中国科学: 信息科学
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS

支持大属性集合的抗泄露属性基加密机制

周彦伟[①], 徐然[①], 乔子芮[②*], 杨坤伟[①*], 杨波[①]

① 陕西师范大学 计算机科学学院，西安 710062
② 西安邮电大学 网络空间安全学院，西安 710121
* E-mail: qzr_snnu@163.com, yangkunwei@snnu.edu.cn

收稿日期: ; 接受日期:
国家自然科学基金(批准号：62272287); 陕西省重点研发计划项目(批准号：2024GX-YBXM-074); 中央高校基本科研业务费专项资金(批准号：GK202301009)资助项目.

摘要 现实环境中各种泄露攻击的存在，使得攻击者能够获得用户秘密信息的部分泄露，导致密码算法的传统安全性在有泄露攻击的环境下不再成立. 为进一步防止泄露攻击对数据安全性的危害，密码学研究者提出了一系列具有抗泄露攻击能力的密码算法. 属性基加密(Attribute-based Encryption, ABE)机制由于其能为数据提供细粒度的访问控制能力，在现实环境中得到了广泛的关注和应用. 然而，在现有抗泄露 ABE 机制的构造中，其系统公开参数的尺寸与其所能支持属性集合的大小成正比，导致其无法在大属性环境中使用. 为进一步增强抗泄露 ABE 机制的实用性，本文提出了支持大属性集合的抗泄露 ABE 机制的新型构造方法. 为获得更优的计算效率，本文首先在素数阶群上提出了支持大属性集合的抗泄露 ABE 机制的构造方法，并基于判定的并行双线性 Diffie-Hellman 指数假设证明了该方案的安全性，同时通过性能分析表明该方案具有较优的计算、存储和通信效率. 为获得更紧致的形式化安全性证明过程，本文随后在合数阶群上提出了支持大属性集合的抗泄露 ABE 机制的构造方法，并基于合数阶群上改进的子群判定假设证明了该方案的安全性.

关键词 抗泄露; 属性加密; 大属性集; 对偶系统加密

1 引言

传统密码机制的安全性是在理想模型中被证明的，然而在实际应用中，由于边信道、冷启动等泄露攻击的存在导致密码算法的私钥、随机数等秘密信息会产生泄露[1][2]，对系统的安全性造成极大的威胁. 为进一步保证攻击者在获取泄露信息后，密码系统依然具有其原始的安全性，密码学研究者提出了一系列抗泄露的密码机制，例如，抗泄露的公钥加密机制[3-5]、抗泄露的身份基加密机制[6-8]等.

1.1 研究现状

属性基加密(Attribute-based Encryption, ABE)机制基于访问策略为数据提供了细粒度的访问控制能力，当属性与访问策略相匹配时才能完成相应的解密操作，实现了“一对多”的高效加密模式. 在基于密文策略的属性基加密 (Ciphertext-Policy Attribute-Based Encryption, CP-ABE)机制中，密钥与属性相关联，密文与访问策略相关联，在基于密钥策略的属性基加密(Key-Policy Attribute-Based Encryption, KP-ABE)机制中则正好相反. 目前，研究人

引用格式: 周彦伟, 徐然, 乔子芮, 等. 支持大属性集合的抗泄露属性基加密机制. 中国科学 信息科学,

员已经对 ABE 机制开展了一系列的研究工作. Li 等人[9]提出了加权的 CP-ABE 机制, 该方案支持离线加密与外包解密技术, 构造了更加灵活高效的细粒度访问控制策略. Li 等人[10]的方案实现了策略隐藏, 保护了用户的隐私, 并构造了可追踪的 ABE 方案. Ge 等人[11]在保持数据完整性的同时实现对 ABE 机制密文的撤销, 其在撤销过程中不需要数据所有者在线, 保证了方案的可验证性. 但上述方案都只是基于理想情况设计的, 没有考虑攻击者会获取泄露的秘密信息, 导致上述方案在存在泄露的环境下无法保证其所声称的安全性. 为实现云计算系统中数据访问权限的撤销, Chen 等人[12]设计了具有数据完整性验证功能的可撤销 ABE 机制, 并且证明了上述方案的语义安全性和完整性. 在云计算系统中, 为确保未经授权用户解密操作的正确性, Li 等人[13]提出了一种具有可验证外包解密功能的 ABE 机制, 该方案可同时验证授权用户和未授权用户的转换密文的正确性, 并在标准模型下证明该方案具有选择 CPA 安全性.

为了保证 ABE 机制在泄露攻击下的安全性, 许多具备抗泄露攻击能力的 ABE 机制相继被提出[14-16]. Zhang 等人[17]提出了基于属性的哈希证明系统, 并以此为底层工具构造了抗泄露的属性基加密方案. Li 等人[18]提出了连续辅助输入模型下抗泄露的 KP-ABE 机制, 该方案可适用于视频点播、付费电视等应用场景. 为了解决密文长度大、计算效率低的问题, Zhang 等人[19]在连续辅助输入模型下设计了一个新颖的属性基广播加密方案, 其具有密文大小恒定的特征, 并且解密计算的复杂度仅取决于接收端的个数. Guo 等人[20]的方案将挑战后泄露模型与连续泄露模型和辅助输入泄露模型相结合, 提出了抗挑战后连续辅助输入泄露的安全模型, 并在该模型下提出了抗泄露的 CP-ABE 机制. Ma 等人[21]提出了多权威的抗泄露 ABE 方案, 实现了对多授权应用场景下泄露攻击的抵抗. Li 等人[22]提出了分层的抗泄露 ABE 方案, 分层的策略减轻了密钥生成中心繁重的密钥管理负担.

然而，上述抗泄露 ABE 机制的构造中，其系统公开参数的尺寸与其所能支持属性集的大小成正比, 导致其由于系统参数过长而无法在大属性环境下使用, 使得它们的应用前景受限. 具体地讲，在上述方案中，公开参数的尺寸随着属性的数量线性增长, 属性域的范围较大时系统可能会耗尽其功能, 需完全重建. 例如当系统扩张时需要向系统内添加大量的属性, 超过了系统初始部署时设定的界限, 那么就需要重新部署系统. 为进一步解决上述问题, 本文拟提出支持大属性集合的抗泄露 ABE 机制, 实现支持指数级属性域的抗泄露 ABE 机制的设计目标.

1.2 我们的出发点及主要工作

ABE 机制实现了细粒度的访问控制, 保证了数据的机密性与隐私性, 已在实际环境中被广泛应用. 然而大多数 ABE 机制都忽略了私钥、随机数等秘密信息的泄露, 为了抵抗现实应用中的泄露攻击, 研究者设计了抗泄露的 ABE 机制, 但相应方案的工作效率较低, 不支持大属性集合. 为进一步设计具有更优性能的抗泄露 ABE 机制, 本文拟设计支持大属性集合的抗泄露 ABE 机制. 具体分为：

（1）为获得更优的工作效率，在素数阶群上设计支持大属性集合的抗泄露 ABE 机制, 并基于判定的并行双线性 Diffie-Hellman 指数假设证明该方案的安全性. 通过性能分析表明与现有抗泄露 ABE 机制相比, 本文构造具有更优的计算、存储和通信效率, 更适合现实应用环境的高效部署需求.

（2）为获得更紧致的安全性证明，在合数阶群上设计支持大属性集合的抗泄露 ABE 机制, 并基于合数阶群上改进的子群判定假设证明该方案的安全性.

特别地，本文构造的公开参数尺寸与属性数量无关，且拥有指数级的属性域大小, 更符合现实环境中抗泄露 ABE 机制的大属性集部署需求.

2 基础知识

用 κ 表示安全参数； $a \leftarrow_R A$ 表示从集合 A 中均匀随机的选取元素 a； $\mathsf{negl}(\kappa)$ 表示在安全参数 κ 上是

计算可忽略的；$a \leftarrow \mathcal{A}(b)$表示算法$\mathcal{A}$在输入$b$的作用下输出相应的计算结果$a$.

2.1 合数阶双线性群及相应的子群判定假设

群生成算法$\mathcal{G}(1^\kappa)$输入安全参数κ，输出元组$\mathbb{G}=(N=p_1p_2p_3, g_1, G, G_T, e(\cdot))$，$G$和$G_T$是阶为合数$N$的乘法循环群，$p_1, p_2, p_3$是等长的大素数，$p_i$是子群$G_i$的阶，$g_1, g_2, g_3$分别是子群$G_1, G_2, G_3$的生成元. 特别地，对于$i, j = 1,2,3$且$i \neq j$，可将子群$G_{ij}$中的元素$T_{ij} \in G_{ij}$写为$T_{ij} = g_i^{x_i} g_j^{y_j}$,其中$x_i, y_j \in Z_N$. 此外，子群$G_i$和$G_j$中的元素能够联合表示子群$G_{ij}$中的元素，即若有$T_i \in G_i$和$T_j \in G_j$，那么$T_iT_j \in G_{ij}$. 双线性映射$e: G \times G \to G_T$满足以下性质.

双线性. 对于任意的$a, b \leftarrow_R Z_N$与$g \in G$，有$e(g^a, g^b) = e(g,g)^{ab}$成立.

非退化性. 对于任意的$e(g,g) \neq 1_{G_T}$成立，其中1_{G_T}是群G_T的生成元.

可计算性. 对于任意的$A, B \in G$，有$e(A,B)$可在多项式时间内完成计算.

子群正交性. 对于任意的$h_i \in G_i$与$h_j \in G_j$，当$i \neq j$时，有$e(h_i, h_j) = 1$.

文献[14]提出了合数阶群上改进的子群判定假设，并对改进假设的困难性进行了证明. 改进的子群判定假设分别叙述如下：

定义 1（改进的子群判定假设 1）. 群生成算法$\mathcal{G}(1^\kappa)$输出$\mathbb{G}=(N=p_1p_2p_3, g_1, G, G_T, e(\cdot))$，给定两个元组$(\mathbb{G}, g_1, X_3, \{T_{0i}\}_{i=1,2,\cdots,m})$和$(\mathbb{G}, g_1, X_3, \{T_{1i}\}_{i=1,2,\cdots,m})$，其中$g_1 \leftarrow_R G_1$，$X_3 \leftarrow_R G_3$，$T_{0i} \leftarrow_R G_{12}$和$T_{1i} \leftarrow_R G_1$. 令$D = (\mathbb{G}, g_1, X_3)$，对于任意的概率多项式时间算法$\mathcal{A}$，其成功区分元组$(D, T_{0i})_{i=1,2,\cdots,m}$和$(D, T_{1i})_{i=1,2,\cdots,m}$的优势

$$\mathrm{Adv}^{SD-1}(\kappa) = \left| \Pr\left[\mathcal{A}\left(D, \{T_{0i}\}_{i=1,2,\cdots,m}\right) = 1\right] - \Pr\left[\mathcal{A}\left(D, \{T_{1i}\}_{i=1,2,\cdots,m}\right) = 1\right] \right| \leq \mathrm{negl}(\kappa)$$

是可忽略的，其中概率来源于随机值的选取与使用.

定义 2（改进的子群判定假设 2）. 群生成算法$\mathcal{G}(1^\kappa)$输出$\mathbb{G}=(N=p_1p_2p_3, g_1, G, G_T, e(\cdot))$，给定两个元组$(\mathbb{G}, g_1, \{X_{1i}X_{2i}\}_{i=1,2,\cdots,m}, X_3, Y_2Y_3, T_0)$和$(\mathbb{G}, g_1, \{X_{1i}X_{2i}\}_{i=1,2,\cdots,m}, X_3, Y_2Y_3, T_1)$，其中$g_1, X_{1i} \leftarrow_R G_1$，$X_{2i}, Y_2 \leftarrow_R G_2$，$X_3, Y_3 \leftarrow_R G_3$，$T_0 \leftarrow_R G$和$T_1 \leftarrow_R G_{13}$. 令$D = (\mathbb{G}, g_1, \{X_{1i}X_{2i}\}_{i=1,2,\cdots,m}, X_3, Y_2Y_3)$，对于任意的概率多项式时间算法$\mathcal{A}$，其成功区分元组$(D, T_0)$和$(D, T_1)$的优势

$$\mathrm{Adv}^{SD-2}(\kappa) = \left| \Pr\left[\mathcal{A}(D, T_0) = 1\right] - \Pr\left[\mathcal{A}(D, T_1) = 1\right] \right| \leq \mathrm{negl}(\kappa)$$

是可忽略的，其中概率来源于随机值的选取与使用.

定义 3（改进的子群判定假设 3）. 群生成算法$\mathcal{G}(1^\kappa)$输出$\mathbb{G}=(N=p_1p_2p_3, g_1, G, G_T, e(\cdot))$，给定两个元组$(\mathbb{G}, g_1, \{g^{\alpha_i}X_2, g^{s_i}Y_2\}_{i=1,2,\cdots,m}, X_3, Z_2, T_0)$和$(\mathbb{G}, g_1, \{g^{\alpha_i}X_2, g^{s_i}Y_2\}_{i=1,2,\cdots,m}, X_3, Z_2, T_1)$，其中$g_1 \leftarrow_R G_1$，$X_3 \leftarrow_R G_3$，$(a_i, s_i)_{i=1,2,\cdots,m} \leftarrow_R (Z_N)^2$，$X_2, Y_2, Z_2 \leftarrow_R G_2$，$T_0 = \prod_{i=1}^{m} e(g_1, g_1)^{\alpha_i s_i}$和$T_1 \leftarrow_R G_T$. 令$D = (\mathbb{G}, g_1, \{g^{\alpha_i}X_2, g^{s_i}Y_2\}_{i=1,2,\cdots,m}, X_3, Z_2)$，对于任意的概率多项式时间算法$\mathcal{A}$，其成功区分元组$(D, T_0)$和$(D, T_1)$的优势

$$\mathrm{Adv}^{SD-3}(\kappa)=\left|\Pr\left[\mathcal{A}(D,T_0)=1\right]-\Pr\left[\mathcal{A}(D,T_1)=1\right]\right|\le \mathrm{negl}(\kappa)$$

是可忽略的, 其中概率来源于随机值的选取与使用.

2.2 判定的并行双线性 Diffie-Hellman 指数假设

定义 4（判定的并行双线性 Diffie-Hellman 指数假设）. 令 $\tilde{G}$ 和 $\tilde{G}_T$ 是两个阶为大素数 p 的乘法循环群, 满足双线性映射 $e:\tilde{G}\times\tilde{G}\to\tilde{G}_T$, 且 g 是群 $\tilde{G}$ 的生成元. 随机选取 $a,s,b_1,\cdots,b_q\leftarrow_R\left(Z_p\right)^{q+2}$. 令公开参数为

$$D=\begin{pmatrix} g,g^s,g^a,g^{a^2},\cdots,g^{a^q},g^{b_1},g^{b_2},\cdots,g^{b_q}\\ \forall_{1\le j\le q},g^{ab_j},\cdots,g^{a^qb_j},g^{a/b_j^2},g^{a^2/b_j^2},\cdots,g^{a^q/b_j^2}\\ \forall_{1\le j,k\le q,k\ne j},g^{ab_k/b_j^2},\cdots,g^{a^qb_k/b_j^2},g^{a^{q+1}b_k/b_j^2},\cdots,g^{a^{2q}b_k/b_j^2}\\ \forall_{1\le j\le q}g^{s\cdot b_j},g^{a/b_j},\cdots,g^{a^q/b_j},g^{a^{q+2}/b_j},\cdots,g^{a^{2q}/b_j}\\ \forall_{1\le j,k\le q,k\ne j}g^{a\cdot s\cdot b_k/b_j},\cdots,g^{a^q\cdot s\cdot b_k/b_j} \end{pmatrix}$$

对于元组 $(D,Z_1)=\left(D,e(g,g)^{a^{q+1}s}\right)$ 与 $(D,Z_2)=(D,R)$, 其中 R 是 $\tilde{G}_T$ 中的随机元素. 对于任意的概率多项式时间算法 $\mathcal{A}$, 其成功区分元组 (D,Z_1) 和 (D,Z_2) 的优势

$$\mathrm{Adv}_{\mathcal{A}}(\kappa)=\left|\Pr\left[\mathcal{A}(D,Z_1)=1\right]-\Pr\left[\mathcal{A}(D,Z_2)=1\right]\right|\le \mathrm{negl}(\kappa)$$

是可忽略的, 其中概率来源于随机值的选取与使用.

2.3 线性秘密共享方案

基于属性集合 S 的线性秘密共享方案(Linear Secret Sharing Scheme, LSSS)满足下述条件：

存在一个 $l\times n$ 的矩阵 $\mathbf{M}$, 将其称为秘密共享矩阵. 对于 $i=1,2,\cdots,l$, 矩阵 $\mathbf{M}$ 的每一行由函数 ρ 映射到属性集合 $\rho(i)$（称 ρ 为行属性映射函数）, 选取随机数 $s,y_2,...y_n\leftarrow\left(Z_p\right)^{n+1}$, 对于列向量 $\vec{y}=(s,y_2,...,y_n)^{\top}$, s 为共享的秘密, $\mathbf{M}\vec{y}$ 是秘密 s 共享的 l 个分量, 即有 $\vec{\lambda}=(\lambda_1,\lambda_2,\cdots,\lambda_l)^{\top}=\mathbf{M}\vec{y}$. 特别地, 将上述访问策略表示为 $\psi=(\mathbf{M},\rho)$. 定义 $I=\{i:i\in[l]\wedge\rho(i)\in S\}$. 若属性集合 S 满足访问策略 $\psi=(\mathbf{M},\rho)$, 即 $\psi(S)=1$, 且 $\{\lambda_i\}$ 是秘密 s 的共享分量, 则存在向量 $\{\omega_i\in Z_p\}_{i\in I}$ 使得 $\sum_{i\in I}\omega_i\lambda_i=s$ 成立.

2.4 Goldreich-Levin 定理

定理 1 (Goldreich-Levin 定理). 令 q 是一个大素数, H 是有限域 $GF(q)$ 的一个子集. 定义单向映射函数 $f:H^m\to\{0,1\}^*$. 任意选取 $s\leftarrow H^m$ 和 $r\leftarrow GF(q)^m$, 计算 $y=f(s)$. 如果存在概率多项式时间 t 内的区分器 D 使得 $\left|\Pr\left[D(y,r,\langle r,s\rangle)=1\right]-\Pr\left[D(y,r,u)=1\right]\right|=\varepsilon$ 成立（其中 $u\leftarrow_R GF(q)$）, 则存在可逆器 U 在时间 $t'=t\cdot poly(m,|H|,1/\varepsilon)$ 内使得 $\Pr\left[s\leftarrow H^m,y\leftarrow f(s):U(y)=s\right]\ge\frac{\varepsilon^3}{512\cdot m\cdot q^2}$ 成立.

换句话讲，对于有限域 $GF(q)$ 上的两个 m 长的向量 s 和 r，若存在区分器 D 能在多项式时间能以不可

忽略的优势区分两个元组$(y,r,\langle r,s\rangle)$和(y,r,u)，那么存在可逆器U能以不可忽略的优势攻破映射函数$f:H^m\to\{0,1\}^*$的单向性. 进一步讲, 区分器在已知秘密值s的泄露信息$y=f(s)$(通常情况下, 泄露信息是关于秘密值的函数值)和辅助参数向量r的前提下, 其依然无法区分内积值$\langle r,s\rangle$和均匀随机值u, 因此当任意的概率多项式时间敌手获知了秘密值s的泄露信息$y=f(s)$和向量r时, 内积值$\langle r,s\rangle$对其而言依然是均匀随机的. 此外, 在辅助输入模型中, 泄露输出的长度是无界的, 但它要求敌手从已知的泄露信息中恢复出密钥信息是不可能的. 定理 1 在实现内积计算结果均匀随机的同时保证了映射函数$f:H^m\to\{0,1\}^*$是不可逆的, 该性质正好与辅助输入模型的要求相吻合. 特别地, 文献[23]指出满足定理 1 要求的向量长度为$m=(3\log q)^{1/\varepsilon}$，并给出了上述定理的详细证明，本文不再赘述.

3 属性基加密机制的定义及抗泄露的安全模型

本节主要回顾 CP-ABE 机制的形式化定义及泄露容忍的选择明文攻击（Leakage-resilient Choose-plaintext Attack, LR-CPA）安全性游戏$Exp^{LR-CPA}_{CP-ABE,\mathcal{A}}(\lambda_{sk},\kappa)$的介绍.

3.1 CP-ABE 机制的形式化定义

CP-ABE 机制由下述 4 个概率多项式时间算法组成:

（1）初始化算法. 该算法输入安全参数κ，输出主私钥*msk*与系统公开参数*params*. 该算法可表示为：$(params,msk)\leftarrow\mathsf{Setup}(1^\kappa)$.

（2）密钥生成算法. 该算法输入主私钥*msk*与用户的属性集合S，输出用户的密钥*sk*. 该算法可表示为：$sk\leftarrow\mathsf{KeyGen}(msk,S)$.

（3）加密算法. 该算法输入待加密消息M与访问结构$\psi=(\mathbf{M},\rho)$，输出相应的密文*ct*. 该算法可表示为：$ct\leftarrow\mathsf{Enc}(M,(\mathbf{M},\rho))$.

（4）解密算法. 该算法输入密文*ct*与用户的密钥*sk*，若*sk*所对应的属性集合S满足密文*ct*的访问结构$\psi=(\Gamma,\rho)$（即$\psi(S)=1$），则输出相应的消息M；否则输出$\perp$. 该算法可表示为：$M/\perp\leftarrow\mathsf{Dec}(ct,sk)$.

3.2 正确性

对于 CP-ABE 机制而言, 若属性集合S满足相应的访问策略$\psi=(\mathbf{M},\rho)$，即$\psi(S)=1$，那么有

$$\Pr\left[M=M'\ \middle|\ ct\leftarrow\mathsf{Enc}(M,(\mathbf{M},\rho)),M'\leftarrow\mathsf{Dec}(ct,sk)\right]\le\mathsf{negl}(\kappa)$$

成立，其中$(params,msk)\leftarrow\mathsf{Setup}(1^\kappa)$和$sk\leftarrow\mathsf{KeyGen}(msk,S)$.

3.3 安全模型

为了模拟现实环境中密码原语所面临的各种泄露攻击, 在安全模型中引入泄露谕言机实现对泄露攻击的模拟, 敌手通过访问泄露谕言机获得关于秘密信息的泄露内容. 因此, 下述游戏$Exp^{LR-CPA}_{CP-ABE,\mathcal{A}}(\lambda_{sk},\kappa)$通

过为敌手 $\mathcal{A}$ 提供访问泄露谕言机 $O_{sk}^{\lambda_{sk}}(\kappa)$ 的能力达到模拟相应 CP-ABE 机制抗泄露攻击的能力. 在下述游戏 $Exp_{CP-ABE,\mathcal{A}}^{LR-CPA}(\lambda_{sk},\kappa)$ 中, 如果概率多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势获胜, 那么在存在泄露的情况下, 相应的 CP-ABE 机制拥有 LR-CPA 安全性.

$Exp_{CP-ABE,\mathcal{A}}^{LR-CPA}(\lambda_{sk},\kappa)$:

(1) $(params,msk)\rightarrow \mathsf{Setup}(1^{\kappa})$.

(2) $(\psi^*,M_0,M_1)\leftarrow \mathcal{A}^{O_{sk}^{\lambda_{sk}}(\kappa),O^{\mathsf{KeyGen}(\cdot)}}(params)$. ψ^*是挑战访问策略, 且$|M_0|=|M_1|$.

(3) $ct_b^*\leftarrow \mathsf{Enc}(\psi^*,M_b), b\leftarrow_R\{0,1\}$.

(4) $b'\leftarrow \mathcal{A}^{O_{\neq\psi^*}^{KenGen}(\cdot)}(params,ct_b^*)$

(5) *If* $b=b'$, *output* 1, *Otherwise*, *return* 0.

其中 $O_{sk}^{\lambda_{sk}}(\kappa)$ 是泄露谕言机, 表示敌手 $\mathcal{A}$ 获得任意属性集合 S （包括满足挑战访问策略 $\psi^*=(\mathbf{M}^*,\rho^*)$ 的属性集合）对应私钥 sk 的泄露信息, 但敌手 $\mathcal{A}$ 获得相同私钥的泄露信息长度不超过系统设定的泄露参数 λ_{sk}; $O^{\mathsf{KeyGen}}(\cdot)$ 表示密钥生成谕言机, 敌手 $\mathcal{A}$ 能获得任意属性集合 S 对应的私钥 sk, 并且 $O_{\neq\psi^*}^{\mathsf{KeyGen}}(\cdot)$ 表示敌手 $\mathcal{A}$ 不能获得满足挑战访问策略 ψ^* 的属性集合 S 所对应的私钥 sk.

4 支持大属性集合的高效抗泄露 CP-ABE 机制

在本节中, 本文提出素数阶群上支持大属性集合的抗泄露ABE机制的具体构造, 并基于判定的并行双线性Diffie-Hellman指数假设证明其安全性.

4.1 我们的构造

本文抗泄露 CP-ABE 机制具体包含下述四个算法.

（1）初始化算法 $(params,msk)\leftarrow \mathsf{Setup}(1^{\kappa})$ 的具体操作如下：

令 $\tilde{G}$ 是阶为 p, 生成元为 g 的乘法循环群, $\tilde{G}_T$ 是阶为 p 的乘法循环群, 满足双线性映射 $e:\tilde{G}\times\tilde{G}\rightarrow\tilde{G}_T$. 设属性全集为 $U=Z_{\mathrm{p}}$. 任意选取随机数 $u,h,w,v\leftarrow_R(\tilde{G})^4$ 和 $\alpha_1,\alpha_2,\cdots,\alpha_m\leftarrow_R(Z_p)^m$. 令主私钥为 $msk=(\alpha_1,\alpha_2,\cdots,\alpha_m)$, 其中 $m=(3\log q)^{1/\varepsilon}$（$m$ 的取值由定理 1 确定[21]）和 $0<\varepsilon<1$. 最后公开系统参数 $params=\left(g,u,v,h,w,\left\{e(g,g)^{\alpha_i}\right\}_{i=1,2,\cdots,m}\right)$.

（2）密钥生成算法 $sk\leftarrow \mathsf{KeyGen}(msk,S=\{A_1,A_2,\cdots,A_k\})$ 的具体操作如下：

任意选取随机数 $r,r_1,r_2,\cdots,r_k\leftarrow_R(Z_p)^{k+1}$（其中 $k=|S|$, 即 k 为属性集合 $S=\{A_1,A_2,\cdots,A_k\}$ 中属性的数量）, 计算 $\left\{K_i=g^{\alpha_i}w^r\right\}_{i=1,2,\cdots,m}$ 和 $K_0=g^r$. 对于 $\tau=1,2,\cdots,k$, 计算 $K_{\tau,1}=\mathrm{g}^{r_\tau}$ 和 $K_{\tau,2}=\left(u^{A_\tau}h^{r_\tau}\right)v^{-r}$. 最后输出属性集合 S 所对应的私钥 $sk=\left(S,\{K_i\}_{i=1,2,\cdots,m},K_0,\left\{K_{\tau,1},K_{\tau,2}\right\}_{\tau=1,2,\cdots,k}\right)$.

（3）加密算法 $ct\leftarrow \mathsf{Enc}(M,(\mathbf{M},\rho))$ 的具体操作如下：

输入待加密的消息 M 和访问策略 $\psi=(\mathbf{M},\rho)$, 其中 $\mathbf{M}$ 是一个 $l\times n$ 矩阵, ρ 是矩阵 $\mathbf{M}$ 的行属性映射函数. 任意选取随机数 $s_1,s_2,\cdots,s_m\leftarrow_R(Z_p)^m$ 和 $y_2,\cdots,y_n\leftarrow_R(Z_p)^{n-1}$, 并计算

$$\vec{\lambda}=(\lambda_1,\lambda_2,\cdots,\lambda_l)^{\top}=\mathbf{M}\vec{y},\ C=M\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i}\text{ 和 }\left\{C_i=g^{s_i}\right\}_{i=1,2,\cdots,m},$$

其中 $\vec{y}=\left(\sum_{i=1}^{m}s_i,y_2,\cdots,y_n\right)$ 和 $\sum_{i=1}^{m}s_i$ 是要分享的秘密值. 特别地, 向量 $\vec{\lambda}$ 协助解密者实现共享秘密的恢复.

任意选取 l 个随机数 $t_1,t_2,\cdots,t_l\leftarrow_R\left(Z_p\right)^l$, 对于 $\tau=1,2,\cdots,l$, 计算

$$C_{\tau,1}=w^{\lambda_\tau}v^{t_\tau},\ C_{\tau,2}=\left(u^{\rho(\tau)}h\right)^{-t_\tau}\text{ 和 }C_{\tau,3}=g^{t_\tau}.$$

最后输出相应的加密密文 $ct=\left(\psi=(\mathbf{M},\rho),C,\{C_i\}_{i=1,2,\cdots,m},\left\{C_{\tau,1},C_{\tau,2},C_{\tau,3}\right\}_{\tau=1,2,\cdots,l}\right)$.

（4）解密算法 $M/\perp\leftarrow\mathrm{Dec}(ct,sk)$ 的具体操作如下：

输入密文 $ct=\left(\psi=(\mathbf{M},\rho),C,\{C_i\}_{i=1,2,\cdots,m},\left\{C_{\tau,1},C_{\tau,2},C_{\tau,3}\right\}_{\tau=1,2,\cdots,l}\right)$ 及属性集合 S 对应的密钥 $sk=\left(S,\{K_i\}_{i=1,2,\cdots,m},K_0,\left\{K_{\tau,1},K_{\tau,2}\right\}_{\tau=1,2,\cdots,k}\right)$, 定义 $I=\{i:i\in[l]\wedge\rho(i)\in S\}$. 如果密钥的属性集合 S 不满足密文的访问策略 $\psi=(\mathbf{M},\rho)$, 即 $\psi(S)\neq1$, 那么输出 $\perp$; 否则有 $\psi(S)=1$, 那么存在 $\left\{\omega_i\in Z_p\right\}_{i\in I}$, 使得 $\sum_{i\in I}\omega_i\mathbf{M}_i=(1,0,\cdots,0)$ 成立, 其中 $\mathbf{M}_i$ 是矩阵 $\mathbf{M}$ 的第 i 行. 计算

$$E=\frac{\prod_{i=1}^{m}e(C_i,K_i)}{\prod_{i\in I}\left(e(C_{i,1},K_0)e(C_{i,2},K_{i,1})e(C_{i,3},K_{i,2})\right)^{\omega_i}}.$$

最后输出明文消息 $M=C/E$.

4.2 正确性

如果私钥 sk 的属性集合 S 满足密文 ct 的访问策略 $\psi=(\mathbf{M},\rho)$, 那么有 $\sum_{i\in I}\omega_iM_i=(1,0,\cdots,0)$, 本节抗泄露 CP-ABE 机制的正确性由下述等式获得.

$$\begin{aligned}E&=\frac{\prod_{i=1}^{m}e\left(g,g^{\alpha_i s_i}\right)e(g,w)^{rs_i}}{\prod_{i\in I}e(g,w)^{r\omega_i\lambda_i}\,e(g,v)^{rt_i\omega_i}\,e\left(g,u^{\rho(i)}h\right)^{-r_\tau t_i\omega_i}\,e\left(g,u^{\rho(i)}h\right)^{r_\tau t_i\omega_i}\,e(g,v)^{-rt_i\omega_i}}\\&=\frac{\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i}\,e(g,w)^{rs_i}}{e(g,w)^{r\sum_{i\in I}\omega_i\lambda_i}}=\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i}\end{aligned}$$

其中 $\sum_{i\in I}\omega_i\lambda_i=\sum_{i\in I}\omega_i\mathbf{M}_i\vec{y}=\sum_{i=1}^{m}s_i$.

4.3 安全性证明

定理 2. 如果存在概率多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 攻破上述 CP-ABE 机制的 LR-CPA 安全性, 那么存在敌手 $\mathcal{B}$ 以相同的优势解决判定的并行双线性 Diffie-Hellman 指数假设的困难性.

证明：敌手 $\mathcal{B}$ 获得判定的并行双线性 Diffie-Hellman 指数假设的公开参数 D 和挑战元组 Z, 如果 $Z=e(g,g)^{sa^{q+1}}$, 则 $\mathcal{B}$ 需输出 1 表示 Z 为判定的并行双线性 Diffie-Hellman 指数假设元组; 否则 $\mathcal{B}$ 输出 0 表

示 $Z\in G_T$，即 Z 不是判定的并行双线性 Diffie-Hellman 指数假设元组. $\mathcal{B}$ 初始化列表 L 用于记录密钥生成询问过程的应答结果 (S,sk). 敌手 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 间的消息交互过程如下所述:

（1）初始化算法. 敌手 $\mathcal{B}$ 收到敌手 $\mathcal{A}$ 意欲挑战的访问策略 $\psi^*=(\mathbf{M}^*,\rho^*)$，其中 $\mathbf{M}^*$ 是一个 $l\times n$ 矩阵，ρ^* 是矩阵 $\mathbf{M}^*$ 的行属性映射函数. $\mathcal{B}$ 选取任意的随机数 $a_1,a_2,\cdots,a_m\leftarrow_R (Z_p)^m$，对于 $i=1,2,\cdots,m$，计算 $e(g,g)^{\alpha_i}=e\left(g^a,g^{a^q}\right)\cdot e(g,g)^{a_i}$，隐含有 $\alpha_i=a^{q+1}+a_i$. 任意选取 $t_1,t_2,t_3,\cdots,t_m,\overline{v},\overline{u},\overline{h}\leftarrow_R (Z_p)^{m+3}$，$\mathcal{B}$ 计算

$$t=\sum_{i=1}^{m}t_i,\quad u=g^{\overline{u}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{tM_{j,k}^*},\quad h=g^{\overline{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{-\rho^*(j)tM_{j,k}^*},\quad w=g^a \text{ 和 } v=g^{\overline{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j}\right)^{tM_{j,k}^*}.$$

最后，敌手 $\mathcal{B}$ 公开系统参数 $params=\left(g,u,v,h,w,\left\{e(g,g)^{\alpha_i}\right\}_{i=1,2,\cdots,m}\right)$. 特别地，为保证生成挑战密文的正确性，系统建立时选取用于生成挑战密文的 m 个随机参数 $t_1,t_2,t_3,\cdots,t_m$，并基于 $t=\sum_{i=1}^{m}t_i$ 进行参数的初始化.

（2）阶段 1. 该阶段，敌手 $\mathcal{A}$ 适应性地进行多项式有界次的下述询问.

① 秘密钥询问. 敌手 $\mathcal{A}$ 对不满足挑战访问策略 $\psi^*=(\mathbf{M}^*,\rho^*)$ 的属性集合 $S=\{A_1,A_2,\cdots,A_k\}$ 进行密钥生成询问. 由于属性集合 S 不满足挑战访问结构 ψ^*，因此存在一个向量 $\vec{\omega}=(\omega_1,\omega_2,\cdots,\omega_n)^{\top}\in(Z_p)^n$（其中 $\omega_1=-1$），使得对于 $i\in I=\{i\,|\,i\in[l]\wedge\rho^*(i)\in S\}$ 有 $\langle\mathbf{M}_i^*,\vec{\omega}\rangle=0$ 成立. $\mathcal{B}$ 任意选取随机数 $\overline{r}\leftarrow_R Z_p$，通过计算 $K_0=g^{\overline{r}}\prod_{j=1}^{n}\left(g^{a^{q+1-j}}\right)^{\omega_j}$，隐含地设置了 $r=\overline{r}+\omega_1a^q+\omega_2a^{q-1}+\cdots+\omega_na^{q+1-n}=\overline{r}+\sum_{i=1}^{n}\omega_ia^{q+1-i}$.

对于 $i=1,2,\cdots,m$，敌手 $\mathcal{B}$ 计算

$$K_i=g^{a_i}\left(g^a\right)^{\overline{r}}\prod_{j=2}^{n}\left(g^{a^{q+2-j}}\right)^{\omega_j}=g^{a^{q+1}}g^{a_i}g^{a\overline{r}}\prod_{j=1}^{n}g^{\omega_ja^{q+2-j}}=g^{\alpha_i}w^r.$$

对于属性 $A_\tau\in S$（其中 τ 是 A_τ 在属性集合 S 中的下标），敌手 $\mathcal{B}$ 需要计算 $K_{\tau,1}=g^{r_\tau}$ 和 $K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}$，其中 $K_{\tau,2}$ 是由 $\left(u^{A_\tau}h\right)^{r_\tau}$ 和 v^{-r} 两个独立的部分组成，可单独进行计算. 下面将分别讨论如何计算 $\left(u^{A_\tau}h\right)^{r_\tau}$ 和 v^{-r}. 由于 $v=g^{\overline{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j}\right)^{tM_{j,k}^*}$ 和 $r=\overline{r}+\sum_{i=1}^{n}\omega_ia^{q+1-i}$，那么 v^{-r} 的计算过程如下：

$$\begin{aligned}v^{-r}&=v^{-\overline{r}}\left(g^{\overline{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}g^{ta^kM_{j,k}^*/b_j}\right)^{-\sum_{i=1}^{n}\omega_ia^{q+1-i}}=v^{-\overline{r}}\left(g^{\overline{v}}\right)^{-\sum_{i=1}^{n}\omega_ia^{q+1-i}}\left(\prod_{j=1}^{l}\prod_{k=1}^{n}g^{ta^kM_{j,k}^*/b_j}\right)^{-\sum_{i=1}^{n}\omega_ia^{q+1-i}}\\&=v^{-\overline{r}}\prod_{i=1}^{n}\left(g^{a^{q+1-i}}\right)^{-\overline{v}\omega_i}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{i=1}^{n}g^{-\omega_itM_{j,k}^*a^{q+1+k-i}/b_j}\\&=\phi\prod_{j=1}^{l}\prod_{i=1}^{n}g^{-\omega_itM_{j,i}^*a^{q+1}/b_j}=\phi\prod_{j=1}^{l}g^{-\langle\vec{\omega},\vec{M}_j^*\rangle ta^{q+1}/b_j}=\phi\prod_{j=1,\rho^*(j)\notin S}^{l}g^{-\langle\vec{\omega},\vec{M}_j^*\rangle ta^{q+1}/b_j}\end{aligned}$$

其中 $\phi=v^{-\overline{r}}\prod_{i=1}^{n}\left(g^{a^{q+1-i}}\right)^{-\overline{v}\omega_i}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{i=1,i\neq k}^{n}\left(g^{a^{q+1+k-i}/b_j}\right)^{-\omega_itM_{j,k}^*}$.

对于 ϕ，敌手 $\mathcal{B}$ 可用公开元组 D 中的相关已知参数计算获得，但剩余的 $\prod_{j=1,\rho^*(j)\notin S}^{l}g^{-\langle\vec{\omega},\vec{M}_j^*\rangle ta^{q+1}/b_j}$ 中包含了

敌手 $\mathcal{B}$ 的未知参数 $g^{a^{q+1}}$，因此只能通过计算 $\left(u^{A_\tau}h\right)^{r_\tau}$ 将其消除. 也就是说，在 $\left(u^{A_\tau}h\right)^{r_\tau}$ 的计算结果中需包含 $\prod_{j=1,\rho^*(j)\notin S}^{l} g^{\left\langle\tilde{\omega},\vec{M}_j^*\right\rangle ta^{q+1}/b_j}$，具体计算过程如下所述: 对于每一个属性 $A_\tau\in S$，敌手 $\mathcal{B}$ 随机选取 $\bar{r}_\tau\leftarrow_R Z_p$，并计算

$$K_{\tau,1}=g^{\bar{r}_\tau}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}\left(g^{b_\eta}\right)^{\frac{\bar{r}}{A_\tau-\rho^*(\eta)}}\prod_{i=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}\left(g^{b_\eta a^{q+1-i}}\right)^{\frac{\omega_i}{A_\tau-\rho^*(\eta)}}=g^{\bar{r}_\tau}g^{\bar{r}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}}g^{\sum\limits_{i=1}^{n}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta\omega_i a^{q+1-i}}{A_\tau-\rho^*(\eta)}}$$

$$=g^{\bar{r}_\tau+\bar{r}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}+\sum\limits_{i=1}^{n}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta\omega_i a^{q+1-i}}{A_\tau-\rho^*(\eta)}}=g^{\bar{r}_\tau+\left(\bar{r}+\sum\limits_{i=1}^{n}\omega_i a^{q+1-i}\right)\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}}$$

$$=g^{\bar{r}_\tau+r\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}}$$

$$=g^{r_\tau}$$

其中 $\rho^*(i)\notin S$ 保证 $A_\tau-\rho^*(i)\neq 0$ 成立. 特别地，敌手 $\mathcal{B}$ 通过计算 $K_{\tau,2}=g^{r_\tau}$ 隐含地设置了

$$r_\tau=\bar{r}_\tau+r\sum_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}=\bar{r}_\tau+\bar{r}\sum_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}+\sum_{i=1}^{n}\sum_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta\omega_i a^{q+1-i}}{A_\tau-\rho^*(\eta)}.$$

下面敌手 $\mathcal{B}$ 计算 $K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}$，并且通过对 $\left(u^{A_\tau}h\right)^{r_\tau}$ 的计算，消除 v^{-r} 中的未知项 $\prod_{j=1,\rho^*(j)\notin S}^{l} g^{-\left\langle\tilde{\omega},\vec{M}_j^*\right\rangle ta^{q+1}/b_j}$. 特别地，敌手 $\mathcal{B}$ 由已知参数计算可知

$$u^{A_\tau}h=\left(g^{\bar{u}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{tM_{j,k}^*}\right)^{A_\tau}g^{\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{-\rho^*(j)tM_{j,k}^*}=g^{\bar{u}A_\tau+\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{\left(A_\tau-\rho^*(j)\right)tM_{j,k}^*}$$

$$K_{\tau,2}/g^{\bar{r}_\tau}=g^{r\sum\limits_{i=1,\rho^*(i)\notin S}^{l}\frac{b_i}{A_\tau-\rho^*(i)}}=g^{\bar{r}\sum\limits_{i\in[l],\rho^*(i)\notin S}^{l}\frac{b_i}{A_\tau-\rho^*(i)}+\sum\limits_{i\in[l],\rho^*(i)\notin S}^{l}\frac{\omega_i b_i a^{q+1-i}}{A_\tau-\rho^*(i)}}$$

对于属性 $A_\tau\in S$，敌手 $\mathcal{B}$ 计算

$$\left(u^{A_\tau}h\right)^{r_\tau}=\left(u^{A_\tau}h\right)^{\bar{r}_\tau+\bar{r}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}+\sum\limits_{i=1}^{n}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta\omega_i a^{q+1-i}}{A_\tau-\rho^*(\eta)}}$$

$$=\left(u^{A_\tau}h\right)^{\bar{r}_\tau}\left(g^{\bar{u}A_\tau+\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{\left(A_\tau-\rho^*(j)\right)tM_{j,k}^*}\right)^{\bar{r}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}+\sum\limits_{i=1}^{n}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta\omega_i a^{q+1-i}}{A_\tau-\rho^*(\eta)}}$$

$$=\left(u^{A_\tau}h\right)^{\bar{r}_\tau}\left(K_{\tau,2}/g^{\bar{r}_\tau}\right)^{\bar{u}A_\tau+\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}\left(g^{a^k b_\eta/b_j^2}\right)^{\bar{r}\left(A_\tau-\rho^*(j)\right)tM_{j,k}^*/\left(A_\tau-\rho^*(\eta)\right)}$$

$$\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{i=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}\left(g^{a^{q+1+k-i}b_i/b_j^2}\right)^{\left(A_\tau-\rho^*(j)\right)\omega_i tM_{j,k}^*/\left(A_\tau-\rho^*(\eta)\right)}$$

$$=\left(u^{A_\tau}h\right)^{\bar{r}_\tau}\left(K_{\tau,2}/g^{\bar{r}_\tau}\right)^{\bar{u}A_\tau+\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}g^{\bar{r}\left(A_\tau-\rho^*(j)\right)M_{j,k}^*b_\eta ta^k/\left(A_\tau-\rho^*(\eta)\right)b_j^2}$$

$$\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{i=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}g^{\left(A_\tau-\rho^*(j)\right)\omega_i M_{j,k}^*b_i ta^{q+1+k-i}/\left(A_\tau-\rho^*(\eta)\right)b_j^2}$$

$$=\psi\prod_{i=1}^{n}\prod_{j=1,\rho^*(j)\notin S}^{l}g^{\left(A_\tau-\rho^*(j)\right)\omega_i M_{j,i}^*b_j ta^{q+1+i-i}/\left(A_\tau-\rho^*(j)\right)b_j^2}=\psi\prod_{j=1,\rho^*(j)\notin S}^{l}g^{\left\langle\tilde{\omega},\vec{M}_j^*\right\rangle ta^{q+1}/b_j}$$

其中

$$\psi=\left(u^{A_\tau}h\right)^{\overline{r}_\tau}\left(K_{\tau,2}/g^{\overline{r}_\tau}\right)^{\overline{u}A_\tau+\overline{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}g^{\overline{r}\left(A_\tau-\rho^*(j)\right)M^*_{j,k}b_\eta ta^k/\left(A_\tau-\rho^*(\eta)\right)b_j^2}$$
$$\prod_{j=1}^{l}\prod_{k=1,k\neq i}^{n}\prod_{i=1}^{n}\prod_{\eta=1,\eta\neq j,\rho^*(\eta)\notin S}^{l}g^{\left(A_\tau-\rho^*(j)\right)\omega_i M^*_{j,k}b_i ta^{q+1+k-i}/\left(A_\tau-\rho^*(\eta)\right)b_j^2}$$
$$=\left(u^{A_\tau}h\right)^{\overline{r}_\tau}\left(K_{\tau,2}/g^{\overline{r}_\tau}\right)^{\overline{u}A_\tau+\overline{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}\left(g^{a^k b_i/b_j^2}\right)^{\overline{r}\left(A_\tau-\rho^*(j)\right)tM^*_{j,k}/\left(A_\tau-\rho^*(i)\right)}$$
$$\prod_{j=1}^{l}\prod_{k=1,k\neq i}^{n}\prod_{i=1}^{n}\prod_{\eta=1,\eta\neq j,\rho^*(\eta)\notin S}^{l}\left(g^{a^{q+1+k-i}b_i/b_j^2}\right)^{\left(A_\tau-\rho^*(j)\right)\omega_i tM^*_{j,k}/\left(A_\tau-\rho^*(i)\right)}$$

特别地，敌手 $\mathcal{B}$ 可用公开元组 D 中的相关已知参数计算获得 ψ. 因此有 $K_{\tau,3}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}=\psi\varphi$. 最后，敌手 $\mathcal{B}$ 将 (S,sk) 存入列表 L 中，并将 $sk=\left(S,\{K_i\}_{i=1,2,\cdots,m},K_0,\{K_{\tau,1},K_{\tau,2}\}_{\tau=1,2,\cdots,k}\right)$ 返回给敌手 $\mathcal{A}$.

② 泄露询问. 敌手 $\mathcal{A}$ 将 $\left(S,f_i:\{0,1\}^*\to\{0,1\}^{\lambda_i}\right)$ 发送给敌手 $\mathcal{B}$，其中 S 是相应的属性集合（S 可满足挑战访问策略 $\psi^*=(\mathbf{M}^*,\rho^*)$），$f_i:\{0,1\}^*\to\{0,1\}^{\lambda_i}$ 是高效可计算的泄露函数. 若 $(S,sk)\in L$，将 $f_i(sk)$ 返回给敌手 $\mathcal{A}$. 特别地，敌手 $\mathcal{A}$ 关于同一属性集合 S 的泄露询问获得的相应私钥泄露信息的最大长度为 λ_{sk}，即对属性集合 S 进行 n 次泄露询问后，有 $\sum_{i=1}^{n}\lambda_i\le\lambda_{sk}$ 成立. 否则（即 $(S,sk)\notin L$），对属性集合 S 进行私钥生成询问后将相应的泄露信息 $f_i(sk)$ 返回给敌手 $\mathcal{A}$. 特别地，若集合 S 满足挑战访问策略 $\psi^*=(\mathbf{M}^*,\rho^*)$，则敌手 $\mathcal{B}$ 可以使用与密钥生成算法相类似的方法输出该属性集合对应的私钥 sk.

（3）挑战. 敌手 $\mathcal{A}$ 向 $\mathcal{B}$ 提交两个等长的挑战消息 M_0 和 M_1. 敌手 $\mathcal{B}$ 随机选取 $\beta\leftarrow_R\{0,1\}$，计算

$$C=M_\beta\prod_{i=1}^{m}Z^{t_i}e\left(g,\left(g^s\right)^{t_i}\right)^{a_i}\text{ 和 }C_i=\left(g^s\right)^{t_i}\ (i=1,2,\cdots,m).$$

隐含地设置了 $s_1=t_1s$，$s_2=t_2s$，…，$s_n=t_ms$. 敌手 $\mathcal{B}$ 随机选取 $\overline{y}_2,\overline{y}_3,\cdots,\overline{y}_n\leftarrow_R\left(Z_p\right)^{n-1}$，计算 $\tilde{\lambda}=\sum_{i=2}^{n}M^*_{\tau,i}\overline{y}_i$（其中 $\tilde{\lambda}$ 是敌手 $\mathcal{B}$ 完全可计算的）. 对于 $\tau=1,2,\cdots,l$，敌手 $\mathcal{B}$ 计算

$$C_{\tau,1}=w^{\tilde{\lambda}_\tau}\left(g^{sb_\tau}\right)^{-\overline{v}}\prod_{j=1,j\neq\tau}^{l}\prod_{k=1}^{n}\left(g^{sa^kb_\tau/b_j}\right)^{-tM^*_{j,k}}$$
$$C_{\tau,2}=\left(g^{sb_\tau}\right)^{-\left(\overline{u}\rho^*(\tau)+\overline{h}\right)}\prod_{j=1,j\neq\tau}^{l}\prod_{k=1}^{n}\left(g^{sa^kb_\tau/b_j^2}\right)^{-\left(\rho^*(\tau)-\rho^*(j)\right)M^*_{j,k}}$$
$$C_{\tau,3}=\left(g^{sb_\tau}\right)^{-1}$$

令 $t_\tau=-sb_\tau$，$\tilde{\lambda}=\sum_{i=2}^{n}M^*_{\tau,i}\overline{y}_i$ 和 $\lambda_\tau=\tilde{\lambda}+\sum_{i=1}^{n}M^*_{\tau,i}tsa^{i-1}$，由下述分析可知，$C_{\tau,1},C_{\tau,2}$ 和 $C_{\tau,3}$ 是本文抗泄露 ABE 机制正常形式的密文元素.

$$
\begin{aligned}
C_{\tau,1} &= w^{\tilde{\lambda}_\tau}\left(g^{sb_\tau}\right)^{-\bar{v}}\prod_{j=1,j\neq\tau}^{l}\prod_{k=1}^{n}\left(g^{sa^k b_\tau/b_j}\right)^{-tM^*_{j,k}}\\
&= w^{\tilde{\lambda}_\tau}\left(g^{sb_\tau}\right)^{-\bar{v}}\prod_{i=1}^{n}g^{tM^*_{\tau,i}sa^i}\prod_{k=1}^{n}g^{-tM^*_{\tau,k}a^k sb_\tau/b_\tau}\prod_{j=1,j\neq\tau}^{l}\prod_{k=1}^{n}g^{-tM^*_{j,k}a^k sb_\tau/b_j}\\
&= w^{\tilde{\lambda}_\tau}\left(g^{sb_\tau}\right)^{-\bar{v}}\prod_{i=1}^{n}g^{tM^*_{\tau,i}sa^i}\prod_{j=1}^{l}\prod_{k=1}^{n}g^{-tM^*_{j,k}a^k sb_\tau/b_j} = w^{\tilde{\lambda}_\tau}\prod_{i=1}^{n}g^{tM^*_{\tau,i}sa^i}\left(g^{\bar{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}g^{t_k M^*_{j,k}a^k/b_j}\right)^{-sb_\tau}\\
&= w^{\tilde{\lambda}_\tau}\prod_{i=1}^{n}\left(g^{a}\right)^{tM^*_{\tau,i}sa^{i-1}}\left(g^{\bar{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j}\right)^{tM^*_{j,k}}\right)^{-sb_\tau} = w^{\tilde{\lambda}_\tau+\sum_{i=1}^{n}tM^*_{\tau,i}sa^{i-1}}\left(g^{\bar{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j}\right)^{tM^*_{j,k}}\right)^{-sb_\tau}\\
&= w^{\lambda_\tau}v^{t_\tau}\\
C_{\tau,2} &= \left(g^{sb_\tau}\right)^{-\left(\bar{u}\rho^*(\tau)+\bar{h}\right)}\prod_{j=1,j\neq\tau}^{l}\prod_{k=1}^{n}\left(g^{sa^k b_\tau/b_j^2}\right)^{-\left(\rho^*(\tau)-\rho^*(j)\right)tM^*_{j,k}}\\
&= \left(g^{sb_\tau}\right)^{-\left(\bar{u}\rho^*(\tau)+\bar{h}\right)}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{\left(\rho^*(\tau)-\rho^*(j)\right)tM^*_{j,k}a^k/b_j^2}\right)^{-sb_\tau}\\
&= \left(g^{\bar{u}\rho^*(\tau)}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{tM^*_{j,k}\rho^*(\tau)}g^{\bar{h}}\prod_{j=1,}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)g^{-\rho^*(j)tM^*_{j,k}}\right)^{-sb_\tau}\\
&= \left(\left(g^{\bar{u}}\prod_{j=1,}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{tM^*_{j,k}}\right)^{\rho^*(\tau)}g^{\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)g^{-\rho^*(j)tM^*_{j,k}}\right)^{-sb_\tau}\\
&= \left(u^{\rho^*(\tau)}h\right)^{-t_\tau}\\
C_{\tau,3} &= \left(g^{sb_\tau}\right)^{-1} = g^{t_\tau}
\end{aligned}
$$

其中敌手 $\mathcal{B}$ 隐含地设置了 $\vec{y}=\left(ts, tsa+\tilde{y}_2,\cdots,tsa^{n-1}+\tilde{y}_n\right)$. 由于 $\vec{\lambda}=\left(\lambda_1,\lambda_2,\cdots,\lambda_l\right)^{\top}=\mathbf{M}^*\vec{y}$，因此，对于 $\tau=1,2,\cdots,l$，有 $\lambda_\tau=\sum_{i=1}^{n}\mathbf{M}^*_{\tau,i}tsa^{i-1}+\sum_{i=2}^{n}\mathbf{M}^*_{\tau,i}\tilde{y}_i$，其中 $\mathbf{M}^*_{\tau,i}$ 是矩阵 $\mathbf{M}^*$ 的第 τ 行第 j 列的元素.

最后，敌手 $\mathcal{B}$ 发送挑战密文 $ct=\left(\psi^*=\left(\mathbf{M}^*,\rho^*\right),C,\left\{C_i\right\}_{i=1,2,\cdots,m},\left\{C_{\tau,1},C_{\tau,2},C_{\tau,3}\right\}_{\tau=1,2,\cdots,l}\right)$ 给敌手 $\mathcal{A}$.

（4）阶段二. 该阶段与阶段一相类似，敌手 $\mathcal{B}$ 以相同的方式应答敌手 $\mathcal{A}$ 的密钥生成询问，但该阶段禁止敌手 $\mathcal{A}$ 进行泄露询问.

（5）猜测. 敌手 $\mathcal{A}$ 输出对随机数 β 的猜测 β'. 若 $\beta=\beta'$，则敌手 $\mathcal{B}$ 输出 1，表示 $Z=e\left(g,g\right)^{sa^{q+1}}$；否则，敌手 $\mathcal{B}$ 输出 0，表示 $Z=e\left(g,g\right)^{sa^{q+1}+\eta}$，其中 η 是 Z_p 上的随机值，即 Z 是群 G_T 上的随机元素.

① 若 $Z=e\left(g,g\right)^{sa^{q+1}}$，有

$$
\begin{aligned}
C &= M_\beta\prod_{i=1}^{m}Z^{t_i}e\left(g,\left(g^s\right)^{t_i}\right)^{a_i} = M_\beta\prod_{i=1}^{m}e\left(g,g\right)^{st_ia^{q+1}}e\left(g,\left(g^s\right)^{t_i}\right)^{a_i}\\
&= M_\beta\prod_{i=1}^{m}e\left(g,g\right)^{st_i\left(a^{q+1}+a_i\right)} = M_\beta\prod_{i=1}^{m}e\left(g,g\right)^{\alpha_i s_i}
\end{aligned}
$$

则敌手 $\mathcal{A}$ 获得了关于消息 M_β 的有效加密密文 ct. 若敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 攻破本文 CP-ABE 机制的 LR-CPA 安全性，那么敌手 $\mathcal{B}$ 能以同样的优势输出 1. 即

$$\Pr\left[\mathcal{B}\left(D,Z=e\left(g,g\right)^{sa^{q+1}}\right)=1\right]=\frac{1}{2}+\varepsilon\,.$$

②若 $Z=e(g,g)^{sa^{q+1}+\eta}$，则有

$$\begin{aligned}C&=M_\beta\prod_{i=1}^{m}Z^{t_i}e\left(g,\left(g^s\right)^{t_i}\right)^{a_i}=M_\beta\prod_{i=1}^{m}e\left(g,g\right)^{st_ia^{q+1}+t_i\eta}e\left(g,\left(g^s\right)^{t_i}\right)^{a_i}\\&=M_\beta\prod_{i=1}^{m}e\left(g,g\right)^{st_i\left(a^{q+1}+a_i\right)}e\left(g,g\right)^{t_i\eta}=M_\beta\prod_{i=1}^{m}e\left(g,g\right)^{\alpha_is_i}e\left(g,g\right)^{t_i\eta}\\&=M_\beta e\left(g,g\right)^{\eta\sum_{i=1}^{m}t_i}\prod_{i=1}^{m}e\left(g,g\right)^{\alpha_is_i}=M_\beta e\left(g,g\right)^{\eta t}\prod_{i=1}^{m}e\left(g,g\right)^{\alpha_is_i}\end{aligned}$$

则敌手 $\mathcal{A}$ 获得了关于随机消息 $M_\beta e(g,g)^{\eta t}$ 的有效加密密文 ct，即挑战密文 ct 中不包含随机数 β 的任何信息，那么敌手 $\mathcal{B}$ 以 $\frac{1}{2}$ 的概率输出 1. 即

$$\Pr\left[\mathcal{B}\left(D,Z\in G_T\right)=1\right]=\frac{1}{2}\,.$$

综上所述, 如果存在多项式时间的敌手 $\mathcal{A}$ 能以不可忽略的优势 ε 攻破本文 CP-ABE 机制的 LR-CPA 安全性, 那么存在敌手 $\mathcal{B}$ 以同样的优势 ε 解决判定的并行双线性 Diffie-Hellman 指数假设的困难性.

4.4 抗泄露性分析

在上述 CP-ABE 机制的 LR-CPA 安全性证明中, 敌手 $\mathcal{A}$ 通过概率多项式次的泄露询问获得了关于属性集合 S 对应私钥 $sk=\left(S,\left\{K_i=g^{\alpha_i}w^r\right\}_{i=1,2,\cdots,m},K_0,\left\{K_{\tau,1},K_{\tau,2}\right\}_{\tau=1,2,\cdots,k}\right)$ 的泄露信息 $f(sk)$，由于 sk 的核心信息是主私钥 $msk=(\alpha_1,\alpha_2,\cdots,\alpha_m)$，因此敌手 $\mathcal{A}$ 通过泄露询问获得了关于主私钥 $msk=\vec{\alpha}$ 的泄露信息 $\tilde{f}(\vec{\alpha})$. 一般情况下, 泄露信息 $\tilde{f}(\vec{\alpha})$ 的获得会增加敌手 $\mathcal{A}$ 在上述游戏中获胜的优势, 除非泄露信息不影响对加密算法中隐藏明文操作所使用元素的随机性, 下面将分析主私钥的泄露信息 $\tilde{f}(\vec{\alpha})$ 对用于隐藏明文的元素 $\prod_{i=1}^{m}e(g,g)^{\alpha_is_i}$ 的随机性是没有影响的.

已知密文中对消息 M 的隐藏操作为 $C=M\prod_{i=1}^{m}e(g,g)^{\alpha_is_i}=Me(g,g)^{\sum_{i=1}^{m}\alpha_is_i}$，由定理1可知，已知相应的参数为 $\vec{\alpha}=(\alpha_1,\alpha_2,\cdots,\alpha_n)$ 和 $\vec{s}=(s_1,s_2,\cdots,s_n)$，对于任意的概率多项式时间敌手 $\mathcal{A}$，有关系

$$\left|\Pr\left[\mathcal{A}\left(y,r,\langle r,s\rangle\right)=1\right]-\Pr\left[\mathcal{A}\left(y,r,u\right)=1\right]\right|=\varepsilon$$

成立, 其中 ε 是安全参数上可忽略的值和 $y=\tilde{f}(\vec{\alpha})$ 为关于主私钥的泄露信息. 由定理1可知，$\prod_{i=1}^{m}e(g,g)^{\alpha_is_i}$ 与群 $\tilde{G}_T$ 上的均匀随机元素是不可区分的, 因此实现了对消息 M 的完美隐藏, 即使敌手获得了关于主私钥的泄露信息 $y=\tilde{f}(\vec{\alpha})$，密文元素 $C=M\prod_{i=1}^{m}e(g,g)^{\alpha_is_i}$ 依然保持与均匀随机值间的不可区分性. 因此即使敌手 $\mathcal{A}$ 获得了相应的泄露信息, 上述CP-ABE机制依然保持其所声称的LR-CPA安全性, 即在相应的安全性游戏中敌手无法以不可忽略的优势获知挑战密文所对应的原始明文, 即使是1比特的信息也无法掌握.

4.5 性能分析

在本节中, 将本文方案与现有的抗泄露ABE机制进行综合分析和对比, 结果表明本文方案实现了更高的计算效率, 更适合在现实应用中使用. 本节用 l 表示属性集合中的属性数量, 且 $m=\left(3\log p_2\right)^{1/\varepsilon}$.

（1）计算效率

首先对计算效率进行了比较, 结果如表1所示, 本节方案具有较高的计算效率, 其中 T_E 表示模指数运算, T_P 表示循环群上的乘法运算, T_B 表示双线性映射操作. 特别地, 本文方案的相关运算是在素数阶群中完成的, 而对比方案[20-22]中的相关运算是在合数阶群中实现的, 由于素数阶群上的各运算的计算效率要优于合数阶群上的, 因此由表1可知本节所提方案的计算效率较高.

表1 本文方案与相关抗泄露ABE机制的计算效率比较结果

方案	密钥生成算法	加密算法	解密算法
Guo 等人的机制[20]	$(4m+2+2l)T_E+(4m+l+1)T_P$	$(2m+3l)T_E+lT_P$	$3T_B$
Ma 等人的机制[21]	$2mT_E$	$(m+2l+2lm)T_E+(2m+1)T_P$	$4T_B$
Li 等人的机制[22]	$(2m+5+6l)T_E+(m+4l+4)T_P$	$(m+2+5l)T_E+2lT_P$	$4T_B$
本节方案	$(m+3+3l)T_E+2mT_P$	$(2m+2l)T_E+2lT_P$	$4T_B$

（2）存储与通信效率

本文方案与相关ABE机制的存储和通信效率的比较结果如表2所示, 其中 $|\tilde{G}_T|$ 表示乘法群上元素的长度, $|\tilde{G}|$ 表示加法群上元素的长度. 本文通过公开参数的大小来比较存储效率. 由表2可知本文方案的公开参数大小不随着属性的数量的变化而变化, 不与属性集合的大小构成线性关系, 因此本文方案实现了更高的存储效率, 可以应用在大属性域的环境中. 另外, 本文通过密文的长度比较通信效率, 本文方案的通信效率与已有方案基本持平. 综上所述, 本文方案与现有抗泄露ABE方案相比具有较高的存储和通信效率. 特别地, 文献[21]是多属性权威环境下的抗泄露ABE机制, 其公开参数只有全局身份, 因此它的公开参数大小与属性集合的大小 l 无关.

表2 本文方案与相关抗泄露ABE机制的性能比较结果

方案	存储效率	通信效率	是否支持大属性集合
Guo 等人的机制[20]	$1\left\|\tilde{G}_T\right\|+(3+2m+l)\left\|\tilde{G}\right\|$	$(2l+m+1)\left\|\tilde{G}\right\|$	不支持
Ma 等人的机制[21]	$2m\left\|\tilde{G}\right\|$	$(3lm+1)\left\|\tilde{G}\right\|$	不支持
Li 等人的机制[22]	$(1+m+l)\left\|\tilde{G}_T\right\|+m\left\|\tilde{G}\right\|$	$(3l+m+2)\left\|\tilde{G}\right\|$	不支持
本节方案	$(m+5)\left\|\tilde{G}\right\|$	$(3l+m+1)\left\|\tilde{G}\right\|$	支持

5 基于静态假设的支持大属性集的抗泄露 CP-ABE 机制

虽然上一节所提出的抗泄露CP-ABE机制实现了对大属性集合的支持, 但该方案的安全性是在非静态的复杂性假设上被证明的; 此外, 现有基于静态安全性假设构造的抗泄露CP-ABE机制均不支持大属性集合. 因此, 针对上述问题, 本节提出了基于静态假设的支持大属性集的抗泄露CP-ABE机制的具体构造, 并基于相应的静态安全性假设证明了该构造的安全性.

5.1 具体构造

（1）初始化算法 $(params, msk) \leftarrow \mathsf{Setup}(1^{\kappa})$ 的具体操作如下：

令乘法循环群 G 和 G_T 的阶为 $N = p_1 p_2 p_3$，满足双线性映射 $e: G \times G \to G_T$. 群 G_1， G_2 和 G_3 是群 G 的三个子群，且 p_i 是子群 G_i 的阶，令 g_1 是群 G_1 的生成元， g_2 是群 G_2 的生成元， g_3 是群 G_3 的生成元，属性全集是 $U = Z_{\mathrm{p}}$. 任意选取随机数 $w, u, h, v \leftarrow_R (G_1)^4$, $X_3 \leftarrow_R G_3$ 和 $\alpha_1, \alpha_2, \cdots, \alpha_m \leftarrow_R (Z_p)^m$，令 $msk = (\alpha_1, \alpha_2, \cdots, \alpha_m)$，其中 $m = (3\log q)^{1/\varepsilon}$ 和 $0 < \varepsilon < 1$. 最后公开系统参数 $params = \left(g_1, X_3, u, w, h, v, \left\{e(g_1, g_1)^{\alpha_i}\right\}_{i=1,2,\cdots,m}\right)$.

（2）密钥生成算法 $sk \leftarrow \mathsf{KeyGen}(msk, S = \{A_1, A_2, \cdots, A_k\})$ 的具体操作如下：

对于 $i = 1, 2, \cdots, m$，任意选取 $R, \tilde{R}_1, \tilde{R}_2, \cdots, \tilde{R}_m \leftarrow_R (G_3)^{m+1}$ 和 $r \leftarrow_R Z_p$，计算

$$\left\{K_i = g_1^{\alpha_i} w^r \tilde{R}_i\right\}_{i=1,2,\cdots,m} \text{ 和 } K_0 = g_1^r R.$$

随机选取 $r_1, r_2, \cdots, r_k \leftarrow_R (Z_p)^k$ 和 $R_1, R_2, \cdots, R_k, \bar{R}_1, \bar{R}_2, \cdots, \bar{R}_k \leftarrow_R (G_3)^{2k}$，对于 $\tau = 1, 2, \cdots, k$，计算

$$K_{\tau,1} = g_1^{r_\tau} R_\tau \text{ 和 } K_{\tau,2} = \left(u^{A_\tau} h\right)^{r_\tau} v^{-r} \bar{R}_\tau.$$

最后输出属性集合 $S = \{A_1, A_2, \cdots, A_k\}$ 所对应的私钥 $sk = \left(S, \{K_i\}_{i=1,2,\cdots,m}, K_0, \{K_{\tau,1}, K_{\tau,2}\}_{\tau=1,2,\cdots,k}\right)$.

（3）加密算法 $ct \leftarrow \mathsf{Enc}(M, (M, \rho))$ 的具体操作如下.

输入待加密的消息 M 和访问策略 $\psi = (\mathbf{M}, \rho)$，其中 $\mathbf{M}$ 是一个 $l \times n$ 矩阵， ρ 是 $\mathbf{M}$ 的行属性映射函数. 任意选取随机数 $s_1, s_2, \cdots, s_m \leftarrow_R (Z_p)^m$ 和 $y_2, \cdots, y_n \leftarrow_R (Z_p)^{n-1}$，计算

$$\vec{\lambda} = (\lambda_1, \lambda_2, \cdots, \lambda_l)^{\top} = \mathbf{M}\vec{y}, \quad C = M \prod_{i=1}^{m} e(g_1, g_1)^{\alpha_i s_i} \text{ 和 } \left\{C_i = g_1^{s_i}\right\}_{i=1,2,\cdots,m}.$$

其中 $\vec{y} = \left(\sum_{i=1}^{m} s_i, y_2, \cdots, y_n\right)$. 任意选取随机数 $t_1, t_2, \cdots, t_l \leftarrow_R (Z_p)^l$，对于 $\tau = 1, 2, \cdots, l$，计算

$$C_{\tau,1} = w^{\lambda_\tau} v^{t_\tau}, \quad C_{\tau,2} = \left(u^{\rho(\tau)} h\right)^{-t_\tau} \text{ 和 } C_{\tau,3} = g_1^{t_\tau}.$$

最后输出相应的加密密文 $ct = \left(\psi = (\mathbf{M}, \rho), C, \{C_i\}_{i=1,2,\cdots,m}, \{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\}_{\tau=1,2,\cdots,l}\right)$.

（4）解密算法 $M \leftarrow \mathsf{Dec}(ct, sk)$ 的具体操作如下：

输入密文 $ct = \left(\psi = (\mathbf{M}, \rho), C, \{C_i\}_{i=1,2,\cdots,m}, \{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\}_{\tau=1,2,\cdots,l}\right)$，属性集合 S 对应的密钥 $sk = \left(S, \{K_i\}_{i=1,2,\cdots,m}, K_0, \{K_{\tau,1}, K_{\tau,2}\}_{\tau=1,2,\cdots,k}\right)$，定义 $I = \{i : \rho(i) \in S\}$. 令 $\{\omega_i \in Z_p\}_{i \in I}$，如果属性集合 S 满足访问策略 $\psi = (\mathbf{M}, \rho)$，那么有 $\sum_{i \in I} \omega_i \mathbf{M}_i = (1, 0, \cdots, 0)$ 成立，其中 $\mathbf{M}_i$ 是矩阵 $\mathbf{M}$ 的第 i 行. 计算

$$E=\frac{\prod_{i=1}^{m}e(C_i,K_i)}{\prod_{i\in I}\left(e(C_{i,1},K_0)e(C_{i,2},K_{i,1})e(C_{i,3},K_{i,2})\right)^{\omega_i}}$$

其中 i 是属性 $\rho(i)$ 在属性集合 S 中的索引. 最后输出相应的明文消息 $M=C/E$.

5.2 正确性

如果属性集合 S 满足访问策略 $\psi=(\mathbf{M},\rho)$, 那么 $\sum_{i\in I}\omega_i\mathbf{M}_i=(1,0,\cdots,0)$ 和 $\sum_{i\in I}\omega_i\lambda_i=s_i$, 本节抗泄露 CP-ABE 机制的正确性由下述等式获得.

$$\begin{aligned}E&=\frac{\prod_{i=1}^{m}e\left(g_1^{s_i},g_1^{\alpha_i}w^rR_\eta\right)}{\prod_{i\in I}\left(e\left(w^{\lambda_i}v^{t_i},g_1^rR\right)e\left(\left(u^{\rho(i)}h\right)^{-t_i},g_1^{r_i}R_i\right)e\left(g_1^{t_i},\left(u^{A_i}h\right)^{r_i}v^{-r}R_i\right)\right)^{\omega_i}}\\&=\frac{\prod_{i=1}^{m}e(g_1,g_1)^{\alpha_is_i}\,e(g_1,w)^{rs_i}}{\prod_{i\in I}e(g_1,w)^{r\omega_i\lambda_i}\,e(g_1,v)^{rt_i\omega_i}\,e\left(g_1,u^{\rho(i)}h\right)^{-r_it_i\omega_i}\,e\left(g_1,u^{\rho(i)}h\right)^{r_it_i\omega_i}\,e(g_1,v)^{-rt_i\omega_i}}\\&=\frac{\prod_{i=1}^{m}e(g_1,g_1)^{\alpha_is_i}\,e(g_1,w)^{rs_i}}{e(g_1,w)^{r\sum_{i\in I}\omega_i\lambda_i}}=\prod_{i=1}^{m}e(g_1,g_1)^{\alpha_is_i}\end{aligned}$$

5.3 安全性证明

本文基于一系列游戏证明上述 CP-ABE 机制的 LR-CPA 安全性. 令 $\psi^*=(\mathbf{M}^*,\rho^*)$ 为挑战的访问结构, 且游戏中概率多项式时间敌手 $\mathcal{A}$ 无法对满足挑战访问策略 $\psi^*=(\mathbf{M}^*,\rho^*)$ 的属性集合 S 进行密钥生成询问. 首先本文将分别给出半功能密文和半功能密钥的具体定义.

（1）半功能密文的形式为（红色部分为半功能形式与正常形式的区别）:

$$ct_{sf}=\left(C=M\prod_{i=1}^{m}e(g_1,g_1)^{\alpha_is_i},\left\{C_i=g_1^{s_i}\,g_2^{c_i}\right\}_{i=1,2,\cdots,m},\left\{C_{\tau,1}=w^{\lambda_\tau}v^{t_\tau}\,g_2^{d_\tau},C_{\tau,2}=\left(u^{\rho(\tau)}h\right)^{-t_\tau},C_{\tau,3}=g_1^{t_\tau}\right\}_{\tau=1,2,\cdots,l}\right)$$

其中 $c_1,c_2,\cdots,c_m\leftarrow(Z_p)^m$ 和 $d_1,d_2,\cdots,d_l\leftarrow(Z_p)^l$.

（2）第 I 型的半功能密钥为:

$$sk_{sf}^1=\left(\left(K_i=g_1^{\alpha_i}w^rg_2^{z_i}R_\eta\right)_{i=1,2,\cdots,m},K_0=g_1^rg_2^xR,\left\{K_{\tau,1}=g_1^{r_\tau}R_\tau,K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}R_\tau\right\}_{\tau=1,2,\cdots,k}\right)$$

其中 $z_1,z_2,\cdots,z_m\leftarrow(Z_p)^m$ 和 $x\leftarrow Z_p$.

（3）第 II 型的半功能密钥为:

$$sk_{sf}^2=\left(\left(K_i=g_1^{\alpha_i}w^rR_\eta\right)_{i=1,2,\cdots,m},K_0=g_1^rg_2^\mu R,\left\{K_{\tau,1}=g_1^{r_\tau}R_\tau,K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}R_\tau\right\}_{\tau=1,2,\cdots,k}\right)$$

其中 $\mu\leftarrow Z_p$. 安全性证明时密钥的形式应为第 II 型的半功能密钥, 由于相应的复杂性假设无法直接证明

正常密钥与第 II 型半功能密钥是不可区分的, 因此设置了第 I 型的半功能密钥作为过渡形式以实现上述证明. 由于第 I 型半功能密钥空间中存在可以正常解密半功能密文的个体（称这样的半功能密钥为名义半功能密钥）, 因此它不能作为本节方案安全性证明时半功能密钥的最终形式. 特别地，文献[16]详细解释了即使名义的第 I 型半功能密钥能够解密半功能密文，但解密结果并不会增加敌手在游戏中获胜的优势，即敌手在前后两个游戏中的视图是不可区分的.

各游戏的具体过程定义如下:

游戏 $Game_{real}$: 该游戏是原始的 LR-CPA 安全性游戏 $Exp_{CP-ABE,\mathcal{A}}^{LR-CPA}\left(\lambda_{sk},\kappa\right)$, 在该游戏中, 挑战密文与密钥生成询问的应答都是正常形式的, 即在该游戏中概率多项式时间敌手 $\mathcal{A}$ 获得了正常形式的挑战密文和私钥, 因此敌手 $\mathcal{A}$ 在该游戏中获胜的优势就是相应的敌手在实验 $Exp_{CP-ABE,\mathcal{A}}^{LR-CPA}\left(\lambda_{sk},\kappa\right)=1$ 中获胜的优势.

游戏 $Game_{res}$: 该游戏与游戏 $Game_{real}$ 相类似，但在 $Game_{res}$ 中，敌手 $\mathcal{A}$ 不能对满足条件 $S=S^{*} \bmod N$ 和 $S=S^{*} \bmod p_2$ 的属性集合 S 进行密钥生成询问, 其中 S^{*} 是满足挑战策略 $\psi^{*}=\left(\mathbf{M}^{*},\rho^{*}\right)$ 的属性集合.

游戏 $Game_0$: 该游戏与游戏 $Game_{res}$ 相类似，但在 $Game_0$ 中挑战密文被转换成半功能的形式, 即在该游戏中敌手 $\mathcal{A}$ 获得了半功能形式的挑战密文.

游戏 $Game_{k,1}\left(k=1,2,\cdots,L\right)$（其中 L 表示敌手 $\mathcal{A}$ 进行密钥生成询问的总次数）: 该游戏与游戏 $Game_0$ 相类似，但在 $Game_{k,1}$ 中, 对于前 $k-1$ 次密钥生成询问, 敌手 $\mathcal{A}$ 获得第 II 型的半功能密钥, 第 k 次密钥生成询问返回第 I 型的半功能密钥, 剩余的 $L-k$ 次密钥生成询问返回正常形式的密钥.

游戏		挑战密文	密钥生成询问					
			1	…	$i-1$	i	…	L
$\text{Game}_{\text{real}}$		挑战消息的正常密文	正常密钥					
Game_0		挑战消息的半功能密文	正常密钥					
Game_1	$\text{Game}_{1,1}$	挑战消息的半功能密文	第I型半功能密钥	正常密钥				
	$\text{Game}_{1,2}$	挑战消息的半功能密文	第II型半功能密钥	正常密钥				
⋮								
Game_{i-1}	$\text{Game}_{i-1,1}$	挑战消息的半功能密文	第II型半功能密钥		第I型半功能密钥	正常密钥		
	$\text{Game}_{i-1,2}$	挑战消息的半功能密文	第II型半功能密钥			正常密钥		
Game_i	$\text{Game}_{i,1}$	挑战消息的半功能密文	第II型半功能密钥			第I型半功能密钥	正常密钥	
	$\text{Game}_{i,2}$	挑战消息的半功能密文	第II型半功能密钥				正常密钥	
⋮								
Game_L	$\text{Game}_{L,1}$	挑战消息的半功能密文	第II型半功能密钥					第I型半功能密钥
	$\text{Game}_{L,2}$	挑战消息的半功能密文	第II型半功能密钥					
$\text{Game}_{\text{final}}$		随机消息的半功能密文	第II型半功能密钥					

图 1　本节方案安全性证明过程中挑战密文和密钥的变化情况

游戏 $Game_{k,2}\left(k=1,2,\cdots,L\right)$: 该游戏与游戏 $Game_{k,1}$ 相类似，但在 $Game_{k,2}$ 中, 对于前 k 次密钥生成询问, 敌手 $\mathcal{A}$ 获得第 II 型的半功能密钥, 剩余的 $L-k$ 次密钥生成询问返回正常形式的密钥.

游戏 $Game_{final}$: 该游戏与 $Game_{L,2}$ 相类似，但在 $Game_{final}$ 中，将挑战密文转换成随机消息的半功能密文.

上述游戏中挑战密文和密钥的变化情况如图 1 所示[24]. 对于任意的概率多项式时间敌手 $\mathcal{A}$，其在上述游戏 $Game_i$ 中获胜的概率 $\Pr[Game_i]$ 定义为

$$\Pr[Game_i]=\Pr[b'=b\ in\ Game]$$

引理 1. 如果存在概率多项式时间的敌手 $\mathcal{A}$ 以不可忽略的优势区分游戏 $Game_{real}$ 与 $Game_{res}$，则存在另一敌手 $\mathcal{B}$ 攻破改进的合数阶子群判定假设 2.

证明: 敌手 $\mathcal{B}$ 接收到改进的合数阶子群判定假设 2 的元组 $(\mathbb{G},g_1,X_1X_2,X_3,Y_2Y_3,T)$. 令 $\psi^*=(\mathbf{M}^*,\rho^*)$ 为挑战访问策略，S^* 是满足挑战访问策略的属性集合. 敌手 $\mathcal{A}$ 对属性集合 S 进行密钥生成询问，S 需满足条件 $S=S^* \bmod N$ 和 $S=S^* \bmod p_2$. 敌手 $\mathcal{B}$ 计算 $a=\gcd(S-S^*,N)$ 和 $b=N/a$，其中 $N=p_1p_2p_3$. 此时分为下述三种情况讨论:

（1）如果 $a=p_1p_2$ 和 $b=p_3$，敌手 $\mathcal{B}$ 可以通过验证 $(X_1X_2)^a=1$ 是否成立来判断 $a=p_1p_2$ 是否成立. 如果成立，敌手 $\mathcal{B}$ 可以通过验证 $e(Y_2Y_3,T)^b$ 是否为 1 来区分 $T\in G_{13}$ 或者 $T\in G$.

（2）如果 $a=p_2p_3$ 和 $b=p_1$，敌手 $\mathcal{B}$ 可以通过验证 $(Y_2Y_3)^a=1$ 是否成立来判断 $a=p_2p_3$ 是否成立. 如果成立，敌手 $\mathcal{B}$ 可以通过验证 $e(X_1X_2,T)^b$ 是否为 1 来区分 $T\in G_{13}$ 或者 $T\in G$.

（3）如果 $a=p_2$ 和 $b=p_1p_3$，敌手 $\mathcal{B}$ 可以通过验证 $T^b=1$ 是否为 1 来区分 $T\in G_{13}$ 或者 $T\in G$.

如果敌手 $\mathcal{A}$ 能以不可忽略的优势区分游戏 $Game_{real}$ 与 $Game_{res}$，那么敌手 $\mathcal{B}$ 能以同样的优势攻破合数阶子群判定假设 2，因此有 $\left|\Pr[Game_{real}]-\Pr[Game_{res}]\right|\le \mathsf{negl}(\kappa)$.

引理 2. 如果存在概率多项式时间的敌手 $\mathcal{A}$ 以不可忽略的优势区分游戏 $Game_{res}$ 与 $Game_0$，则存在另一敌手 $\mathcal{B}$ 能以相同的优势攻破改进的合数阶子群判定假设 1.

证明: 敌手 $\mathcal{B}$ 接收到改进的合数阶子群判定假设 1 的挑战元组 $\left(\mathbb{G},g_1,X_3,\{T_i\}_{i=1,2,\cdots,m}\right)$，其目标是判断 $\{T_i\in G_{12}\}_{i=1,2,\cdots,m}$，还是 $\{T_i\in G_1\}_{i=1,2,\cdots,m}$. 敌手 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 间执行下述游戏，具体过程如下所述:

（1）初始化. 敌手 $\mathcal{B}$ 随机选取 $u,h,v\leftarrow_R (G_1)^3$ 和 $\eta,\alpha_1,\alpha_2,\cdots,\alpha_m\leftarrow_R (Z_p)^{m+1}$，输出系统公开参数 $params=\left(g_1,X_3,u,v,h,w,\left\{e(g_1,g_1)^{\alpha_i}\right\}_{i=1,2,\cdots,m}\right)$，其中 $w=g^{\eta}$，并秘密保持主私钥 $msk=(\alpha_1,\alpha_2,\cdots,\alpha_m)$. 敌手 $\mathcal{A}$ 提交挑战访问策略 $\psi^*=(\mathbf{M}^*,\rho^*)$ 和挑战消息 (M_0,M_1) 给敌手 $\mathcal{B}$，其中 $\mathbf{M}^*$ 是一个 $l\times n$ 矩阵，ρ^* 是矩阵 $\mathbf{M}^*$ 的行属性映射函数.

（2）阶段一. 敌手 $\mathcal{A}$ 适应性地进行多项式有界次下述询问.

① 密钥生成询问. 敌手 $\mathcal{A}$ 对不满足挑战访问策略 $\psi^*=(\mathbf{M}^*,\rho^*)$ 的属性集合 $S=\{A_1,A_2,...,A_k\}$ 进行密钥生成询问. 敌手 $\mathcal{B}$ 任意选取 $R,\tilde{R}_1,\tilde{R}_2,\cdots,\tilde{R}_m\leftarrow_R (G_3)^{m+1}$ 和 $r\leftarrow_R Z_p$，对于 $i=1,2,\cdots,m$，计算 $K_i=g_1^{\alpha_i}w^r\tilde{R}_i$ 和 $K_0=g_1^rR$. 随机选取 $r_1,r_2,\cdots,r_k\leftarrow_R (Z_p)^k$ 和 $R_1,R_2,\cdots,R_k,\bar{R}_1,\bar{R}_2,\cdots,\bar{R}_k\leftarrow_R (G_3)^{2k}$，对于 $\tau=1,2,\cdots,k$，计算 $K_{\tau,1}=g_1^{r_\tau}R_\tau$ 和 $K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}\bar{R}_\tau$. 最后添加私钥 $sk=\left(S,\{K_i\}_{i=1,2,\cdots,m},K_0,\{K_{\tau,1},K_{\tau,2}\}_{\tau=1,2,\cdots,k}\right)$ 到列表 L 中，并输出 sk 给敌手 $\mathcal{A}$.

② 泄露询问. 敌手 $\mathcal{A}$ 通过提交 $\left(S, f_i:\{0,1\}^* \to \{0,1\}^{\lambda_i}\right)$ 给敌手 $\mathcal{B}$ 进行泄露询问, 其中 S 是属性集合（S 可满足挑战访问策略 $\psi^* = \left(\mathbf{M}^*, \rho^*\right)$）, $f_i:\{0,1\}^* \to \{0,1\}^{\lambda_i}$ 是高效可计算的泄露函数. 若 $(S, sk) \in L$, 敌手 $\mathcal{B}$ 将 $f_i(sk)$ 返还给敌手 $\mathcal{A}$. 否则, 对属性集合 S 进行密钥生成询问后将相应的泄露信息 $f_i(sk)$ 发给 $\mathcal{A}$.

（3）挑战. 敌手 $\mathcal{B}$ 随机选取 $\beta \leftarrow_R \{0,1\}$, 并计算 $C = M_\beta \prod_{i=1}^{m} e\left(g_1^{\alpha_i}, T_i\right)$ 和 $\{C_i = T_i\}_{i=1,2,\cdots,m}$. 随机选取 $y_2, \cdots, y_n \leftarrow_R \left(Z_p\right)^{n-1}$, 对于 $i = 1,2,\cdots,l$, 计算 $D_i = \left(\prod_{j=1}^{l} T_j\right)^{\mathbf{M}_{i,1}^*} (g_1)^{\mathbf{M}_{i,2}^* y_2} (g_1)^{\mathbf{M}_{i,3}^* y_3} \cdots (g_1)^{\mathbf{M}_{i,n}^* y_n}$, 其中 $\mathbf{M}_{i,j}^*$ 表示矩阵 $\mathbf{M}^*$ 中第 i 行第 j 列的元素. 任意选取随机数 $t_1, t_2, \cdots, t_l \leftarrow_R \left(Z_p\right)^l$, 对于 $\tau = 1,2,\cdots,l$, 计算

$$C_{\tau,1} = \left(D_\tau\right)^\eta v^{t_\tau},\ C_{\tau,2} = \left(u^{\rho^*(\tau)} h\right)^{-t_\tau} \text{ 和 } C_{\tau,3} = g_1^{t_\tau}.$$

最后输出相应的挑战密文 $ct_\beta = \left(\psi^* = \left(\mathbf{M}^*, \rho^*\right), C, \{C_i\}_{i=1,2,\cdots,m}, \left\{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\right\}_{\tau=1,2,\cdots,l}\right)$ 给敌手 $\mathcal{A}$.

（4）阶段二. 该阶段与阶段一相类似, 敌手 $\mathcal{B}$ 以相同的方式应答敌手 $\mathcal{A}$ 的密钥生成询问，但该阶段禁止敌手 $\mathcal{A}$ 进行泄露询问.

（5）猜测. 敌手 $\mathcal{A}$ 输出对随机数 β 的猜测 β'. 若 $\beta = \beta'$, 则敌手 $\mathcal{B}$ 输出 1, 表示敌手 $\mathcal{A}$ 在该游戏中获胜; 否则, 敌手 $\mathcal{B}$ 输出 0.

下面分两类讨论挑战密文 $ct_\beta = \left(C, \{C_i\}_{i=1,2,\cdots,m}, \left\{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\right\}_{\tau=1,2,\cdots,l}\right)$ 的形式：

① 若对于 $i = 1,2,\cdots,m$, 有 $T_i \in G_{12}$（为方便分析本文将其写为 $T_i = g_1^{s_i} g_2^{c_i}$, 其中 $s_i, c_i \in Z_p$）, 那么有

$$D_i = \left(\prod_{j=1}^{l} T_j\right)^{\mathbf{M}_{i,1}^*} (g_1)^{\mathbf{M}_{i,2}^* y_2} (g_1)^{\mathbf{M}_{i,3}^* y_3} \cdots (g_1)^{\mathbf{M}_{i,n}^* y_n} = \left(\prod_{j=1}^{l} g_1^{s_j} g_2^{c_j}\right)^{\mathbf{M}_{i,1}^*} (g_1)^{\mathbf{M}_{i,2}^* y_2} (g_1)^{\mathbf{M}_{i,3}^* y_3} \cdots (g_1)^{\mathbf{M}_{i,n}^* y_n}$$

$$= (g_1)^{\sum_{j=1}^{l} s_j \mathbf{M}_{i,1}^* + \mathbf{M}_{i,2}^* y_2 + \mathbf{M}_{i,3}^* y_3 + \cdots + \mathbf{M}_{i,n}^* y_n} (g_2)^{\sum_{j=1}^{l} c_j \mathbf{M}_{i,1}^*}$$

$$C_{\tau,1} = \left(D_\tau\right)^\eta v^{t_\tau} = (w)^{\sum_{j=1}^{l} s_j \mathbf{M}_{i,1}^* + \mathbf{M}_{i,2}^* y_2 + \mathbf{M}_{i,3}^* y_3 + \cdots + \mathbf{M}_{i,n}^* y_n} (g_2)^{\eta \sum_{j=1}^{l} c_j \mathbf{M}_{i,1}^*} v^{t_\tau}$$

那么挑战密文为

$$ct_\beta = \left(C = M_\beta \prod_{i=1}^{m} e(g_1, g_1)^{\alpha_i s_i}, \left\{g_1^{s_i} g_2^{c_i}\right\}_{i=1,2,\cdots,m}, \left\{C_{\tau,1} = w^{\lambda_\tau} (g_2)^{\eta \sum_{j=1}^{l} c_j \mathbf{M}_{i,1}^*} v^{t_\tau}, C_{\tau,2} = \left(u^{\rho(\tau)} h\right)^{-t_\tau}, C_{\tau,3} = g_1^{t_\tau}\right\}_{\tau=1,2,\cdots,l}\right),$$

其中隐含地设置了 $\lambda_\tau = \sum_{j=1}^{l} s_j \mathbf{M}_{i,1}^* + \mathbf{M}_{i,2}^* y_2 + \mathbf{M}_{i,3}^* y_3 + \cdots + \mathbf{M}_{i,n}^* y_n$ 和 $\vec{\lambda} = \left(\lambda_1, \lambda_2, \cdots, \lambda_l\right)^\top = \mathbf{M}^* \vec{y}$, 其中 $\vec{y} = \left(\sum_{i=1}^{m} s_i, y_2, \cdots, y_n\right)$. 此时挑战密文 ct_β 为半功能密文, 敌手 $\mathcal{B}$ 模拟了游戏 $Game_0$.

② 若对于 $i = 1,2,\cdots,m$, 有 $T_i \in G_1$（为方便分析本文将其写为 $T_i = g_1^{s_i}$, 其中 $s_i \in Z_p$）, 那么有

$$D_i=\left(\prod_{j=1}^{l}T_j\right)^{\mathbf{M}^*_{i,1}}\left(g_1\right)^{\mathbf{M}^*_{i,2}y_2}\left(g_1\right)^{\mathbf{M}^*_{i,3}y_3}\cdots\left(g_1\right)^{\mathbf{M}^*_{i,n}y_n}=\left(\prod_{j=1}^{l}g_1^{s_j}\right)^{\mathbf{M}^*_{i,1}}\left(g_1\right)^{\mathbf{M}^*_{i,2}y_2}\left(g_1\right)^{\mathbf{M}^*_{i,3}y_3}\cdots\left(g_1\right)^{\mathbf{M}^*_{i,n}y_n}$$

$$=\left(g_1\right)^{\sum_{j=1}^{l}s_j\mathbf{M}^*_{i,1}+\mathbf{M}^*_{i,2}y_2+\mathbf{M}^*_{i,3}y_3+\cdots+\mathbf{M}^*_{i,n}y_n}$$

$$C_{\tau,1}=\left(D_\tau\right)^{\eta}v^{t_\tau}=\left(w\right)^{\sum_{j=1}^{l}s_j\mathbf{M}^*_{i,1}+\mathbf{M}^*_{i,2}y_2+\mathbf{M}^*_{i,3}y_3+\cdots+\mathbf{M}^*_{i,n}y_n}v^{t_\tau}$$

那么挑战密文为

$$ct_\beta=\left(C=M_\beta\prod_{i=1}^{m}e\left(g_1,g_1\right)^{\alpha_i s_i},\left\{g_1^{s_i}\right\}_{i=1,2,\cdots,m},\left\{C_{\tau,1}=w^{\lambda_\tau}v^{t_\tau},C_{\tau,2}=\left(u^{\rho(\tau)}h\right)^{-t_\tau},C_{\tau,3}=g_1^{t_\tau}\right\}_{\tau=1,2,\cdots,l}\right).$$

此时挑战密文 ct_β 为正常密文, 敌手 $\mathcal{B}$ 模拟了游戏 $Game_{res}$.

综上所述, 如果敌手 $\mathcal{A}$ 能以不可忽略的优势区分游戏 $Game_{res}$ 与 $Game_0$, 那么敌手 $\mathcal{B}$ 能以相同的优势攻破改进的合数阶子群判定假设 1, 因此有 $\left|\Pr\left[Game_{res}\right]-\Pr\left[Game_0\right]\right|\le\mathsf{negl}(\kappa)$.

引理 3. 如果存在概率多项式时间的敌手 $\mathcal{A}$ 以不可忽略的优势区分游戏 $Game_0$ 与 $Game_{1,1}$, 则存在敌手 $\mathcal{B}$ 能以相同的优势攻破改进的合数阶子群判定假设 2.

证明: 敌手 $\mathcal{B}$ 接收到合数阶子群判定假设 2 的挑战元组 $\left(\mathbb{G},g_1,\left\{X_{1i}X_{2i}\right\}_{i=1,2,\cdots,m},X_3,Y_2Y_3,T\right)$（为方便分析，本文将 $X_{1i}X_{2i}$ 写为 $g_1^{x_i}g_2^{z_i}$，其中 $x_i,z_i\leftarrow_R\left(Z_p\right)^2$），其目标是判断 $T\in G$, 还是 $T\in G_{13}$. 敌手 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 间执行下述游戏，具体过程如下所述:

（1）初始化. 敌手 $\mathcal{B}$ 随机选取 $u,h,v\leftarrow_R\left(G_1\right)^3$ 和 $\eta,\alpha_1,\alpha_2,\cdots,\alpha_m\leftarrow_R\left(Z_p\right)^{m+1}$, 输出系统公开参数 $params=\left(g_1,X_3,u,v,h,w,\left\{e\left(g_1,g_1\right)^{\alpha_i}\right\}_{i=1,2,\cdots,m}\right)$, 其中 $w=g_1^{\eta}$, 并秘密保持主私钥 $msk=\left(\alpha_1,\alpha_2,\cdots,\alpha_m\right)$. 敌手 $\mathcal{A}$ 提交挑战访问策略 $\psi^*=\left(\mathbf{M}^*,\rho^*\right)$ 和挑战消息 $\left(M_0,M_1\right)$ 给敌手 $\mathcal{B}$.

（2）阶段一. 敌手 $\mathcal{A}$ 适应性地进行多项式有界次的下述询问.

① 密钥生成询问. 对于敌手 $\mathcal{A}$ 提交的第 1 次密钥生成询问, 敌手 $\mathcal{B}$ 任意选取 $R',R'_1,R'_2,\cdots,R'_m\leftarrow_R\left(G_3\right)^{m+1}$ 和 $\tilde{r}\leftarrow_R Z_p$, 计算 $\left\{K_i=g_1^{\alpha_i}w^{\tilde{r}}T^{\eta}R'_i\right\}_{i=1,2,\cdots,m}$ 和 $K_0=g_1^{\tilde{r}}TR'$. 随机选取 $r_1,r_2,\cdots,r_k\leftarrow_R\left(Z_p\right)^k$ 和 $R_1,R_2,\cdots,R_k,\bar{R}_1,\bar{R}_2,\cdots,\bar{R}_k\leftarrow_R\left(G_3\right)^{2k}$, 对于 $\tau=1,2,\cdots,k$, 计算 $K_{\tau,1}=g_1^{r_\tau}R_\tau$ 和 $K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}\bar{R}_\tau$, 最后添加私钥 $sk=\left(S,\left\{K_i\right\}_{i=1,2,\cdots,m},K_0,\left\{K_{\tau,1},K_{\tau,2}\right\}_{\tau=1,2,\cdots,k}\right)$ 到列表 L 中，并输出 sk 给 $\mathcal{A}$.

对于剩余的密钥生成询问, 敌手 $\mathcal{B}$ 任意选取 $R,\tilde{R}_1,\tilde{R}_2,\cdots,\tilde{R}_m\leftarrow_R\left(G_3\right)^{m+1}$ 和 $r\leftarrow_R Z_p$, 计算 $\left\{K_i=g_1^{\alpha_i}w^r\tilde{R}_i\right\}_{i=1,2,\cdots,m}$ 和 $K_0=g_1^rR$. 随机选取 $r_1,r_2,\cdots,r_k\leftarrow_R\left(Z_p\right)^k$ 和 $R_1,R_2,\cdots,R_k,\bar{R}_1,\bar{R}_2,\cdots,\bar{R}_k\leftarrow_R\left(G_3\right)^{2k}$, 对于 $\tau=1,2,\cdots,k$, 计算 $K_{\tau,1}=g_1^{r_\tau}R_\tau$ 和 $K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}\bar{R}_\tau$, 添加属性集合 S 对应的私钥 $sk=\left(S,\left\{K_i\right\}_{i=1,2,\cdots,m},K_0,\left\{K_{\tau,1},K_{\tau,2}\right\}_{\tau=1,2,\cdots,k}\right)$ 到 L 中，并输出 sk 给敌手 $\mathcal{A}$. 特别地，上述私钥 sk 是正常密钥.

② 泄露询问. 敌手 $\mathcal{A}$ 通过提交 $\left(S,f_i:\left\{0,1\right\}^*\to\left\{0,1\right\}^{\lambda_i}\right)$ 给敌手 $\mathcal{B}$ 进行泄露询问, 其中 S 是相应的属性集合, $f_i:\left\{0,1\right\}^*\to\left\{0,1\right\}^{\lambda_i}$ 是高效可计算的泄露函数. 若 $\left(S,sk\right)\in L$, 敌手 $\mathcal{B}$ 将 $f_i\left(sk\right)$ 返还给敌手 $\mathcal{A}$. 否则, 对属性集合 S 进行密钥生成询问后将相应的泄露信息 $f_i\left(sk\right)$ 发给敌手 $\mathcal{A}$.

（**3**）**挑战**. 敌手 $\mathcal{B}$ 选取随机数 $\beta \leftarrow_R \{0,1\}$，计算 $C = M_\beta \prod_{i=1}^{m} e\left(g_1^{\alpha_i}, X_{1i}X_{2i}\right)$ 和 $\{C_i = X_{1i}X_{2i}\}_{i=1,2,\cdots,m}$. 随机选取 $y_2,\cdots,y_n \leftarrow_R \left(Z_p\right)^{n-1}$，对于 $i=1,2,\cdots,l$，计算

$$D_i = \left(\prod_{j=1}^{l} X_{1j}X_{2j}\right)^{\mathbf{M}_{i,1}^*} (g_1)^{\mathbf{M}_{i,2}^* y_2} (g_1)^{\mathbf{M}_{i,3}^* y_3} \cdots (g_1)^{\mathbf{M}_{i,n}^* y_n} = \left(\prod_{j=1}^{l} g_1^{x_j} g_2^{z_j}\right)^{\mathbf{M}_{i,1}^*} (g_1)^{\mathbf{M}_{i,2}^* y_2} (g_1)^{\mathbf{M}_{i,3}^* y_3} \cdots (g_1)^{\mathbf{M}_{i,n}^* y_n}$$
$$= (g_1)^{\sum_{j=1}^{l} x_j \mathbf{M}_{i,1}^* + \mathbf{M}_{i,2}^* y_2 + \mathbf{M}_{i,3}^* y_3 + \cdots + \mathbf{M}_{i,n}^* y_n} (g_2)^{\sum_{j=1}^{l} z_j \mathbf{M}_{i,1}^*}$$

其中 $\mathbf{M}_{i,j}^*$ 表示矩阵 $\mathbf{M}^*$ 中第 i 行第 j 列的元素. 任意选取随机数 $t_1,t_2,\cdots,t_l \leftarrow_R \left(Z_p\right)^l$，对于 $\tau = 1,2,\cdots,l$，计算

$$C_{\tau,1} = \left(D_\tau\right)^\eta v^{t_\tau}，\ C_{\tau,2} = \left(u^{\rho^*(\tau)} h\right)^{-t_\tau} \text{ 和 } C_{\tau,3} = g_1^{t_\tau}.$$

最后输出相应的挑战密文 $ct_\beta = \left(C, \{C_i\}_{i=1,2,\cdots,m}, \{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\}_{\tau=1,2,\cdots,l}\right)$ 给敌手 $\mathcal{A}$.

则挑战密文可表示为

$$ct_\beta = \left(C = M_\beta \prod_{i=1}^{m} e(g_1,g_1)^{\alpha_i s_i}, \left\{g_1^{s_i} g_2^{c_i}\right\}_{i=1,2,\cdots,m}, \left\{C_{\tau,1} = w^{\lambda_\tau} v^{t_\tau} (g_2)^{\mathbf{M}_{i,1}^* \eta \sum_{j=1}^{l} z_j}, C_{\tau,2} = \left(u^{\rho^*(\tau)} h\right)^{-t_\tau}, C_{\tau,3} = g_1^{t_\tau}\right\}_{\tau=1,2,\cdots,l}\right),$$

其中 $C_{\tau,1} = \left(D_\tau\right)^\eta v^{t_\tau} = \left((g_1)^{\sum_{i=1}^{l} x_i \mathbf{M}_{i,1}^* + \mathbf{M}_{i,2}^* y_2 + \mathbf{M}_{i,3}^* y_3 + \cdots + \mathbf{M}_{i,n}^* y_n} (g_2)^{\mathbf{M}_{i,1}^* \sum_{j=1}^{l} z_j}\right)^\eta v^{t_\tau} = w^{\lambda_\tau} v^{t_\tau} (g_2)^{\mathbf{M}_{i,1}^* \eta \sum_{j=1}^{l} z_j}$. 隐含地设置了 $\lambda_i = \sum_{i=1}^{l} x_i \mathbf{M}_{i,1}^* + \mathbf{M}_{i,2}^* y_2 + \mathbf{M}_{i,3}^* y_3 + \cdots + \mathbf{M}_{i,n}^* y_n$. 特别地，挑战密文 ct_β 是消息 M_β 的半功能密文.

（**4**）**阶段二**. 该阶段与阶段一相类似，敌手 $\mathcal{B}$ 以相同的方式应答敌手 $\mathcal{A}$ 的密钥生成询问，但该阶段禁止敌手 $\mathcal{A}$ 进行泄露询问.

（**5**）**猜测**. 敌手 $\mathcal{A}$ 输出对随机数 β 的猜测 β'. 若 $\beta = \beta'$，则敌手 $\mathcal{B}$ 输出 1，表示敌手 $\mathcal{A}$ 在该游戏中获胜；否则，敌手 $\mathcal{B}$ 输出 0.

对于第 1 次密钥生成询问的应答 $sk = \left(S, \{K_i\}_{i=1,2,\cdots,m}, K_0, \{K_{\tau,1}, K_{\tau,2}\}_{\tau=1,2,\cdots,k}\right)$，分下面两类情况讨论：

① 若 $T \in G$ (本文将其写为 $T = g_1^x g_2^z g_3^t \in G$，其中 $x,z,t \in Z_p$)，那么有

$$sk = \left(\left(K_i = g_1^{\alpha_i} w^{\tilde{r}+x} g_2^{z\eta} g_3^{t\eta} R_i'\right)_{i=1,2,\cdots,m}, K_0 = g_1^{\tilde{r}+x} g_2^z g_3^t R', \left\{K_{\tau,1} = g_1^{r_\tau} R_\tau, K_{\tau,2} = \left(u^{A_\tau} h\right)^{r_\tau} v^{-r} \overline{R}_\tau\right\}_{\tau=1,2,\cdots,k}\right)$$

隐含地设置了 $r = \tilde{r} + x$，$\tilde{R}_i = g_3^{t\eta} R_i'$ 和 $R = g_3^t R'$. 则当 $T \in G$ 时，第 1 次密钥生成询问的应答是第 I 型的半功能密钥，即敌手 $\mathcal{B}$ 模拟了游戏 $Game_{1,1}$.

② 若 $T \in G_{13}$ (本文将其写为 $T = g_1^x g_3^t \in G$，其中 $x,t \in Z_p$)，那么有

$$sk = \left(\left(K_i = g_1^{\alpha_i} w^{\tilde{r}+x} g_3^{t\eta} R_i'\right)_{i=1,2,\cdots,m}, K_0 = g_1^{\tilde{r}+x} g_3^t R', \left\{K_{\tau,1} = g_1^{r_\tau} R_\tau, K_{\tau,2} = \left(u^{A_\tau} h\right)^{r_\tau} v^{-r} R_\tau\right\}_{\tau=1,2,\cdots,k}\right)$$

则当 $T \in G_{13}$ 时，第 1 次密钥生成询问的应答是正常密钥，即敌手 $\mathcal{B}$ 模拟了游戏 $Game_0$.

综上所述，如果存在概率多项式时间的敌手 $\mathcal{A}$ 以不可忽略的优势区分游戏 $Game_0$ 与 $Game_{1,1}$，则存在敌手 $\mathcal{B}$ 能以相同的优势攻破改进的合数阶子群判定假设 2，因此有 $\left|\Pr[Game_0] - \Pr[Game_{1.1}]\right| \le \mathsf{negl}(\kappa)$.

引理 4. 对于 $k = 1,2,\cdots,L$，如果存在概率多项式时间的敌手 $\mathcal{A}$ 以不可忽略的优势区分游戏 $Game_{k,1}$ 与

$Game_{k,2}$，则存在敌手 $\mathcal{B}$ 能以相同的优势攻破改进的合数阶子群判定假设 2.

证明: 敌手 $\mathcal{B}$ 收到改进的合数阶子群判定假设 2 的挑战元组 $\left(\mathbb{G}, g_1, \{X_{1i}X_{2i}\}_{i=1,2,\cdots,m}, X_3, Y_2Y_3, T\right)$，其目标是判断 $T \in G$，还是 $T \in G_{13}$. 敌手 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 间执行下述游戏，具体过程如下所述：

（1）初始化. 敌手 $\mathcal{B}$ 随机选取 $u,h,v \leftarrow_R (G_1)^3$ 和 $\eta,\alpha_1,\alpha_2,\cdots,\alpha_m \leftarrow_R (Z_p)^{m+1}$，生成系统公开参数 $params = \left(g_1, X_3, u, v, h, w, \left\{e(g,g)^{\alpha_i}\right\}_{i=1,2,\cdots,m}\right)$，其中 $w = g_1^{\eta}$，并秘密保持主私钥 $msk = (\alpha_1,\alpha_2,\cdots,\alpha_m)$. 敌手 $\mathcal{A}$ 提交挑战访问策略 $\psi^* = (M^*, \rho^*)$ 和挑战消息 (M_0, M_1) 给敌手 $\mathcal{B}$.

（2）阶段一. 敌手 $\mathcal{A}$ 适应性地进行多项式有界次下述询问.

① 密钥生成询问. 对于前 $k-1$ 次密钥生成询问，敌手 $\mathcal{B}$ 任意选取 $R', \tilde{R}_1, \tilde{R}_2, \cdots, \tilde{R}_m \leftarrow_R (G_3)^{m+1}$ 和 $r \leftarrow_R Z_p$，对于 $i = 1,2,\cdots,m$，计算 $\left\{K_i = g_1^{\alpha_i} w^r \tilde{R}_i\right\}_{i=1,2,\cdots,m}$ 和 $K_0 = g_1^r Y_2 Y_3 R'$. 随机选取 $r_1, r_2, \cdots, r_k \leftarrow_R (Z_p)^k$ 和 $R_1, R_2, \cdots, R_k, \bar{R}_1, \bar{R}_2, \cdots, \bar{R}_k \leftarrow_R (G_3)^{2k}$，对于 $\tau = 1,2,\cdots,k$，计算 $K_{\tau,1} = g_1^{r_\tau} R_\tau$ 和 $K_{\tau,2} = \left(u^{A_\tau} h\right)^{r_\tau} v^{-r} \bar{R}_\tau$，输出 $sk = \left(S, \{K_i\}_{i=1,2,\cdots,m}, K_0, \{K_{\tau,1}, K_{\tau,2}\}_{\tau=1,2,\cdots,k}\right)$ 给敌手 $\mathcal{A}$. 特别地，上述私钥 sk 是第 II 型的半功能密钥.

对于第 k 次密钥生成询问，敌手 $\mathcal{B}$ 任意选取 $R', \tilde{R}_1', \tilde{R}_2', \cdots, \tilde{R}_m' \leftarrow_R (G_3)^{m+1}$ 和 $r \leftarrow_R Z_p$，对于 $i = 1,2,\cdots,m$，计算 $\left\{K_i = g_1^{\alpha_i} w^{\tilde{r}} T^{\eta} \tilde{R}_i'\right\}_{i=1,2,\cdots,m}$ 和 $K_0 = g_1^{\tilde{r}} T Y_2 Y_3 R'$. 随机选取 $r_1, r_2, \cdots, r_k \leftarrow_R (Z_p)^k$ 和 $R_1, R_2, \cdots, R_k, \bar{R}_1, \bar{R}_2, \cdots, \bar{R}_k \leftarrow_R (G_3)^{2k}$，对于 $\tau = 1,2,\cdots,k$，计算 $K_{\tau,1} = g_1^{r_\tau} R_\tau$ 和 $K_{\tau,2} = \left(u^{A_\tau} h\right)^{r_\tau} v^{-r} \bar{R}_\tau$. 最后输出属性集合所对应的私钥 $sk = \left(S, \{K_i\}_{i=1,2,\cdots,m}, K_0, \{K_{\tau,1}, K_{\tau,2}\}_{\tau=1,2,\cdots,k}\right)$ 给敌手 $\mathcal{A}$.

对于剩余的密钥生成询问，敌手 $\mathcal{B}$ 任意选取 $R, \tilde{R}_1, \tilde{R}_2, \cdots, \tilde{R}_m \leftarrow_R (G_3)^{m+1}$ 和 $r \leftarrow_R Z_p$，对于 $i = 1,2,\cdots,m$，计算 $\left\{K_i = g_1^{\alpha_i} w^r \tilde{R}_i\right\}_{i=1,2,\cdots,m}$ 和 $K_0 = g_1^r R$. 随机选取 $r_1, r_2, \cdots, r_k \leftarrow_R (Z_p)^k$ 和 $R_1, R_2, \cdots, R_k, \bar{R}_1, \bar{R}_2, \cdots, \bar{R}_k \leftarrow_R (G_3)^{2k}$，对于 $\tau = 1,2,\cdots,k$，计算 $K_{\tau,1} = g_1^{r_\tau} R_\tau$ 和 $K_{\tau,2} = \left(u^{A_\tau} h\right)^{r_\tau} v^{-r} \bar{R}_\tau$，输出 $sk = \left(S, \{K_i\}_{i=1,2,\cdots,m}, K_0, \{K_{\tau,1}, K_{\tau,2}\}_{\tau=1,2,\cdots,k}\right)$ 给敌手 $\mathcal{A}$. 特别地，上述私钥 sk 是正常密钥.

② 泄露询问. 敌手 $\mathcal{A}$ 通过提交 $\left(S, f_i : \{0,1\}^* \to \{0,1\}^{\lambda_i}\right)$ 给敌手 $\mathcal{B}$ 进行泄露询问，其中 S 是相应的属性集合，$f_i : \{0,1\}^* \to \{0,1\}^{\lambda_i}$ 是高效可计算的泄露函数. 若 $(S, sk) \in L$，敌手 $\mathcal{B}$ 将 $f_i(sk)$ 返还给敌手 $\mathcal{A}$. 否则，对属性集合 S 进行密钥生成询问后将相应的泄露信息 $f_i(sk)$ 发给敌手 $\mathcal{A}$.

（3）挑战. 敌手 $\mathcal{B}$ 选取随机数和 $\beta \leftarrow_R \{0,1\}$，计算 $C = M_\beta \prod_{i=1}^{m} e\left(g_1^{\alpha_i}, X_{1i}X_{2i}\right)$ 和 $\left\{C_i = \left(X_{1i}X_{2i}\right)^{s_i}\right\}_{i=1,2,\cdots,m}$. 随机选取 $y_2, \cdots, y_n \leftarrow_R (Z_p)^{n-1}$，对于 $i = 1,2,\cdots,l$，计算 $D_i = \left(\prod_{j=1}^{l} X_{1j}X_{2j}\right)^{\mathbf{M}^*_{i,1}} (g_1)^{\mathbf{M}^*_{i,2}y_2} (g_1)^{\mathbf{M}^*_{i,3}y_3} \cdots (g_1)^{\mathbf{M}^*_{i,n}y_n}$. 任意选取随机数 $t_1, t_2, \cdots, t_l \leftarrow_R (Z_p)^l$，对于 $\tau = 1,2,\cdots,l$，计算 $C_{\tau,1} = (D_\tau)^{\eta} v^{t_\tau}$，$C_{\tau,2} = \left(u^{\rho^*(\tau)} h\right)^{-t_\tau}$ 和 $C_{\tau,3} = g_1^{t_\tau}$. 最后输出相应的挑战密文 $ct_\beta = \left(C, \{C_i\}_{i=1,2,\cdots,m}, \{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\}_{\tau=1,2,\cdots,l}\right)$ 给敌手 $\mathcal{A}$. 特别地，挑战密文 ct_β 是消息 M_β 的半功能密文.

（4）阶段二. 该阶段与阶段一相类似, 敌手 $\mathcal{B}$ 以相同的方式应答敌手 $\mathcal{A}$ 的密钥生成询问，但该阶段禁止敌手 $\mathcal{A}$ 进行泄露询问.

（5）猜测. 敌手 $\mathcal{A}$ 输出对随机数 β 的猜测 β'. 若 $\beta=\beta'$, 则敌手 $\mathcal{B}$ 输出 1, 表示敌手 $\mathcal{A}$ 在该游戏中获胜; 否则, 敌手 $\mathcal{B}$ 输出 0.

对于第 k 次密钥生成询问的应答 $sk=\left(S,\left\{K_i\right\}_{i=1,2,\cdots,m},K_0,\left\{K_{\tau,1},K_{\tau,2}\right\}_{\tau=1,2,\cdots,k}\right)$，分下面两类情况讨论：

① 若 $T=g_1^x g_2^z g_3^t\in G$, 那么有

$$sk=\left(\left(K_i=g_1^{\alpha_i}w^{\tilde{r}+x}g_2^{z\eta}g_3^{t\eta}\tilde{R}_i'\right)_{i=1,2,\cdots,m},K_0=g_1^{\tilde{r}+x}g_2^z g_3^t Y_2Y_3R',\left\{K_{\tau,1}=g_1^{r_\tau}R_\tau,K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}\overline{R}_\tau\right\}_{\tau=1,2,\cdots,k}\right)$$

隐含地设置了 $r=\tilde{r}+x$, $\tilde{R}_i=g_3^{t\eta}\tilde{R}_i'$ 和 $R=g_3^tY_3R'$. 则第 k 次密钥生成询问的应答是第 I 型的半功能密钥, 即敌手 $\mathcal{B}$ 模拟了游戏 $Game_{k,1}$.

② 若 $T=g_1^x g_3^t\in G_{13}$, 那么有

$$sk=\left(\left(K_i=g_1^{\alpha_i}w^{\tilde{r}+x}g_3^{t\eta}\tilde{R}_i'\right)_{i=1,2,\cdots,m},K_0=g_1^{\tilde{r}+x}g_3^t Y_2Y_3R',\left\{K_{\tau,1}=g_1^{r_\tau}R_\tau,K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}\overline{R}_\tau\right\}_{\tau=1,2,\cdots,k}\right)$$

则第 k 次密钥生成询问的应答是第 II 型的半功能密钥, 即敌手 $\mathcal{B}$ 模拟了游戏 $Game_{k,2}$.

综上所述, 如果存在概率多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势区分游戏 $Game_{k,1}$ 与 $Game_{k,2}$, 则存在敌手 $\mathcal{B}$ 能以相同的优势攻破改进的合数阶子群判定假设 2, 因此有 $\left|\Pr\left[Game_{k.1}\right]-\Pr\left[Game_{k.2}\right]\right|\le \mathsf{negl}(\kappa)$.

引理 5. 对于 $k=2,\cdots,L$，如果存在概率多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势区分游戏 $Game_{k-1,2}$ 与 $Game_{k,1}$, 则存在敌手 $\mathcal{B}$ 能以相同的优势攻破改进的合数阶子群判定假设 2.

由引理 3 的证明可知 $\left|\Pr\left[Game_{k-1.2}\right]-\Pr\left[Game_{k.1}\right]\right|\le \mathsf{negl}(\kappa)$. 引理 5 的证明过程与引理 3 类似, 篇幅所限, 本文不再赘述引理 5 的证明.

引理 6. 如果存在概率多项式时间敌手 $\mathcal{A}$ 能以不可忽略的优势区分游戏 $Game_{L,2}$ 与 $Game_{final}$, 则存在敌手 $\mathcal{B}$ 能以相同的优势攻破改进的合数阶子群判定假设 3.

证明: 敌手 $\mathcal{B}$ 收到合数阶子群判定假设 3 的挑战元组 $\left(\mathbb{G},g_1,\left\{g_1^{\alpha_i}X_2,g_1^{s_i}Y_2\right\}_{i=1,2,\cdots,m},X_3,Z_2,T\right)$, 其目标是判断 $T=\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i}$, 还是 $T\in G_T$. 敌手 $\mathcal{B}$ 与敌手 $\mathcal{A}$ 间执行下述游戏，具体过程如下所述:

（1）初始化. 敌手 $\mathcal{B}$ 随机选取 $u,h,v\leftarrow_R\left(G_1\right)^3$ 和 $\eta\leftarrow Z_p$, 生成系统公开参数 $params=\left(g_1,X_3,u,v,h,w,\left\{e\left(g_1^{\alpha_i}X_2,g_1\right)\right\}_{i=1,2,\cdots,m}\right)$, 其中 $w=g^\eta$, 隐含地设置了主私钥为 $msk=\left(\alpha_1,\alpha_2,\cdots,\alpha_m\right)$. 敌手 $\mathcal{A}$ 提交挑战访问策略 $\psi^*=\left(\mathbf{M}^*,\rho^*\right)$ 和挑战消息 $\left(M_0,M_1\right)$ 给敌手 $\mathcal{B}$.

（2）阶段一. 敌手 $\mathcal{A}$ 适应性地进行多项式有界次下述询问.

① 密钥生成询问. 敌手 $\mathcal{A}$ 对不满足挑战访问策略 $\psi^*=\left(\mathbf{M}^*,\rho^*\right)$ 的属性集合 $S=\left\{A_1,A_2,...,A_k\right\}$ 进行密钥生成询问. 敌手 $\mathcal{B}$ 任意选取 $R',\tilde{R}_1,\tilde{R}_2,\cdots,\tilde{R}_m\leftarrow_R\left(G_3\right)^{m+1}$ 和 $r\leftarrow_R Z_p$, 对于 $i=1,2,\cdots,m$, 计算 $\left\{K_i=\left(g^{\alpha_i}X_2\right)g_1^{\alpha_i}w^r\tilde{R}_i\right\}_{i=1,2,\cdots,m}$ 和 $K_0=g_1^rZ_2R$. 选取 $r_1,r_2,\cdots,r_k\leftarrow\left(Z_p\right)^k$ 和 $R_1,R_2,\cdots,R_k,\overline{R}_1,\overline{R}_2,\cdots,\overline{R}_k\leftarrow_R\left(G_3\right)^{2k}$, 对于 $\tau=1,2,\cdots,k$, 计算 $K_{\tau,1}=g_1^{r_\tau}R_\tau$ 和 $K_{\tau,2}=\left(u^{A_\tau}h\right)^{r_\tau}v^{-r}\overline{R}_\tau$, 输出属性集合所对应的私钥

$sk=\left(S,\left\{K_i\right\}_{i=1,2,\cdots,m},K_0,\left\{K_{\tau,1},K_{\tau,2}\right\}_{\tau=1,2,\cdots,k}\right)$给敌手$\mathcal{A}$. 特别地, 上述私钥$sk$是第 II 型的半功能密钥.

② 泄露询问. 敌手$\mathcal{A}$通过提交$\left(S,f_i:\{0,1\}^*\to\{0,1\}^{\lambda_i}\right)$给敌手$\mathcal{B}$进行泄露询问, 其中$S$是相应的属性集合, $f_i:\{0,1\}^*\to\{0,1\}^{\lambda_i}$是高效可计算的泄露函数. 若$(S,sk)\in L$, 敌手$\mathcal{B}$将$f_i(sk)$返还给敌手$\mathcal{A}$. 否则, 对属性集合$S$进行密钥生成询问后将相应的泄露信息$f_i(sk)$发给敌手$\mathcal{A}$.

（3）挑战. 敌手$\mathcal{B}$选取随机数$\beta\leftarrow_R\{0,1\}$, 计算$C=M_\beta T$和$\left\{C_i=g^{s_i}Y_2\right\}_{i=1,2,\cdots,m}$. 随机选取$y_2,\cdots,y_n\leftarrow_R\left(Z_p\right)^{n-1}$, 对于$i=1,2,\cdots,l$, 计算

$$D_i=\left(\prod_{j=1}^{l}g_1^{s_j}Y_2\right)^{\mathbf{M}^*_{i,1}}(g_1)^{\mathbf{M}^*_{i,2}y_2}(g_1)^{\mathbf{M}^*_{i,3}y_3}\cdots(g_1)^{\mathbf{M}^*_{i,n}y_n}=(g_1)^{\mathbf{M}^*_{i,1}\sum_{j=1}^{l}s_j+\mathbf{M}^*_{i,2}y_2+\mathbf{M}^*_{i,3}y_3+\cdots+\mathbf{M}^*_{i,n}y_n}\left(Y_2\right)^{l\mathbf{M}^*_{i,1}}.$$

任意选取随机数$t_1,t_2,\cdots,t_l\leftarrow_R\left(Z_p\right)^l$, 对于$\tau=1,2,\cdots,l$, 计算$C_{\tau,1}=\left(D_\tau\right)^\eta v^{t_\tau}$, $C_{\tau,2}=\left(u^{\rho^*(\tau)}h\right)^{-t_\tau}$和$C_{\tau,3}=g_1^{t_\tau}$. 最后输出相应的挑战密文$ct_\beta=\left(C,\left\{C_i\right\}_{i=1,2,\cdots,m},\left\{C_{\tau,1},C_{\tau,2},C_{\tau,3}\right\}_{\tau=1,2,\cdots,l}\right)$给敌手$\mathcal{A}$.

则挑战密文可表示为

$$ct_\beta=\left(C=M_\beta T,\left\{C_i=g^{s_i}Y_2\right\}_{i=1,2,\cdots,m},\left\{C_{\tau,1}=w^{\lambda_\tau}v^{t_\tau}\left(Y_2\right)^{l\eta\mathbf{M}_{i,1}},C_{\tau,2}=\left(u^{\rho^*(\tau)}h\right)^{-t_\tau},C_{\tau,3}=g_1^{t_\tau}\right\}_{\tau=1,2,\cdots,l}\right),$$

其中$C_{\tau,1}=\left(D_\tau\right)^\eta v^{t_\tau}=w^{\lambda_\tau}v^{t_\tau}\left(Y_2\right)^{l\eta\mathbf{M}_{i,1}}$. 隐含地设置了$\lambda_i=\mathbf{M}^*_{i,1}\sum_{j=1}^{l}s_j+\mathbf{M}^*_{i,2}y_2+\mathbf{M}^*_{i,3}y_3+\cdots+\mathbf{M}^*_{i,n}y_n$和$\vec{\lambda}=\left(\lambda_1,\lambda_2,\cdots,\lambda_l\right)^\top=\mathbf{M}^*\vec{y}$, 其中$\vec{y}=\left(\sum_{i=1}^{m}s_i,y_2,\cdots,y_n\right)$. 特别地, 挑战密文$ct_\beta$是消息$M_\beta$的半功能密文.

（4）阶段二. 该阶段与阶段一相类似, 敌手$\mathcal{B}$以相同的方式应答敌手$\mathcal{A}$的密钥生成询问，但该阶段禁止敌手$\mathcal{A}$进行泄露询问.

（5）猜测. 敌手$\mathcal{A}$输出对随机数β的猜测β'. 若$\beta=\beta'$, 则敌手$\mathcal{B}$输出 1, 表示敌手$\mathcal{A}$在该游戏中获胜; 否则, 敌手$\mathcal{B}$输出 0.

下面分两类讨论挑战密文$ct_\beta=\left(C,\left\{C_i\right\}_{i=1,2,\cdots,m},\left\{C_{\tau,1},C_{\tau,2},C_{\tau,3}\right\}_{\tau=1,2,\cdots,l}\right)$的形式：

① 若$T=\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i}$, 那么挑战密文为

$$ct_\beta=\left(C=M_\beta\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i},\left\{C_i=g^{s_i}Y_2\right\}_{i=1,2,\cdots,m},\left\{C_{\tau,1}=w^{\lambda_\tau}v^{t_\tau}\left(Y_2\right)^{l\eta\mathbf{M}_{i,1}},C_{\tau,2}=\left(u^{\rho^*(\tau)}h\right)^{-t_\tau},C_{\tau,3}=g_1^{t_\tau}\right\}_{\tau=1,2,\cdots,l}\right)$$

此时挑战密文ct_β为消息M_β的半功能密文, 敌手$\mathcal{B}$模拟了游戏$Game_{L,2}$.

②若$T\in G_T$, 此时T可写为$T=e(g,g)^\mu\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i}$, 其中$\mu\in Z_p$是$Z_p$上的随机数, 则挑战密文$ct_\beta$为随机消息$M_\beta e(g,g)^\mu$的半功能密文, 敌手$\mathcal{B}$模拟了游戏$Game_{final}$.

综上所述, 如果敌手$\mathcal{A}$能以不可忽略的优势区分游戏$Game_{L,2}$与$Game_{final}$, 那么敌手$\mathcal{B}$能以相同的优势攻破改进的合数阶子群判定假设 3, 因此有$\left|\Pr\left[Game_{L.2}\right]-\Pr\left[Game_{final}\right]\right|\le\mathsf{negl}(\kappa)$.

定理 3. 若改进的子群判定假设 1, 2, 3 成立, 那么不存在概率多项式时间的敌手能以不可忽略的优势

攻破上述抗泄露 CP-ABE 机制的 LR-CPA 安全性, 即本节构造的 CP-ABE 机制具有 LR-CPA 安全性.

证明: 由引理 1 到引理 6 可知, $Game_{final}$ 与 $Game_{real}$ 是不可区分的, 即如表 3 所示, 有关系式 $\left|\Pr\left[Game_{real}\right]-\Pr\left[Game_{final}\right]\right|\le \mathsf{negl}(\kappa)$ 成立. 由于敌手 $\mathcal{A}$ 在游戏 $Game_{final}$ 中获胜的优势是可忽略的, 因此敌手 $\mathcal{A}$ 在游戏 $Game_{real}$ 中获胜的优势也是可忽略的, 则本节的 CP-ABE 机制具有 LR-CPA 安全性.

表3 定理3的具体证明过程

引理	结论	备注
引理 1	$\left\|\Pr\left[Game_{real}\right]-\Pr\left[Game_{res}\right]\right\|\le \mathsf{negl}(\kappa)$	
引理 2	$\left\|\Pr\left[Game_{res}\right]-\Pr\left[Game_{0}\right]\right\|\le \mathsf{negl}(\kappa)$	
引理 3	$\left\|\Pr\left[Game_{0}\right]-\Pr\left[Game_{1.1}\right]\right\|\le \mathsf{negl}(\kappa)$	
引理 4	$\left\|\Pr\left[Game_{k.1}\right]-\Pr\left[Game_{k.2}\right]\right\|\le \mathsf{negl}(\kappa)$	$k=1,2,\cdots,L$
引理 5	$\left\|\Pr\left[Game_{k-1.2}\right]-\Pr\left[Game_{k.1}\right]\right\|\le \mathsf{negl}(\kappa)$	$k=2,\cdots,L$
引理 6	$\left\|\Pr\left[Game_{L.2}\right]-\Pr\left[Game_{final}\right]\right\|\le \mathsf{negl}(\kappa)$	
结论	$\left\|\Pr\left[Game_{real}\right]-\Pr\left[Game_{final}\right]\right\|\le \mathsf{negl}(\kappa)$	

5.4 性能比较

第 4 章已将本文构造与现有相关构造进行了性能对比，那么本节将对本文所提出的两种方案进行性能对比（将第 4 章的方案称为方案一，第 5 章的方案称为方案二），具体结果如表 4 所示，其中方案一是在素数阶群上构造的，相较于在合数阶群上构造的方案二而言，其计算效率更高，但它的安全性是基于非静态假设证明的；然而，方案二则基于静态假设获得了更加紧致的安全性归约. 特别地，方案一和方案二均能满足实际应用环境对大属性集合的部署需求.

表4 本文两种方案的性能对比

机制	方案一	方案二
设计目标	设计支持大属性集合的高效抗泄露 ABE 机制	设计支持大属性集合的具有紧致安全性归约的抗泄露 ABE 机制
关键技术	素数阶群+非静态安全性假设	合数阶群+静态安全假设
性能优点	计算效率高+支持大属性集合	紧致的安全性归约+支持大属性集合
性能不足	安全性归约损耗较大	计算效率较低

6 结论

ABE机制提供了实现数据细粒度访问控制的最有效手段，为了保证ABE机制在存在泄露攻击的现实环境中仍保持其安全性，一系列的抗泄露ABE机制已被提出. 然而，现有的抗泄露ABE机制其公开参数的长度与属性集合的大小呈线性关系, 导致现有构造的实用性不强. 因此, 本文提出了支持大属性集的抗泄露ABE机制. 本文首先在素数阶群上提出了支持大属性集的高效抗泄露ABE机制, 通过判定的并行双线性Diffie-Hellman指数假设

证明了该方案的安全性，并且综合性能分析表明其实现了更高的效率. 另外为了获得更紧致的形式化安全性证明过程, 本文提出了合数阶上支持大属性集的抗泄露属ABE机制, 并基于改进的合数阶群上的子群判定假设证明了其安全性.

本文构造与现有抗泄露ABE机制一样仅获得了挑战前的泄露容忍性, 即禁止敌手在获得挑战密文后进行泄露询问. 由于挑战后泄露容忍性更接近现实应用环境的实际需求, 因此本文下一步将在现有挑战后泄露容忍性的研究基础上, 提出抵抗挑战后泄露攻击的抗泄露ABE机制. 此外, 目前对属性基加密机制抗泄露性的研究主要集中在具体方案的设计领域, 本文将以属性基哈希证明系统为底层工具研究抗泄露属性基加密机制的通用构造方法, 并从挑战前和挑战后两个角度出发考虑通用构造的设计.

参考文献

1 Moritz Lipp, Andreas Kogler, David F. Oswald, Michael Schwarz, Catherine Easdon, Claudio Canella, Daniel Gruss. PLATYPUS: Software-based Power Side-Channel Attacks on x86. 42nd IEEE Symposium on Security and Privacy, S&P 2021, San Francisco, CA, USA, 24-27 May 2021, PP: 355-371

2 Kalle Ngo, Elena Dubrova, Qian Guo, Thomas Johansson. A Side-Channel Attack on a Masked IND-CCA Secure Saber KEM Implementation. IACR Transactions on Cryptographic Hardware and Embedded Systems. 2021, 2021(4): 676-707

3 Lin Lyu, Shengli Liu, Dawu Gu. Structure-preserving public-key encryption with leakage-resilient CCA security. Theoretical Computer Science, 2019, 795: 57-80 (2019)

4 Meijuan Huang, Bo Yang, Yanwei Zhou, Xuewei Hu. Continual Leakage-Resilient Hedged Public-Key Encryption. Computer Journal, 2022, 65(6): 1574-1585

5 Suvradip Chakraborty, C. Pandu Rangan. Public Key Encryption Resilient to Post-challenge Leakage and Tampering Attacks. Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, PP: 23-43.

6 Yanwei Zhou, Zhaolong Wang, Zirui Qiao, Ying Wang, Bo Yang, Yi Mu, Mingwu Zhang. Identity-Based Encryption with Continuous Leakage-Resilient CCA Security from Static Complexity Assumption. Computer Journal, 2023, 66(4): 924-940

7 Cailing Cai, Xianrui Qin, Tsz Hon Yuen, Siu-Ming Yiu. Tight Leakage-Resilient Identity-based Encryption under Multi-challenge Setting. ASIA CCS'22: ACM Asia Conference on Computer and Communications Security, Nagasaki, Japan, 30 May 2022 - 3 June 2022, PP: 42-53.

8 Ryo Nishimaki, Takashi Yamakawa. Leakage-Resilient Identity-Based Encryption in Bounded Retrieval Model with Nearly Optimal Leakage-Ratio. Public-Key Cryptography - PKC 2019 - 22nd IACR International Conference on Practice and Theory of Public-Key Cryptography, Beijing, China, April 14-17, 2019, PP: 466-495

9 Hang Li, Keping Yu, Bin Liu, Chaosheng Feng, Zhiguang Qin, Gautam Srivastava. An Efficient Ciphertext-Policy Weighted Attribute-Based Encryption for the Internet of Health Things. IEEE Journal of Biomedical and Health Informatics, 2022, 26(5): 1949-1960

10 Jiguo Li, Yichen Zhang, Jianting Ning, Xinyi Huang, Geong Sen Poh, Debang Wang. Attribute-Based Encryption with Privacy Protection and Accountability for CloudIoT. IEEE Transactions on Cloud Computing. 2022, 10(2): 762-773

11 Chunpeng Ge, Willy Susilo, Joonsang Baek, Zhe Liu, Jinyue Xia, Liming Fang. Revocable Attribute-Based Encryption with Data Integrity in Clouds. IEEE Transactions on Dependable and Secure Computing. 2022, 19(5): 2864-2872

12 Shaobo Chen, Jiguo Li, Yichen Zhang, Jinguang Han. Efficient Revocable Attribute-Based Encryption with Verifiable Data Integrity. IEEE Internet of Things Journal. 2024, 11(6): 10441-10451

13 Jiguo Li, Yao Wang, Yichen Zhang, Jinguang Han. Full Verifiability for Outsourced Decryption in Attribute-Based Encryption. IEEE Transactions on Services Computing. 2020, 13(3): 478-487

14 Zhiwei Wang, Siu-Ming Yiu. Attribute-Based Encryption Resilient to Auxiliary Input. Provable Security - 9th International Conference, ProvSec 2015, Kanazawa, Japan, November 24-26, 2015, PP: 371-390

15 Leyou Zhang, Yujie Shang. Leakage-resilient Attribute-based Encryption with CCA2 Security. Leakage-resilient Attribute-based Encryption with CCA2 Security. 2019, 21(5): 819-827

16 Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, Brent Waters. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. Advances in Cryptology - EUROCRYPT 2010, 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Monaco / French Riviera, May 30 - June 3, 2010, PP: 62-91

17 Mingwu Zhang, Yudi Zhang, Yixin Su, Qiong Huang, Yi Mu. Attribute-Based Hash Proof System Under Learning-With-Errors Assumption in Obfuscator-Free and Leakage-Resilient Environments. IEEE Systems Journal. 2017, 11(2): 1018-1026

18 Jiguo Li, Qihong Yu, Yichen Zhang, Jian Shen: Key-policy attribute-based encryption against continual auxiliary input leakage. Inf. Sci. 2019, 470: 175-188.

19 Leyou Zhang, Jingxia Zhang, Yupu Hu. Attribute-based encryption resilient to continual auxiliary leakage with constant size ciphertexts. The Journal of ChinaUniversities of Posts and Telecommunications, 2016, 23(3): 18-28

20 Yuyan Guo, Zhenhua Lu, Mingming Jiang, Dongbing Zhang. Ciphertext-Policy Attribute-Based Encryption Against Post-challenge Continuous Auxiliary Inputs Leakage. International Journal of Network Security, 2022, 24(3):511-520

21 Haiying Ma, Zhanjun Wang, Jinhua Wang, Zhijin Guan. Multi-Authority Attribute-based Encryption Resilient against Auxiliary-Input Leakage. Journal of Computers, 2020, 31(1):134-147

22 Jiguo Li, Qihong Yu, Yichen Zhang: Hierarchical attribute-based encryption with continuous leakage-resilience. Information Sciences. 2019, 484: 113-134

23 Yevgeniy Dodis, Shafi Goldwasser, Yael Tauman Kalai, Chris Peikert, Vinod Vaikuntanathan. Public-Key Encryption Schemes with Auxiliary Inputs. Theory of Cryptography, 7th Theory of Cryptography Conference, TCC 2010, Zurich, Switzerland, February 9-11, 2010, PP: 361-381

24 周彦伟. 公钥密码学:算法构造及安全性证明. 科学出版社, 北京, 2024

Leakage-resilient Attribute-based Encryption Scheme with Large Universe

ZHOU Yan-Wei[①③] XU Ran[①] QIAO Zi-Rui[②] YANG Kun-Wei[①] YANG Bo[①]

① School of Computer Science, Shaanxi Normal University, Xi'an 710062, Shaanxi, China

② School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

③ State Key Laboratory of Cryptology, Beijing 100878, China

* E-mail: qzr_snnu@163.com, byang@snnu.edu.cn

Abstract: Various leakage attacks in the actual environment allow attackers to obtain partial leakage of user secret information from cryptographic algorithms, resulting in traditional security no longer maintaining security in environments with leakage attacks. Cryptography researchers have proposed a series of cryptographic algorithms with leakage resilience to prevent the harm of leakage attacks on data security. The attribute-based encryption (ABE) scheme has received widespread attention and application in real-world environments due to its ability to provide fine-grained access control for data. However, in constructing existing leakage-resilient ABE schemes, the size of the system's public parameters is directly proportional to the size of the attribute set it can support, making it unable to be used in large attribute set environments. This paper proposes a new construction method for the leakage-resilient ABE scheme that supports large attribute sets. Firstly, to achieve better computational efficiency, this paper proposes a construction method for a leakage-resilient ABE scheme that supports large attribute sets on prime order groups and proves the security of this scheme based on the q-parallel bilinear Diffie Hellman exponent assumption. At the same time, performance analysis shows that our scheme has better computational, storage, and communication efficiency. Finally, to obtain a tight formal security proof, this paper proposes a construction method for a leakage ABE scheme that

supports large attribute sets on composite order groups. It proves the security of the above scheme based on the improved assumption of subgroup determination on composite order groups.

Key words: Leakage-resilience; Attribute-based Encryption; Large Universe; Dual System Encryption