

支持策略更新的外包属性加密

林素青^{1,2}

(1. 中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093;
2. 中国科学院大学, 北京 100049)

摘要: 为满足云存储密态数据高效灵活的访问需求, 提出支持策略更新的外包属性加密方案。以经典的属性加密方案为基础模块, 采用类密钥盲化方法和外包解密技术, 在确保明文数据和用户私钥不泄露的条件下, 实现密文访问策略的代理更新, 同时切实有效地降低终端用户的解密计算量。方案支持非单调的访问结构, 在标准模型和假设下可证明具有选择 IND-CPA 安全性和私钥安全性, 与文献同类方案相比, 实现了安全性和终端访问效率的进一步优化。

关键词: 属性加密; 外包解密; 策略更新; 私钥安全性

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00055

Outsourced attribute-based encryption with policy update

LIN Su-qing^{1,2}

(1. The State Key Lab of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
2. University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: In order to achieve the efficient and flexible access control for the encrypted data stored in the cloud, an outsourced attribute-based encryption scheme with policy update was proposed. Based on the standard attribute-based encryption scheme, the functionality of policy update from delegation for a ciphertext without revealing any confidential information of the plaintext and private keys by utilizing the techniques of key blinding and outsourcing decryption was accomplished. Simultaneously, the decryption overhead for a user to recover the plaintext was effectively reduced. The scheme supports non-monotonic access structure and can be proved to have selective IND-CPA security and private key security under standard assumptions, respectively, in the standard model. Compared with similar schemes from literatures, the scheme provides better security and efficiency.

Key words: attribute-based encryption, outsourced decryption, policy update, private key security

1 引言

属性加密 (ABE)^[1]在保护数据隐私性的同时, 能实现细粒度且非交互的访问控制, 在云计算的数据安全存储和信息资源共享方面有良好的应用前景, 经过属性加密的云存储密态数据利用加密

过程中嵌入访问策略可以完成对密态数据访问权限的设置。若授权访问的用户采用“下载—解密—重加密—上传”的方式来更新密态数据的访问策略, 则需付出较高的计算和通信代价。密文策略的属性基代理重加密 (CP-AB-PRE)^[2]结合密文策略的属性加密 (CP-ABE) 和外包解密技术, 借

收稿日期: 2016-04-05; 修回日期: 2016-05-08。通信作者: 林素青, suqinglin2016@126.com

基金项目: 国家自然科学基金资助项目 (No.61379142)

Foundation Item: The National Natural Science Foundation of China (No.61379142)

助代理服务器, 可实现密态数据访问策略的代理更新, 能有效减轻用户的计算量和通信量。

目前, 关于 CP-AB-PRE 的研究工作很多, 但安全性和效率方面均有待提高。2009 年, Liang 等^[2]以文献[3]的 CP-ABE 方案为基础, 构造出首个 CP-AB-PRE 方案, 并在选择策略模型下证明方案具有选择明文不可区分 (IND-CPA) 安全性。此后, Luo 等^[4]提出在 DBDH 假设下可证明安全, 具有重加密可控制性质的 CP-AB-PRE 方案, 并用类似于文献[5]的方法, 将解密中双线性对运算的个数减少为常数, 但解密过程中包含双线性对运算, 对于资源有限的弱终端用户仍然是难以承受的负担。2011 年, Green 等^[6]提出支持外包解密的属性加密方案, 利用密钥盲化方法, 将解密过程中绝大部分双线性对和模指数运算外包给代理服务器, 在不泄露明文数据和用户私钥的前提下, 将终端用户的解密计算量降到最低。利用文献[6]的方法可将大多数基于双线性对运算而构造的属性加密方案^[7-9]拓展为外包属性加密方案 (OABE)。Lai 等^[10]在文献[6]方案的基础上考虑外包解密的安全验证问题, 提出支持可验证外包解密的 ABE 方案, 并在标准模型下证明方案的安全性。随后, Lin 等^[11]系统地解决了外包解密的安全验证问题, 构造的方案在实现效率方面比文献[10]方案提高近一半。此外, Li 等^[12]运用 MapReduce 方法实现 ABE 的加密外包, Li 等^[13,14]借助 2 个代理服务器, 构造密钥分发和解密运算均可外包的 ABE 方案。Ma 等^[15]全面考虑属性加密和解密的外包可验证问题, 借鉴在线—离线 CP-ABE 方案^[16]的构造方法, 以文献[17]方案为基础模块, 提出支持可验证外包加解密的在线—离线 OABE 方案。2015 年, Shao 等^[18]提出在线—离线的 CP-AB-PRE 方案, 支持线性秘密共享方案 (LSSS, linear secret sharing scheme) 表达的访问结构, 实现密文访问策略的代理更新, 同时, Shao 等指出, 结合外包解密方法, 可大幅度地减少终端用户的解密计算量, 并证明方案具有选择 IND-CPA 安全性。但该方案仅支持单调的 LSSS 访问结构, 且安全性所基于的假设仅证明在通用群模型下成立。

本文提出具有策略更新功能的密文策略外包属

性基代理重加密 (CP-OAB-PRE) 方案, 以经典的属性加密方案^[3]为基础, 借用文献[4]中 CP-AB-PRE 方案的构造方式, 结合外包解密技术^[6], 构造支持非单调访问结构的 CP-OAB-PRE 方案, 并全面考虑方案关于明文数据和用户私钥的安全性, 在标准模型和假设下证明方案具有选择 IND-CPA 安全性和私钥安全性。与文献同类方案相比, 本文的方案能同时实现安全性和终端访问效率的进一步优化。

2 预备知识

2.1 符号说明

记 $\mathbf{N}$ 为自然数集, $\mathbf{R}$ 为实数集。 $1^\lambda (\lambda \in \mathbf{N})$ 表示 λ 个 1 形成的字符串, λ 为安全参数。 $b \in_R S$ 表示从属性集合 S 中均匀随机选取元素 b 。 1_G 表示群 G 的单位元。 $p (p \in \Theta(2^\lambda))$ 记为素数, Z_p 由模 p 剩余类全体 $\{0, 1, \dots, p-1\}$ 构成, Z_p^* 表示 $Z_p \setminus \{0\}$ 。

2.2 双线性映射与困难问题假设

定义 1 可忽略函数。函数 $negl: \mathbf{N} \rightarrow \mathbf{R}$ 是可忽略的, 如果对于任意 $c > 0$, 存在 $\lambda_0 > 0$, 则当 $\lambda > \lambda_0$ 时, 有 $negl(\lambda) < \frac{1}{\lambda^c}$ 。

定义 2 双线性映射。设 G 和 G_T 分别表示素数 p 阶乘法循环群。称 $e: G \times G \rightarrow G_T$ 为双线性映射, 如果其满足如下条件, 称 G 为素数 p 阶双线性群, 若存在群 G_T 和双线性映射 e , 使下述性质成立。

1) 可计算性: 对于任意的元素 $u, v \in G$, 存在有效算法计算 $e(u, v)$ 。

2) 非退化性: 若 g 为群 G 的生成元, 则 $e(g, g) \neq 1_{G_T}$ 。

3) 双线性性: 对于任意的 $u, v \in G$, 以及 $a, b \in Z_p^*$, 有等式 $e(u^a, v^b) = e(u, v)^{ab}$ 成立。

下面描述计算 Diffie-Hellman (CDH) 假设和判定双线性 Diffie-Hellman (DBDH) 假设。

定义 3 CDH 假设。设 G 表示素数 p 阶乘法群, g 为群 G 的生成元。对于任意概率多项式时间 (PPT) 算法 X , 存在可忽略函数 $negl$ 满足 $\Pr[X(g, g^a, g^b) = g^{ab}] \leq negl(\lambda)$, 其中, $a, b \in_R Z_p^*$ 。

定义 4 DBDH 假设。设 G 和 G_T 分别表示素

数 p 阶乘法群, g 为群 G 的生成元, $e: G \times G \rightarrow G_T$ 表示双线性映射。对于任意概率多项式时间算法 X , 存在可忽略函数 $negl$ 满足

$$|\Pr[X(g, g^a, g^b, g^c, e(g, g)^{abc}) = 1] - \Pr[X(g, g^a, g^b, g^c, T) = 1]| \leq negl(\lambda)$$

其中, $a, b, c \in_R Z_p^*$, $T \in_R G_T$ 。

2.3 访问结构

访问结构表示一些非空的访问集合构成的全体, 其所含的访问集合为授权集合, 其余的访问集合为非授权集合。

定义 5^[19] 设 n 个参与者全体表示为 $\{P_1, \dots, P_n\}$, $A \subseteq 2^{\{P_1, \dots, P_n\}}$ 是由参与者全体的子集构成的集合。如果对于 A 中任意的 2 个集合 D, C , 均满足: 若 $D \in A$, $D \subseteq C$, 则 $C \in A$, 那么称集合 A 是单调的。由参与者全体 $\{P_1, \dots, P_n\}$ 的非空子集构成的集合 A 就称为一个访问结构, 即 $A \subseteq 2^{\{P_1, \dots, P_n\}} \setminus \{\emptyset\}$ 。若 A 是单调的, 则称为单调的访问结构。 A 中的元素均为授权集合, 不在 A 中的元素均为非授权集合。

此方案基于与门访问结构, 与门访问结构是用逻辑与操作联结属性(可以为正属性或负属性)而得的非单调访问结构。设属性空间为 U , 访问策略 A 用与门访问结构表示为 $\bigwedge_{i \in I} \underline{i}$, 其中 $I \subseteq U$, $\underline{i}$ 代表一个属性。称一个属性集合 $S \subseteq U$ 满足访问结构 (或访问策略) A , 对于任意的 $i \in I$ 。

1) 若正属性 i 出现在访问策略 A 中, 即 $\underline{i} = i$, 则 $i \in S$ 。

2) 若负属性 $\neg i$ 出现在访问策略 A 中, 即 $\underline{i} = \neg i$, 则 $i \notin S$ 。

2.4 CP-OAB-PRE 的算法描述

假设代理服务器是半可信任的, 即代理服务器能诚实可靠地执行计算但有偷窥私密信息的好奇心, 构造密文策略的外包属性基代理重加密 (CP-OAB-PRE) 方案, 算法描述如下。

1) $Setup(1^\lambda, U)$: 系统建立算法。输入安全参数 λ 和属性空间 U , 输出公共参数 PK 和主私钥 MSK 。

2) $KGen(PK, MSK, S)$: 密钥生成算法。输入公共参数 PK 、主私钥 MSK 以及属性集合 S , 输出密钥 SK_S 。

3) $Enc(PK, M, A)$: 加密算法。输入公共参数 PK 、消息 M 以及访问策略 A , 输出密文 CT_A 。

4) $RKGen(PK, SK_S, A')$: 重加密密钥生成算法。输入公共参数 PK 、属性集合 S 对应的密钥 SK_S 以及访问策略 A' , 输出重加密密钥 $RK_{S \rightarrow A'}$ 。

5) $REnc(PK, RK_{S \rightarrow A'}, CT_A)$: 重加密算法。输入公共参数 PK , 重加密密钥 $RK_{S \rightarrow A'}$ 、访问策略 A 对应的密文 CT_A 。若 S 不满足 A , 输出错误标识符 $\perp$; 若 S 满足 A , 输出访问策略 A' 对应的重加密密文 $CT_{A'}$ 。

6) $Dec(SK_S, CT_A)$: 解密算法。输入属性集合 S 对应的密钥 SK_S , 访问策略 A 对应的密文 CT_A 。若 S 不满足 A , 则输出错误标识符 $\perp$; 若 S 满足 A , 输出 M 。

7) $TKGen(PK, SK_S)$: 外包密钥生成算法。输入公共参数 PK 、属性集合 S 对应的密钥 SK_S , 输出外包解密密钥 TK_S 和数据恢复密钥 RK_S 。

8) $Dec_{out}(TK_S, CT_A)$: 外包解密算法。输入属性集合 S 对应的外包解密密钥 TK_S , 访问策略 A 对应的密文 CT_A 。若属性集合 S 不满足访问策略 A , 输出错误标识符 $\perp$; 若属性集合 S 满足访问策略 A , 输出外包解密密文 CT'_A 。

9) $Dec'(RK_S, CT'_A)$: 解密算法。输入数据恢复密钥 RK_S 和外包解密密文 CT'_A , 输出 M 。

正确性: CP-OAB-PRE 方案是正确的, 当且仅当对于任意正确产生的公共参数 PK 和主私钥 MSK , 任意的属性集合 S 、访问结构 A 以及消息 M , 若 S 满足 A , 则有

$$M = Dec(KGen(PK, MSK, S), Enc(PK, M, A))$$

对于任意正确生成的密钥 SK_S , 以及外包解密密钥 TK_S 和数据恢复密钥 RK_S , 若 S 满足 A , 则有

$$M = Dec'(RK_S, Dec_{out}(TK_S, Enc(PK, M, A)))$$

对于任意正确生成的重加密密钥 $RK_{S' \rightarrow A}$, 以及正确产生的密文 $CT_{A'}$, 若 S' 满足 A' , 且 S 满足 A , 则有

$$M = Dec'(RK_S, Dec_{out}(TK_S, REnc(PK, RK_{S' \rightarrow A}, CT_{A'})))$$

2.5 CP-OAB-PRE 的安全模型

本节分别定义 CP-OAB-PRE 方案关于密文和重加密密文的 IND-CPA 安全性, 以及私钥安全性。为刻画方案关于密文的 IND-CPA 安全性, 任意 PPT 敌手 X 与挑战者之间的游戏描述如下。

1) $Setup$: 系统建立阶段。挑战者调用算法

$Setup(1^\lambda, U)$ 得到公共参数 PK 和主私钥 MSK ，并将公共参数 PK 发送给敌手 X 。

2) *Phase 1*: 第1个询问阶段。敌手 X 提交3类询问: ① 对应于属性集合 S 的密钥; ② 对应于属性集合 S 的外包解密密钥; ③ 对应于属性集合 S 和访问策略 A 的重加密密钥, 挑战者给出相应的回复。

3) *Challenge*: 敌手 X 提交2个等长的消息 M_0, M_1 , 以及访问策略 A^* 给挑战者, 要求敌手询问过密钥或重加密密钥的所有 S 都不能满足 A^* 。挑战者均匀随机选取 $b \in \{0, 1\}$, 调用加密算法 $Enc(PK, M_b, A^*)$, 得到挑战密文 CT^* 。

4) *Phase 2*: 第2个询问阶段。敌手 X 继续提交密钥、外包解密密钥以及重加密密钥询问, 要求询问密钥或重加密密钥的所有 S 不能满足 A^* , 挑战者给出相应的回复。

5) *Guess*: 猜测阶段。敌手 X 输出对 b 的猜测 $b' \in \{0, 1\}$ 。

定义6 CP-OAB-PRE 方案关于原密文是 IND-CPA 安全的, 如果任意的 PPT 敌手 X 在上述游戏中的优势是可忽略的, 即 $\left| \Pr[b' = b] - \frac{1}{2} \right| \leq \text{negl}(\lambda)$ 。

若敌手在 *Setup* 这个阶段之前先提出将要攻击的密文指标 A^* , 则称此模型下的安全为选择 IND-CPA 安全。

下面定义 CP-OAB-PRE 方案关于重加密密文的安全性。*Setup*、*Phase 1*、*Phase 2*、*Guess* 4个阶段与上述定义相同, *Challenge* 阶段描述如下。

Challenge: 敌手 X 提交2个等长的消息 M_0, M_1 , 以及访问策略 A^* 给挑战者, 要求敌手询问过密钥或重加密密钥的所有 S 都不能满足 A^* 。挑战者选取属性集合 S , 调用算法 $KGen(PK, MSK, S)$ 生成密钥 SK_S , 再调用算法 $RKGen(PK, SK_S, A^*)$ 得到重加密密钥 $RK_{S \rightarrow A^*}$, 选取属性集合 S 满足的访问策略 A , 均匀随机选取 $b \in \{0, 1\}$, 调用加密算法 $Enc(PK, M_b, A)$ 得到 CT_b , 再调用重加密算法 $REnc(PK, RK_{S \rightarrow A^*}, CT_b)$ 得到 CT^* , 作为挑战密文输出给敌手。

定义7 CP-OAB-PRE 方案关于重加密密文是 IND-CPA 安全的, 如果任意的 PPT 敌手 X 在上述游戏中的优势是可忽略的, 即 $\left| \Pr[b' = b] - \frac{1}{2} \right| \leq$

$\text{negl}(\lambda)$ 。

若敌手在 *Setup* 这个阶段之前先提出将要攻击的密文指标 A^* , 则称此模型下的安全为选择 IND-CPA 安全。

在代理重加密过程中, 代理服务器将获取由用户私钥生成的重加密密钥, 为确保重加密密钥不泄露用户私钥的信息, 定义 CP-OAB-PRE 方案的私钥安全性。任意 PPT 敌手 X 与挑战者之间的游戏描述如下。

1) *Setup*: 系统建立阶段。挑战者调用算法 $Setup(1^\lambda, U)$ 得到公共参数 PK 和主私钥 MSK , 并将公共参数 PK 发送给敌手 X 。

2) *Query Phase*: 询问阶段。敌手 X 提交3类询问: ① 对应于属性集合 S 的密钥; ② 对应于属性集合 S 的外包解密密钥; ③ 对应于属性集合 S 和访问策略 A 的重加密密钥, 挑战者给出相应的回复。

3) *Output*: 敌手 X 输出属性集合 S^* 和相应的密钥 SK_{S^*} 。挑战者随机选取消息 M 和访问策略 A , 其中, S^* 满足 A , 调用加密算法 $Enc(PK, M, A)$ 得到密文 CT_A , 若用解密算法 $Dec(SK_{S^*}, CT_A)$ 能得到 M , 则称敌手 X 赢得游戏。

定义8 CP-OAB-PRE 方案具有私钥安全性, 如果任意的 PPT 敌手 X 赢得上述游戏的概率是可忽略的。

若敌手在 *Setup* 这个阶段之前先提出将要攻击的属性集合 S^* , 则称此模型下的安全为选择私钥安全性。

3 本文方案

结合文献[6]的密钥盲化方法和外包解密技术, 构造支持策略更新的外包属性加密方案, 称之为密文策略的外包属性基代理重加密 (CP-OAB-PRE) 方案。为保证用户私钥的安全性, 文献[20]采用与密钥盲化类似的方法, 即类密钥盲化方法生成重加密密钥, 使之即使在盲化因子遭遇泄露的情况下, 敌手也不能获取真正的解密密钥。

3.1 方案的构造

设 λ 为安全参数, $U = \{1, 2, \dots, n\}$ 表示属性空间。CP-OAB-PRE 方案的算法描述如下。

1) *Setup*($1^\lambda, U$): 系统建立算法。选取一个素

数 p 阶双线性群系统 (G, G_T, e) , $e: G \times G \rightarrow G_T$ 表示从群 G 至群 G_T 的双线性映射。设 g 为群 G 的一个生成元, $H: G_T \rightarrow Z_p$ 表示抗碰撞散列函数。随机选取 $\hat{g}, h \in_R G$, $y, t_1, \dots, t_{3n} \in_R Z_p^*$ 。定义 $Y = e(g^y, \hat{g})$, $T_i = g^{t_i}, i \in [3n]$ 。算法输出公共参数 $PK = (e, g, \hat{g}, h, Y, T_1, \dots, T_{3n})$ 和主私钥 $MSK = (y, t_1, \dots, t_{3n})$ 。

2) $KGen(PK, MSK, S)$: 密钥生成算法。随机选取 $r_i, r'_i, r''_i \in_R Z_p^*, i \in [n]$ 。记 $r = \sum_{i=1}^n r_i$, 设 $\hat{D} = \hat{g}^{y-r}$, 并按照如下方式定义 $D_i, F_i, i \in U$ 。

$$D_i = (D_{i1}, D_{i2}) = \begin{cases} (\hat{g}^{r_i} T_{r'_i}, g^{r'_i}), & i \in S \\ (\hat{g}^{r_i} T_{2n+i}, g^{r'_i}), & i \notin S \end{cases}$$

$$F_i = (F_{i1}, F_{i2}) = (\hat{g}^{r_i} T_{2n+i}, g^{r''_i}), i \in U$$

算法输出密钥 $SK_S = (S, \hat{D}, \{D_i, F_i\}_{i \in U})$ 。

3) $Enc(PK, M, A)$: 加密算法。设访问策略 A 表示为 $\bigwedge_{i \in I} \underline{i}$, $i \in I \subseteq U$, 其中, $\underline{i}$ 代表一个属性。随机选取 $s \in_R Z_p^*$, 设 $\bar{C} = M \cdot Y^s$, $\hat{C} = g^s$, $\check{C} = h^s$,

$$C_i = \begin{cases} T_i^s, \underline{i} = i, i \in I \\ T_{n+i}^s, \underline{i} = \neg i, i \in I \\ T_{2n+i}^s, i \notin I \end{cases}$$

算法输出密文 $CT_A = (A, \bar{C}, \hat{C}, \check{C}, \{C_i\}_{i \in U})$ 。

4) $RKGen(SK_S, A')$: 重加密密钥生成算法。随机选取 $\theta_1, \theta_2, \dots, \theta_n \in_R Z_p^*$, 密钥盲化因子 $\hat{d} \in_R G_T$, 令 $d = H(\hat{d})$ 。设 $\hat{D}' = \hat{D}^d = (\hat{g}^{y-r})^d$, $\bar{D} = g^{\sum_{i=1}^n \theta_i}$, $D'_i = (D'_{i1}, D'_{i2}) = (D_{i1}^d h^{\theta_i}, D_{i2}^d)$, $F'_i = (F'_{i1}, F'_{i2}) = (F_{i1}^d h^{\theta_i}, F_{i2}^d)$, $i \in U$ 。

然后, 执行加密算法 $Enc(PK, \hat{d}, A')$ 所描述的相同的运算, 但不选取 $\check{C} = h^s$ 这项, 得到密文 $\tilde{C}_{A'}$ 。算法输出重加密密钥 $RK_{S \rightarrow A'} = (S, A', \hat{D}', \{D'_i, F'_i\}_{i \in U}, \bar{D}, \tilde{C}_{A'})$ 。

5) $REnc(RK_{S \rightarrow A'}, CT_A)$: 重加密算法。若 S 不满足 A , 输出错误标识符 $\perp$; 否则, 分情况讨论如下。

$$\textcircled{1} i \in I, \underline{i} = i \text{ 且 } i \in S, \text{ 计算 } E'_i = \frac{e(\hat{C}, D'_{i1})}{e(C_i, D'_{i2})} =$$

$$\frac{e(g^s, (\hat{g}^{r_i} g^{t_{r'_i}})^d h^{\theta_i})}{e(T_i^s, (g^{r'_i})^d)} = e(g, \hat{g})^{r_i s d} e(g, h)^{s \theta_i}$$

$$\textcircled{2} i \in I, \underline{i} = \neg i \text{ 且 } i \notin S, \text{ 计算 } E'_i = \frac{e(\hat{C}, D'_{i1})}{e(C_i, D'_{i2})} =$$

$$\frac{e(g^s, (\hat{g}^{r_i} g^{t_{2n+i}})^d h^{\theta_i})}{e(T_{n+i}^s, (g^{r'_i})^d)} = e(g, \hat{g})^{r_i s d} e(g, h)^{s \theta_i}$$

$$\textcircled{3} i \notin I, \text{ 计算}$$

$$E'_i = \frac{e(\hat{C}, F'_{i1})}{e(C_i, F'_{i2})} = \frac{e(g^s, (\hat{g}^{r_i} g^{t_{2n+i}})^d h^{\theta_i})}{e(T_{2n+i}^s, (g^{r''_i})^d)} = e(g, \hat{g})^{r_i s d} e(g, h)^{s \theta_i}$$

$$\text{然后, 求解得到 } C' = \frac{e(\hat{C}, \hat{D}') \prod_{i=1}^n E'_i}{e(\bar{C}, \bar{D})} = \frac{e(g^s, (\hat{g}^{y-r})^d) \prod_{i=1}^n (e(g, \hat{g})^{r_i s d} e(g, h)^{s \theta_i})}{e\left(h^s, g^{\sum_{i=1}^n \theta_i}\right)} = e(g, \hat{g})^{y s d}。$$

算法输出重加密密文 $CT_{A'} = (A', \bar{C}, C', \tilde{C}_{A'})$ 。

6) $Dec(SK_S, CT_{A'})$: 解密算法。若属性集合 S 不满足访问策略 A , 输出错误标识符 $\perp$; 若属性集合 S 满足访问策略 A , 则分情况讨论如下。

① $CT_{A'}$ 为原密文

$$\text{a) } \underline{i} = i \text{ 且 } i \in S, \text{ 计算 } E_i = \frac{e(\hat{C}, D_{i1})}{e(C_i, D_{i2})} =$$

$$\frac{e(g^s, \hat{g}^{r_i} g^{t_{r'_i}})}{e(T_i^s, g^{r'_i})} = e(g, \hat{g})^{r_i s};$$

$$\text{b) } \underline{i} = \neg i \text{ 且 } i \notin S, \text{ 计算 } E_i = \frac{e(\hat{C}, D_{i1})}{e(C_i, D_{i2})} =$$

$$\frac{e(g^s, \hat{g}^{r_i} g^{t_{2n+i}})}{e(T_{n+i}^s, g^{r'_i})} = e(g, \hat{g})^{r_i s};$$

$$\text{c) } i \notin I, \text{ 计算 } E_i = \frac{e(\hat{C}, F_{i1})}{e(C_i, F_{i2})} = \frac{e(g^s, \hat{g}^{r_i} g^{t_{2n+i}})}{e(T_{2n+i}^s, g^{r''_i})} =$$

$$e(g, \hat{g})^{r_i s}。$$

然后, 求解 $e(\hat{C}, \hat{D}) \prod_{i=1}^n E_i = e(g^s, \hat{g}^{y-r})$

$$\prod_{i=1}^n e(g, \hat{g})^{r_i s} = e(g, \hat{g})^{y s} = Y^s, \text{ 于是, 可得 } M = \frac{\bar{C}}{Y^s}。$$

② $CT_{A'}$ 为重加密密文

用密钥 SK_S 对原密文 $\tilde{C}_A$ 解密, 得到 d , 再计

算 $M = \frac{\bar{C}}{C'^{\frac{1}{d}}}$ 。

7) $TKGen(PK, SK_S)$: 外包密钥生成算法。随机选取 $z \in Z_p^*$, 设 $\hat{D}'' = \hat{D}^z$, $D_i'' = (D_{i1}'', D_{i2}'') = (D_{i1}^z, D_{i2}^z)$, $F_i'' = (F_{i1}'', F_{i2}'') = (F_{i1}^z, F_{i2}^z)$, $i \in U$ 。

算法输出外包解密密钥 $TK_S = (S, \hat{D}'', \{D_i'', F_i''\}_{i \in U})$ 和数据恢复密钥 $RK_S = z$ 。

8) $Dec_{out}(TK_S, CT_A)$: 外包解密算法。若属性集合 S 不满足访问策略 A , 输出错误标识符 $\perp$; 若属性集合 S 满足访问策略 A , 则分情况讨论如下。

① $CT_A = (A, \bar{C}, \hat{C}, \tilde{C}, \{C_i\}_{i \in U})$ 为原密文

a) $\underline{i} = i$ 且 $i \in S$, 计算 $E_i'' = \frac{e(\hat{C}, D_{i1}'')}{e(C_i, D_{i2}'')} = \frac{e(g^s, (\hat{g}^{r_i} g^{t_{n+i} r_i'})^z)}{e(T_i^s, (g^{r_i'})^z)} = e(g, \hat{g})^{r_i s z}$;

b) $\underline{i} = \neg i$ 且 $i \notin S$, 计算 $E_i'' = \frac{e(\hat{C}, D_{i1}'')}{e(C_i, D_{i2}'')} = \frac{e(g^s, (\hat{g}^{r_i} g^{t_{n+i} r_i'})^z)}{e(T_{n+i}^s, (g^{r_i'})^z)} = e(g, \hat{g})^{r_i s z}$;

c) $i \notin I$, 计算 $E_i'' = \frac{e(\hat{C}, F_{i1}'')}{e(C_i, F_{i2}'')} = \frac{e(g^s, (\hat{g}^{r_i} g^{t_{2n+i} r_i'})^z)}{e(T_{2n+i}^s, (g^{r_i'})^z)} = e(g, \hat{g})^{r_i s z}$ 。

然后, 求解得到 $C'' = e(\hat{C}, \hat{D}'') \prod_{i=1}^n E_i'' = e(g^s, (\hat{g}^{y-r})^z) \prod_{i=1}^n e(g, \hat{g})^{r_i s z} = e(g, \hat{g})^{y s z} = Y^{s z}$ 。算法输出

$CT'_A = (A, \bar{C}, C'', \tilde{C})$

② $CT_A = (A, \bar{C}, C', \tilde{C}_A)$ 为重加密密文

用外包解密密钥 TK_S 对原密文 $\tilde{C}_A$ 执行上述运算, 得到 $\tilde{C}'_A$, 其中不包含 $\tilde{C}$ 项。算法输出外包解密密文 $CT'_A = (A, \bar{C}, C', \tilde{C}'_A)$

9) $Dec'(RK_S, CT'_A)$: 解密算法。

① $CT'_A = (A, \bar{C}, C', \tilde{C})$ 为原密文的外包解密密文。

可得 $M = \frac{\bar{C}}{(C'')^{\frac{1}{|RK_S|}}} = \frac{M \cdot Y^s}{(Y^{s z})^{\frac{1}{z}}}$ 。

② $CT'_A = (A, \bar{C}, C', \tilde{C}'_A)$ 为重加密密文的外包

解密密文。

用数据恢复密钥 RK_S 对 $\tilde{C}'_A$ 执行上述运算, 可得 $\hat{d}$, 从而得到 $d = H(\hat{d})$, 再计算 $M = \frac{\bar{C}}{C'^{\frac{1}{d}}}$ 。

3.2 安全性分析

定理 1 若 DBDH 假设成立, 则所构造的 CP-OAB-PRE 方案关于原密文具有选择 IND-CPA 安全性。

证明 假设存在 PPT 敌手 X 能以不可忽略的优势 ε 攻破方案的选择 IND-CPA 安全性, 则可以构造算法 B , 以不可忽略的优势 $\frac{\varepsilon}{2}$ 解决 DBDH 问题。

挑战者选取素数 p 阶群 G , G_T , $e: G \times G \rightarrow G_T$ 表示双线性映射, g 是群 G 的一个生成元, 并随机选取 $a, b, c \in_R Z_p^*$, 得到 g^a, g^b, g^c 。挑战者均匀随机选取 $\tau \in \{0, 1\}$, 若 $\tau = 1$, 输出 $(g, g^a, g^b, g^c, e(g, g)^{abc})$; 若 $\tau = 0$, 输出 (g, g^a, g^b, g^c, T) , 其中, $T \in_R G_T$ 。设 B 得到挑战问题组 (g, g^a, g^b, g^c, P) , 其中, $P \in G_T$ 。为判定 P 是否为 $e(g, g)^{abc}$, B 调用 X 执行如下步骤。

1) *Init*: 初始化阶段。敌手 X 发布要挑战的访问策略 $A^* = \bigwedge_{i \in I^*} \underline{i}$, 其中 $\underline{i}$ 表示一个属性。

2) *Setup*: 系统建立阶段。 B 设定 $\hat{g} = g^b$, $Y = e(g^a, \hat{g}) = e(g, g)^{ab}$, 随机选取 $x \in_R Z_p^*$, 并令 $h = g^x$ 。 B 随机选取 $\alpha_i, \beta_i, \gamma_i \in_R Z_p^*, i \in U$, 按照如下方式生成公共参数。

①若 $i \in I^*$ 且 $\underline{i} = i$, 定义 $T_i = g^{\alpha_i}$, $T_{n+i} = g^{b\beta_i}$, $T_{2n+i} = g^{b\gamma_i}$ 。

②若 $i \in I^*$ 且 $\underline{i} = \neg i$, 定义 $T_i = g^{b\alpha_i}$, $T_{n+i} = g^{\beta_i}$, $T_{2n+i} = g^{b\gamma_i}$ 。

③若 $i \notin I^*$, 定义 $T_i = g^{b\alpha_i}$, $T_{n+i} = g^{b\beta_i}$, $T_{2n+i} = g^{\gamma_i}$ 。

3) *Phase 1*: 第 1 个询问阶段。

①敌手 X 询问对应于属性集合 S 的密钥, 其中, S 不满足 A^* 。

必然存在一个属性 $j \in I$, 满足: $j \in S$ 且 $\underline{j} = \neg j$, 或者, $j \notin S$ 且 $\underline{j} = j$ 。不失一般性, 这里假设 B 选取 $j \in I$ 满足 $j \in S$ 且 $\underline{j} = \neg j$, 另外的情况可做类似讨论。

B 随机选取 $r_i, r'_i, r''_i \in_R Z_p^*, i \in U$, 隐含定义

$\hat{r}_j = a + r_j$, $\hat{r}_i = r_i$, $i \in U, \{j\}$ 。设 $r = \sum_{i=1}^n \hat{r}_i =$

$a + \sum_{i=1}^n r_i$, 则 $\hat{D} = \hat{g}^{a-r} = \hat{g}^{-\sum_{i=1}^n r_i}$ 。分情况讨论并定义 $D_i = (D_{i1}, D_{i2}), i \in U$ 如下。

a) 若 $i \in S$ 且 $i \neq j$

$i \in I^*$ 且 $\underline{i} = i$, 定义 $D_i = (\hat{g}^{r_i} g^{\alpha_i r'_i}, g^{r'_i}) = (\hat{g}^{r_i} T_{i1}^{r'_i}, g^{r'_i})$;

$i \in I^*$ 且 $\underline{i} = \neg i$, 或者 $i \notin I^*$, 定义 $D_i = (\hat{g}^{r_i} g^{b\alpha_i r'_i}, g^{r'_i}) = (\hat{g}^{r_i} T_{i1}^{r'_i}, g^{r'_i})$ 。

b) 若 $i \in S$ 且 $i = j$, 定义 $D_j = (\hat{g}^{r_j + \alpha_j r'_j}, (g^a)^{\frac{1}{\alpha_j}} g^{r'_j}) = (\hat{g}^{r_j} g^{b\alpha_j(-\frac{a}{\alpha_j} + r'_j)}, g^{\frac{-a}{\alpha_j} + r'_j}) = (\hat{g}^{r_j} T_{j1}^{r'_j}, g^{r'_j})$, 其中, 隐含定义 $\hat{r}'_j = \frac{-a}{\alpha_j} + r'_j$ 。

c) 若 $i \notin S$

$i \in I^*$ 且 $\underline{i} = \neg i$, 定义 $D_i = (\hat{g}^{r_i} g^{\beta_i r'_i}, g^{r'_i}) = (\hat{g}^{r_i} T_{n+i,1}^{r'_i}, g^{r'_i})$;

$i \in I^*$ 且 $\underline{i} = i$, 或者 $i \notin I^*$, 定义 $D_i = (\hat{g}^{r_i} g^{b\beta_i r'_i}, g^{r'_i}) = (\hat{g}^{r_i} T_{n+i,1}^{r'_i}, g^{r'_i})$ 。

下面类似描述 $F_i = (F_{i1}, F_{i2}), i \in U$ 的定义。

a) 若 $i \neq j$

$i \in I^*$, 定义 $F_i = (\hat{g}^{r_i} g^{b\gamma_i r''_i}, g^{r''_i}) = (\hat{g}^{r_i} T_{2n+i,1}^{r''_i}, g^{r''_i})$;

$i \notin I^*$, 定义 $F_i = (\hat{g}^{r_i} g^{\gamma_i r''_i}, g^{r''_i}) = (\hat{g}^{r_i} T_{2n+i,1}^{r''_i}, g^{r''_i})$ 。

b) 若 $i = j$, 定义 $F_j = (\hat{g}^{r_j + \gamma_j r''_j}, (g^a)^{\frac{1}{\gamma_j}} g^{r''_j}) = (\hat{g}^{r_j} g^{b\gamma_j(-\frac{a}{\gamma_j} + r''_j)}, g^{\frac{-a}{\gamma_j} + r''_j}) = (\hat{g}^{r_j} T_{2n+j,1}^{r''_j}, g^{r''_j})$, 其中, 隐含定义 $\hat{r}''_j = -\frac{a}{\gamma_j} + r''_j$ 。

B 最终输出密钥 $SK_S = (S, \hat{D}, \{D_i, F_i\}_{i \in U})$ 。

②敌手 X 询问对应于属性集合 S 和访问策略 A' 的重加密密钥, 其中 S 不满足 A^* 。

B 按照①中描述的步骤生成对应于属性集合 S 的密钥 $SK_S = (S, \hat{D}, \{D_i, F_i\}_{i \in U})$, 然后, 随机选取 $\theta_1, \theta_2, \dots, \theta_n \in_R \mathbb{Z}_p^*$, 密钥盲化因子 $\hat{d} \in_R G_T$, 令 $d = H(\hat{d})$ 。定义 $\hat{D}' = \hat{D}^d$, $D'_i = (D'_{i1}, D'_{i2}) = (D_{i1}^d h^{\theta_i}, D_{i2}^d)$, $F'_i = (F'_{i1}, F'_{i2}) = (F_{i1}^d h^{\theta_i}, F_{i2}^d)$, $i \in U$, 以及 $\tilde{D} = g^{\sum_{i=1}^n \theta_i}$, 调用加密算法 $Enc(PK, \hat{d}, A')$ 得到 $\tilde{C}_{A'}$, 输出重加密密钥 $RK_{S \rightarrow A'} = (S, A', \hat{D}', \{D'_i, F'_i\}_{i \in U}, \tilde{D}, \tilde{C}_{A'})$ 。

$F'_i\}_{i \in U}, \tilde{D}, \tilde{C}_{A'})$ 。

③敌手 X 询问对应于属性集合 S 的外包解密密钥。

若 S 不满足 A^* , B 按照 1) 中描述的步骤生成对应于属性集合 S 的密钥 $SK_S = (S, \hat{D}, \{D_i, F_i\}_{i \in U})$, 然后, 随机选取 $z \in \mathbb{Z}_p^*$, 设 $\hat{D}'' = \hat{D}^z$, $D''_i = (D''_{i1}, D''_{i2}) = (D_{i1}^z, D_{i2}^z)$, $F''_i = (F''_{i1}, F''_{i2}) = (F_{i1}^z, F_{i2}^z)$, $i \in U$, 输出外包解密密钥 $TK_S = (S, \hat{D}'', \{D''_i, F''_i\}_{i \in U})$ 。

若 S 满足 A^* , B 随机选取 $z, r_i, r'_i, r''_i \in_R \mathbb{Z}_p^*$,

$i \in [n]$ 。记 $r = \sum_{i=1}^n r_i$, 设

$$\hat{D}'' = \hat{g}^{z-r}$$

$$D''_i = (D''_{i1}, D''_{i2}) = \begin{cases} (\hat{g}^{r_i} T_{i1}^{r'_i}, g^{r'_i}), & i \in S \\ (\hat{g}^{r_i} T_{n+i,1}^{r'_i}, g^{r'_i}), & i \notin S \end{cases}$$

$$F''_i = (F''_{i1}, F''_{i2}) = (\hat{g}^{r_i} T_{2n+i,1}^{r''_i}, g^{r''_i}), i \in U$$

输出外包解密密钥 $TK_S = (S, \hat{D}'', \{D''_i, F''_i\}_{i \in U})$ 。

4) *Phase 2*: 第 2 个询问阶段。与第 1 个询问阶段 *Phase 1* 相同, 敌手 X 提交密钥询问, 重加密密钥询问, 以及外包解密密钥询问, B 分别按照①、②、③的步骤, 给出相应的回复。

5) *Challenge*: 挑战阶段。敌手 X 提交 2 个等长的消息 M_0, M_1 。 B 均匀随机选取 $b \in \{0, 1\}$, 并设

$$\bar{C} = M_b \cdot P, \quad C = g^c, \quad \tilde{C} = C^x$$

$$C_i = \begin{cases} C^{\alpha_i}, & \underline{i} = i, i \in I^* \\ C^{\beta_i}, & \underline{i} = \neg i, i \in I^* \\ C^{\gamma_i}, & i \notin I^* \end{cases}$$

B 输出挑战密文 $CT^* = (A^*, \bar{C}, C, \tilde{C}, \{C_i\}_{i \in U})$ 。

Guess: 猜测阶段。敌手 X 输出 $b' \in \{0, 1\}$, 作为对 b 的猜测。若 $b' = b$, B 输出 $v' = 1$, 猜测 $P = e(g, g)^{abc}$; 若 $b' \neq b$, B 输出 $v' = 0$, 猜测 P 是 G_T 中随机选取的元素。

因此, B 成功破解 DBDH 假设的优势为

$$\begin{aligned} Adv_B &= \left| \Pr[B \text{ 成功}] - \frac{1}{2} \right| \\ &= \left| \frac{1}{2} \Pr[v' = v \mid v = 1] + \frac{1}{2} \Pr[v' = v \mid v = 0] - \frac{1}{2} \right| \\ &= \left| \frac{1}{2} \Pr[b' = b] + \frac{1}{2} \times \frac{1}{2} - \frac{1}{2} \right| \end{aligned}$$

$$= \left| \frac{1}{2} \left(\varepsilon + \frac{1}{2} \right) + \frac{1}{2} \times \frac{1}{2} - \frac{1}{2} \right| = \frac{\varepsilon}{2}$$

定理 2 若 DBDH 假设成立, 则 CP-OAB-PRE 方案关于重加密密文具有选择 IND-CPA 安全性。

证明 考虑挑战者与敌手之间的两类游戏。

Game₀: CP-OAB-PRE 方案关于重加密密文的选择 IND-CPA 安全性的真实定义。挑战密文为 $CT_{A^*} = (A^*, \bar{C}, C', \hat{C}_{A^*})$, 其中 $\bar{C} = M_b \cdot e(g, \hat{g})^{ys}$,

$C' = e(g, \hat{g})^{ysd}$, $\hat{C}_{A^*} = (\bar{C}', \hat{C}', \{C'_i\}_{i \in U})$, 且

$$\bar{C}' = \hat{d} \cdot e(g, \hat{g})^{ys}$$

$$\hat{C}' = g^{\hat{s}}$$

$$C'_i = \begin{cases} T_i^{\hat{s}}, & i = i, i \in I^* \\ T_{n+i}^{\hat{s}}, & i = \neg i, i \in I^* \\ T_{2n+i}^{\hat{s}}, & i \notin I^* \end{cases}$$

这里, $b \in_R \{0, 1\}$, $s, \tilde{s} \in_R Z_p^*$, $\hat{d} \in_R G_T$, $d = H(\hat{d})$, $A^* = \bigwedge_{i \in I^*} \underline{i}$, $i \in I^* \subseteq U$ 。

Game₁: 挑战密文 $CT_{A^*} = (A^*, \bar{C}, C', \hat{C}_{A^*})$ 中的 $C' = e(g, \hat{g})^{ysd}$, $d \in_R Z_p^*$, $\bar{C}' \in_R G_T$, 其余过程与 **Game₀** 相同。

由定理 1 的证明可知, 在 DBDH 假设下, $\hat{d}$ 与群 G_T 中随机选取的元素是计算不可区分的, 于是 **Game₀** 与 **Game₁** 计算不可区分。下面证明在 DBDH 假设下, 任意 PPT 敌手攻破 **Game₁** 的优势是可忽略的。证明的前期描述, 以及 *Init*、*Setup*、*Phase 1*、*Phase 2*、*Guess* 等阶段均与定理 1 的证明相同。

Challenge: 挑战阶段。敌手 X 交 2 个等长的消息 M_0, M_1 。B 均匀随机选取 $b \in \{0, 1\}$, 隐含定义 $d = \frac{1}{c}$, 设 $\bar{C} = M_b \cdot P$, $C' = Y = e(g, g)^{ab}$, $\bar{C}' \in_R G_T$, $\hat{C}' = C = g^{\hat{s}}$, 且 $\{C'_i\}_{i \in U}$ 与定理 1 挑战阶段中的 $\{C_i\}_{i \in U}$ 同样设置。

与定理 1 证明完全类似的分析, 可得, 在 DBDH 假设下, 任意 PPT 敌手攻破 **Game₁** 的优势是可忽略的, 而 **Game₀** 与 **Game₁** 是计算不可区分的, 于是, 任意 PPT 敌手攻破 **Game₀** 的优势是可忽略的, 从而, CP-OAB-PRE 方案关于重加密密文具有选择 IND-CPA 安全性。

定理 3 若 CDH 假设成立, 则 CP-OAB-PRE 方案具有选择私钥安全性。

证明 假设存在 PPT 敌手 X 能以不可忽略的优势攻破选择私钥安全性, 则可以设计算法 B 以不可忽略的概率求解 CDH 问题。B 得到挑战问题组 (g, g^a, g^b) , 其中, g 是素数 p 阶群 G 的生成元, $a, b \in_R Z_p^*$, 为计算 g^{ab} , B 调用 X 执行如下步骤。

1) *Init*: 初始化阶段。敌手 X 发布要挑战的属性集合 S^* 。

2) *Setup*: 系统建立阶段。B 设定 $h = g^a$, 随机选取 $k \in_R Z_p^*$, 令 $\hat{g} = g^k$, 并设 $Y = e(g^a, \hat{g}) = e(g^a, g^b)$ 。

B 随机选取 $\alpha_i, \beta_i, \gamma_i \in_R Z_p^*, i \in U$, 按照如下方式生成公共参数。

① 若 $i \in S^*$, 定义 $T_i = g^{\alpha_i}$, $T_{n+i} = g^{b\beta_i}$, $T_{2n+i} = g^{b\gamma_i}$ 。

② 若 $i \notin S^*$, 定义 $T_i = g^{b\alpha_i}$, $T_{n+i} = g^{\beta_i}$, $T_{2n+i} = g^{b\gamma_i}$ 。

B 输出公共参数 $PK = (e, g, \hat{g}, h, Y, T_1, \dots, T_{3n})$ 。

3) *Query Phase*: 询问阶段。

① 敌手 X 询问对应于属性集合 S 的密钥, 其中 $S \neq S^*$ 。

必然存在一个属性 j , 满足 $j \in S^*$ 且 $j \notin S$, 或 $j \notin S^*$ 且 $j \in S$ 。不失一般性, 这里假设 B 选取 j 满足 $j \in S^*$ 且 $j \notin S$, 另外的情况可做类似讨论。

B 随机选取 $r_i, r'_i, r''_i \in_R Z_p^*, i \in U$, 隐含定义

$$\hat{r}_j = ab + r_j, \hat{r}_i = r_i, i \in U, \{j\}。设 r = \sum_{i=1}^n \hat{r}_i = ab + \sum_{i=1}^n r_i,$$

则 $\hat{D} = \hat{g}^{ab-r} = \hat{g}^{-\sum_{i=1}^n r_i}$ 。分情况讨论并定义 $D_i = (D_{i1}, D_{i2}), i \in U$ 如下。

a) $i \in S$

$i \in S^*$, 定义 $D_i = (\hat{g}^{r_i} g^{\alpha_i r'_i}, g^{r'_i}) = (\hat{g}^{r_i} T_i^{r'_i}, g^{r'_i})$;
 $i \notin S^*$, 定义 $D_i = (\hat{g}^{r_i} g^{b\alpha_i r'_i}, g^{r'_i}) = (\hat{g}^{r_i} T_i^{r'_i}, g^{r'_i})$ 。

b) $i \notin S$ 且 $i \neq j$

$i \in S^*$, 定义 $D_i = (\hat{g}^{r_i} g^{b\beta_i r'_i}, g^{r'_i}) = (\hat{g}^{r_i} T_{n+i}^{r'_i}, g^{r'_i})$;
 $i \notin S^*$, 定义 $D_i = (\hat{g}^{r_i} g^{\beta_i r'_i}, g^{r'_i}) = (\hat{g}^{r_i} T_{n+i}^{r'_i}, g^{r'_i})$ 。

c) $i \notin S$ 且 $i = j$

$$\text{定义 } D_j = (\hat{g}^{r_j + br'_j}, \hat{g}^{\frac{r'_j - a}{\beta_j}}) = (\hat{g}^{ab+r_j} g^{\frac{(r'_j - a)k}{\beta_j}}, g^{\frac{(r'_j - a)k}{\beta_j}}) =$$

$$(\hat{g}^{\hat{r}_j} T_{n+j}^{r'_j}, g^{r'_j}), \text{ 其中, 隐含定义 } \hat{r}'_j = \frac{(r'_j - a)k}{\beta_j}。$$

下面类似描述 $F_i = (F_{i1}, F_{i2}), i \in U$ 的定义。

d) 若 $i \neq j$ ，定义 $F_i = (\hat{g}^{r_i} g^{b\gamma_i r_i'}, g^{r_i'}) = (\hat{g}^{r_i} T_{2n+i}^{r_i'}, g^{r_i'})$;

e) 若 $i = j$ ，定义 $F_j = (\hat{g}^{r_j} g^{b\gamma_j r_j'}, \hat{g}^{\frac{(r_j'-a)}{\gamma_j}}) = (\hat{g}^{ab+r_j} g^{\frac{(r_j'-a)k}{\gamma_j}}, g^{\frac{(r_j'-a)k}{\gamma_j}}) = (\hat{g}^{\hat{r}_j} T_{2n+j}^{r_j'}, g^{r_j'})$ ，其中，隐含定义 $\hat{r}_j' = \frac{(r_j''-a)k}{\gamma_j}$ 。

B 最终输出密钥 $SK_S = (S, \hat{D}, \{D_i, F_i\}_{i \in U})$ 。

② 敌手 X 问对应于属性集合 S^* 和访问策略 A' 的重加密密钥。

B 随机选取一个属性 $j \in S^*$ ，并随机选取 $\theta_i, r_i, r_i', r_i'' \in_R Z_p^*, i \in U$ ，密钥盲化因子 $\hat{d} \in_R G_T$ ，令 $d = H(\hat{d})$ 。隐含定义 $\hat{r}_i = ab + r_i$ ， $\hat{r}_i' = r_i$ ， $i \in U, \{j\}$ 。设 $r = \sum_{i=1}^n \hat{r}_i = ab + \sum_{i=1}^n r_i$ ，则 $\hat{D}' =$

$(\hat{D})^d = \left(\hat{g}^{-\sum_{i=1}^n r_i} \right)^d$ 。分情况讨论并定义 $D_i' = (D_{i1}', D_{i2}')$ ， $i \in U$ 如下。

a) $i \neq j$ ，定义 $F_i' = (\hat{g}^{dr_i} g^{bd\gamma_i r_i'} h^{\theta_i}, g^{dr_i'}) = ((\hat{g}^{r_i} T_{2n+i}^{r_i'})^d h^{\theta_i}, (g^{r_i'})^d)$ ，

$i \notin S^*$ ，定义 $D_i' = (\hat{g}^{dr_i} g^{d\beta_i r_i'} h^{\theta_i}, g^{dr_i'}) = ((\hat{g}^{r_i} T_{n+i}^{r_i'})^d h^{\theta_i}, (g^{r_i'})^d)$ ；

$i \in S^*$ ，定义 $D_i' = (\hat{g}^{dr_i} g^{d\alpha_i r_i'} h^{\theta_i}, g^{dr_i'}) = ((\hat{g}^{r_i} T_i^{r_i'})^d h^{\theta_i}, (g^{r_i'})^d)$ ；

b) $i = j$ ，定义 $D_j' = (\hat{g}^{dr_j+a\theta_j} g^{d\alpha_j r_j'}, g^{dr_j'}) = ((\hat{g}^{r_j+ab})^d (g^{\alpha_j r_j'})^d (g^a)^{-bdk+\theta_j k}, g^{dr_j'}) = ((\hat{g}^{\hat{r}_j} T_j^{r_j'})^d h^{\hat{\theta}_j}, (g^{r_j'})^d)$ ， $F_j' = (\hat{g}^{dr_j+a\theta_j} g^{bd\gamma_j r_j'}, g^{dr_j'}) = ((\hat{g}^{r_j+ab})^d (g^{b\gamma_j r_j'})^d (g^a)^{-bdk+\theta_j k}, (g^{r_j'})^d) = ((\hat{g}^{\hat{r}_j} T_{2n+j}^{r_j'})^d h^{\hat{\theta}_j}, (g^{r_j'})^d)$ ，其中，隐含定义 $\hat{\theta}_j = -bdk + \theta_j k$ 。

设 $\tilde{D} = g^{-bdk+\theta_j k} g^{\sum_{i \in [n], i \neq j} \theta_i}$ ， B 调用加密算法 $Enc(PK, \hat{d}, A')$ 得到 $\tilde{C}_{A'}$ ，输出重加密密钥

$$RK_{S \rightarrow A'} = (S, A', \hat{D}', \{D_i', F_i'\}_{i \in U}, \tilde{D}, \tilde{C}_{A'})$$

③ 敌手 X 询问对应于属性集合 S 的外包解密密钥。若 $S \neq S^*$ ， B 按照①中描述的步骤生成对应于属性集合 S 的密钥 SK_S ，后续的做法与定理 1 中 3) 的第 1 种情形相同。若 $S = S^*$ ， B 的做法与

定理 1 中 3) 的第 2 种情形相同。

4) **Output**：输出阶段。敌手 X 输出对应于属性集合 S^* 的密钥 $SK_{S^*} = (S^*, \hat{D}, \{D_i, F_i\}_{i \in U})$ 。 B 选取属性集合 S^* 满足的访问策略 $A^* = \left(\bigwedge_{i \in S^*} i \right) \wedge \left(\bigwedge_{i \notin S^*} \neg i \right)$ ，随机选取消息 M ，加密得到密文 CT_{A^*} 。如果能用密钥 SK_{S^*} 对 CT_{A^*} 解密得到 M ，则必有下列等式成立

$$e(g, \hat{D}) \prod_{i=i \wedge i \in S^*} \frac{e(g, D_{i1})}{e(T_i, D_{i2})} \prod_{i=\neg i \wedge i \in S^*} \frac{e(g, D_{i1})}{e(T_{n+i}, D_{i2})} = e(g, \hat{g})^{ab}$$

$$\text{于是, } \hat{D} \prod_{i=i \wedge i \in S^*} (D_{i1} D_{i2}^{-\alpha_i}) \prod_{i=\neg i \wedge i \in S^*} (D_{i1} D_{i2}^{-\beta_i}) = \hat{g}^{ab},$$

由此， B 可计算得到 $g^{ab} = (\hat{g}^{ab})^{\frac{1}{k}}$ 。

所以，若敌手 X 能以不可忽略的概率输出合法密钥 SK_{S^*} ，则 B 能以不可忽略的概率求解 CDH 问题，这与 CDH 假设矛盾。

4 方案的对比分析

将构造的 CP-OAB-PRE 方案与文献同类方案进行比较，分别从安全性、功能和效率等方面分析，主要关注数据安全性，密钥安全性，访问策略的表达能力，以及终端用户的解密计算量等。

如表 1 所示，本文方案与文献[2, 4]方案均全面考虑了可能存在的安全隐患。由于代理服务器在得到重加密密钥时，会获取关于密钥盲化因子的密文，而密钥盲化因子的信息泄露将直接威胁到用户私钥和明文数据的安全性，因此，不仅需要讨论明文数据的安全性，更需要论证用户私钥的安全性。文献[18]仅提供方案的数据安全性的相关论证，密钥安全性也可类似得证，但其安全性所基于的假设仅在通用群模型下证明成立。文献[2]方案的安全性所基于的 ADBDH 假设^[2]和 CTDH 假设^[2]分别比标准的 DBDH 和 CDH 假设较强，而本文方案的安全性均基于标准的假设。

如表 2 所示，本文方案与文献[2, 4]的方案均适用于非单调的与门访问结构，能表达正负属性均存在的情形，而文献[18]的方案适用于单调的访问结构，表达仅存在正属性的情形。本文方案支持外包解密运算，终端用户的解密计算量仅需要一个模指数运算，这与文献[18]的方案最少的终端解密计算量相同，而文献[2, 4]方案的终端解密计算量均需要较多的双线性对运算。

表1 安全性对比

方案	数据安全性		密钥安全性	
	假设	安全级别	假设	安全级别
文献[18]	$q-1$ 型 DPBDHE	选择 IND-CPA	—	—
文献[2]	ADBDH	选择 IND-CPA	CTDH	主私钥安全性
文献[4]	DBDH	选择 IND-CPA	CBDH	私钥安全性
本文方案	DBDH	选择 IND-CPA	CDH	私钥安全性

注：“—”表示文献未提供相应的安全性证明。

表2 功能效率对比

方案	访问结构	是否支持外包解密	终端解密计算量
文献[18]	线性秘密共享方案	是	E 或 $E+P$
文献[2]	与门访问结构	否	$(n+2)P$
文献[4]	与门访问结构	否	$3P$
本文方案	与门访问结构	是	E

注： E 和 P 分别表示模指数运算和双线性对运算； n 表示属性空间 U 的大小。

5 结束语

本文提出密文策略的外包属性基代理重加密（CP-OAB-PRE）方案，既支持密态数据访问策略的代理更新，又支持外包解密运算，满足弱终端用户的访问需求。终端授权访问用户可将解密的大部分计算量外包给代理服务器处理，然后只需完成剩余极小的计算量，便可得到明文数据。本文方案考虑代理服务器为半可信任的情形，即需要确保代理服务器诚实可靠地执行代理重加密和外包解密运算。针对代理服务器不可信任的情形，利用文献[11, 21]的方法可分别对外包解密和代理重加密增加验证机制，得到可验证的 CP-OAB-PRE 方案。

参考文献：

- [1] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//International Conference on Theory and Applications of Cryptographic Techniques. c2005:457-473.
- [2] LIANG X, CAO Z, LIN H, et al. Attribute based proxy re-encryption with delegating capabilities[C]//The 4th International Symposium on Information, Computer, and Communications Security, ACM. c2009: 276-286.
- [3] CHEUNG L, NEWPORT C. Provably secure ciphertext policy ABE[C]//The 14th ACM conference on Computer and Communications Security. c2007: 456-465.
- [4] LUO S, HU J, CHEN Z. Ciphertext policy attribute-based proxy re-encryption[C]//The 12th Information and Communications Security. c2010: 401-415.
- [5] HOHENBERGER S, WATERS B. Attribute-based encryption with fast decryption[M]//Public-Key Cryptography-PKC 2013. Berlin: Springer. 2013: 162-179.
- [6] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the Decryption of ABE Ciphertexts[C]//USENIX Security Symposium. c2011.
- [7] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communications Security. c2006: 89-98.
- [8] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[C]//Advances in Cryptology-EUROCRYPT. c2010: 62-91.
- [9] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization[C]//Public Key Cryptography-PKC. c2011: 53-70.
- [10] LAI J, DENG R H, GUAN C, et al. Attribute-based encryption with verifiable outsourced decryption[J]. Information Forensics and Security, 2013, 8(8): 1343-1354.
- [11] LIN S, ZHANG R, MA H, et al. Revisiting attribute-based encryption with verifiable outsourced decryption[J]. Information Forensics and Security, 2015, 10(10): 2119-2130.
- [12] LI J, JIA C, LI J, et al. Outsourcing encryption of attribute-based encryption with mapreduce[C]//The 14th Information and Communications Security. c2012: 191-201.

- [13] LI J, CHEN X, LI J, et al. Fine-grained access control system based on outsourced attribute-based encryption[C]//Computer Security-ESORICS. c2013: 592-609.
- [14] LI J, HUANG X, LI J, et al. Securely outsourcing attribute-based encryption with checkability[J]. Parallel and Distributed Systems, 2014, 25(8): 2201-2210.
- [15] MA H, ZHANG R, WAN Z, et al. Verifiable and exculpable outsourced attribute-based encryption for access control in cloud computing[J]. IEEE Transactions on Parallel and Distributed Systems, 2015:1.
- [16] HOHENBERGER S, WATERS B. Online/offline attribute-based encryption[M]//Public-Key Cryptography-PKC 2014. Berlin: Springer, 2014: 293-310.
- [17] ROUSELAKIS Y, WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption[C]//The 2013 ACM SIGSAC Conference on Computer & Communications Security. c2013: 463-474.
- [18] SHAO J, LU R, LIN X. Fine-grained data sharing in cloud computing for mobile devices[C]//Computer Communications (INFOCOM). c2015: 2677-2685.
- [19] BEIMEL A. Secure schemes for secret sharing and key distribution[M]//Israel Institute of Technology. Haifa: Technion, 1996.
- [20] LIANG K, SUSILO W. Searchable attribute-based mechanism with efficient data sharing for secure cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(9): 1981-1992.
- [21] LIIN S, ZHANG R, WANG M. Verifiable attribute-based proxy re-encryption for secure public cloud data sharing[J]. Security and Communication Networks, 2016.

作者简介：



林素青（1982-），女，浙江温州人，中国科学院信息工程研究所博士生，主要研究方向为信息安全、密码学。