中国科学: 信息科学 2024 年 第 54 卷 第 12 期: 2761–2777
SCIENTIA SINICA Informationis
论文

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

* 通信作者. E-mail: qzr@snnu.edu.cn, yangkunwei@snnu.edu.cn

收稿日期: 2024–06–05; 修回日期: 2024–09–09; 接受日期: 2024–10–25; 网络出版日期: 2024–12–09

国家自然科学基金 (批准号: 62272287)、陕西省重点研发计划 (批准号: 2024GX-YBXM-074)、四川大学数据安全防护与智能治理教育部重点实验室开放课题 (批准号: SCUSAKFKT202401Y) 和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集环境中使用. 为进一步增强抗泄露 ABE 机制的实用性和适用性, 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. 此外, 本文还对上述两种抗泄露 ABE 机制的基本性能进行了对比和分析

关键词 泄露容忍性, 属性基加密机制, 大属性集合, 辅助输入泄露

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一定的泄露 [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, 因此泄露容忍性已成为密码原语当前必备的安全属性之一.

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, 2024, 54: 2761–2777, doi: 10.1360/SSI-2024-0198
Zhou Y W, Xu R, Qiao Z R, et al. Leakage-resilient attribute-based encryption scheme with large universe (in Chinese). Sci Sin Inform, 2024, 54: 2761–2777, doi: 10.1360/SSI-2024-0198

© 2024《中国科学》杂志社 www.scichina.com infocn.scichina.com

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

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, 研究人员已经对 ABE 机制开展了一系列的研究工作. Li 等 [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 [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 [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. 为实现云计算系统中数据访问权限的撤销, Chen 等 [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 [13] 提出了具有可验证外包解密功能的 ABE 机制, 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. 然而, 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 [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 [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 [19] 在连续辅助输入模型下设计了一个属性基广播加密方案, 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 [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 [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 [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. 虽然上述构造能够抵抗泄露攻击, 但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. 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, 实现支持大属性域的抗泄露 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, 但相应方案的实用性和适用性较差, 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. 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, 更符合现实环境中抗泄露 ABE 机制的大属性集部署需求.

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

2 基础知识

本节将介绍证明所需的复杂性假设、Goldreich-Levin 定理等基础知识. 本文用 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.

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 和 p_3 是等长的三个大素数, p_i 是子群 G_i 的阶, g_1, g_2 和 g_3 分别是子群 G_1, G_2 和 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:

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

(2) 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.

(3) 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.

特别地, 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 $(\mathbb{G}, g_1, X_3, \{T_{0i}\}_{i=1,2,\ldots,m})$ 和 $(\mathbb{G}, g_1, X_3, \{T_{1i}\}_{i=1,2,\ldots,m})$, 其中 $g_1\leftarrow_R G_1$, $X_3\leftarrow_R G_3$, $T_{0i}\leftarrow_R G_{12}$ 和 $T_{1i}\leftarrow_R G_1$. 对于任意的概率多项式时间算法 $\mathcal{A}$, 其成功区分元组 $(D,T_{0i})_{i=1,2,\ldots,m}$ 和 $(D,T_{1i})_{i=1,2,\ldots,m}$ 的优势

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

是可忽略的, 其中 $D=(\mathbb{G}, g_1, X_3)$, 且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 $(\mathbb{G}, g_1, \{X_{1i}X_{2i}\}_{i=1,2,\ldots,m}X_3, Y_2Y_3, T_0)$ 和 $(\mathbb{G}, g_1, \{X_{1i}X_{2i}\}_{i=1,2,\ldots,m}X_3, Y_2Y_3, T_1)$, 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 $T_1\leftarrow_R G_{13}$. 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

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

是可忽略的, 其中 $D=(\mathbb{G}, g_1, \{X_{1i}X_{2i}\}_{i=1,2,\ldots,m}X_3, Y_2Y_3)$, 且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 $(\mathbb{G}, g_1, \{g^{\alpha_i}X_2, g^{s_i}Y_2\}_{i=1,2,\ldots,m}X_3, Z_2, T_0)$ 和 $(\mathbb{G}, g_1, \{g^{\alpha_i}X_2, g^{s_i}Y_2\}_{i=1,2,\ldots,m}X_3, Z_2, T_1)$, 其中 $g_1\leftarrow_R G_1$, $X_2, Y_2, Z_2\leftarrow_R G_2$, $X_3\leftarrow_R G_3$, $\alpha_i, s_i\leftarrow_R Z_N$, $T_0=\prod_{i=1}^m e(g_1,g_1)^{\alpha_i s_i}$ 和 $T_1\leftarrow_R G_T$. 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

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

是可忽略的, 其中 $D=(\mathbb{G}, g_1, \{g^{\alpha_i}X_2, g^{s_i}Y_2\}_{i=1,2,\ldots,m}X_3, Z_2)$, 且概率来源于随机值的选取与使用.

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

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 $a,s,b_1,\ldots,b_q\leftarrow_R(Z_p)^{q+2}$. 令公开参数为

$$D=\left(\begin{array}{l} g,g^s,g^a,g^{a^2},\ldots,g^{a^q},g^{b_1},g^{b_2},\ldots,g^{b_q} \\ \forall_{1\leqslant j\leqslant q},g^{ab_j},\ldots,g^{a^qb_j},g^{a/b_j^2},g^{a^2/b_j^2},\ldots,g^{a^q/b_j^2} \\ \forall_{1\leqslant j,k\leqslant q,k\neq j},g^{ab_k/b_j^2},\ldots,g^{a^qb_k/b_j^2},g^{a^{q+1}b_k/b_j^2},\ldots,g^{a^{2q}b_k/b_j^2} \\ \forall_{1\leqslant j\leqslant q}g^{s\cdot b_j},g^{a/b_j},\ldots,g^{a^q/b_j},g^{a^{q+2}/b_j},\ldots,g^{a^{2q}/b_j} \\ \forall_{1\leqslant j,k\leqslant q,k\neq j}g^{a\cdot s\cdot b_k/b_j},\ldots,g^{a^q\cdot s\cdot b_k/b_j} \end{array}\right),$$

对于元组 $(D,Z_1)=(D,e(g,g)^{a^{q+1}s})$ 与 $(D,Z_2)=(D,R)$, 其中 R 是 $\tilde{G}_T$ 中的随机元素. 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

$$\mathsf{Adv}_{\mathcal{A}}(\kappa)=|\Pr[\mathcal{A}(D,Z_1)=1]-\Pr[\mathcal{A}(D,Z_2)=1]|\leqslant\mathsf{negl}(\kappa)$$

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满足下述条件: 存在一个 $l\times n$ 的矩阵 $\boldsymbol{M}$, 将其称为秘密共享矩阵. 对于 $i=1,2,\ldots,l$, 矩阵 $\boldsymbol{M}$ 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 $s,y_2,\ldots,y_n\leftarrow(Z_p)^{n+1}$, 对于列向量 $\boldsymbol{y}=(s,y_2,\ldots,y_n)^{\mathrm{T}}$, s 为共享的秘密, $\boldsymbol{My}$ 是秘密 s 共享的 l 个分量, 即有 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\ldots,\lambda_l)^{\mathrm{T}}=\boldsymbol{My}$. 特别地, 将上述访问策略表示为 $\psi=(\boldsymbol{M},\rho)$. 定义 $I=\{i:i\in[l]\wedge\rho(i)\in S\}$. 若属性集合 S 满足访问策略 $\psi=(\boldsymbol{M},\rho)$, 即 $\psi(S)=1$, 且 $\{\lambda_i\}_{i=1,2,\ldots,l}$ 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 [23]) 令 q 是一个大素数, H 是有限域 $\mathrm{GF}(q)$ 的一个子集. 定义单向映射函数 $f:H^m\to\{0,1\}^*$. 任意选取 $\boldsymbol{s}\leftarrow H^m$ 和 $\boldsymbol{r}\leftarrow\mathrm{GF}(q)^m$, 计算 $y=f(\boldsymbol{s})$. 如果存在概率多项式时间 t 内的区分器 D 使得 $|\Pr[D(y,\boldsymbol{r},\langle\boldsymbol{r},\boldsymbol{s}\rangle)=1]-\Pr[D(y,\boldsymbol{r},u)=1]|=\varepsilon$ 成立 (其中 $u\leftarrow_R\mathrm{GF}(q)$ 和 $m=(3\log q)^{1/\varepsilon}$), 则存在可逆器 U 在时间 $t'=t\cdot\mathrm{poly}(m,|H|,1/\varepsilon)$ 内使得 $\Pr[\boldsymbol{s}\leftarrow H^m,y\leftarrow f(\boldsymbol{s}):U(y)=\boldsymbol{s}]\geqslant\frac{\varepsilon^3}{512\cdot m\cdot q^2}$ 成立.

定理 1 表明若存在区分器能在多项式时间内以不可忽略的优势区分两个元组 $(y,\boldsymbol{r},\langle\boldsymbol{r},\boldsymbol{s}\rangle)$ 和 $(y,\boldsymbol{r},u)$, 那么存在可逆器能以不可忽略的优势攻破映射函数 f 的单向性. 进一步讲, 区分器在已知秘密值 $\boldsymbol{s}$ 的泄露信息 y (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 $\boldsymbol{r}$ 的前提下, 其依然无法区分内积值 $\langle\boldsymbol{r},\boldsymbol{s}\rangle$ 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 $\boldsymbol{s}$ 的泄露信息 y 和向量 $\boldsymbol{r}$ 时, 内积值 $\langle\boldsymbol{r},\boldsymbol{s}\rangle$ 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 在确保内积计算结果均匀随机的同时保证了映射函数 f 是不可逆的, 该性质正好与辅助输入模型的要求相吻合.

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

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 chosen-plaintext attack, LR-CPA) 安全性游戏 $\mathsf{Exp}^{\text{LR-CPA}}_{\text{CP-ABE},\mathcal{A}}(\kappa)$ 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: $(\text{params}, \text{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$. 特别地, params 是下述 3 个算法的隐含输入.

(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: $\text{sk} \leftarrow \mathsf{KeyGen}(\text{msk}, S)$.

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

(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 $\psi = (\boldsymbol{M}, \rho)$ (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 $M/\perp \leftarrow \mathsf{Dec}(\text{ct}, \text{sk})$.

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 $\psi = (\boldsymbol{M}, \rho)$, 即 $\psi(S) = 1$, 那么有 $\Pr[M = M' | \text{ct} \leftarrow \mathsf{Enc}(M, (\boldsymbol{M}, \rho)), M' \leftarrow \mathsf{Dec}(\text{ct}, \text{sk})] \leqslant \mathsf{negl}(\kappa)$ 成立, 其中 $(\text{params}, \text{msk}) \leftarrow \mathsf{Setup}(1^\kappa)$ 和 $\text{sk} \leftarrow \mathsf{KeyGen}(\text{msk}, S)$.

3.3 安全模型

安全模型模拟了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 $\mathsf{Exp}^{\text{LR-CPA}}_{\text{CP-ABE},\mathcal{A}}(\kappa)$ 通过为敌手 $\mathcal{A}$ 提供访问泄露谕言机 $\mathcal{O}^{\mathsf{Leak}}_{\text{sk}}(\kappa)$ 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 $\mathsf{Exp}^{\text{LR-CPA}}_{\text{CP-ABE},\mathcal{A}}(\kappa)$ 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, 那么存在泄露的情况下, 相应的 CP-ABE 机制拥有 LR-CPA 安全性.

$\mathsf{Exp}^{\text{LR-CPA}}_{\text{CP-ABE},\mathcal{A}}(\kappa)$:

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

(2) $(\psi^*, M_0, M_1) \leftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{Leak}}_{\text{sk}}(\kappa), \mathcal{O}^{\mathsf{KeyGen}(\cdot)}}(\text{params})$,

(3) $ct^*_b \leftarrow \mathsf{Enc}(\psi^*, M_b)$, 其中$b \leftarrow_R \{0,1\}$;

(4) $b' \leftarrow \mathcal{A}^{\mathcal{O}^{\mathsf{KeyGen}}_{\neq\psi^*}(\cdot)}(\text{params}, ct^*_b)$;

(5) If $b = b'$, output 1; otherwise, return 0,

其中 ψ^* 是挑战访问策略, $|M_0| = |M_1|$; $\mathcal{O}^{\mathsf{Leak}}_{\text{sk}}(\kappa)$ 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 $\psi^* = (\boldsymbol{M}^*, \rho^*)$ 的属性集合) 对应私钥 sk 的泄露信息; $\mathcal{O}^{\mathsf{KeyGen}}(\cdot)$ 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 $\mathcal{O}^{\mathsf{KeyGen}}_{\neq\psi^*}(\cdot)$ 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.

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

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 本文的构造

本文抗泄露 CP-ABE 机制具体包含下述 4 个算法.

(1) 初始化算法 $(\text{params}, \text{msk}) \leftarrow \mathsf{Setup}\,(1^\kappa)$ 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 $e: \tilde{G}\times\tilde{G}\to\tilde{G}_T$. 设属性全集为 $U=Z_p$. 任意选取随机数 $u,h,w,v{\leftarrow_R}(\tilde{G})^4$ 和 $\alpha_1,\alpha_2,\ldots,\alpha_m{\leftarrow_R}(Z_p)^m$. 令主私钥为 $\text{msk}=(\alpha_1,\alpha_2,\ldots,\alpha_m)$, 其中 $m=(3\log p)^{1/\varepsilon}$ (m 的取值由定理 1 确定 [21]) 和 $0<\varepsilon<1$. 最后公开系统参数 $\text{params}=(g,u,v,h,w,\{e(g,g)^{\alpha_i}\}_{i=1,2,\ldots,m})$.

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

任意选取随机数 $r,r_1,\ldots,r_k{\leftarrow_R}(Z_p)^{k+1}$ (其中 $k=|S|$, 即 k 为属性集合 $S=\{A_1,\ldots,A_k\}$ 中属性的数量), 计算 $\{K_i=g^{\alpha_i}w^r\}_{i=1,2,\ldots,m}$ 和 $K_0=g^r$. 对于 $\tau=1,2,\ldots,k$, 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 $\text{sk}=(S,\{K_i\}_{i=1,2,\ldots,m},K_0,\{K_{\tau,1},K_{\tau,2}\}_{\tau=1,2,\ldots,k})$.

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

输入待加密的消息 M 和访问策略 $\psi=(\boldsymbol{M},\rho)$, 其中 $\boldsymbol{M}$ 是一个 $l\times n$ 矩阵, ρ 是矩阵 $\boldsymbol{M}$ 的行属性映射函数. 任意选取随机数 $s_1,s_2,\ldots,s_m{\leftarrow_R}(Z_p)^m$ 和 $y_2,\ldots,y_n{\leftarrow_R}(Z_p)^{n-1}$, 并计算 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\ldots,\lambda_l)^{\mathrm{T}}=\boldsymbol{My}$, $C=M\prod_{i=1}^m e(g,g)^{\alpha_i s_i}$ 和 $\{C_i=g^{s_i}\}_{i=1,2,\ldots,m}$, 其中 $\boldsymbol{y}=(\sum_{i=1}^m s_i,y_2,\ldots,y_n)$ 和 $\sum_{i=1}^m s_i$ 是要分享的秘密值. 特别地, 向量 $\boldsymbol{\lambda}$ 协助解密者实现共享秘密的恢复. 任意选取 l 个随机数 $t_1,t_2,\ldots,t_l{\leftarrow_R}(Z_p)^l$, 对于 $\tau=1,2,\ldots,l$, 计算 $C_{\tau,1}=w^{\lambda_\tau}v^{t_\tau}$, $C_{\tau,2}=\left(u^{\rho(\tau)}h\right)^{-t_\tau}$ 和 $C_{\tau,3}=g^{t_\tau}$. 最后输出相应的加密密文 $\text{ct}=(\psi=(\boldsymbol{M},\rho),C,\{C_i\}_{i=1,2,\ldots,m},\{C_{\tau,1},C_{\tau,2},C_{\tau,3}\}_{\tau=1,2,\ldots,l})$.

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

输入密文 $\text{ct}=(\psi=(\boldsymbol{M},\rho),C,\{C_i\}_{i=1,2,\ldots,m},\{C_{\tau,1},C_{\tau,2},C_{\tau,3}\}_{\tau=1,2,\ldots,l})$ 及属性集合 S 对应的密钥 $\text{sk}=(S,\{K_i\}_{i=1,2,\ldots,m},K_0,\{K_{\tau,1},K_{\tau,2}\}_{\tau=1,2,\ldots,k})$, 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 $\psi=(\boldsymbol{M},\rho)$, 即 $\psi(S)\neq 1$, 那么输出 $\perp$; 否则有 $\psi(S)=1$, 那么存在 $\{\omega_i\in Z_p\}_{i\in I}$, 使得 $\sum_{i\in I}\omega_i\boldsymbol{M}_i=(1,0,\ldots,0)$ 成立, 其中 $\boldsymbol{M}_i$ 是矩阵 $\boldsymbol{M}$ 的第 i 行. 最后计算 $E=\frac{\prod_{i=1}^m e(C_i,K_i)}{\prod_{i\in I}\left(e(C_{i,1},K_0)e(C_{i,2},K_{i,1})e(C_{i,3},K_{i,2})\right)^{\omega_i}}$, 并输出明文消息 $M=C/E$.

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 $\psi=(\boldsymbol{M},\rho)$, 那么有 $\sum_{i\in I}\omega_i M_i=(1,0,\ldots,0)$ 成立, 本节抗泄露 CP-ABE 机制的正确性由下述等式获得:

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

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

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

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 游戏开始前, 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 $Z\in\tilde{G}_T$ (将群 $\tilde{G}_T$ 上的随机元素写为 $Z=e(g,g)^{sa^{q+1}+\eta}$, 其中 η 是 Z_p 上的随机值), 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 $\psi^*=(\boldsymbol{M}^*,\rho^*)$, 其中 $\boldsymbol{M}^*$ 是一个 $l\times n$ 矩阵, ρ^* 是矩阵 $\boldsymbol{M}^*$ 的行属性映射函数. $\mathcal{B}$ 选取任意的随机数 $a_1,a_2,\ldots,a_m\leftarrow_R(Z_p)^m$, 对于 $i=1,2,\ldots,m$, 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 $t_1,t_2,t_3,\ldots,t_m,\bar{v},\bar{u},\bar{h}\leftarrow_R(Z_p)^{m+3}$, $\mathcal{B}$ 计算

$$t=\sum_{i=1}^{m}t_i,\ u=g^{\bar{u}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{tM^*_{j,k}},\ h=g^{\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j^2}\right)^{-^*(j)tM^*_{j,k}},$$

$$w=g^a,\ v=g^{\bar{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k/b_j}\right)^{tM^*_{j,k}}.$$

最后, 敌手 $\mathcal{B}$ 公开系统参数 $\mathrm{params}=(g,u,v,h,w,\{e(g,g)^{\alpha_i}\}_{i=1,2,\ldots,m})$. 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 $t_1,t_2,t_3,\ldots,t_m$, 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.

(i) 秘密钥询问. 敌手 $\mathcal{A}$ 对不满足挑战访问策略 $\psi^*=(\boldsymbol{M}^*,\rho^*)$ 的属性集合 $S=\{A_1,\ldots,A_k\}$ 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^*, 因此存在向量 $\boldsymbol{\omega}=(\omega_1,\omega_2,\ldots,\omega_n)^{\mathrm{T}}\in(Z_p)^n$ (其中 $\omega_1=-1$), 使得对于 $i\in I=\{i|i\in[l]\wedge\rho^*(i)\in S\}$ 有 $\langle\boldsymbol{M}_i^*,\boldsymbol{\omega}\rangle=0$ 成立. $\mathcal{B}$ 任意选取随机数 $\bar{r}\leftarrow_R Z_p$, 通过计算 $K_0=g^{\bar{r}}\prod_{j=1}^{n}(g^{a^{q+1-j}})^{\omega_j}$, 隐含地设置了 $r=\bar{r}+\omega_1a^q+\omega_2a^{q-1}+\cdots+\omega_na^{q+1-n}=\bar{r}+\sum_{i=1}^{n}\omega_ia^{q+1-i}$. 对于 $i=1,2,\ldots,m$, 敌手 $\mathcal{B}$ 计算 $K_i=g^{a_i}(g^a)^{\bar{r}}\prod_{j=2}^{n}(g^{a^{q+2-j}})^{\omega_j}=g^{a^{q+1}}g^{a_i}g^{a\bar{r}}\prod_{j=1}^{n}g^{\omega_ja^{q+2-j}}=g^{\alpha_i}w^r$. 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 $K_{\tau,2}=(u^{A_\tau}h)^{r_\tau}v^{-r}$, 其中 $K_{\tau,2}$ 是由 $(u^{A_\tau}h)^{r_\tau}$ 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 $(u^{A_\tau}h)^{r_\tau}$ 和 v^{-r}.

由于 $v=g^{\bar{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}(g^{a^k/b_j})^{tM^*_{j,k}}$ 和 $r=\bar{r}+\sum_{i=1}^{n}\omega_ia^{q+1-i}$, 那么 v^{-r} 的计算过程如下:

$$\begin{aligned}v^{-r}&=v^{-\bar{r}}\left(g^{\bar{v}}\prod_{j=1}^{l}\prod_{k=1}^{n}g^{ta^kM^*_{j,k}/b_j}\right)^{-\sum_{i=1}^{n}\omega_ia^{q+1-i}}\\&=v^{-\bar{r}}\left(g^{\bar{v}}\right)^{-\sum_{i=1}^{n}\omega_ia^{q+1-i}}\left(\prod_{j=1}^{l}\prod_{k=1}^{n}g^{ta^kM^*_{j,k}/b_j}\right)^{-\sum_{i=1}^{n}\omega_ia^{q+1-i}}\\&=v^{-\bar{r}}\prod_{i=1}^{n}\left(g^{a^{q+1-i}}\right)^{-\bar{v}\omega_i}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{i=1}^{n}g^{-\omega_itM^*_{j,k}a^{q+1+k-i}/b_j}\end{aligned}$$

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

$$
\begin{aligned}
&= \phi \prod_{j=1}^{l} \prod_{i=1}^{n} g^{-\omega_i t M_{j,i}^* a^{q+1}/b_j} \\
&= \phi \prod_{j=1}^{l} g^{-\left\langle \boldsymbol{\omega}, \boldsymbol{M}_j^* \right\rangle t a^{q+1}/b_j} \\
&= \phi \prod_{j=1,\rho^*(j)\notin S}^{l} g^{-\left\langle \boldsymbol{\omega}, \boldsymbol{M}_j^* \right\rangle t a^{q+1}/b_j},
\end{aligned}
$$

其中 $\phi = v^{-\bar{r}} \prod_{i=1}^{n} \left(g^{a^{q+1-i}}\right)^{-\bar{v}\omega_i} \prod_{j=1}^{l} \prod_{k=1}^{n} \prod_{i=1,i\neq k}^{n} \left(g^{a^{q+1+k-i}/b_j}\right)^{-\omega_i t M_{j,k}^*}$. 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 $\prod_{j=1,\rho^*(j)\notin S}^{l} g^{-\langle \boldsymbol{\omega}, \boldsymbol{M}_j^* \rangle t a^{q+1}/b_j}$ 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 $\prod_{j=1,\rho^*(j)\notin S}^{l} g^{\langle \boldsymbol{\omega}, \boldsymbol{M}_j^* \rangle t a^{q+1}/b_j}$, 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

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

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 $\prod_{j=1,\rho^*(j)\notin S}^{l} g^{-\langle \boldsymbol{\omega}, \boldsymbol{M}_j^* \rangle t a^{q+1}/b_j}$. 特别地, 敌手 $\mathcal{B}$ 由已知参数计算可知

$$
\begin{aligned}
u^{A_\tau} h &= \left(g^{\bar{u}} \prod_{j=1}^{l} \prod_{k=1}^{n} \left(g^{a^k/b_j^2}\right)^{t M_{j,k}^*} \right)^{A_\tau} g^{\bar{h}} \prod_{j=1}^{l} \prod_{k=1}^{n} \left(g^{a^k/b_j^2}\right)^{-^*(j) t M_{j,k}^*} \\
&= g^{\bar{u} A_\tau + \bar{h}} \prod_{j=1}^{l} \prod_{k=1}^{n} \left(g^{a^k/b_j^2}\right)^{(A_\tau - ^*(j)) t M_{j,k}^*},
\end{aligned}
$$

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

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

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

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

$$
\begin{aligned}
&= \left(u^{A_\tau}h\right)^{\bar{r}_\tau}\left(g^{\bar{u}A_\tau+\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\left(g^{a^k}/b_j^2\right)^{(A_\tau-\rho^*(j))tM^*_{j,k}}\right)^{\bar{r}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta}{A_\tau-\rho^*(\eta)}+\sum\limits_{i=1}^{n}\sum\limits_{\eta=1,\rho^*(\eta)\notin S}^{l}\frac{b_\eta\omega_i a^{q+1-i}}{A_\tau-\rho^*(\eta)}}\\
&= \left(u^{A_\tau}h\right)^{\bar{r}_\tau}\left(K_{\tau,2}/g^{\bar{r}_\tau}\right)^{\bar{u}A_\tau+\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}\left(g^{a^k b_\eta/b_j^2}\right)^{\bar{r}(A_\tau-\rho^*(j))tM^*_{j,k}/(A_\tau-\rho^*(\eta))}\\
&\quad\cdot\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{i=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}\left(g^{a^{q+1+k-i}b_i/b_j^2}\right)^{(A_\tau-\rho^*(j))\omega_i tM^*_{j,k}/(A_\tau-\rho^*(\eta))}\\
&= \left(u^{A_\tau}h\right)^{\bar{r}_\tau}\left(K_{\tau,2}/g^{\bar{r}_\tau}\right)^{\bar{u}A_\tau+\bar{h}}\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}g^{\bar{r}(A_\tau-^*(j))M^*_{j,k}b_\eta ta^k/(A_\tau-\rho^*(\eta))b_j^2}\\
&\quad\cdot\prod_{j=1}^{l}\prod_{k=1}^{n}\prod_{i=1}^{n}\prod_{\eta=1,\rho^*(\eta)\notin S}^{l}g^{(A_\tau-\rho^*(j))\omega_i M^*_{j,k}b_i ta^{q+1+k-i}/(A_\tau-\rho^*(\eta))b_j^2}\\
&= \psi\prod_{i=1}^{n}\prod_{j=1,\rho^*(j)\notin S}^{l}g^{(A_\tau-\rho^*(j))\omega_i M^*_{j,i}b_j ta^{q+1+i-i}/(A_\tau-\rho^*(j))b_j^2}\\
&= \psi\prod_{j=1,\rho^*(j)\notin S}^{l}g^{\langle\boldsymbol{\omega},\boldsymbol{M}^*_j\rangle ta^{q+1}/b_j},
\end{aligned}
$$

其中

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

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 $\mathrm{sk}=(S,\{K_i\}_{i=1,2,\ldots,m},K_0,\{K_{\tau,1},K_{\tau,2}\}_{\tau=1,2,\ldots,k})$ 返回给敌手 $\mathcal{A}$.

(ii) 泄露询问. 敌手 $\mathcal{A}$ 将 $(S,f_i:\{0,1\}^*\to\{0,1\}^{\lambda_i})$ 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 $\psi^*=(\boldsymbol{M}^*,\rho^*)$), $f_i:\{0,1\}^*\to\{0,1\}^{\lambda_i}$ 是高效可计算的泄露函数. 若 $(S,\mathrm{sk})\in L$, 将 $f_i(\mathrm{sk})$ 返回给 $\mathcal{A}$. 特别地, 若集合 S 满足挑战访问策略 $\psi^*=(\boldsymbol{M}^*,\rho^*)$, 则 $\mathcal{B}$ 可以使用与密钥生成算法相类似的方法产生该属性集合对应的私钥 sk, 然后再返回相应的泄露信息 $f_i(\mathrm{sk})$.

(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 $C=M_\beta\prod_{i=1}^{m}Z^{t_i}e(g,(g^s)^{t_i})^{a_i}$ 和 $C_i=(g^s)^{t_i}$ $(i=1,2,\ldots,m)$. 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 $\bar{y}_2,\bar{y}_3,\ldots,\bar{y}_n\leftarrow_R(Z_p)^{n-1}$, 计算 $\tilde{\lambda}=\sum_{i=2}^{n}M^*_{\tau,i}\bar{y}_i$ (其中 $\tilde{\lambda}$ 是敌手 $\mathcal{B}$ 完全可

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

计算的). 对于 $\tau=1,2,\ldots,l$, 敌手 $\mathcal{B}$ 计算

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

令 $t_\tau=-sb_\tau$, $\tilde{\lambda}=\sum_{i=2}^{n}M^*_{\tau,i}\bar{y}_i$ 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)^{-(\rho^*(\tau)-^*(j))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^{(\rho^*(\tau)-\rho^*(j))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}
$$

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

其中敌手 $\mathcal{B}$ 隐含地设置了 $\boldsymbol{y}=\left(ts, tsa+\tilde{y}_2, \ldots, tsa^{n-1}+\tilde{y}_n\right)$. 由于 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\ldots,\lambda_l)^{\mathrm{T}}=\boldsymbol{M}^*\boldsymbol{y}$, 因此, 对于 $\tau=1,2,\ldots,l$, 有 $\lambda_\tau=\sum_{i=1}^n \boldsymbol{M}^*_{\tau,i}tsa^{i-1}+\sum_{i=2}^n \boldsymbol{M}^*_{\tau,i}\tilde{y}_i$, 其中 $\boldsymbol{M}^*_{\tau,i}$ 是矩阵 $\boldsymbol{M}^*$ 的第 τ 行第 j 列的元素. 最后, 敌手 $\mathcal{B}$ 发送挑战密文 $\mathrm{ct}=\left(\psi^*=\left(\boldsymbol{M}^*,\rho^*\right), C, \{C_i\}_{i=1,2,\ldots,m}, \{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\}_{\tau=1,2,\ldots,l}\right)$ 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 $Z=e(g,g)^{sa^{q+1}}$; 否则, 敌手 $\mathcal{B}$ 输出 0, 表示 $Z=e(g,g)^{sa^{q+1}+\eta}$, 其中 η 是 Z_p 上的随机值, 则 Z 是群 $\tilde{G}_T$ 的随机元素.

若 $Z=e(g,g)^{sa^{q+1}}$, 有

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

则 $\mathcal{A}$ 获得了关于消息 M_β 的有效加密密文 ct. 若 $\mathcal{A}$ 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 $\mathcal{B}$ 能以同样的优势输出 1. 即 $\Pr[\mathcal{B}(D,Z=e(g,g)^{sa^{q+1}})=1]=\frac{1}{2}+\varepsilon$.

若 $Z=e(g,g)^{sa^{q+1}+\eta}$, 则有

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

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

辅助输入模型允许敌手拥有一类不可逆的辅助函数 $f()$, 将这类不可逆的辅助函数作用于私钥 sk, 使敌手获得 sk 的函数值信息 $f(\mathrm{sk})$, 从而模拟 sk 的各种泄露情况, 但无论通过这些函数泄露的信息有多少, 甚至密钥 sk 在信息论意义上已被完全泄露, 但敌手从泄露信息恢复原始私钥是不可能的. 下面本小节将分析上述 CP-ABE 机制具备辅助输入模型下的泄露容忍性.

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 $\mathrm{sk}=(S,\{K_i=g^{\alpha_i}w^r\}_{i=1,2,\ldots,m},K_0,\{K_{\tau,1},K_{\tau,2}\}_{\tau=1,2,\ldots,k})$ 的泄露信息 $f(\mathrm{sk})$, 由于 sk 的核心信息是主私钥 $\mathbf{msk}=(\alpha_1,\alpha_2,\ldots,\alpha_m)$, 因此敌手 $\mathcal{A}$ 通过泄露询问获得了关于主私钥 $\mathbf{msk}$ 的泄露信息 $\tilde{f}(\mathbf{msk})$. 一般情况下, 泄露信息 $\tilde{f}(\mathbf{msk})$ 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 $\tilde{f}(\mathbf{msk})$ 对用于隐藏明文的元素 $\prod_{i=1}^m e(g,g)^{\alpha_i s_i}$ 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 $C=M\prod_{i=1}^m e(g,g)^{\alpha_i s_i}=Me(g,g)^{\sum_{i=1}^m \alpha_i s_i}$, 由定理 1 可知, 已知相应的参数为 $\mathbf{msk}=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ 和 $\boldsymbol{s}=(s_1,s_2,\ldots,s_n)$, 对于任意的概率多项式时间敌手 $\mathcal{A}$,

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

表 1　本文方案与相关抗泄露 ABE 机制的计算效率比较结果

Table 1　Comparison of computational efficiency between our proposal and the previous ABE schemes

Scheme	Key generation	Encryption	Decryption
Guo et al. [20]	$(4m+2+2l)\,T_E+(4m+l+1)\,T_P$	$(2m+3l)\,T_E+lT_P$	$3T_B$
Ma et al. [21]	$2mT_E$	$(m+2l+2lm)\,T_E+(2m+1)\,T_P$	$4T_B$
Li et al. [22]	$(2m+5+6l)\,T_E+(m+4l+4)\,T_P$	$(m+2+5l)\,T_E+2lT_P$	$4T_B$
This work	$(m+3+3l)\,T_E+2mT_P$	$(2m+2l)\,T_E+2lT_P$	$4T_B$

表 2　本文方案与相关抗泄露 ABE 机制的性能比较结果

Table 2　Comparison of performance between our proposal and the previous ABE schemes

Scheme	Storage efficiency	Communication efficiency	Whether large universe are supported
Guo et al. [20]	$1\lvert\tilde{G}_T\rvert+(3+2m+l)\lvert\tilde{G}\rvert$	$(2l+m+1)\lvert\tilde{G}\rvert$	Nonsupport
Ma et al. [21]	$2m\lvert\tilde{G}\rvert$	$(3lm+1)\lvert\tilde{G}\rvert$	Nonsupport
Li et al. [22]	$(1+m+l)\lvert\tilde{G}_T\rvert+m\lvert\tilde{G}\rvert$	$(3l+m+2)\lvert\tilde{G}\rvert$	Nonsupport
This work	$(m+5)\lvert\tilde{G}\rvert$	$(3l+m+1)\lvert\tilde{G}\rvert$	Support

有关系 $|\Pr[\mathcal{A}(y,\boldsymbol{s},\langle\mathbf{msk},\boldsymbol{s}\rangle)=1]-\Pr[\mathcal{A}(y,\boldsymbol{s},u)=1]|=\varepsilon$ 成立, 其中 ε 是安全参数上可忽略的值和 $y=\tilde{f}(\mathbf{msk})$ 为关于主私钥的泄露信息. 由定理 1 可知, $\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i}$ 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 $y=\tilde{f}(\mathbf{msk})$, 密文元素 $C=M\prod_{i=1}^{m}e(g,g)^{\alpha_i s_i}$ 依然保持与均匀随机值间的不可区分性. 因此在辅助输入模型中 (定理 1 保证了对本文泄露信息求逆的困难性), 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.

4.5　性能分析

本小节将本文方案与现有的抗泄露 ABE 机制进行综合分析和对比, 其中用 l 表示属性集合中的属性数量, 且 $m=(3\log p)^{1/\varepsilon}$.

(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.

(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.

5　基于静态假设的支持大属性集的抗泄露 CP-ABE 机制

虽然第 4 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

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

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

令乘法循环群 G 和 G_T 的阶为 $N = p_1p_2p_3$, 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 3 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 $U = Z_N$. 任意选取随机数 $w, u, h, v \leftarrow_R (G_1)^4$, $X_3 \leftarrow_R G_3$ 和 $\alpha_1, \alpha_2, \ldots, \alpha_m \leftarrow_R (Z_N)^m$, 令 $\text{msk} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$, 其中 $m = (3\log N)^{1/\varepsilon}$ 和 $0 < \varepsilon < 1$. 最后公开系统参数 $\text{params} = (g_1, X_3, u, w, h, v, \{e(g_1, g_1)^{\alpha_i}\}_{i=1,2,\ldots,m})$.

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

对于 $i = 1, \ldots, m$, 选取 $R, \tilde{R}_1, \ldots, \tilde{R}_m \leftarrow_R (G_3)^{m+1}$ 和 $r \leftarrow_R Z_N$, 计算 $\{K_i = g_1^{\alpha_i} w^r \tilde{R}_i\}_{i=1,\ldots,m}$ 和 $K_0 = g_1^r R$. 随机选取 $r_1, r_2, \ldots, r_k \leftarrow_R (Z_N)^k$ 和 $R_1, R_2, \ldots, R_k, \bar{R}_1, \bar{R}_2, \ldots, \bar{R}_k \leftarrow_R (G_3)^{2k}$, 对于 $\tau = 1, 2, \ldots, k$, 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 $S = \{A_1, A_2, \ldots, A_k\}$ 所对应的私钥 $\text{sk} = (S, \{K_i\}_{i=1,2,\ldots,m}, K_0, \{K_{\tau,1}, K_{\tau,2}\}_{\tau=1,2,\ldots,k})$.

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

输入待加密的消息 M 和访问策略 $\psi = (\boldsymbol{M}, \rho)$, 其中 $\boldsymbol{M}$ 是一个 $l \times n$ 矩阵, ρ 是 $\boldsymbol{M}$ 的行属性映射函数. 任意选取随机数 $s_1, s_2, \ldots, s_m \leftarrow_R (Z_N)^m$ 和 $y_2, \ldots, y_n \leftarrow_R (Z_N)^{n-1}$, 计算 $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \ldots, \lambda_l)^{\mathrm{T}} = \boldsymbol{My}$, $C = M \prod_{i=1}^m e(g_1, g_1)^{\alpha_i s_i}$ 和 $\{C_i = g_1^{s_i}\}_{i=1,2,\ldots,m}$, 其中 $\boldsymbol{y} = (\sum_{i=1}^m s_i, y_2, \ldots, y_n)$. 任意选取随机数 $t_1, t_2, \ldots, t_l \leftarrow_R (Z_N)^l$, 对于 $\tau = 1, 2, \ldots, l$, 计算 $C_{\tau,1} = w^{\lambda_\tau} v^{t_\tau}$, $C_{\tau,2} = \left(u^{\rho(\tau)} h\right)^{-t_\tau}$ 和 $C_{\tau,3} = g_1^{t_\tau}$. 最后输出相应的加密密文 $\text{ct} = (\psi = (\boldsymbol{M}, \rho), C, \{C_i\}_{i=1,2,\ldots,m}, \{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\}_{\tau=1,2,\ldots,l})$.

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

输入密文 $\text{ct} = (\psi = (\boldsymbol{M}, \rho), C, \{C_i\}_{i=1,2,\ldots,m}, \{C_{\tau,1}, C_{\tau,2}, C_{\tau,3}\}_{\tau=1,2,\ldots,l})$, 属性集合 S 对应的密钥 $\text{sk} = (S, \{K_i\}_{i=1,2,\ldots,m}, K_0, \{K_{\tau,1}, K_{\tau,2}\}_{\tau=1,2,\ldots,k})$, 定义 $I = \{i : \rho(i) \in S\}$. 令 $\{\omega_i \in Z_N\}_{i \in I}$, 如果属性集合 S 满足访问策略 $\psi = (\boldsymbol{M}, \rho)$, 那么有 $\sum_{i \in I} \omega_i \boldsymbol{M}_i = (1, 0, \ldots, 0)$ 成立, 其中 $\boldsymbol{M}_i$ 是矩阵 $\boldsymbol{M}$ 的第 i 行. 计算 $E = \frac{\prod_{i=1}^m e(C_i, K_i)}{\prod_{i \in I} (e(C_{i,1}, K_0) e(C_{i,2}, K_{i,1}) e(C_{i,3}, K_{i,2}))^{\omega_i}}$, 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 $\psi = (\boldsymbol{M}, \rho)$, 那么 $\sum_{i \in I} \omega_i \boldsymbol{M}_i = (1, 0, \ldots, 0)$ 和 $\sum_{i \in I} \omega_i \lambda_i = s_i$, 本小节抗泄露 CP-ABE 机制的正确性由下述等式获得:

$$
\begin{aligned}
E &= \frac{\prod_{i=1}^m e(g_1^{s_i}, g_1^{\alpha_i} w^r R_\eta)}{\prod_{i \in I} \left(e(w^{\lambda_i} v^{t_i}, g_1^r R) e((u^{(i)} h)^{-t_i}, g_1^{r_i} R_i) e(g_1^{t_i}, (u^{A_i} h)^{r_i} v^{-r} R_i)\right)^{\omega_i}} \\
&= \frac{\prod_{i=1}^m e(g_1, g_1)^{\alpha_i s_i} e(g_1, w)^{r s_i}}{\prod_{i \in I} e(g_1, w)^{r \omega_i \lambda_i} e(g_1, v)^{r t_i \omega_i} e(g_1, u^{(i)} h)^{-r_\tau t_i \omega_i} e(g_1, u^{(i)} h)^{r_i t_i \omega_i} e(g_1, v)^{-r t_i \omega_i}} \\
&= \frac{\prod_{i=1}^m e(g_1, g_1)^{\alpha_i s_i} e(g_1, w)^{r s_i}}{e(g_1, w)^{r \sum_{i \in I} \omega_i \lambda_i}} \\
&= \prod_{i=1}^m e(g_1, g_1)^{\alpha_i s_i}.
\end{aligned}
$$

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

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 $\psi^* = (\boldsymbol{M}^*, \rho^*)$ 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 $\psi^* = (\boldsymbol{M}^*, \rho^*)$ 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

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

其中 $c_1, c_2, \ldots, c_m \leftarrow_R (Z_N)^m$ 和 $d_1, d_2, \ldots, d_l \leftarrow_R (Z_N)^l$.

(2) 第 I 型的半功能密钥为

$$\mathrm{sk}_{\mathrm{sf}}^1 = \left((K_i = g_1^{\alpha_i} w^r g_2^{z_i} R_\eta)_{i=1,2,\ldots,m}, K_0 = g_1^r g_2^x R, \left\{ K_{\tau,1} = g_1^{r_\tau} R_\tau, K_{\tau,2} = (u^{A_\tau} h)^{r_\tau} v^{-r} R_\tau \right\}_{\tau=1,2,\ldots,k} \right),$$

其中 $z_1, z_2, \ldots, z_m \leftarrow_R (Z_N)^m$ 和 $x \leftarrow_R Z_N$.

(3) 第 II 型的半功能密钥为

$$\mathrm{sk}_{\mathrm{sf}}^2 = \left((K_i = g_1^{\alpha_i} w^r R_\eta)_{i=1,2,\ldots,m}, K_0 = g_1^r g_2^\mu R, \left\{ K_{\tau,1} = g_1^{r_\tau} R_\tau, K_{\tau,2} = (u^{A_\tau} h)^{r_\tau} v^{-r} R_\tau \right\}_{\tau=1,2,\ldots,k} \right),$$

其中 $\mu \leftarrow_R Z_N$.

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), 因此它不能作为本小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:

(1) 游戏 $\mathsf{Game}_{\mathrm{real}}$: 该游戏是原始的 LR-CPA 安全性游戏 $\mathsf{Exp}_{\text{CP-ABE},\mathcal{A}}^{\text{LR-CPA}}(\kappa)$, 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 $\mathcal{A}$ 在该游戏中获胜的优势就是相应的敌手在实验 $\mathsf{Exp}_{\text{CP-ABE},\mathcal{A}}^{\text{LR-CPA}}(\kappa) = 1$ 中获胜的优势. (2) 游戏 $\mathsf{Game}_{\mathrm{res}}$: 该游戏与游戏 $\mathsf{Game}_{\mathrm{real}}$ 相类似, 但在 $\mathsf{Game}_{\mathrm{res}}$ 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 $\psi^* = (\boldsymbol{M}^*, \rho^*)$ 的属性集合. (3) 游戏 Game_0: 该游戏与游戏 $\mathsf{Game}_{\mathrm{res}}$ 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. (4) 游戏 $\mathsf{Game}_{k,1}\,(k = 1, 2, \ldots, L)$ (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 $\mathsf{Game}_{k,1}$ 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. (5) 游戏 $\mathsf{Game}_{k,2}\,(k = 1, 2, \ldots, L)$: 该游戏与游戏 $\mathsf{Game}_{k,1}$ 相类似, 但在 $\mathsf{Game}_{k,2}$ 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. (6) 游戏 $\mathsf{Game}_{\mathrm{final}}$: 该游戏与 $\mathsf{Game}_{L,2}$ 相类似, 但在 $\mathsf{Game}_{\mathrm{final}}$ 中, 将挑战密文转换成随机消息的半功能密文. 由于在游戏 $\mathsf{Game}_{\mathrm{final}}$ 中, $\mathcal{A}$ 未获得任何关于挑战消息的信息, 因此其在该游戏中获胜的优

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

势为 0. 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 $\Pr[\mathsf{Game}_i]$ 定义为 $\Pr[\mathsf{Game}_i] = \Pr[b' = b \text{ in } \mathsf{Game}_i]$.

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 $\mathsf{Game}_{\mathrm{real}}$ 与 $\mathsf{Game}_{\mathrm{res}}$, 则存在敌手 $\mathcal{B}$ 攻破改进的合数阶子群判定假设 2, 即 $|\Pr[\mathsf{Game}_{\mathrm{real}}] - \Pr[\mathsf{Game}_{\mathrm{res}}]| \leqslant \mathsf{negl}(\kappa)$.

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 $\mathsf{Game}_{\mathrm{res}}$ 与 Game_0, 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 1, 即 $|\Pr[\mathsf{Game}_{\mathrm{res}}] - \Pr[\mathsf{Game}_0]| \leqslant \mathsf{negl}(\kappa)$.

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 $\mathsf{Game}_{1,1}$, 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, 即 $|\Pr[\mathsf{Game}_0] - \Pr[\mathsf{Game}_{1,1}]| \leqslant \mathsf{negl}(\kappa)$.

引理4 对于 $k = 1, 2, \ldots, L$, 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 $\mathsf{Game}_{k,1}$ 与 $\mathsf{Game}_{k,2}$, 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, 即 $|\Pr[\mathsf{Game}_{k,1}] - \Pr[\mathsf{Game}_{k,2}]| \leqslant \mathsf{negl}(\kappa)$.

引理5 对于 $k = 2, \ldots, L$, 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 $\mathsf{Game}_{k-1,2}$ 与 $\mathsf{Game}_{k,1}$, 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, 即 $|\Pr[\mathsf{Game}_{k-1,2}] - \Pr[\mathsf{Game}_{k,1}]| \leqslant \mathsf{negl}(\kappa)$.

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 $\mathsf{Game}_{L,2}$ 与 $\mathsf{Game}_{\mathrm{final}}$, 则存在敌手 $\mathcal{B}$ 以相同的优势攻破改进的合数阶子群判定假设 3, 即 $|\Pr[\mathsf{Game}_{L,2}] - \Pr[\mathsf{Game}_{\mathrm{final}}]| \leqslant \mathsf{negl}(\kappa)$.

由于篇幅所限, 本文不再讨论上述引理的证明过程, 具体证明详见本文的完整版[1)]. 特别地, 文献 [16,24] 对类似的证明方法均有介绍.

定理3 若改进的子群判定假设 1~3 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, 即本小节构造的 CP-ABE 机制具有 LR-CPA 安全性.

证明 由引理 1~6 可知, $\mathsf{Game}_{\mathrm{final}}$ 与 $\mathsf{Game}_{\mathrm{real}}$ 是不可区分的, 则有

$$|\Pr[\mathsf{Game}_{\mathrm{real}}] - \Pr[\mathsf{Game}_{\mathrm{final}}]| \leqslant \mathsf{negl}(\kappa)$$

成立. 在游戏 $\mathsf{Game}_{\mathrm{final}}$ 中敌手 $\mathcal{A}$ 仅获知了随机消息的半功能密文, 因此 $\mathcal{A}$ 在该游戏中获胜的优势是可忽略的. 由于游戏 $\mathsf{Game}_{\mathrm{final}}$ 和 $\mathsf{Game}_{\mathrm{real}}$ 是不可区分的, 因此敌手 $\mathcal{A}$ 在游戏 $\mathsf{Game}_{\mathrm{real}}$ 中获胜的优势也是可忽略的, 即 $\left|\Pr[\mathsf{Game}_{\mathrm{real}}] - \frac{1}{2}\right| \leqslant \mathsf{negl}(\kappa)$, 则上述 CP-ABE 机制具有 LR-CPA 安全性.

5.4 性能比较

第 4 节已将本文构造与现有相关构造进行了性能对比, 那么本小节将对本文所提出的两种方案进行性能对比 (将第 4 节的方案称为方案一, 第 5 节的方案称为方案二), 具体结果如表 3 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, 方案一和二均能满足实际应用环境对大属性集合的部署需求. 此外, 上述两个方案均具有辅助输入模型下的泄露容忍性.

1) https://github.com/XRstar1/leakage.git.

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

表 3 本文两种方案的性能对比

Table 3 Performance comparison of two constructions proposed in this paper

Scheme	Scheme created in Section 4	Scheme created in Section 5
Design objective	Leakage-resilient attribute-based encryption scheme with large universe	Leakage-resilient attribute-based encryption scheme with large universe and tight security reduction
Key technology	Prime order bilinear groups + non-static security assumption	Composite order bilinear groups + static security assumption
Advantage	High computation efficiency + large universe	Tight security reduction + large universe
Deficiency	Large security reduction loss	Low computation efficiency
Leakage model	Auxiliary input model	Auxiliary input model

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.

参考文献

1 Lipp M, Kogler A, Oswald D F, et al. PLATYPUS: software-based power side-channel attacks on x86. In: Proceedings of the 42nd IEEE Symposium on Security and Privacy, 2021. 355–371
2 Ngo K, Dubrova E, Guo Q, et al. A side-channel attack on a masked IND-CCA secure saber KEM implementation. TCHES, 2021, 2021: 676–707
3 Lyu L, Liu S, Gu D. Structure-preserving public-key encryption with leakage-resilient CCA security. Theor Comput Sci, 2019, 795: 57–80
4 Huang M, Yang B, Zhou Y, et al. Continual leakage-resilient hedged public-key encryption. Comput J, 2022, 65: 1574–1585
5 Chakraborty S, Rangan C P. Public key encryption resilient to post-challenge leakage and tampering attacks. In: Proceedings of Cryptographers' Track at the RSA Conference, 2019. 23–43
6 Zhou Y, Wang Z, Qiao Z, et al. Identity-Based encryption with continuous leakage-resilient CCA security from static complexity assumption. Comput J, 2023, 66: 924–940
7 Cai C L, Qin X R, Yuen T H, et al. Tight leakage-resilient identity-based encryption under multi-challenge setting. In: Proceedings of the ACM on Asia Conference on Computer and Communications Security, 2022. 42–53
8 Nishimaki R, Yamakawa T. Leakage-resilient identity-based encryption in bounded retrieval model with nearly optimal leakage-ratio. In: Proceedings of IACR International Workshop on Public Key Cryptography, 2019. 466–495
9 Li H, Yu K, Liu B, et al. An efficient ciphertext-policy weighted attribute-based encryption for the Internet of Health Things. IEEE J Biomed Health Inform, 2022, 26: 1949–1960
10 Li J, Zhang Y, Ning J, et al. Attribute based encryption with privacy protection and accountability for CloudIoT. IEEE Trans Cloud Comput, 2022, 10: 762–773
11 Ge C, Susilo W, Baek J, et al. Revocable attribute-based encryption with data integrity in clouds. IEEE Trans Dependable Secure Comput, 2022, 19: 2864–2872
12 Chen S, Li J, Zhang Y, et al. Efficient revocable attribute-based encryption with verifiable data integrity. IEEE Int Things J, 2024, 11: 10441–10451
13 Li J, Wang Y, Zhang Y, et al. Full verifiability for outsourced decryption in attribute based encryption. IEEE Trans Serv Comput, 2020, 13: 478–487
14 Wang Z W, Yiu S M. Attribute-based encryption resilient to auxiliary input. In: Proceedings of International

https://www.sciengine.com/doi/10.1360/SSI-2024-0198

Conference on Provable Security, 2015. 371–390
15 Zhang L Y, Shang Y J. Leakage-resilient attribute-based encryption with CCA2 security. Int J Netw Secur, 2019, 21: 819–827
16 Lewko A B, Okamoto T, Sahai A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption. In: Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2010. 62–91
17 Zhang M, Zhang Y, Su Y, et al. Attribute-based hash proof system under learning-with-errors assumption in obfuscator-free and leakage-resilient environments. IEEE Syst J, 2017, 11: 1018–1026
18 Li J, Yu Q, Zhang Y, et al. Key-policy attribute-based encryption against continual auxiliary input leakage. Inf Sci, 2019, 470: 175–188
19 Zhang L, Zhang J X, Hu Y P. Attribute-based encryption resilient to continual auxiliary leakage with constant size ciphertexts. J China Univ Posts TeleCommun, 2016, 23: 18–28
20 Guo Y Y, Lu Z H, Jiang M M, et al. Ciphertext-policy attribute-based encryption against post-challenge continuous auxiliary inputs leakage. Int J Netw Secur, 2022, 24: 511–520
21 Ma H Y, Wang Z J, Wang J H, et al. Multi-authority attribute-based encryption resilient against auxiliary-input leakage. J Comput, 2020, 31: 134–147
22 Li J, Yu Q, Zhang Y. Hierarchical attribute based encryption with continuous leakage-resilience. Inf Sci, 2019, 484: 113–134
23 Dodis Y, Goldwasser S, Kalai Y T, et al. Public-key encryption schemes with auxiliary inputs. In: Proceedings of Theory of Cryptography Conference, 2010. 361–381
24 周彦伟. 公钥密码学: 算法构造及安全性证明. 北京: 科学出版社, 2024

Leakage-resilient attribute-based encryption scheme with large universe

Yanwei ZHOU[1], Ran XU[1], Zirui QIAO[2*], Kunwei YANG[1*] & Bo YANG[1]

1. *School of Computer Science, Shaanxi Normal University, Xi'an* 710062*, China*;
2. *School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an* 710121*, China*
* Corresponding author. E-mail: qzr@snnu.edu.cn, yangkunwei@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.

Keywords leakage-resilience, attribute-based encryption, large universe, auxiliary input leakage

https://www.sciengine.com/doi/10.1360/SSI-2024-0198