计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2016.20140787
53(8):1867-1878,2016

抗连续辅助输入泄漏的属性基加密方案

马海英[1] 曾国荪[2] 包志华[3] 陈建平[1] 王金华[4] 王占君[4]
[1](南通大学计算机科学与技术学院 江苏南通 226019)
[2](同济大学计算机科学与技术系 上海 201804)
[3](南通大学电子信息学院 江苏南通 226019)
[4](南通大学理学院 江苏南通 226019)
(m_hying@163.com)

Attribute-Based Encryption Scheme Resilient Against Continuous Auxiliary-Inputs Leakage

Ma Haiying[1], Zeng Guosun[2], Bao Zhihua[3], Chen Jianping[1], Wang Jinhua[4], and Wang Zhanjun[4]
[1](*School of Computer Science and Technology, Nantong University, Nantong, Jiangsu* 226019)
[2](*Department of Computer Science and Technology, Tongji University, Shanghai* 201804)
[3](*School of Electronics and Information, Nantong University, Nantong, Jiangsu* 226019)
[4](*School of Science, Nantong University, Nantong, Jiangsu* 226019)

Abstract For the leakage of secret keying material under side-channel attacks in attribute-based encryption, these existing solutions only allow attackers to get length-bounded leakage on the secret key. First of all, we combine the model of continuous auxiliary-inputs leakage with dual system encryption to achieve strong leakage resilience. Secondly, we reasonably design the generation of secret key to reduce its size, and then devise the first attribute-based encryption that remains secure even if the attacker can obtain the leakage of continuous auxiliary inputs. In the end, our scheme is proved fully secure in the standard model based on reasonable assumptions, even if the attacker gets the leakage of the secret key from an auxiliary-input function. Our scheme achieves the continuous and unbounded leakage of both the master key and the private key, and does not assume fully erasure of old secret keys during the key-update query. In addition, it has a desirable composition feature. Compared with relevant solutions, this scheme not only benefits the best leakage resilience, but also has shorter length of master keys and private keys.

Key words attribute-based encryption; continuous auxiliary-inputs leakages; dual system encryption; Goldreich-Levin theorem; provable security

摘 要 针对属性基加密(attribute-based encryption, ABE)机制中边信道攻击下的密钥泄漏问题,现有的解决方案仅允许密钥的有界泄漏. 将连续辅助输入泄漏模型和双系统加密相结合,通过合理设计主密钥和用户私钥的生成过程,提出了一种抗连续辅助输入泄漏的 ABE 方案. 基于合数阶群的子群判定假设和域 GF(q)上 Goldreich-Levin 定理,在标准模型下,证明该方案在攻击者获知辅助输入密钥泄漏信息的情况下仍具有自适应安全性. 该方案实现了主密钥和用户私钥的连续无界泄漏,在密钥更新

收稿日期:2014-08-28;**修回日期**:2015-04-16
基金项目:国家自然科学基金项目(61402244,61371111,11371207,61272107,61273103);南通大学博士科研启动基金项目(15B10);南通大学校级自然科学基金项目(15z06)
This work was supported by the National Natural Science Fundation of China (61402244, 61371111, 11371207, 61272107, 61273103), the Doctoral Start-up Scientific Research Foundation of Nantong University (15B10), and the Natural Science Foundation of Nantong University (15z06).

询问时无需假定旧密钥必须从内存中彻底清除,且具有较好的合成性质. 与相关的解决方案相比,该方案不仅具有最好的抗泄漏容忍性,而且具有较短的密钥长度.

关键词 属性基加密;连续辅助输入泄漏;双系统加密;Goldreich-Levin 定理;可证明安全性

中图法分类号 TP309

现代密码学假定所有攻击者均不能获知保密密钥的任何信息,但在实际应用中,攻击者可以通过边信道攻击[1-3],利用密码算法运行时的物理特征信息(例如时间、能耗、音频等)和内存泄漏[4],获知关于密钥和系统内部秘密状态的部分信息. 针对边信道攻击下的密钥泄漏问题,抗泄漏密码机制[5-11]在允许攻击者获知密钥和系统保密状态泄漏信息的前提下,仍然能够保障密码系统的安全性. 为了模拟密钥泄漏的程度,该机制定义了作用在密钥和系统内部秘密状态上的可计算泄漏函数,并将该泄漏函数的输出结果作为密钥泄漏信息,显然,必要的限制是泄漏函数不能完全暴露密钥. 2010 年,Dodis 等人[7]提出了抗泄漏密码机制中的一个重要公开难题"允许密钥的连续(和整体无界)泄漏,且不限制密钥泄漏的类型".

近年来,学者们提出了许多抗密钥泄漏模型[6-11],逐步减少对泄漏函数的限制. 2009 年 Akavia 等人[6]在密码学理论会议(theory of cryptography conference, TCC)上首先提出了相对泄漏模型,要求泄漏函数输出信息的总长度不能超过预定上界值,该上界值必须小于密钥长度. 2010 年,Alwen 等人[8]提出了有界检索泄漏模型,减少了对泄漏函数限制,允许攻击者获知更多的泄漏信息. Dodis 等人[9]在 TCC 会议上提出了辅助输入泄漏模型,该模型对泄漏函数的唯一限制是,任意攻击者利用泄漏信息计算出保密密钥的概率都是可以忽略的. 因此,辅助输入泄漏模型能够考虑泄漏能力更强的泄漏函数,进一步减少了对泄漏函数的限制. 上述研究方案[5-9]仅考虑了密钥在其整个生命周期中的泄漏问题. Brakerski 等人[10]提出连续泄漏模型,允许密钥进行更新,并限制在相邻两次更新之间密钥泄漏信息不能超过预定上界值,但在系统的整个生命周期中密钥泄漏的总量是整体无界的,解决了上述公开难题的第 1 部分. Yuen 等人[11]将连续泄漏模型和辅助输入泄漏模型相结合,提出了抗连续辅助泄漏的身份基加密机制,有效解决了身份基加密中抗密钥泄漏的公开难题,但极大地增加了主密钥和用户私钥的长度及相应的计算开销.

在 2005 年欧洲密码学会议上,Sahai 和 Waters[12]提出了属性基加密机制(attribute-based encryption, ABE)的概念. 在该 ABE 方案[12]中,可信授权机构根据用户的属性集合为其颁发私钥,密文和属性集合相关,当私钥属性集合与密文属性集合的匹配度满足系统的门限策略时,用户才能正确解密密文. 为了在密文中表达更灵活的访问控制策略,2007 年 Bethencourt 等人[13]提出了"密文策略"的 ABE 机制(ciphertext policy ABE, CP-ABE),将访问控制策略嵌入在密文中,密钥与属性集合相关联,只有密钥的属性满足密文的访问策略时,才能正确恢复明文. 然而,该 CP-ABE 方案仅满足选择安全性. Lewko 等人[14]采用双系统加密技术[15]实现了自适应安全的 CP-ABE 机制. 由于 ABE 以属性为公钥,能够表示灵活的访问控制策略,显著减少加密节点的处理开销和传输共享数据的网络带宽,从而使它在细粒度访问控制[16-18]、单向广播[16]、群密钥管理[19-20]、隐私保护[17,21-22]等领域具有广泛的应用前景. 此外,针对 ABE 机制中存在的密钥撤销开销大、密钥滥用、密钥托管和密钥盗版进化等问题[23],学者们提出了不少好的研究成果[24-29]. 然而,目前解决 ABE 中边信道攻击下的密钥泄漏问题的研究还不多见.

针对 ABE 中存在边信道攻击下的密钥泄漏问题,2011 年 Lewko 等人[30]在 TCC 年会上将双系统加密和有界泄漏模型相结合,提出一种自适应安全的抗连续内存泄漏的 ABE 方案,同时支持主密钥和用户属性私钥的泄漏,但仅允许密钥的有界泄漏,且要求在密钥更新时旧密钥必须从内存中安全删除. 到目前为止,属性基加密机制中的抗密钥泄漏的公开难题尚未完全解决.

为了探索解决 ABE 中抗密钥泄漏的公开问题,本文将 CP-ABE[14]方案和连续辅助输入泄漏模型[11]相结合,提出抗连续辅助输入泄漏的 ABE 模型. 1)该模型具有较好的合成性质,即可以将 ABE 的属性私钥应用到签名、认证等密码方案中,只要这些方案在无泄漏情况下是可证明安全的,则它们的合成方案在该泄漏模型下依然是安全的. 由于 ABE 的密钥构造方法种类繁多,使得 ABE 较容易与其他密码系统

结合使用.2)该模型允许主密钥和用户属性私钥的连续无界泄漏,不限制密钥泄漏的位数,且无需标识密钥的版本号.3)每次密钥更新时不需要将旧版本密钥从内存中完全清除,即允许泄漏旧密钥的信息.因此,本文试图解决了 ABE 中的抗密钥泄漏的公开难题,即允许密钥的连续和整体无界泄漏,且不限制泄漏类型.

借鉴 BHHO 方案[9]中主密钥和用户私钥的构造思想,本文通过修改 CP-ABE[14]方案,将系统主密钥扩展成一个 m 维向量,构造出 m 个 CP-ABE 子系统,并在保证安全性的前提下,通过共用 m 个子系统主密钥中的关键盲化因子和 m 个子系统的属性公钥,大大缩减了主密钥和系统公钥的长度.为了证明文中方案的安全性,需要将方案中的正常密文和正常密钥转化成半功能密文和半功能密钥,正常密钥可以解密正常密文和半功能密文,但半功能密钥只能解密正常密文.在证明过程中采用混合证明方法,首先将正常密文转化成半功能的;然后,将用户私钥逐个转变成半功能的,为了使攻击者可以询问主密钥和解密私钥的泄漏信息,需要使用修改的 Goldreich-Levin 定理[9]将半功能密钥的盲化因子限制为 λ 位(λ 为方案的安全参数),基于合数阶群上的静态假设,可以确保攻击者不能感知这些转变过程,从而证明该方案在攻击者获知辅助输入密钥泄漏信息的情况下仍具有自适应安全性.该方案允许主密钥和属性私钥的连续无界泄漏,每次密钥更新时无需将旧密钥从内存中完全清除,且具有较好的合成性质.

1 预备知识

1.1 符号说明

本文中,符号 $x\leftarrow Z_N$ 表示在 Z_N 中随机选取元素 x;$x,y,z\leftarrow Z_N$ 表示在 Z_N 中独立且均匀地随机选取元素 x,y,z.令 $negl(n):\mathbb{N}\rightarrow\mathbb{R}$ 表示一个对 n 可忽略的函数,即对任意 $c>0$,有 $negl(n)\leqslant n^{-c}$.令 $|x|$ 表示项 x 二进位的个数,N 和 m 是正整数,G 是 N 阶循环群,$\cdot$ 表示向量的内积或群元素的乘积,$*$ 表示向量之间对应分量的乘积.对任意向量 $\boldsymbol{v}=\langle v_1,v_2,\cdots,v_m\rangle\in G^m$,$u\in G$,$b\in Z_N$,$\boldsymbol{a}=\langle a_1,a_2,\cdots,a_m\rangle\in Z_N^m$,定义 $u^{\boldsymbol{a}}:=\langle u^{a_1},u^{a_2},\cdots,u^{a_m}\rangle$,$\boldsymbol{v}^b:=\langle v_1^b,v_2^b,\cdots,v_m^b\rangle$.

1.2 合数阶双线性群和困难性假设

一个合数阶双线性群可以用一个四元组($N=p_1p_2p_3,G,G_T,e$)来描述,其中 p_1,p_2,p_3 是 3 个互不相等素数,G 和 G_T 均是 N 阶循环群,映射 $e:G\times G\rightarrow G_T$ 满足:1)双线性.$\forall g,h\in G;a,b\in Z_N$:$e(g^a,h^b)=e(g,h)^{ab}$.2)非退化性.$\exists u\in G$,使得 $e(u,u)$ 在 G_T 中的阶为 N.3)可计算性.群 G 和 G_T 上的运算和双线性映射 e 在多项式时间内可以完成计算.

令 G_1,G_2,G_3 分别表示群 G 的 p_1,p_2,p_3 阶子群,g_1,g_2,g_3 分别是子群 G_1,G_2,G_3 的生成元,任意元素 $g\in G$ 都可以表示为 $g_1^{x_1}g_2^{x_2}g_3^{x_3}$ 的形式,其中,$x_i\in Z_{p_i}$($i=1,2,3$),并把 $g_1^{x_1},g_2^{x_2},g_3^{x_3}$ 分别称为子群 G_1,G_2,G_3 的项.如果 g 是群 G 的生成元,则 $g^{p_1p_2}$ 是 G_3 的生成元,$g^{p_1p_3}$ 是 G_2 的生成元,$g^{p_2p_3}$ 是 G_1 的生成元.因此,当 $g_i\in G_i,g_j\in G_j$,且 $i\neq j$ 时,$e(g_i,g_j)$ 为 G_T 的单位元,这称为子群 G_1,G_2 和 G_3 之间的正交性,它是本文构造方案的一个主要工具.此外,令 $G_{1,2},G_{1,3},G_{2,3}$ 分别表示群 G 的 p_1p_2,p_1p_3,p_2p_3 阶子群.

为了证明文中方案的安全性,下面给出合数阶群上子群判定假设,该假设在文献[14]中已进行详细介绍.在这些假设中,令 λ 是系统的安全参数,Pr 是概率函数,PPT 算法表示一个概率多项式时间算法.

假设 1. 给定合数阶双线性群($N=p_1p_2p_3,G,G_T,e$),$g_1\leftarrow G_1,g_3\leftarrow G_3$,$D=(N,G,G_T,e,g_1,g_3)$,随机选择 $z,v\in Z_N$,计算 $T_1=g_1^z$,$T_2=g_1^zg_2^v$,任意 PPT 攻击者 $\mathcal{A}$ 区分元组(D,T_1)和元组(D,T_2)的优势都是可以忽略的.

假设 2. 给定合数阶双线性群($N=p_1p_2p_3,G,G_T,e$);随机选取 $z,v,\mu,p\leftarrow Z_N,g_1\leftarrow G_1,g_3\leftarrow G_3$,$D=(N,G,G_T,e,g_1,g_3,g_1^zg_2^v,g_2^\mu g_3^p)$,随机选取 $w,\kappa,\sigma\leftarrow Z_N$,计算 $T_1=g_1^wg_3^\sigma$,$T_2=g_1^wg_2^\kappa g_3^\sigma$,任意 PPT 攻击者 $\mathcal{A}$ 区分元组(D,T_1)和元组(D,T_2)的优势都是可以忽略的.

假设 3. 给定合数阶双线性群($N=p_1p_2p_3,G,G_T,e$),随机选择 $\alpha,v,\mu,z\leftarrow Z_N,g_1\leftarrow G_1;g_2\leftarrow G_2$,$g_3\leftarrow G_3$,$D=(N,G,G_T,e,g_1,g_2,g_3,g_1^\alpha g_2^v,g_1^zg_2^\mu)$,$T_1=e(g_1,g_1)^{\alpha z}$,$T_2\leftarrow G_T$,任意 PPT 攻击者 $\mathcal{A}$ 区分元组(D,T_1)和元组(D,T_2)的优势都是可以忽略的.

1.3 访问结构和线性秘密共享方案(LSSS)

定义 1. 访问结构[24].设 $\mathcal{P}=\{\mathcal{P}_1,\mathcal{P}_2,\cdots,\mathcal{P}_n\}$ 是 n 个属性的集合,由 $\mathcal{P}$ 的某些非空子集构成的集族 $\mathcal{A}\subseteq 2^{\mathcal{P}}\backslash\varnothing$ 称为访问结构.如果对任意属性集合 B,

C,满足:若 $B\in\mathbb{A}$ 且 $B\subseteq C$,则 $C\in\mathbb{A}$,那么称访问结构 $\mathbb{A}$ 是单调的. $\mathbb{A}$ 中的所有属性集合称为授权集,不在 $\mathbb{A}$ 中的属性集合称为非授权集.

定义 2. LSSS[24]. 称属性集合 $\mathcal{P}=\{\mathcal{P}_1,\mathcal{P}_2,\cdots,\mathcal{P}_n\}$ 上的一个秘密共享方案 Π 是线性的,如果满足:1)将属性的秘密分享值构造成 Z_p 上的一个向量;2) 对于方案 Π,存在一个秘密份额生成矩阵 $\boldsymbol{A}_{n_1\times n_2}$ 和行标号函数 $\rho:\{1,2,\cdots,n_1\}\to\mathcal{P}$,令 $s\in Z_p$ 是待共享的秘密值,随机选择 $r_2,r_3,\cdots,r_{n_2}\in Z_p$,构成向量 $\boldsymbol{v}=\langle s,r_2,\cdots,r_{n_2}\rangle$,令 $\boldsymbol{v}^{\mathrm{T}}$ 为 $\boldsymbol{v}$ 的转置,则 $\boldsymbol{A}\boldsymbol{v}^{\mathrm{T}}$ 是 n_1 个秘密份额构成的向量,利用标号函数,将秘密份额 $\lambda_i=(\boldsymbol{A}\boldsymbol{v}^{\mathrm{T}})_i(1\leqslant i\leqslant n_1)$ 分配给属性 $\rho(i)$.

LSSS 的可重构性质:假定 Π 是访问结构 $\mathbb{A}$ 的线性秘密共享方案,令 $S\in\mathbb{A}$ 是授权集,定义 $I=\{i:\rho(i)\in S\}\subseteq\{1,2,\cdots,n_1\}$,则存在多项式时间算法计算 $\{c_i\in Z_p\}_{i\in I}$,使得对于秘密共享值 s 的任意有效份额 $\{\lambda_i\}_{i\in\{1,2,\cdots,n_1\}}$,满足 $\Sigma_{i\in I}c_i\lambda_i=s$.

1.4 域 GF(q)上 Goldreich-Levin 定理

定理 1. 域 GF(q)上的 Goldreich-Levin 定理[9]. 令 q 是一个大素数,H 是 GF(q)的任意子集,n 是一个正整数,任意函数 $f:H^n\to\{0,1\}^*$. 令 $\boldsymbol{s}\leftarrow H^n$,$\xi\leftarrow f(\boldsymbol{s})$,$\boldsymbol{r}\leftarrow\mathrm{GF}(q)^n$,如果存在区分器 $\mathcal{D}$ 在时间 t 内使得 $|Pr[\mathcal{D}(\xi,\boldsymbol{r},(\boldsymbol{r}\cdot\boldsymbol{s}))=1]-Pr[\zeta\leftarrow\mathrm{GF}(q):\mathcal{D}(\xi,\boldsymbol{r},\zeta)=1]|=\varepsilon$,则存在一个可逆器 $\mathcal{A}$,在 $t'=t\cdot poly(n,|H|,1/\varepsilon)$ 时间内求得 $\boldsymbol{s}$ 的概率为

$$Pr[\boldsymbol{s}\leftarrow H^n,\xi\leftarrow f(\boldsymbol{s}):\mathcal{A}(\xi)=\boldsymbol{s}]\geqslant\frac{\varepsilon^3}{512nq^2}.$$

2 抗连续辅助输入泄漏 ABE 及其安全模型

2.1 抗连续辅助输入泄漏 ABE 的定义

一个抗连续辅助输入泄漏的 ABE 方案由以下 6 个算法构成:初始化(Setup)、加密(Enc)、私钥生成(Keygen)、解密(Dec)、主密钥更新(MskUpdate)、用户私钥更新(UskUpdate).

1) Setup(λ,U)$\to$(PK,MSK). 该概率多项式时间(PPT)初始化算法输入系统安全参数 λ 和系统的属性全集 U,输出系统主密钥 MSK 和公钥 PK.

2) Enc($M,\mathbb{A},PK$)$\to C$. 该 PPT 加密算法输入一个待加密消息 M、一个访问结构 $\mathbb{A}$ ($\boldsymbol{A},\rho$)和系统公钥 PK,输出密文 C.

3) KeyGen(ω,MSK)$\to SK_\omega$. 该 PPT 私钥生成算法输入用户的属性集合 ω、主密钥 MSK,输出用户私钥 SK_ω.

4) Dec(SK_ω,C)$\to M$. 解密算法输入用户私钥 SK_ω 和在$\mathbb{A}$($\boldsymbol{A},\rho$)下加密的密文 C,仅当 ω 满足访问结构$\mathbb{A}$($\boldsymbol{A},\rho$)时,用户才能解密密文,否则,解密失败.

5) MskUpdate(MSK)$\to MSK'$. 主密钥更新算法输入当前主密钥 MSK,输出更新后的主密钥 MSK'.

6) UskUpdate(SK_ω)$\to SK'_\omega$:用户私钥更新算法输入用户私钥 SK_ω,输出更新后的用户私钥 SK'_ω.

2.2 安全性模型

定义 3. 本文方案的安全模型可以通过攻击者 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的交互游戏进行定义如下:

1) 初始化阶段. 挑战者 $\mathcal{C}$ 运行方案中的 Setup 算法,生成系统当前主密钥 MSK 和公钥 PK,将 PK 发送给攻击者 $\mathcal{A}$,创建列表 L_{MSK},用于保存主密钥 MSK 的所有版本,包括每个时间段更新前的 MSK 和当前最新 MSK. 挑战者 $\mathcal{C}$ 创建列表 L_{USK},并将其置为空集$\varnothing$.

2) 询问阶段 1. $\mathcal{A}$ 可以向 $\mathcal{C}$ 多次询问下面 3 类预言机:①私钥生成预言机 KGO($\cdot$). $\mathcal{A}$ 提交一个属性集合 $\omega\subseteq U$ 给 $\mathcal{C}$,$\mathcal{C}$ 运行 KeyGen(MSK,ω)算法,输出私钥 SK_ω,并将其保存到列表 L_{USK}. 然后,$\mathcal{C}$ 将 SK_ω 发送给 $\mathcal{A}$. ②泄漏预言机 MLO($\cdot$). 给定一个概率多项式时间可计算的函数族 $\mathcal{F}$,$\mathcal{A}$ 输入一个多项式时间可计算函数 $f\in\mathcal{F}$,计算 $f(L_{MSK},\varnothing,MSK,\varnothing,PK,\varnothing)$,获知关于主密钥 MSK 的泄漏信息. ③主密钥更新预言机 UMO($\cdot$). $\mathcal{C}$ 运行 UpdateMSK(MSK),输出更新后的主密钥 MSK',并设置 $MSK\leftarrow MSK'$.

3) 挑战阶段 1. $\mathcal{A}$ 选择一个挑战访问结构$\mathbb{A}^*$,并将其发送给挑战者 $\mathcal{C}$. $\mathcal{C}$ 选择属性集合 ω^*,使得 ω^* 满足访问结构$\mathbb{A}^*$,运行私钥生成算法 KeyGen(MSK,ω^*),生成用户私钥 SK_{ω^*},并生成列表 $L_{\boldsymbol{A}^*}$,将 SK_{ω^*} 放入 $L_{\boldsymbol{A}^*}$.

4) 询问阶段 2. $\mathcal{A}$ 可以向 $\mathcal{C}$ 多次询问下面 4 类预言机:①私钥生成预言机 KGO($\cdot$). 与询问阶段 1 相同. ②泄漏预言机 MLO($\cdot$). $\mathcal{A}$ 输入一个多项式时间可计算函数 $f\in\mathcal{F}$,计算 $f(L_{MSK},L_{\boldsymbol{A}^*},MSK,SK_{\omega^*},PK,\mathbb{A}^*)$,获知关于主密钥 MSK 和解密私钥 SK_{ω^*} 的泄漏信息. ③主密钥更新预言机 UMO($\cdot$). 与询问阶段 1 相同. ④用户私钥更新预言机 UUO($\cdot$). $\mathcal{C}$ 运行 UpdateUSK(SK_{ω^*})算法,生成一个新的用户私钥 SK'_{ω^*},设置 $SK_{\omega^*}\leftarrow SK'_{\omega^*}$.

5) 挑战阶段 2. 攻击者 $\mathcal{A}$ 将 2 个等长的消息 M_0 和 M_1 提交给 $\mathcal{C}$. $\mathcal{C}$ 选择随机位 $b\in\{0,1\}$,计算

挑战密文 $C^*=\mathrm{Enc}(M_b,\mathbb{A}^*,PK)$,并将 C^* 发送给 $\mathcal{A}$.

6) 询问阶段 3. $\mathcal{A}$ 仅能询问 KGO(·),且要求这些私钥中的属性集合均不满足挑战访问结构$\mathbb{A}^*$.

7) 猜测阶段. $\mathcal{A}$ 依据密文 C^* 给出一个猜测值 b'.

当 $b'=b$,且在询问阶段 1,2,3 中,攻击者 $\mathcal{A}$ 没有询问满足访问结构$\mathbb{A}^*$的用户私钥,称 $\mathcal{A}$ 赢得这个游戏,且定义 $\mathcal{A}$ 在该游戏中的优势为$|Pr[b'=b]-1/2|$.

借鉴 Yuen 等人[11]提出的抗连续辅助输入泄漏模型,给出在 CP-ABE 中连续辅助输入函数族的定义. 令 L_{MSK} 为 CP-ABE 中系统主密钥 MSK 的集合,S^* 表示所有满足挑战访问结构$\mathbb{A}^*$的私钥集合,S 表示其他私钥集合,使得 $S^*\cap S=\varnothing$. 假设 $L_{\boldsymbol{A}^*}$ 表示满足挑战访问结构$\mathbb{A}^*$的一些私钥集合,即 $L_{\boldsymbol{A}^*}\subseteq S^*$,$MSK$ 和 SK_{ω^*} 分别表示当前主密钥和当前满足挑战访问结构的私钥,k 为私钥 SK_{ω^*} 的长度.

定义 4. 连续辅助输入函数族 $\mathcal{F}_{\boldsymbol{A}^*\text{-ow}}(\chi(k))$是一类概率多项式时间(PPT)可计算的函数族 $f:\{0,1\}^*\to\{0,1\}^*$,使得对所有的 $PK,\mathbb{A}^*,S,f(L_{MSK},L_{\boldsymbol{A}^*},MSK,SK_{\omega^*},PK,\mathbb{A}^*)$,任意 PPT 算法输出一个 $SK_{\omega^*}\in S^*$ 的概率均不超过 $\chi(k)$,其中,困难参数 $\chi(k)\geqslant 2^{-k}$,且 $MSK,PK,SK_{\omega^*},S,L_{MSK},L_{\boldsymbol{A}^*}$ 和 $\mathbb{A}^*$ 都是随机生成的.

定义 5. 如果对于任意概率多项式时间的攻击者$\mathcal{A}$在上述安全模型游戏中的优势均是可忽略的,且安全模型中的 $\mathcal{F}$ 是连续辅助输入函数族 $\mathcal{F}_{\boldsymbol{A}^*\text{-ow}}(\chi(k))$,则称该 ABE 方案在 $\mathcal{F}_{\boldsymbol{A}^*\text{-ow}}(\chi(k))$下是 IND-CPA 安全的,记作 $\chi(k)$-CAI-CPA 安全性,其中,$\chi(k)\geqslant 2^{-k}$.

3 抗连续辅助输入泄漏的 ABE 方案

令 G,G_T 是阶为 $N=p_1p_2p_3$ 的循环群,其中,p_1,p_2,p_3 是 3 个互不相同的素数,$e:G\times G\to G_T$ 是双线性映射,G_i 是群 G 的阶为 p_i 的子群,$G_{i,j}$是群 G 的阶为 p_ip_j 的子群$(i\neq j)$. U 为系统全体属性的集合.

1) Setup(λ,U). 令 $0<\varepsilon<1$,$m=(3\times\mathrm{lb}\,p_2)^{1/\varepsilon}$,初始化算法选择随机向量 $\boldsymbol{\alpha}=\langle\alpha_1,\alpha_2,\cdots,\alpha_m\rangle\in Z_N^m$ 和 $\boldsymbol{a}=\langle a_1,a_2,\cdots,a_m\rangle\in Z_N^m$,选择随机生成元 $g_1,h_1,h_2,\cdots,h_m\in G_1,g_3\in G_3$. 对每个属性 $i\in U$,随机选取 $s_i\in Z_N$ 和一个 G_3 部分随机数 $\rho_i^*\in Z_N$. 该算法随机选取 $t^*,\rho_{m+1}^*\in Z_N$ 和 G_3 部分随机向量 $\boldsymbol{\rho}^*\in Z_N^m$,计算并输出系统公钥 PK 和主密钥 MSK 如下:

$$PK=(N,g_1,g_3,g_1^{a_1},g_1^{a_2},\cdots,g_1^{a_m},y=e(h_1,g_1)^{a_1}e(h_2,g_1)^{a_2}\cdots e(h_m,g_1)^{a_m},T_i=g_1^{s_i},\forall i\in U),$$

$$MSK=(\boldsymbol{K}^*=\langle h_1^{a_1}g_1^{a_1t^*},h_2^{a_2}g_1^{a_2t^*},\cdots,h_m^{a_m}g_1^{a_mt^*}\rangle*g_3^{\boldsymbol{\rho}^*},L^*=g_1^{t^*}g_3^{\rho_{m+1}^*},K_i^*=T_i^{t^*}g_3^{\rho_i^*},\ \forall i\in U).$$

2) KeyGen(MSK,ω). 私钥生成算法随机选择 $t,\rho_{m+1}\in Z_N$ 和 G_3 部分随机向量 $\boldsymbol{\rho}\in Z_N^m$,并对每个属性 $i\in\omega$,选择 G_3 部分随机数 $\rho_i\in Z_N$. 该算法计算用户私钥 SK_ω 如下:

$$SK_\omega=(\omega,\boldsymbol{K}=\langle k_1,k_2,\cdots,k_m\rangle,L,K_i,\forall i\in\omega)=(\omega,\boldsymbol{K}^**\langle g_1^{a_1t},g_1^{a_2t},\cdots,g_1^{a_mt}\rangle*g_3^{\boldsymbol{\rho}},L^*g_1^tg_3^{\rho_{m+1}},K_i^*T_i^tg_3^{\rho_i},\forall i\in\omega).$$

3) Enc(M,$\mathbb{A}(\boldsymbol{A},\rho)$)$\to C$. 访问结构$\mathbb{A}(\boldsymbol{A},\rho)$由一个 $n_1\times n_2$ 矩阵 $\boldsymbol{A}$ 和一个映射 $\rho:\{1,2,\cdots,n_1\}\to U$ 组成,加密算法随机选取一个向量 $\boldsymbol{v}=\langle s,v_2,\cdots,v_{n_2}\rangle\in Z_N^{n_2}$. 对矩阵 $\boldsymbol{A}$ 的每一行 $\boldsymbol{A}_x$ 和 $j=1,2,\cdots,m$,随机选择 $r_{j,x}\in Z_N$,计算密文为

$$C=(\mathbb{A}(\boldsymbol{A},\rho),C_0=My^s,C_1=g_1^s,C_{j,x}=g_1^{a_j\boldsymbol{A}_x\cdot\boldsymbol{v}}T_{\rho(x)}^{-r_{j,x}},D_{j,x}=g_1^{r_{j,x}},\forall j,x).$$

4) Dec(C,SK_ω)$\to M$. 解密算法首先为 $\boldsymbol{A}$ 的每一行 $\boldsymbol{A}_x$ 计算一组常量 $c_x\in Z_N$,使得 $\sum_{\rho(x)\in\omega}c_x\boldsymbol{A}_x=\langle 1,0,\cdots,0\rangle$. 为消去密文中盲化因子,计算:

$$\prod_{j=1}^{m}\left[\frac{e(k_j,C_1)}{\prod_{\rho(x)\in\omega}(e(C_{j,x},L)e(K_{\rho(x)},D_{j,x}))^{c_x}}\right]=(e(h_1,g_1)^{a_1}e(h_2,g_2)^{a_2}\cdots e(h_m,g_1)^{a_m})^s=y^s,$$

恢复消息 $M=C_0/y^s$.

5) UpdateMSK(MSK)$\to MSK'$. 该主密钥更新算法随机选择 $t^{*'},\rho_{m+1}^{*'}\in Z_N$,随机向量 $\boldsymbol{\rho}^{*'}\in Z_N^m$,计算新的主密钥:

$$MSK'=(\boldsymbol{K}^{*'}=\boldsymbol{K}^**\langle g_1^{a_1t^{*'}},g_1^{a_2t^{*'}},\cdots,g_1^{a_mt^{*'}}\rangle*g_3^{\boldsymbol{\rho}^{*'}},L^{*'}=L^*g_1^{t^{*'}}g_3^{\rho_{m+1}^{*'}},K_i'=K_iT_i^{t^{*'}}g_3^{\rho_i^{*'}},\forall i\in U).$$

6) UpdateUSK(SK_ω)$\to SK'_\omega$. 该私钥更新算法随机选择 $t',\rho'_{m+1}\in Z_N$ 和 G_3 部分随机向量 $\boldsymbol{\rho}'\in Z_N^m$,并对每个属性 $i\in\omega$,选择 G_3 部分随机数 $\rho'_i\in Z_N$,计算新的属性私钥:

$$\mathrm{SK}'_\omega=(\omega,\boldsymbol{K}*\langle g_1^{a_1t'},g_1^{a_2t'},\cdots,g_1^{a_mt'}\rangle*g_3^{\boldsymbol{\rho}'},Lg_1^{t'}g_3^{\rho'_{m+1}},K_iT_i^{t'}g_3^{\rho'_i},\forall i\in\omega).$$

4 安全性证明和泄漏性能分析

4.1 安全性证明

为了证明本文抗连续辅助输入泄漏 ABE 的

安全性,需要构造半功能私钥和半功能密文,半功能私钥分为Ⅰ型半功能私钥和Ⅱ型半功能私钥.为了生成半功能私钥和密文,对每个属性 $i\in U$,随机选择 $q_i\in Z_N$,半功能密文和半功能私钥定义如下:

定义 6. KeygenSF1(MSK,ω).该Ⅰ型半功能私钥生成算法随机选择 $\theta\in Z_N$,随机向量 $\boldsymbol{\gamma}=\langle\gamma_1,\gamma_2,\cdots,\gamma_m\rangle\in[0,\lambda]^m$,利用正常私钥 $SK_\omega=(\omega,\boldsymbol{K},L,K_i,\forall i\in\omega)$,计算Ⅰ型半功能私钥 SK_ω-Ⅰ如下:

$$\widetilde{\boldsymbol{K}}=\boldsymbol{K}*g_2^{\boldsymbol{\gamma}},\ \widetilde{L}=Lg_2^{\theta},\ \widetilde{K}_i=K_i\cdot g_2^{q_i\theta},\ \forall i\in\omega.$$

定义 7. KeygenSF2(MSK,ω).该Ⅱ型半功能私钥生成算法选择随机向量 $\boldsymbol{\gamma}=\langle\gamma_1,\gamma_2,\cdots,\gamma_m\rangle\in[0,\lambda]^m$,利用正常私钥,计算Ⅱ型半功能私钥 SK_ω-Ⅱ如下:

$$\widetilde{\boldsymbol{K}}=\boldsymbol{K}*g_2^{\boldsymbol{\gamma}},\ \widetilde{L}=L,\ \widetilde{K}_i=K_i,\ \forall i\in\omega.$$

注意:与Ⅰ型半功能私钥不同的是,该Ⅱ型半功能私钥中的 $\theta=0$.

定义 8. EncSF($M,\mathbb{A}(\boldsymbol{A},\rho)$).该半功能密文生成算法随机选择 $\delta\in Z_N$,对访问矩阵 $\boldsymbol{A}$ 的每一行 $\boldsymbol{A}_x$ 和 $j=1,2,\cdots,m$,随机选择 $\delta_{j,x}\in Z_N$,随机向量 $\boldsymbol{u}_j\in Z_N^{n_2}$,利用正常密文,计算半功能密文 C-SF 如下:

$$\text{C-SF}=(\mathbb{A}(\boldsymbol{A},\rho),C_0=My^s,\widetilde{C}_1=g_1^sg_2^{\delta},\forall j,x,$$
$$\widetilde{C}_{j,x}=g_1^{a_j\boldsymbol{A}_x\boldsymbol{v}}T_{\rho(x)}^{-r_{j,x}}g_2^{\boldsymbol{A}_x\boldsymbol{u}_j+\delta_{j,x}q_{\rho(x)}},\widetilde{D}_{j,x}=g_1^{r_{j,x}}g_2^{-\delta_{j,x}}).$$

如果用半功能密钥解密半功能密文,得到1个多余项:$e(g_2,g_2)^{\delta\sum_{j=1}^{m}\gamma_j-\theta\sum_{j=1}^{m}u_{j,1}}$,若私钥中属性集满足密文中访问结构,且 $\delta\sum_{j=1}^{m}\gamma_j-\theta\sum_{j=1}^{m}u_{j,1}=0 \bmod p_2$($u_{j,1}$表示向量 $\boldsymbol{u}_j$ 的第1个分量),则称该Ⅰ型半功能私钥对该半功能密文是名义半功能的.

基于合数阶群上的子群判定假设,采用混合争论技术,借助一系列相邻游戏($Game_{\text{Real}},Game_0,Game_{1,1},Game_{1,2},\cdots,Game_{k-1,2},Game_{k,1},Game_{k,2},\cdots,Game_{\mathcal{Q}-1,2},Game_{\mathcal{Q},1},Game_{\mathcal{Q},2},Game_{\text{Final}}$)的不可区分性,证明本文方案的安全性,其中,$\mathcal{Q}$ 表示在安全性游戏中询问 KGO(·)预言机的次数.

1) $Game_{\text{Real}}$:真实的安全性游戏,私钥和密文都是正常的.

2) $Game_0$:与 $Game_{\text{Real}}$ 类似,除了挑战密文是半功能密文.

3) $Game_{k,1}$:挑战密文是半功能密文,前 $k-1$ 次询问的私钥是Ⅱ型半功能的,第 k 次询问私钥是Ⅰ型半功能的,剩余的私钥是正常的.

4) $Game_{k,2}$:与 $Game_{k,1}$ 类似,除了第 k 次询问的私钥是Ⅱ型半功能的.

5) $Game_{\text{Final}}$:在这个安全性游戏中,所有询问私钥都是Ⅱ型半功能的,且挑战密文是对一个随机明文加密生成的半功能密文.

引理 1. 若假设1成立,对于任意 PPT 攻击者 $\mathcal{A}$,则 $\mathcal{A}$ 区分 $Game_{\text{Real}}$ 和 $Game_0$ 的优势均是可以忽略的.

证明.假定存在一个 PPT 攻击者 $\mathcal{A}$ 以不可忽略的优势区分 $Game_{\text{Real}}$ 和 $Game_0$,则可以构造一个 PPT 算法 $\mathcal{B}$,$\mathcal{B}$ 能以不可忽略的优势打破假设1.$\mathcal{B}$ 接收到假设1的条件$\{g_1,g_3,T\}$,能够模拟 $Game_{\text{Real}}$ 或 $Game_0$.$\mathcal{B}$ 执行初始化算法,令 $m=(3\times\text{lb}\,p_2)^{1/\varepsilon}$,选择随机向量 $\boldsymbol{\alpha}=\langle\alpha_1,\alpha_2,\cdots,\alpha_m\rangle\in Z_N^m$,$\langle\beta_1,\beta_2,\cdots,\beta_m\rangle\in Z_N^m$,$\boldsymbol{a}=\langle a_1,a_2,\cdots,a_m\rangle\in Z_N^m$,$t\in Z_N$,计算 $h_j=g_1^{\beta_j}$,$\forall j\in[1,m]$.对每个属性 $i\in U$,随机选择 $s_i\in Z_N$.$\mathcal{B}$ 生成系统公钥 $\text{PK}=(N,g_1,g_3,g_1^{a_1},g_1^{a_2},\cdots,g_1^{a_m},y=e(h_1,g_1)^{\alpha_1}e(h_2,g_2)^{\alpha_2}\cdots e(h_m,g_1)^{\alpha_m}=e(g_1,g_1)^{\sum_j\alpha_j\beta_j}$,$T_i=g_1^{s_i}$,$\forall i\in U)$,并将其发送给 $\mathcal{A}$,其中,N,g_1,g_3 由假设1给定.

1) 询问阶段1.由于已知 $\langle\alpha_1,\alpha_2,\cdots,\alpha_m\rangle$,$\mathcal{B}$ 执行初始化算法,生成系统正常主密钥 MSK,可以回答攻击者 $\mathcal{A}$ 的所有私钥生成询问、主密钥泄漏和更新询问.

2) 挑战阶段1.攻击者 $\mathcal{A}$ 提交一个挑战访问结构 $\mathbb{A}^*(\boldsymbol{A}^*,\rho^*)$,$\boldsymbol{A}^*$ 是一个 $n_1\times n_2$ 的矩阵,$\mathcal{B}$ 选择一个属性集合 ω^*,使得 ω^* 满足 $\mathbb{A}$,生成一个正常解密私钥 SK_{ω^*}.

3) 询问阶段2.与询问阶段1类似,此外,$\mathcal{B}$ 可以回答 $\mathcal{A}$ 对私钥 SK_{ω^*} 的所有泄漏信息和更新信息.

4) 挑战阶段2.$\mathcal{A}$ 提交2个消息 M_0 和 M_1 给 $\mathcal{B}$,$\mathcal{B}$ 随机选择 $v_2',v_3',\cdots,v_{n_2}'\in Z_N$,对 $\boldsymbol{A}^*$ 的每一行 $\boldsymbol{A}_x^*$ 和 $j=1,2,\cdots,m$,随机选择 $r_{j,x}'\in Z_N$,生成向量 $\boldsymbol{v}'=\langle1,v_2',\cdots,v_{n_2}'\rangle$.$\mathcal{B}$ 选择一个随机位 $b\in\{0,1\}$,计算并输出挑战密文:$C^*=((\boldsymbol{A}^*,\rho^*),C_0=M_be(T^{\sum_{j=1}^{m}\alpha_j\beta_j},g_1),C_1=T,C_{j,x}=T^{a_j\boldsymbol{A}_x^*\cdot\boldsymbol{v}'}T^{-r_{j,x}'s_{\rho(x)}},D_{j,x}=T^{-r_{j,x}'},\forall j,x)$,其中,$T$ 为假设中的挑战项.

5) 询问阶段3.与询问阶段1相同,除了 $\mathcal{A}$ 只能进行私钥生成询问.

如果 $T=g_1^zg_2^v$,则密文是半功能的,其中,

$$C_0=M_be((g_1^zg_2^c)^{\sum_{j=1}^{m}\alpha_j\beta_j},g_1)=M_be(g_1^{\sum_{j=1}^{m}\alpha_j\beta_j},g_1)^z=$$
$$M_be(g_1^{\alpha_1\beta_1}g_1^{\alpha_2\beta_2}\cdots g_1^{\alpha_m\beta_m},g_1)^z=$$
$$M_b(e(h_1,g_1)^{\alpha_1}e(h_2,g_1)^{\alpha_2}\cdots e(h_m,g_1)^{\alpha_m})^z,$$
$$C_1=g_1^zg_2^v,$$

$C_{j,x}=T^{a_j\boldsymbol{A}_x^*\cdot\boldsymbol{v}'}T^{-r_{j,x}s_{\rho(x)}}=$

$(g_1^z g_2^v)^{a_j\boldsymbol{A}_x^*\boldsymbol{v}'}(g_1^z g_2^v)^{-r'_{j,x}s_{\rho(x)}}=$

$g_1^{a_j\boldsymbol{A}_x^*(z\boldsymbol{v}')}g_1^{-zr'_{j,x}s_{\rho(x)}}g_2^{\boldsymbol{A}_x\cdot(a_j\boldsymbol{v}\cdot\boldsymbol{v}')-vr'_{j,x}s_{\rho(x)}}$,

$D_{j,x}=T^{-r'_{j,x}}=(g_1^z g_2^v)^{-r'_{j,x}}=g_1^{-zr'_{j,x}}g_2^{-vr'_{j,x}}$.

对于子群 G_1 部分,挑战密文隐式地设置 $s=z$,$\boldsymbol{v}=z\boldsymbol{v}'$,$r_{j,x}=zr'_{j,x}$.因此,所有的 G_1 部分是均匀分布的,特别地,$\boldsymbol{v}$ 的第 1 个分量是 z.对于 G_2 部分,挑战密文隐式地设置 $\delta_{j,x}=-vr'_{j,x}$,$\boldsymbol{u}_j=a_jv\boldsymbol{v}'$,$q_{\rho^*(x)}=s_{\rho^*(x)}$.所有这些项仅在 G_1 部分出现过,因此,在攻击者看来,这些项与它们模 p_2 的值是无关的,即半功能参数的均匀随机性来自于 $v,a_1,a_2,\cdots,a_m,v'_2,\cdots,v'_{n_2},r'_{j,x},s_{\rho^*(x)}$ 模 p_2 的随机性.因此,这是一个均匀分布的半功能密文.此时 $\mathcal{B}$ 完美模拟 $Game_0$.另一方面,如果 $T=g_1^z$,则挑战密文中没有 G_2 中的项,该密文为正常的,此时,$\mathcal{B}$ 完美模拟 $Game_{\text{Real}}$.

因此,如果 $\mathcal{A}$ 能以不可忽略的优势区分 $Game_{\text{Real}}$ 和 $Game_0$,则 $\mathcal{B}$ 可以相同的优势打破假设 1. 证毕.

引理 2. 如果假设 2 成立,对于任意 PPT 攻击者 $\mathcal{A}$,则 $\mathcal{A}$ 区分 $Game_{k-1,2}$ 和 $Game_{k,1}$ 的优势均是可忽略的.

证明. $\mathcal{B}$ 接收到假设 2 的条件 $\{g_1,g_3,g_1^z g_2^v,g_2^u g_3^p,T\}$,能够模拟 $Game_{k-1,2}$ 或 $Game_{k,1}$.初始化阶段:$\mathcal{B}$ 设置 $m=(3\times\text{lb}\,p_2)^{1/\varepsilon}$,选择随机向量 $\boldsymbol{\alpha}=\langle\alpha_1,\alpha_2,\cdots,\alpha_m\rangle\in Z_N^m$,$\langle\beta_1,\beta_2,\cdots,\beta_m\rangle\in Z_N^m$,$\boldsymbol{a}=\langle a_1,a_2,\cdots,a_m\rangle\in Z_N^m$,$t\in Z_N$,计算 $h_j=g_1^{\beta_j}$,$\forall j\in[1,m]$.对每个属性 $i\in U$,随机选择 $s_i\in Z_N$.$\mathcal{B}$ 生成公钥 $PK=(N,g_1,g_3,g_1^{a_1},\cdots,g_1^{a_m},y=e(h_1,g_1)^{a_1}\cdots e(h_m,g_1)^{a_m}=e(g_1,g_1)^{\sum a_j\beta_j}$,$T_i=g_1$,$\forall i\in U)$,并将其发送给 $\mathcal{A}$,其中,N,g_1,g_3 来自假设 2 的条件.

1) 询问阶段 1.当 $\mathcal{A}$ 询问 ω_r 的私钥,且询问次数 $r>k$ 时,$\mathcal{B}$ 利用 $(\alpha_1,\alpha_2,\cdots,\alpha_m)$ 生成 ω_r 的正常私钥;当 $\mathcal{A}$ 的询问次数 $r<k$ 时,$\mathcal{B}$ 对 G_3 部分随机选择 $\boldsymbol{\rho}\in Z_N^m$,$\rho_{m+1},t,\rho'_i\in Z_N$,$\forall i\in\omega_r$,计算Ⅱ型半功能私钥 $SK_r\text{-}\text{Ⅱ}=(\omega_r,\langle h_1^{\alpha_1}g_1^{a_1t},h_2^{\alpha_2}g_1^{a_2t},\cdots,h_m^{\alpha_m}g_1^{a_mt}\rangle*(g_2^u g_3^p)^{\boldsymbol{\rho}},g_1^t g_3^{\rho_{m+1}},T_i^t g_3^{\rho'_i},\forall i\in\omega_r)$,其中,$\omega_r$ 是 $\mathcal{A}$ 提交的属性集,$g_2^u g_3^p$ 来自假设 2 的条件.显然,这个Ⅱ型半功能私钥 $SK_r\text{-}\text{Ⅱ}$ 是均匀分布的.

当 $r=k$ 时,$\mathcal{A}$ 提交属性集 ω_r 给 $\mathcal{B}$,$\mathcal{B}$ 生成一个正常私钥或Ⅰ型半功能私钥,对 G_3 部分随机选择 $\boldsymbol{\rho}\in Z_N^m$,$\rho_{m+1}\in Z_N$,$\forall i\in\omega_k$,$\rho'_i\in Z_N$,生成私钥 $SK_k=(\omega_k,\langle h_1^{\alpha_1}T^{a_1},h_2^{\alpha_2}T^{a_2},\cdots,h_m^{\alpha_m}T^{a_m}\rangle*g_3^{\boldsymbol{\rho}},Tg_3^{\rho_{m+1}},T^{s_i}g_3^{\rho'_i},\forall i\in\omega_k)$.显然,这个私钥的 G_3 部分是均匀分布的.值得注意的是,$T=g_1^w g_3^\sigma$ 或者 $g_1^w g_2^\kappa g_3^\sigma$,则这个私钥的 G_1 部分隐式地设置 $t=w$.若 $T=g_1^w g_2^\kappa g_3^\sigma$,则该私钥的 G_1 和 G_2 部分也是均匀分布的,且其Ⅰ型半功能参数 $\boldsymbol{\gamma}=\kappa\langle a_1,a_2,\cdots,a_m\rangle$,$\theta=\kappa$,$q_i=s_i$.由于 $\kappa,s_i,a_1,a_2,\cdots,a_m$ 模 p_2 的值是随机的,该私钥是均匀分布的.若 $T=g_1^w g_3^\sigma$,该私钥是均匀分布的正常私钥.

2) 挑战阶段 1.$\mathcal{A}$ 提交一个挑战访问结构 $\mathbb{A}^*(\boldsymbol{A}^*,\rho^*)$,$\mathcal{B}$ 选择一个满足访问结构 $(\boldsymbol{A}^*,\rho^*)$ 的属性集合 ω^*,询问私钥生成预言机 $\text{KGO}(\omega^*)$,当该询问次数 $r<k$ 时,生成Ⅱ型半功能私钥 $SK_{\omega^*}\text{-}\text{Ⅱ}$;当 $r=k$ 时,生成Ⅰ型半功能私钥 $SK_{\omega^*}\text{-}\text{Ⅰ}$;当 $r>k$ 时,生成正常私钥 SK_{ω^*}.此时注意,$\mathcal{A}$ 不能直接获得该私钥.

3) 询问阶段 2.与询问阶段 1 类似,此外,$\mathcal{B}$ 可以回答 $\mathcal{A}$ 的所有私钥 SK_{ω^*} 的泄漏信息.

4) 挑战阶段 2.$\mathcal{A}$ 提交等长消息 M_0 和 M_1 给 $\mathcal{B}$,$\mathcal{B}$ 选择随机数 $v'_2,v'_3,\cdots,v'_{n_2}\in Z_N$,对 $\boldsymbol{A}^*$ 的每一行 $\boldsymbol{A}_x$ 和 $j=1,2,\cdots,m$,随机选择 $r'_{j,x}\in Z_N$,生成向量 $\boldsymbol{v}'=\langle 1,v'_2,\cdots,v'_{n_2}\rangle$.$\mathcal{B}$ 选择一个随机位 $b\in\{0,1\}$,计算并输出挑战密文:

$$C^*=((\boldsymbol{A}^*,\rho^*),\ C_0=M_b e((g_1^z g_2^v)^{\sum_{j=1}^m\alpha_j\beta_j},g_1),$$

$$C_1=g_1^z g_2^v,\ \forall j,x,D_{j,x}=(g_1^z g_2^v)^{r'_{j,x}},$$

$$C_{j,x}=(g_1^z g_2^v)^{a_j\boldsymbol{A}_x\cdot\boldsymbol{v}'}(g_1^z g_2^v)^{-r'_{j,x}s_{\rho(x)}}),$$

其中,$g_1^z g_2^v$ 来自假设条件.

该密文是半功能的,其中

$$C_0=M_b\times e((g_1^z g_2^v)^{\sum_{j=1}^m\alpha_j\beta_j},g_1)=$$

$$M_b\times e(g_1^{z'\sum_{j=1}^m\alpha_j\beta_j},g_1)=$$

$$M_b\times\prod_{j=1}^m e(h_i,g_1)^{z\alpha_j}=M_b\times y^z,$$

$$C_1=g_1^z g_2^v,\ D_{j,x}=(g_1^z g_2^v)^{r'_{j,x}},$$

$$C_{j,x}=(g_1^z g_2^v)^{a_j\boldsymbol{A}_x\cdot\boldsymbol{v}'}(g_1^z g_2^v)^{-r'_{j,x}s_{\rho(x)}}=$$

$$g_1^{a_j\boldsymbol{A}_x z\boldsymbol{v}'}T_{\rho^*(x)}^{-zr'_{j,x}}g_2^{\boldsymbol{A}_x\cdot(a_jv\boldsymbol{v}')-vr'_{j,x}s_{\rho(x)}},$$

对于 G_1 部分,该密文隐式地设置 $s=z$,$\boldsymbol{v}=z\boldsymbol{v}'$,且为均匀分布,此时注意,$\boldsymbol{v}$ 的第 1 个分量是 z.对 G_2 部分,该密文隐式地设置 $\delta=v$,$\boldsymbol{u}_j=a_jv\boldsymbol{v}'$,$\delta_{j,x}=-vr'_{j,x}$,$q_{\rho(x)}=s_{\rho(x)}$.此时,当挑战私钥是Ⅰ型半功能私钥时,则 $q_{\rho(x)}=s_{\rho(x)}$.这个等式必须成立,因为 KeygenSF1 算法和 EncSF 算法中的 q_i 值必须相同.当挑战私钥是Ⅱ型半功能私钥时,私钥没有 q_i 项.

当挑战私钥是Ⅰ型半功能私钥时,私钥和挑战密文中的其余半功能参数如下:

私钥 $\boldsymbol{\gamma}=\theta'\langle a_1,a_2,\cdots,a_m\rangle,\theta=\theta'$.

密文 $\delta=v,\boldsymbol{u}_j=a_jv\langle 1,v_2,v_3,\cdots,v_{n_2}\rangle,\delta_{j,}=-v r'_{j,x}$.

注意 $\boldsymbol{u}_j$ 的第 1 个分量总是等于 a_jv,而攻击者可以从 $\boldsymbol{\gamma}$ 的第 j 个分量和 δ 分别获知 a_j 和 v 模 p_2 的值,$\boldsymbol{\gamma}$ 中的 κ 可从 θ 获知. 若第 k 个私钥的属性满足挑战访问结构时,且

$$\delta\sum_{j=1}^{m}\gamma_j-\theta\sum_{j=1}^{m}u_{j,1}=v\sum_{j=1}^{m}\kappa a_j-v\kappa\sum_{j=1}^{m}a_j=0 \bmod p_2,$$

则该私钥是名义半功能私钥.

由安全性定义可知,$\mathcal{A}$ 只能对该解密钥进行泄漏询问,而不能进行解密钥生成询问. 使用下面引理 3 证明:当挑战私钥的属性集合满足挑战密文的访问策略时,攻击者 $\mathcal{A}$ 区分第 k 个挑战私钥是名义半功能的或真正半功能的优势是可以忽略的. 证毕.

引理 3. 若域 GF(p_2)上的 Goldreich-Levin 定理成立,对任意 PPT 攻击者 $\mathcal{A}$,则 $\mathcal{A}$ 区分第 k 个挑战私钥是名义半功能的或真正半功能的优势是可忽略的.

证明. Goldreich-Levin 定理的挑战者 $\mathcal{C}$ 选取 $\boldsymbol{\Gamma}\in[0,\lambda]^m,\xi=f(\boldsymbol{\Gamma}),\mathbf{1}=\langle 1,1,\cdots,1\rangle\in \mathrm{GF}(p_2)^m$,随机数 $\zeta\in \mathrm{GF}(p_2)$.

$\mathcal{B}$ 和 $\mathcal{A}$ 模拟 $Game_{k,1}$,$\mathcal{B}$ 设置 $m=(3\times \mathrm{lb}\,p_2)^{1/\varepsilon}$,选择随机向量 $\langle h_1,h_2,\cdots,h_m\rangle\in G_1^m,\boldsymbol{\alpha}=\langle\alpha_1,\alpha_2,\cdots,\alpha_m\rangle\in Z_N^m,\boldsymbol{\rho}=\langle\rho_1,\rho_2,\cdots,\rho_m\rangle\in Z_N^m,\boldsymbol{a}=\langle a_1,a_2,\cdots,a_m\rangle\in Z_N^m,\rho_{m+1},t\in Z_N$. 对每个属性 $i\in U$,随机选择 $s_i,\rho'_i\in Z_N$. $\mathcal{B}$ 计算:

$$MSK=(\langle h_1^{\alpha_1}g_1^{a_1t},h_2^{\alpha_2}g_1^{a_2t},\cdots,h_m^{\alpha_m}g_1^{a_mt}\rangle * g_3^{\boldsymbol{\rho}},g_1^tg_3^{\rho_{m+1}},T_i^tg_3^{\rho'_i},\forall i\in U),$$

$$PK=(N,g_1,g_3,g_1^{a_1},g_1^{a_2},\cdots,g_1^{a_m},y=e(h_1,g_1)^{a_1}\cdots e(h_m,g_1)^{a_m},T_i=g_1^{s_i},\forall i\in U).$$

由于 $\mathcal{B}$ 已知系统主密钥和所有子群的生成元,它既可以生成正常私钥也能生成半功能私钥. 因此,$\mathcal{B}$ 可以回答询问阶段 1 中 $\mathcal{A}$ 的所有私钥生成询问.

1) 挑战阶段 1. 攻击者 $\mathcal{A}$ 提交一个挑战访问结构 $(\boldsymbol{A}^*,\rho^*)$,$\boldsymbol{A}^*$ 是一个 $n_1\times n_2$ 的矩阵,$\mathcal{B}$ 选择一个属性集合 ω^*,使得 ω^* 满足 $\boldsymbol{A}^*$. 注意:由安全性定义可知,$\mathcal{A}$ 不能得到与 ω^* 对应的私钥,仅能获得该私钥的泄漏信息.

2) 询问阶段 2. $\mathcal{B}$ 不生成与 ω^* 对应挑战私钥,而是将 $\mathcal{A}$ 对挑战私钥的泄漏询问编码成定义域为 $[0,\lambda]^m$ 的一元 PPT 函数. 通过固定其他私钥的所有值和固定挑战私钥的非半功能参数可以实现这种泄漏,具体过程如下:$\mathcal{B}$ 收到一个实例 $(f(\boldsymbol{\Gamma}),\mathbf{1},\zeta)$,其中,$\mathbf{1}=\langle 1,1,\cdots,1\rangle,\zeta=\boldsymbol{\Gamma}\cdot\mathbf{1}$ 或是随机值. $\mathcal{B}$ 用 $f(\boldsymbol{\Gamma})$来回答 $\mathcal{A}$ 关于挑战私钥的泄漏询问,并隐式地定义解密私钥.

$\mathcal{B}$ 随机选择 $r_1,r_2,\tau_1,\tau_2,\cdots,\tau_m\in Z_{p_2}$,定义 $r_3=(r_2\zeta+r_1r_2)\Big/\sum_{i=1}^{m}\tau_i$,令 g_2 为 G_2 的生成元,$\mathcal{B}$ 隐式地设置挑战私钥的 G_2 部分为 g_2^{γ} 和 g_2^{θ},其中,$\boldsymbol{\gamma}=\boldsymbol{\Gamma}+\langle 0,0,\cdots,0,r_1\rangle,\theta=r_3$,注意,$\boldsymbol{\Gamma}$ 的长度是 m,将 r_1 加到 $\boldsymbol{\Gamma}$ 的最后 1 个分量上. $\mathcal{B}$ 定义挑战私钥的非 G_2 部分满足其合理的分布.

3) 挑战阶段 2. $\mathcal{A}$ 提交 2 个等长消息 M_0 和 M_1 给 $\mathcal{B}$,$\mathcal{B}$ 用向量 $\boldsymbol{u}_i$ 和 $\delta=r_2\in Z_{p_2}$ 构造挑战密文,其中 $u_{i,1}=\tau_i$. 如果 $\zeta=\boldsymbol{\Gamma}\cdot\mathbf{1}$,则:

$$\delta\sum_{i=1}^{m}\gamma_i-\theta\sum_{i=1}^{m}u_{i,1}=r_2[(\boldsymbol{\Gamma}+\langle 0,0,\cdots,0,r_1\rangle)\cdot\mathbf{1}]-r_3\sum_{i=1}^{m}\tau_i=r_2(\boldsymbol{\Gamma}\cdot\mathbf{1})+r_1r_2-r_3\sum_{i=1}^{m}\tau_i=$$

$$r_2\times\frac{r_3\sum_{i=1}^{m}\tau_i-r_1r_2}{r_2}+r_1r_2-r_3\sum_{i=1}^{m}\tau_i=0,$$

此时,挑战私钥是名义半功能私钥. 如果 $\zeta\neq\boldsymbol{\Gamma}\cdot\mathbf{1}$,则挑战私钥是真正半功能的,且是均匀分布的.

4) 询问阶段 3. $\mathcal{B}$ 可以回答 $\mathcal{A}$ 的所有询问.

5) 猜测阶段. $\mathcal{B}$ 可用 $\mathcal{A}$ 的输出区分 $(f(\boldsymbol{\Gamma}),\mathbf{1},\boldsymbol{\Gamma}\cdot\mathbf{1})$和 $(f(\boldsymbol{\Gamma}),\mathbf{1},\zeta)$. 由 Goldreich-Levin 定理可知,若 $\mathcal{A}$ 能以 Δ 的优势区分上述的 2 个元组,$\mathcal{B}$ 能以至少

$$\frac{\Delta^3}{512mp_2^2}=\frac{\Delta^3p_2}{512mp_2^3}=\frac{\Delta^3p_2}{512m}\times\frac{1}{p_2^3}\geqslant\frac{1}{p_2^3}=2^{-m^{\varepsilon}}$$

的概率输出 $\boldsymbol{\Gamma}$,与泄漏函数 f 是不可逆函数矛盾,因此,$\mathcal{A}$ 不能区分该挑战私钥是名义半功能或真正半功能的.

当挑战私钥的属性不满足挑战访问结构时,$\mathcal{A}$ 可以询问该私钥. 由于文中限制在访问结构中每个属性只能使用一次,我们可以断定 $u_{j,1}=a_jv \bmod p_2$ 在信息理论上是隐藏的.

由于挑战私钥的属性集 ω^* 不满足挑战访问结构 $(\boldsymbol{A}^*,\rho^*)$,$\boldsymbol{A}^*$ 中使得 $\rho^*(x)\in\omega^*$ 的所有行 x 生成的行空间 R 不包含向量 $\langle 1,0,\cdots,0\rangle$. 因此,存在一个向量 $\boldsymbol{w}$,使得 $\boldsymbol{w}$ 正交于 $\boldsymbol{R}$,但 $\boldsymbol{w}$ 不正交于 $\langle 1,0,\cdots,0\rangle$,即 $\langle 1,0,\cdots,0\rangle\cdot\boldsymbol{w}\neq 0$. 我们固定一个包含 $\boldsymbol{w}$ 的基,则存在 $d_j\in Z_N$,使得 $\boldsymbol{u}_j=d_j\boldsymbol{w}+\boldsymbol{u}'_j \bmod p_2$,其中 $\boldsymbol{u}'_j$ 属于除 $\boldsymbol{w}$ 外的基向量扩张的空间中,注意到 $\boldsymbol{u}'_j$

是均匀分布的,且无法揭露 d_j 的任何信息.由于 $u_{j,1}=\boldsymbol{u}_j\cdot\langle 1,0,\cdots,0\rangle=d_j\boldsymbol{w}\cdot\langle 1,0,\cdots,0\rangle+\boldsymbol{u}_j'\cdot\langle 1,0,\cdots,0\rangle$,$\boldsymbol{u}_j'$ 不揭露 d_j 的任何信息,且 $\boldsymbol{w}$ 与$\langle 1,0,\cdots,0\rangle$不正交,因此,$u_{j,1}$的值与 d_j 相关.

$\boldsymbol{u}_j$ 和相应的 d_j 仅仅出现在矩阵 $\boldsymbol{A}^*$ 的第 x 行的指数 $\boldsymbol{A}_x^*\cdot\boldsymbol{u}_j+\delta_{j,x}q_{\rho^*(x)}$ 中,然而,并不是每一行的指数都影响 d_j 的值.如果 $\rho^*(x)\in\omega^*$,则 $\boldsymbol{w}$ 与 R 正交.该行的值与 d_j 无关.对其余的行来说,除了一个可以忽略的概率,所有的乘积因子 $\delta_{j,x}\neq 0 \bmod p_2$,因此,$d_j$ 的值被 $\delta_{j,x}$ 和 $q_{\rho^*(x)}$ 盲化.此时,限制访问结构中的每个属性只能出现一次.由于 $\delta_{j,x} \bmod p_2$ 是随机的,$q_{\rho^*(x)}$可以完全隐藏 d_j.文中访问结构中的属性只能出现一次,且只有挑战私钥(Ⅰ型半功能的)可以包含这些项,总之,$u_{j,1}$的值对 $\mathcal{A}$ 是均匀分布的.

6)询问阶段 3.与询问阶段 1 相同,除了 $\mathcal{A}$ 不能询问泄漏预言机.

基于假设 2,$\mathcal{B}$ 完美模拟了 $Game_{k-1,2}$或者以几乎为 1 的概率模拟 $Game_{k,1}$.因此,如果存在一个攻击者 $\mathcal{A}$ 能以不可忽略的优势区分 $Game_{k-1,2}$和 $Game_{k,1}$,则 $\mathcal{B}$ 能以几乎相同的优势打破假设 2. 证毕.

引理 4. 如果假设 2 成立,则任意 PPT 攻击者 $\mathcal{A}$ 区分 $Game_{k,1}$和 $Game_{k,2}$的优势是可以忽略的.

证明. 如果存在一个攻击者 $\mathcal{A}$ 能以不可忽略的优势区分 $Game_{k,1}$和 $Game_{k,2}$,则我们将以相同的优势攻破假设 2.算法 $\mathcal{B}$ 除了挑战私钥的构造方式与引理 2 不同,其他构造阶段相同.本引理的挑战私钥构造如下,随机选取向量 $\boldsymbol{h}\in[0,\lambda]^m$,$SK_{\omega^*}=(\boldsymbol{\omega}^*,\langle h_1^{a_1}T^{a_1},h_2^{a_2}T^{a_2},\cdots,h_m^{a_m}T^{a_m}\rangle*(g_2^{\mu}g_3^{p})^{\boldsymbol{h}}*g_3^{\boldsymbol{\rho}},Tg_3^{\rho_{m+1}},T^{s_i}g_3^{\rho_i'},\forall i\in\omega^*)$.与引理 2 中挑战私钥的区别是项$(g_2^{\mu}g_3^{p})^{\boldsymbol{h}}$,其中,$g_2^{\mu}g_3^{p}$ 是由假设 2 给定的.

如果 $T=g_1^{w}g_2^{k}g_3^{\sigma}$,挑战私钥和挑战密文的半功能参数如下:

$\boldsymbol{\gamma}=k\langle a_1,a_2,\cdots,a_m\rangle+\mu\boldsymbol{h},\theta=k,\delta=v,\boldsymbol{u}_j=a_jv\cdot\boldsymbol{v}'$.

在半功能挑战私钥和半功能密文中 $q_i=s_i$,注意:现在的挑战私钥中半功能参数被向量 $\mu\boldsymbol{h}$ 重新随机化,因此,该挑战私钥不再是名义半功能的,即等式 $\delta\sum_j\gamma_j-\theta\sum_j u_{j,1}=0$ 不再成立.显然,$\mu\boldsymbol{h}$ 使得所有的半功能参数模 p_2 的值完全随机化,且相互无关.所以,挑战私钥是均匀分布的Ⅰ型半功能私钥,$\mathcal{B}$ 完美模拟 $Game_{k,1}$(攻击者 $\mathcal{A}$ 询问的私钥是Ⅱ型半功能私钥、Ⅰ型半功能挑战私钥和正常私钥).

如果 $T=g_1^{w}g_3^{\sigma}$,则该挑战私钥是Ⅱ型半功能,且半功能参数 $\boldsymbol{\gamma}=\mu\boldsymbol{h}$,此时,$\mathcal{B}$ 完美模拟 $Game_{k,2}$(攻击者 $\mathcal{A}$ 询问的私钥是Ⅱ型半功能私钥、Ⅱ型半功能挑战私钥和正常私钥).因此,$\mathcal{B}$ 可以利用 $\mathcal{A}$ 的输出,以相同的优势攻破假设 2. 证毕.

引理 5. 如果假设 3 成立,则任意 PPT 攻击者 $\mathcal{A}$ 区分 $Game_{\mathcal{Q},2}$和 $Game_{\mathrm{Final}}$的优势是可以忽略的.

证明. 如果存在一个攻击者 $\mathcal{A}$ 能以不可忽略的优势区分 $Game_{\mathcal{Q},2}$ 和 $Game_{\mathrm{Final}}$,则我们将以相同的优势攻破假设 3.挑战者 $\mathcal{B}$ 接收到假设 3 的条件$\{g_1,g_2,g_3,g_1^{\alpha}g_2^{v},g_1^{z}g_2^{\mu},T\}$,能够模拟 $Game_{\mathcal{Q},2}$ 和 $Game_{\mathrm{Final}}$.

1)初始化阶段.$\mathcal{B}$ 设置 $m=(3\times\mathrm{lb}\,p_2)^{1/\varepsilon}$,选择随机向量$\langle a_1,a_2,\cdots,a_m\rangle\in Z_N^m$,$\langle\beta_1,\beta_2,\cdots,\beta_m\rangle\in Z_N^m$,对每个属性 $i\in U$,随机选择 $s_i\in Z_N$,$\langle\alpha_1,\alpha_2,\cdots,\alpha_{m-1}\rangle\in Z_N^{m-1}$,隐式设置:

$$\alpha_m=\frac{\alpha-\sum_{j=1}^{m-1}\alpha_i\beta_i}{\beta_m},\ h_j=g_1^{\beta_j}.$$

计算公钥 PK 并发送给 $\mathcal{A}$,其中,N,g_1,g_3 是由 $\mathcal{B}$ 给定.

$$PK=(N,g_1,g_3,g_1^{a_1},g_1^{a_2},\cdots,g_1^{a_m},$$
$$y=e(g_1^{\alpha}g_2^{v},g_1)=e(g_1,g_1)^{\alpha}=$$
$$e(g_1,g_1)^{\sum_{j=1}^{m}\alpha_j\beta_j}=e(h_1,g_1)^{\alpha_1}e(h_2,g_2)^{\alpha_2}\cdots$$
$$e(h_m,g_1)^{\alpha_m},\ T_i=g_1^{s_i},\forall i\in U).$$

2)询问阶段 1.$\mathcal{B}$ 为 $\mathcal{A}$ 的每次询问生成相应的Ⅱ型半功能私钥.即 $\mathcal{B}$ 随机选取 G_3 部分的指数 $t\in Z_N$,$\boldsymbol{h}\in[0,\lambda]^m$,$\boldsymbol{\rho}\in Z_N^m$,$i\in\omega$,随机选择 $\rho_i'\in Z_N$,计算私钥:

$SK_{\omega}=(\omega,g_1^{t}g_3^{\rho_{m+1}},T_i^{t}g_3^{\rho_i'},\ \forall i\in\omega,$

$\langle h_1^{a_1}g_1^{a_1t},\cdots,h_{m-1}^{a_{m-1}}g_1^{a_{m-1}t},(g_1^{\alpha}g_2^{v})g_1^{-\sum_{j=1}^{m-1}\alpha_j\beta_j}\rangle*g_2^{\boldsymbol{h}}*g_3^{\boldsymbol{\rho}})$,

其中,ω 由 $\mathcal{A}$ 选择的,$g_1^{\alpha}g_2^{v}$ 由 $\mathcal{B}$ 给定的.显然,这个具有参数 $\boldsymbol{\gamma}=\boldsymbol{h}+\langle 0,\cdots,0,v\rangle$的Ⅱ型半功能私钥是均匀分布的.

3)挑战阶段 1.攻击者 $\mathcal{A}$ 提交一个挑战访问结构$(\boldsymbol{A}^*,\rho^*)$,$\boldsymbol{A}^*$ 是一个 $n_1\times n_2$ 的矩阵,$\mathcal{B}$ 选择一个属性集合 ω^*,使得 ω^* 满足 $\boldsymbol{A}^*$,并使用询问阶段 1 相同的方法,为其生成一个Ⅱ型半功能挑战私钥.

4)询问阶段 2.与询问阶段 1 相同,此外,$\mathcal{A}$ 还可以询问解密私钥的泄漏信息.

5)挑战阶段 2.$\mathcal{A}$ 提交 2 个等长的消息 M_0 和 M_1,$\mathcal{B}$ 随机选择 $v_2',v_3',\cdots,v_m'\in Z_N$,对 $\boldsymbol{A}^*$ 的每一行

$\boldsymbol{A}_x^*$ 和 $j=1,2,\cdots,m$,随机选择 $r'_{j,x}\in Z_N$. $\mathcal{B}$ 生成向量 $\boldsymbol{v}'=\langle 1,v'_2,v'_3,\cdots,v'_m\rangle$,选择随机位 $b\in\{0,1\}$,计算挑战密文如下:

$$C^*=((\boldsymbol{A}^*,\rho^*),\ C_0=M_bT,\ C_1=g_1^z g_2^\mu,\ \forall j,x,$$

$$C_{j,x}=(g_1^z g_2^\mu)^{a_j\boldsymbol{A}_x\cdot\boldsymbol{v}'}(g_1^z g_2^\mu)^{-r'_{j,x}s_{\rho(x)}},$$

$$D_{j,x}=(g_1^z g_2^\mu)^{r'_{j,x}},$$

其中,$g_1^z g_2^\mu$ 是由假设 3 给定的,T 是一个挑战项. 半功能挑战密文:

$$C_1=g_1^z g_2^\mu,$$

$$C_{j,x}=(g_1^z g_2^\mu)^{a_j\boldsymbol{A}_x\boldsymbol{v}'}(g_1^z g_2^\mu)^{-r'_{j,x}s_{\rho(x)}}=$$

$$g_1^{a_j\boldsymbol{A}_x z\boldsymbol{v}'}T_{\rho^*(x)}^{-zr'_{j,x}}g_2^{\boldsymbol{A}_x(a_j\mu\boldsymbol{v}')-\mu r'_{j,x}s_{\rho(x)}},$$

$$D_{j,x}=(g_1^z g_2^\mu)^{r'_{j,x}}.$$

对 G_1 部分,该密文隐式地设置 $s=z,\boldsymbol{v}=z\boldsymbol{v}'$,$r_{j,x}=zr'_{j,x}$. 因此,$G_1$ 部分是均匀分布的,值得注意的是,向量 $\boldsymbol{v}$ 的第 1 个分量必须是 z. 对 G_2 部分,该密文隐式设置 $\delta=\mu,\boldsymbol{u}_j=a_j\mu\boldsymbol{v}',\delta_{j,x}=-\mu r'_{j,x},q_{\rho(x)}=s_{\rho(x)}$. 由于 $\mathcal{A}$ 仅能看到 $s,\mu,a_1,a_2,\cdots,a_m,v'_2,v'_3,\cdots,v'_{n_2},r'_{j,x},s_{\rho(x)}$ 模 p_1 的值,所以它们模 p_2 的值是均匀分布的,即挑战密文的 G_2 部分是均匀分布的.

6) 询问阶段 3. 与询问阶段 1 相同,除了 $\mathcal{A}$ 不能询问泄漏预言机.

如果 $T=e(g_1,g_1)^{\alpha z}$,挑战密文为消息 M_b 的半功能密文. 否则,挑战密文是随机消息的半功能密文. 因此,$\mathcal{B}$ 可以利用 $\mathcal{A}$ 的输出攻破假设 3. 证毕.

定理 2. 如果假设 1,2,3 成立,则文中抗连续辅助输入泄漏的属性基加密方案是 2^{-m^ε}-CAI-CPA 安全的.

证明. 由引理 1~5 可知,$Game_{\text{Real}}$ 和 $Game_{\text{Final}}$ 是不可区分的. 在 $Game_{\text{Final}}$ 中由于挑战密文是随机消息的密文,因此,攻击者 $\mathcal{A}$ 在 $Game_{\text{Final}}$ 的优势是 0. 综上所述,$\mathcal{A}$ 在 $Game_{\text{Real}}$ 的优势是可以忽略的.

证毕.

4.2 泄漏性能和密钥长度对比

抗密钥泄漏的容忍程度是衡量一种密码机制安全性的重要指标. 总的来说,抗泄漏密码机制的主要目标是尽可能预防和抵抗更多不同类型的边信道攻击,使系统在实际应用中的安全性得到可靠的保障. 本节对比本文方案和相关的 2 个知名方案在抗泄漏容忍程度、主密钥长度和用户私钥长度等方面的性能,表明了本文方案不仅具有最好的抗泄漏容忍性,而且具有较短的主密钥长度和用户私钥长度.

表 1 将本文方案和相关的 2 个知名方案在密钥泄漏容忍程度、主密钥长度和用户私钥长度方面进行详细比较,其中,$n\geqslant 2$,$|U|$ 表示系统全体属性 U 的个数,$|\omega|$ 表示用户属性集合 ω 中属性的个数,$|G|$ 表示群 G 或 G_T 中元素的长度,$0<\varepsilon<1$,YCZY[11] 方案中的 $m=(3\lambda)^{1/\varepsilon}$,$p_2$ 是群 G_2 阶,本文方案令 $m=(3\times\text{lb}\,p_2)^{1/\varepsilon}$.

Table 1 Performance Comparison

表 1 性能比较

Scheme	Length of MSK	Length of SK_ω	Leakage Resilience	Composition Feature	Leakage of Old Secret Key	Fine-Grained Access Control of Ciphertext
LRW[30]-ABE	$(n+2+\|U\|)\|G\|$	$(n+2+\|\omega\|)\|G\|$	Bounded Leakage of MSK and SK_ω	No	No	Enable
YCZY[11]-IBE	$3m\|G\|$	$3m\|G\|$	Continual and Overall Unbounded Leakage of MSK and SK_{id}	Enable	Enable	No
Our Scheme	$(m+1+\|U\|)\|G\|$	$(m+1+\|\omega\|)\|G\|$	Continual and Overall Unbounded Leakage of MSK and SK_ω	Enable	Enable	Enable

根据表 1 可以看出,LRW 方案[30] 提出了一种自适应安全的抗密钥连续泄漏的 ABE 方案,仅允许主密钥和用户属性私钥的有界泄漏,且要求旧版本的密钥必须从内存中完全清除. 此外,该方案不能与其他密码学方案组合使用. 与该方案相比,本文方案允许主密钥和用户属性私钥的连续无界泄漏,每次密钥更新时允许泄漏旧密钥信息,且可以与其他密码方案组合应用. 虽然本文方案适当增加了主密钥和用户私钥的长度,但具有更强的抗密钥泄漏安全性. 与 YCZY-IBE 方案[11] 相比,在具有相同抗泄漏容忍性的前提下,本文方案的主密钥和用户私钥长度显著减少,且能实现加密数据的细粒度共享访问控制.

5 结 论

针对属性基加密机制中边信道攻击下的密钥泄漏问题,本文将连续辅助输入泄漏模型[11] 和双系统加密[15] 相结合,通过合理设计主密钥和用户私钥的生成过程,提出一种抗连续辅助输入泄漏的 ABE

方案,一定程度上解决了 ABE 中的抗密钥泄漏的公开难题.基于合理假设,证明本文方案在攻击者获知辅助输入密钥泄漏信息的情况下仍具有自适应安全性.本文方案的主要贡献有 3 个方面:1)允许主密钥和用户属性私钥的连续无界泄漏;2)允许 ABE 的属性私钥应用到其他密码系统中,具有较好的合成性质;3)每次密钥更新时无需假定将旧版本密钥从内存中完全清除,允许泄漏旧版本密钥的信息.与相关的 2 个知名方案相比,本文方案不仅具有最好的抗泄漏容忍性,而且具有相对较短的主密钥长度和用户私钥长度.

尽管本文方案在一定程度上解决了 ABE 抵制边信道攻击下密钥泄漏的难题,显著增强了 ABE 系统的安全性,但与原来的 CP-ABE 方案[14]相比,系统的密文、主密钥和用户私钥的长度增加较大,且加解密效率较低.因此,如何减少本文方案中的系统主密钥、用户私钥和密文长度,提高加解密的计算效率,将是我们未来研究工作的重要方向.

参 考 文 献

[1] Kocher P C. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems [G] //LNCS 1109: Proc of the 16th Annual Int Cryptology Conf. Berlin: Springer, 1996: 104-113

[2] Boneh D, DeMillo R A, Lipton R J. On the importance of checking cryptographic protocols for faults [G] //LNCS 1233: Proc of the Int Conf on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 1997: 37-51

[3] Kocher P C, Jaffe J, Jun B. Differential power analysis [G] //LNCS 1666: Proc of the 19th Annual Int Cryptology Conf. Berlin: Springer, 1999: 388-397

[4] Halderman A, Schoen S, Heninger N, et al. Lest we remember: Cold boot attacks on encryption keys [C] //Proc of the 17th USENIX Security Symp. Berkeley, CA: USENIX Association, 2008: 45-60

[5] Naor M, Segev G. Public-key cryptosystems resilient to key leakage [G] //LNCS 5677: Proc of the 29th Int Cryptology Conf. Berlin: Springer, 2009: 18-35

[6] Akavia A, Goldwasser S, Vaikuntanathan V. Simultaneous hardcore bits and cryptography against memory attacks [G] //LNCS 5444: Proc of the 29th Int Cryptology Conf. Berlin: Springer, 2009: 474-495

[7] Dodis Y, Haralambiev K, L'opez-Alt A, et al. Cryptography against continuous memory attacks [C] //Proc of the 51st Annual Symp on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society, 2010: 511-520

[8] Alwen J, Dodis Y, Naor M, et al. Public-Key encryption in the bounded-retrieval model [G] //LNCS 6110: Proc of the 29th Annual Int Conf on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 2010: 113-134

[9] Dodis Y, Goldwasser S, Kalai Y T, et al. Public-key encryption schemes with auxiliary inputs [G] //LNCS 5978: Proc of the Theory of Cryptography Conf. Berlin: Springer, 2010: 361-381

[10] Brakerski Z, Kalai Y T, Katz J, et al. Overcoming the hole in the bucket: Public-key cryptography resilient to continual memory leakage [C] //Proc of the 51st Annual Symp on Foundations of Computer Science. Los Alamitos, CA: IEEE Computer Society, 2010: 511-520

[11] Yuen T H, Chow S S M, Zhang Y, et al. Identity-based encryption resilient to continual auxiliary leakage [G] //LNCS 7237: Proc of the 31st Annual Int Conf on the Theory and Application of Cryptographic Techniques. Berlin: Springer, 2012: 117-134

[12] Sahai A, Waters B. Fuzzy identity based encryption [G] //LNCS 3494: Proc of the EUROCRYPT 2005. Berlin: Springer, 2005: 457-473

[13] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of the 2007 IEEE Symp on Security and Privacy. Los Alamitos, CA: IEEE Computer Society, 2007: 321-334

[14] Lewko A, Okamoto T, Sahai A, et al. Fully secure functional encryption: Attribute-Based encryption and (hierarchical) inner product encryption [G] //LNCS 6110: Proc of the EUROCRYPT 2010. Berlin: Springer, 2010: 62-91

[15] Waters B. Dual system encryption: Realizing fully secure ibe and hibe under simple assumptions [G] //LNCS 5677: Proc of the 29th Int Cryptology Conf. Berlin: Springer, 2009: 619-636

[16] Goyal V, Pandey O, Sahai A, et al. Attribute-Based encryption for fine-grained access control of encrypted data [C] //Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89-98

[17] Yu S C, Ren K, Lou W J. Attribute-based content distribution with hidden policy [C] //Proc of the 4th Workshop on Secure Network Protocols (NPSec). Los Alamitos, CA: IEEE Computer Society, 2008: 39-44

[18] Traynor P, Butler K, Enck W, et al. Realizing massive-scale conditional access systems through attribute-based cryptosystems [C] //Proc of the 15th Annual Network and Distributed System Security Symp. Los Alamitos, CA: IEEE Computer Society, 2008: 1-13

[19] Cheung L, Newport C. Provably secure ciphertext policy ABE [C] //Proc of the ACM Conf on Computer and Communications Security. New York, ACM, 2007: 456-465

[20] Cheung L, Cooley J A, Khazan R, et al. Collusion-Resistant group key management using attribute-based encryption [OL]. [2014-06-15]. http://eprint.iacr.org/2007/161.pdf

[21] Yu S C, Ren K, Lou W J. Attribute-based on-demand multicast group setup with membership anonymity [J]. Computer Networks, 2010, 54(3): 377-386

[22] Baden R, Bender A, Spring N, et al. Persona: An online social network with user-defined privacy [C] //Proc of the ACM SIGCOMM 2009 Conf on Data Communication. New York: ACM, 2009: 135-146

[23] Su Jinshu, Cao Dan, Wang Xiaofeng, et al. Attribute-based encryption schemes [J]. Journal of Software, 2011, 22(6): 1299-1315 (in Chinese)
(苏金树, 曹丹, 王小峰. 等. 属性基加密机制[J]. 软件学报, 2011, 22(6): 1299-1315)

[24] Yu S C, Ren K, Lou W J, et al. Defending against key abuse attacks in KP-ABE enabled broadcast system [C] //Proc of the Security and Privacy in Communication Networks. New York: ACM, 2009: 311-329

[25] Li J, Ren K, Zhu B, et al. Privacy-aware attribute-based encryption with user accountability [G] //LNCS 5735: Proc of the Information Security Conf. Berlin: Springer, 2009: 347-362

[26] Wang Y T, Chen K F, Chen J H. Attribute-based traitor tracing [J]. Journal of Information Science and Engineering, 2011, 27(1): 181-195

[27] Boldyreva A, Goyal V, Kumar V. Identity-based encryption with efficient revocation [C] //Proc of the 14th ACM Conf on Computer and Communication Security. New York: ACM, 2008: 417-426

[28] Liu Z, Cao Z F, Wong D C S. Blackbox traceable CP-ABE: How to catch people leaking their keys by selling decryption devices on ebay [C] //Proc of the 20th ACM Conf on Computer and Communications Security. New York: ACM, 2013: 475-486

[29] Ma Haiying, Zeng Guosun. An attribute-based encryption scheme for traitor tracing and revocation together [J]. Chinese Journal of Computers, 2012, 35(9): 1845-1855 (in Chinese)
(马海英, 曾国荪. 可追踪并撤销叛徒的属性基加密方案[J]. 计算机学报, 2012, 35(9): 1845-1855)

[30] Lewko A, Rouselakis Y, Waters B. Achieving Leakage resilience through dual system encryption [C] //Proc of the 8th Theory of Cryptography Conf. New York: ACM, 2011: 70-88

Ma Haiying, born in 1977. PhD, associate professor in Nantong University. Member of China Computer Federation. Her main research interests include public key cryptography and network security.

Zeng Guosun, born in 1964. Professor and PhD supervisor in Tongji University. His main research interests include information security and parallel computing.

Bao Zhihua, born in 1955. Professor in Nantong University. His main research interests include modern communication theory and technology, communications-specific integrated circuit designs.

Chen Jianping, born in 1960. Professor in Nantong University. His main research interests include information security and numeric computation.

Wang Jinhua, born in 1963. PhD, professor, PhD supervisor. His main research interests include combinatorial design theory, combined coding theory, cryptography, and their intersectional fields.

Wang Zhanjun, born in 1978. Received his master degree from Henan Normal University. His main current research interests include public key cryptosystem and algebra.