式不同,描述如下:

(1)重加密密钥问询. 当 A 以 (pk_i, pk_j, T) 问询时,执行过程 $P1$.

(a)当 $c_i = 1 \vee c_i = \phi$,同阶段 1.

(b)当 $c_i = 0 \wedge c_j = 1$,或 $c_i = 0 \wedge c_j = 0$,或 $c_i = 0 \wedge c_j = \phi \wedge t \neq t^*$ 时,选取 $rk_{i \xrightarrow{(1)t} j_R} \in Z_q^*$,令 $\pi = 0$.

(c)当 $c_i = 0 \wedge c_j = \phi \wedge t = t^*$,响应 Fail.

将 $(pk_i, pk_j, T, c_j, (rk_{i \xrightarrow{(1)t} j}, \tilde{A}, \tilde{B}), \beta, \pi)$ 加入 R^{list},响应以 $(rk_{i \xrightarrow{(1)t} j}, \tilde{A}, \tilde{B})$.

(2)重加密问询. 当 A 以 (pk_i, pk_j, C_i) 问询时,若 $(pk_{i,1}^{H_4(pk_{i,2})} pk_{i,2})^s = D \cdot A^{H_3(A,B,D)}$ 不成立,响应 $\perp$,否则从 K^{list} 中恢复出 (pk_i, a_i, b_i, c_i), (pk_j, a_j, b_j, c_j),计算:

(a)当 $c_i = 0 \wedge c_j = \phi \wedge t = t^*$,从 H_1^{list} 中搜索 (m, w, α),从 H_3^{list} 中搜索 (T, t, τ),使得 $(pk_{i,1}^{H_4(pk_{i,2})} pk_{i,2})^{\alpha \cdot \tau} = A$,若不存在这样的项,响应 $\perp$. 否则选取 $\beta_R \in \{0,1\}^{k_1}$, $\gamma_R \in \{0,1\}^{k_2}$,计算:$\sigma = H_1(\beta, \gamma)$, $\tilde{A} = g^\sigma$, $\tilde{B} = H_2(pk_{j,2}^\sigma) \oplus (\beta \parallel \gamma)$, $A' = g^{\alpha \cdot \beta}$,响应以 $C_j = (A', B, \tilde{A}, \tilde{B})$. 将因 α 和 τ 无法从列表中恢复而终止算法称为事件 REErr.

(b)否则 B 以 (pk_i, pk_j, T) 发起重加密密钥问询,获得 $rk_{i \xrightarrow{t} j}$,计算 $A' = A^{rk_{i \xrightarrow{(1)t} j}}$,并响应以 $C_j = (A', B, \tilde{A}, \tilde{B})$.

猜测　A 输出猜测值 $\delta' \in \{0,1\}$,B 选取 $(R, \eta)_R \in H_2^{list}$,输出 R 作为给定 DCDH 实例的结果.

上述哈希问询模拟与实际情形一致,除了事件 $AskH_1*$(A 已以 (m_δ, w^*) 问询过 H_1)、$AskH_2*$(A 已以 g^{ab} 问询过 H_2)、$AskH_3*$(A 已以 (A^*, B^*, D^*) 问询过 H_{31} 且 A 已以 (T^*, t^*) 问询过 H_{32}). 由于 B^* 是 B 从中 $\{0,1\}^{k_1+k_2}$ 随机选取的,因此 $\Pr[AskH_3^*] \leqslant \frac{q_{H_{31}} \cdot q_{H_{32}}}{2^{2(k_1+k_2)}}$, $AskH_1*$ 与 $AskH_2*$ 分析如下.

两种密钥生成问询模拟与实际情形一致.

重加密密钥生成问询除了阶段 2 中的事件 Fail,模拟与实际情形一致. 根据攻击游戏及所采用的安全性证明技术,$Pr[\neg Fail] \geqslant \theta^{q_{rk}}(1-\theta) \geqslant \frac{1}{e(1+q_{rk})}$.

重加密问询除了阶段 2 中的事件 REErr,模拟与实际情形一致. 事件 REErr 发生,意味着敌手在未对 H_1 与 H_3^2 进行相应问询的情况下生成了有效密文,则 $\Pr[REErr] \leqslant \frac{1}{q} \cdot \frac{1}{q} \cdot q_{re} = \frac{q_{re}}{q^2}$.

解密问询模拟与实际情形一致,除了事件 DErr:当 C 是有效密文时,若 C 的生成未经问询 H_1、H_2 和 H_3^2,则 B 中止运算. 令 $AskH_1$ 为事件“已问询 H_1”,$AskH_2$ 为事件“已问询 H_2”,$AskH_{32}$ 为事件“已问询 H_3^2”,则:

$$\begin{aligned}
&\Pr[Valid \mid \neg AskH_1] \\
&= \Pr[Valid \wedge AskH_2 \wedge AskH_{32} \mid \neg AskH_1] \\
&\quad + \Pr[Valid \wedge \neg AskH_2 \wedge AskH_{32} \mid \neg AskH_1] \\
&\quad + \Pr[Valid \wedge AskH_2 \wedge \neg AskH_{32} \mid \neg AskH_1] \\
&\quad + \Pr[Valid \wedge \neg AskH_2 \wedge \neg AskH_{32} \mid \neg AskH_1] \\
&\leqslant \Pr[AskH_2 \wedge AskH_{32} \mid \neg AskH_1] \\
&\quad + \Pr[Valid \wedge AskH_{32} \mid \neg AskH_1 \wedge \neg AskH_2] \\
&\quad + \Pr[Valid \wedge AskH_2 \mid \neg AskH_1 \wedge \neg AskH_{32}] \\
&\quad + \Pr[Valid \mid \neg AskH_1 \wedge \neg AskH_2 \wedge \neg AskH_{32}] \\
&\leqslant \frac{q_{H_2}}{q} \cdot \frac{q_{H_{32}}}{q} + \frac{q_{H_{32}}}{(2^{k_1+k_2}) \cdot q} + \frac{q_{H_2}}{q \cdot q} + \frac{1}{q} \\
&= \frac{q_{H_2} \cdot q_{H_{32}} + q_{H_2}}{q^2} + \frac{q_{H_{32}}}{(2^{k_1+k_2}) \cdot q} + \frac{1}{q}
\end{aligned}$$

同样的,有

$$\begin{aligned}
&\Pr[Valid \mid \neg AskH_2] \\
&\leqslant \frac{q_{H_1}}{2^{k_1+k_2}} \cdot \frac{q_{H_{32}}}{2^{k_1+k_2}} + \frac{q_{H_{32}}}{(2^{k_1+k_2}) \cdot q} + \frac{q_{H_1}}{(2^{k_1+k_2}) \cdot q} + \frac{1}{q} \\
&= \frac{q_{H_1} \cdot q_{H_{32}}}{2^{2(k_1+k_2)}} + \frac{q_{H_1} + q_{H_{32}}}{(2^{k_1+k_2}) \cdot q} + \frac{1}{q},
\end{aligned}$$

$$\begin{aligned}
&\Pr[Valid \mid \neg AskH_{32}] \\
&\leqslant \frac{q_{H_1}}{q} \cdot \frac{q_{H_2}}{q} + \frac{q_{H_1}}{(2^{k_1+k_2}) \cdot q} + \frac{q_{H_2}}{q \cdot q} + \frac{1}{q} \\
&= \frac{q_{H_1} \cdot q_{H_2} + q_{H_2}}{q^2} + \frac{q_{H_1}}{(2^{k_1+k_2}) \cdot q} + \frac{1}{q},
\end{aligned}$$

则有

$$\begin{aligned}
&\Pr[Valid \mid (\neg AskH_1 \vee \neg AskH_2 \vee \neg AskH_{32})] \\
&\leqslant \Pr[Valid \mid \neg AskH_1] + \Pr[Valid \mid \neg AskH_2)] \\
&\quad + \Pr[Valid \mid \neg AskH_{32})] \\
&\leqslant \frac{q_{H_1} \cdot q_{H_{32}}}{2^{2(k_1+k_2)}} + \frac{2q_{H_1} + 2q_{H_{32}}}{2^{k_1+k_2} \cdot q} + \frac{q_{H_2}(q_{H_{32}} + q_{H_1} + 2)}{q^2} + \frac{3}{q}
\end{aligned}$$

假定 A 发起最多 q_d 次解密问询,则

$$\begin{aligned}
\Pr[DErr] \leqslant &\frac{q_{H_1} \cdot q_{H_{32}} \cdot q_d}{2^{2(k_1+k_2)}} + \frac{2(q_{H_1} + q_{H_{32}}) \cdot q_d}{2^{k_1+k_2} \cdot q} \\
&+ \frac{q_{H_2}(q_{H_{32}} + q_{H_1} + 2) \cdot q_d}{q^2} + \frac{3q_d}{q}.
\end{aligned}$$

若事件 $(AskH_2^* \vee (AskH_1^* \mid \neg AskH_2^*) \vee AskH_3^* \vee REErr \vee DErr) \mid \neg Fail$ 不发生,则由 H_2 输出的随机性,A 无法获取猜测 δ 的优势,则

$$\begin{aligned}
\varepsilon - v &= |2\Pr[\delta' = \delta] - 1| \leqslant \Pr[Event] \\
&= (\Pr[AskH_2*] + \Pr[AskH_1* \mid \neg AskH_2*] \\
&\quad + \Pr[AskH_3*] + \Pr[REErr] \\
&\quad + \Pr[DErr]) / \Pr[\neg Fail]
\end{aligned}$$

若 $AskH_2*$ 发生，B 可以解决 DCDH 问题，有

$$\Pr[AskH_1* \mid \neg AskH_2*] \leqslant \frac{q_{H_1}}{2^{k_1+k_2}},$$

$$\Pr[AskH_3*] \leqslant \frac{q_{H_{31}} \cdot q_{H_{32}}}{2^{2(k_1+k_2)}}, \quad \Pr[REErr] \leqslant \frac{q_{re}}{q^2},$$

$$\Pr[\neg Fail] \geqslant \frac{1}{e(1+q_{rk})},$$

$$\Pr[DErr] \leqslant \frac{q_{H_1} \cdot q_{H_{32}} \cdot q_d}{2^{2(k_1+k_2)}} + \frac{2(q_{H_1}+q_{H_{32}}) \cdot q_d}{2^{k_1+k_2} \cdot q} + \frac{q_{H_2}(q_{H_{32}}+q_{H_1}+2) \cdot q_d}{q^2} + \frac{3q_d}{q}$$

则有

$$\begin{aligned}
&\Pr[AskH_2*] \\
&\geqslant \Pr[\neg Fail] \cdot (\varepsilon - v) - \Pr[AskH_1* \mid \neg AskH_2*] \\
&\quad - \Pr[AskH_3*] - \Pr[REErr] - \Pr[DErr]) \\
&\geqslant \frac{\varepsilon - v}{e(1+q_{rk})} - \frac{q_{H_1}}{2^{k_1+k_2}} - \frac{q_{H_{31}} \cdot q_{H_{32}}}{2^{2(k_1+k_2)}} - \frac{q_{re}}{q^2} - \frac{q_{H_1} \cdot q_{H_{32}} \cdot q_d}{2^{2(k_1+k_2)}} \\
&\quad - \frac{2(q_{H_1}+q_{H_{32}}) \cdot q_d}{2^{k_1+k_2} \cdot q} - \frac{q_{H_2}(q_{H_{32}}+q_{H_1}+2) \cdot q_d}{q^2} - \frac{3q_d}{q} \\
&= \frac{\varepsilon - v}{e(1+q_{rk})} - \frac{q_{H_1}}{2^{k_1+k_2}} - \frac{q_{H_{31}} \cdot q_{H_{32}} \cdot (q_d+1)}{2^{2(k_1+k_2)}} \\
&\quad - \frac{q_{re} + (q_{H_{32}}+q_{H_1}+2) \cdot q_{H_2} \cdot q_d}{q^2} \\
&\quad - \frac{2(q_{H_1}+q_{H_{32}}) \cdot q_d}{2^{k_1+k_2} \cdot q} - \frac{3q_d}{q}
\end{aligned}$$

则 B 解决 DCDH 问题的优势为：

$$\begin{aligned}
\varepsilon' &\leqslant \frac{1}{q_{H_2}} \Pr[AskH_2*] \\
&\leqslant \frac{1}{q_{H_2}} \left(\frac{\varepsilon - v}{e(1+q_{rk})} - \frac{q_{H_1}}{2^{k_1+k_2}} - \frac{q_{H_{31}} \cdot q_{H_{32}} \cdot (q_d+1)}{2^{2(k_1+k_2)}} \right. \\
&\quad - \frac{q_{re} + (q_{H_{32}}+q_{H_1}+2) \cdot q_{H_2} \cdot q_d}{q^2} \\
&\quad \left. - \frac{2(q_{H_1}+q_{H_{32}}) \cdot q_d}{2^{k_1+k_2} \cdot q} - \frac{3q_d}{q} \right)
\end{aligned}$$

B 的运行时间 t' 为：

$$t' \leqslant t + (q_{H_1}+q_{H_2}+q_{H_{31}}+q_{H_{32}}+q_{H_4}+q_u+q_c+q_{rk}+q_{re}+q_d)O(1) + (2q_u+2q_c+2q_{rk}+5q_{re}+2q_d+(q_{H_1}+q_{H_{32}})q_{re}+(2q_{H_2}+2q_{H_1}+2q_{H_{32}})q_d)t_{\exp}$$

证毕□.

5 方案性质和效率分析

5.1 主密钥安全性

一个代理重加密方案若具有主密钥安全性，则当代理服务器与受理方相勾结时，无法恢复出完整的委托方私钥[3].

本方案中，勾结者只能根据代理服务器上的 $rk_{i \xrightarrow{(1)t} j} = \frac{\beta}{(a_i H_4(pk_{i,2}) + b_i) \cdot H_3(t \| 0)}$ 与受理方解密得到的 β 恢复出值 $\frac{1}{(a_i H_4(pk_{i,2}) + b_i) \cdot H_3(t \| 0)}$，从中无法恢复出用户私钥 $sk_i = (a_i, b_i)$，因而本方案具有主密钥安全性.

5.2 效率分析

本方案中没有双线性对计算. 双线性对的计算时间是指数计算的两倍以上[13]，因此相对基于双线性对的现有分类代理重加密方案[8,9]，在相同或更强安全性的前提下，本方案具有更高的效率，详见表 1 中各方案的效率和安全性质比较. 篇幅所限，这里仅就理论方案的安全性及计算效率进行讨论，暂不考虑具体实现中的效率与安全性质差异.

表 1 分类代理重加密方案效率与安全性质比较

	文献[8] 方案 1	文献[8] 方案 2	文献[9] 方案	本文方案
安全模型	RO	RO	RO	RO
困难假设	XDH, Co-BDH	BDH, KE	3-QBDH	DCDH
安全性	CPA	CCA	CCA	CCA
主密钥安全性	有	有	无	有
加密效率	$2t_e+1t_p$	$3t_e+1t_p$	$5t_e+1t_p$	$3t_e$
重加密效率	$2t_e+1t_p$	$1t_p+1t_{PKEEnc}$	$2t_e+3t_p$	$3t_e$
原始解密效率	$1t_e+1t_p$	$2t_e+3t_p$	$5t_e+4t_p$	$4t_e$
重加密解密效率	$1t_e+1t_p$	$1t_e+1t_p+2t_{PKEDec}$	$2t_e+1t_p$	$4t_e$

注：其中 t_e、t_p、t_{PKEEnc}、t_{PKEDec} 分别代表一次指数运算、一次双线性对运算以及文献[8]中方案采用的公钥加密系统中一次加密和一次解密的时间.

6 总结

本文提出了一个无双线性对的分类代理重加密方案，并运用安全性证明技术对方案的选择密文安全性和主密钥安全性进行了分析和证明. 与现有同类方案间的理论运算时间的比较结果说明，我们的方案在拥有相同或更强安全性的同时具有更高的效率. 下一步工作将是与具体应用相结合实现分类代理重加密原型系统，并在应用场景中进一步讨论方案具体实现的效率和安全性.

参考文献

[1] M Mambo, E Okamoto. Proxy cryptosystems: delegation of the power to decrypt ciphertexts[J]. IEICE Trans Fund Elect Communications and CS, 1997, E80-A/1: 54 – 63.

[2] M Blaze, et al. Divertible protocols and atomic proxy cryptography[A]. EUROCRYPT′98[C]. 1998. vol. 1403, Springer, Heidelberg, 127 – 144.

[3] G Ateniese, et al. Improved proxy re-encryption schemes with applications to secure distributed storage[J]. ACM Transactions on Information and System Security, 2006, 9(1): 1 – 30.

[4] L Ibraimi, et al. A type-and-identity-based proxy re-encryption scheme and its application in healthcare[A]. SDM′08[C]. LNCS, Springer, Heidelberg, 2008. vol. 5159, 185 – 198.

[5] 袁春,等.基于密码学的访问控制和加密安全数据库[J].电子学报,2006,34(11):2043 – 2046.
YUAN Chun, et al. Progress of cryptographic access control and encryption security database[J]. Acta Electronica Sinica, 2006, 34(11): 2043 – 2046. (in Chinese)

[6] 李斓,冯登国,徐震.RBAC 与 MAC 在多级关系数据库中的综合模型[J].电子学报,2004,32(10):1635 – 1639.
LI Lan, FENG Deng-guo, XU Zhen. A integrated model of RBAC and MAC in multilevel relation database system[J]. Acta Electronica Sinica, 2004, 32(10): 1635 – 1639. (in Chinese)

[7] G Taban, et al. Towards a secure and interoperable DRM architecture[A]. ACM DRM′06[C]. Springer, Heidelberg, 2006. 69 – 78.

[8] Q Tang. Type-based proxy re-encryption and its construction [A]. INDOCRYPT ′08[C]. LNCS, vol. 5365. Springer, Heidelberg, 2008. 130 – 144.

[9] J Weng, et al. Conditional proxy re-Encryption secure against chosen-ciphertext attack [A]. ACM ASIACCS′09 [C]. Springer, Heidelberg, 2009. 322 – 332.

[10] X Liang, et al. Attribute based proxy re-encryption with delegating capabilities[A]. ACM ASIACCS′09[C]. Springer, Heidelberg, 2009. 276 – 286.

[11] Q Tang. On using encryption techniques to enhance sticky policies enforcement[R]. Technical Report TR-CTIT-08-64 (2008), University of Twente, 2008. ISSN 1381 – 3625.

[12] 毛文波.现代密码学理论与实践[M].北京:电子工业出版社,2004. 170 – 171.

[13] M Scott. Computing the tate pairing[A]. CT-RSA′05[C]. LNCS, vol. 3376, Springer, Heidelberg, 2005. 293 – 304.

[14] J Shao, Z Cao. CCA-secure proxy re-encryption without pairings[A]. PKC′09[C], volume 5443 of LNCS, Springer, Heidelberg, 2009. 357 – 376.

[15] R Deng, et al. Chosen-ciphertext secure poxy re-encryption without pairings [A]. CANS′08 [C]. LNCS, vol. 5339, Springer, Heidelberg, 2008. 1 – 17.

[16] J Weng, et al. Efficient unidirectional proxy re-encryption[J/OL]. http://eprint.iacr.org/2009/189. 2009-05-05.

[17] M Green, G Ateniese. Identity-based proxy re-encryption[A]. ACNS′07[C]. LNCS, vol. 4521, Springer, Heidelberg, 2007. 288 – 306.

[18] C Schnorr. Efficient identification and signatures for smart cards[A]. CRYPTO′89[C]. LNCS, vol. 435, Springer, Heidelberg, 1989. 239 – 252.

[19] J Coron. On the exact security of Full Domain Hash[A]. CRYPTO′00[C]. LNCS, vol. 1880, Springer, Heidelberg, 2000. 229 – 235.

作者简介

赵　菁　女,1983 年 1 月出生于辽宁沈阳.2005 进入中国科学院研究生院信息安全国家重点实验室攻读并获取工学博士学位.现从事系统安全与认证授权方面的有关研究.
E-mail:zhaojingsctmnp@hotmail.com

冯登国　男,研究员、博士生导师、信息安全国家重点实验室主任.1965 年出生.目前主要从事信息与网络安全方面的研究与开发工作.1995 年 6 月获通信与信息系统专业博士学位,博士论文获首届全国优秀博士学位论文,1995 年 9 月进入中国科学院研究生院博士后流动站工作,1997 年 11 月入选中国科学院“百人计划”.