可追踪并撤销叛徒的属性基加密方案

马海英[1),2),3)] 曾国荪[1),2)]

[1)](同济大学计算机科学与技术系 上海 201804)

[2)](嵌入式系统与服务计算教育部重点实验室 上海 201804)

[3)](南通大学计算机科学与技术学院 江苏 南通 226019)

摘 要 属性基加密(ABE)是一种有效地对加密数据实现细粒度访问控制的密码学体制.在ABE系统中,存在恶意用户(或叛徒)泄露私钥生成盗版解码器,并将其分发给非法用户的问题.现有的解决方案仅能追查到密钥泄漏者的身份,但不能将其从ABE系统中撤销.文中提出了一种既可追踪又可撤销叛徒的属性基加密方案(ABTR).首先,给出一个具有扩展通配符的属性基加密方案(GWABE),基于3个3素数子群判定假设,采用双系统加密方法证明该GWABE方案是完全安全的.然后,利用完全子树构架将GWABE转化成ABTR方案,并证明该ABTR方案是完全安全的,且用户私钥长度是固定的.而此前的可追踪叛徒的ABE方案仅满足选择安全性.

关键词 属性基加密;访问控制;完全子树框架;叛徒追踪;撤销

中图法分类号 TP309 **DOI号**: 10.3724/SP.J.1016.2012.01845

An Attribute-Based Encryption Scheme for Traitor Tracing and Revocation Together

MA Hai-Ying[1),2),3)] ZENG Guo-Sun[1),2)]

[1)](*Department of Computer Science and Technology, Tongji University, Shanghai* 201804)

[2)](*The Key Laboratory of Embedded System and Service Computing, Ministry of Education, Shanghai* 201804)

[3)](*College of Computer Science and Technology, Nantong University, Nantong, Jiangsu* 226019)

Abstract Attribute-based encryption (ABE) is an effective cryptographic primitive for achieving fine-grained access control of encrypted data. A well-known concern in the ABE system is that malicious users (or traitors) leak their private keys to construct pirate decryption devices and distribute them to illegal users. The existing solutions can only trace the identities of users who leaked their keys, but they can not revoke the leaked keys from the ABE system. This paper proposes an attribute-based encryption scheme for traitor tracing and revocation together (ABTR). We first introduce an ABE scheme with generalized wildcards (GWABE). Under three assumptions of the subgroup decision problem for 3 primes (3P-SDP), we prove that the GWABE scheme is fully secure by using the dual system encryption method. Then we transform the GWABE scheme into an ABTR scheme by using the complete subtree framework. The ABTR scheme is proved to be fully secure, and provides the nice feature of having constant private key size. However, the previous ABE schemes for traitor tracing were only proved secure in the selective model.

Keywords attribute-based encryption; access control; complete subtree framework; traitor tracing; revocation

---

收稿日期:2012-05-03;最终修改稿收到日期:2012-08-03.本课题得到国家"八六三"高技术研究发展计划项目基金(2007AA01Z425,2009AA012201)、国家自然科学基金(61103068)、NSFC-微软亚洲研究院联合资助项目(60970155)、上海市优秀学科带头人计划项目(10XD1404400)、教育部博士点基金(20090072110035)、教育部网络时代的科技论文快速共享专项研究课题(20110740001)资助.
马海英,女,1977年生,博士研究生,讲师,主要研究方向为公钥密码学和网络安全.E-mail: m_hying@163.com. **曾国荪**,男,1964年生,博士,教授,博士生导师,主要研究领域为信息安全、并行计算.

1 引 言

2005 年 Sahai 和 Waters[1] 在欧洲密码学年会上提出了属性基加密机制(Attribute-Based Encryption, ABE)的概念. 在该 ABE 机制中,可信授权机构为用户颁发私钥,用户私钥和密文分别与一组属性相关,当用户的私钥属性与密文属性相互匹配度达到系统规定的门限值时,用户才能解密密文. 该 ABE 机制[1]仅能支持门限访问控制策略. 为了表达更灵活的访问控制策略,2006 年 Goyal 等人[2]在 CCS 会议上提出了密钥策略的 ABE 机制(KP-ABE),实现了对加密数据的细粒度访问控制. 在 KP-ABE 中,密钥与访问策略相关,密文与属性集合相关,只有密文的属性满足密钥的访问策略时,才能解密密文. 2007 年,Bethencourt 等人[3]提出了密文策略的 ABE 机制(CP-ABE). 在 CP-ABE 中,密文与访问策略相关,密钥与属性集合相关,只有密钥的属性满足密文的访问策略时,才能解密密文. 上述两种 ABE 机制实现了基于属性的灵活访问控制策略,使得它们在细粒度访问控制领域具有广阔的应用前景[2-5],例如付费电视系统、审计日志、数据库访问等.

在 ABE 系统中,用户的访问权利与其私钥直接关联[1-6]. 如果合法用户泄露自己的私钥构造盗版解密设备,并将其分发给非法用户,则系统的访问控制策略将会被打破[7]. 特别的,在 ABE 机制中,用户私钥仅与其属性相关,而与用户的任何特定信息(如身份)无关,即使泄露的密钥后来被发现,我们也无法将其与任何合法用户相关联. 因此,合法用户可以轻易的与他人共享自己的私钥而不用担心被发现[7-10]. 针对这个密钥滥用问题,学者们进行了深入的研究,提出了不同的解决方案. 2008 年 Hinek 等人[7]提出基于标号的 ABE 方案,使得密钥代理将会暴露用户的隐私信息,对预防密钥克隆起到威慑作用. 但是,该方案无法追查到密钥滥用者的真实身份. YRLL09[8]和 LRZW09[9]基于 DBDH 和 D-Linear 假设分别提出了防滥用 KP-ABE 方案和可追责的匿名 CP-ABE 方案,解决了 ABE 机制中密钥滥用者的身份追踪问题. WCC11[10]提出了属性基叛徒追踪方案,使用唯一身份标识用户,采用联合安全编码[11]和叛徒追踪[12]技术来确定密钥滥用者的身份. 但是联合安全编码的使用导致密文和公钥长度过大,系统效率过低. 因此,他们将构造一个高效的属性基叛徒追踪方案作为一个公开问题. 然而,上述可追踪叛徒的 ABE 方案[7-10]均不能将叛徒从系统中撤销,从而无法使盗版解密设备无效.

针对用户私钥的泄露问题,Pirretti 等人[13]最早提出可撤销的 ABE 机制,使用户私钥与有效期相关,授权机构周期性更新未撤销用户的私钥,从而使已撤销用户的私钥无效,但该方案不支持用户的即时撤销. Ostrovsky 等人[14]将用户标识作为一个属性,把密文和被撤销用户标识的"非"相关联,实现了 CP-ABE 中用户的即时撤销,但是增加了用户私钥和密文的长度. Attrapadung 和 Imai[15]对其进行了改进,减少撤销的开销,提出广播 ABE 机制. Boldyreva 等人[16]采用二叉树提出可撤销的 ABE 方案,实现了 KP-ABE 中用户的撤销. 但是,现有可撤销的 ABE 方案[13-16]都不能追查到叛徒的真实身份. 综上所述,现有的 ABE 方案都无法同时实现叛徒的追踪和撤销[17]. 为了更好地防止 ABE 系统中盗版密钥的产生和传播,构建既可追踪又可撤销叛徒的属性基加密方案具有十分重要的现实意义.

本文基于完全子树构架[18]提出一个可追踪并撤销叛徒的属性基加密方案(ABTR). 在完全子树构架中,需要根据身份撤销列表将未撤销用户划分成不相交的子集,然后为每个子集的用户生成子密文,整个密文由所有子密文构成. 但是,一般的 ABE 方案无法为由身份撤销列表划分成的用户子集生成密文. 因此,无法利用完全子树构架将一般的 ABE 方案直接转化成 ABTR 方案. 针对这个问题,我们首先给出了具有扩展通配符的属性基加密方案(GWABE),基于 3 个 3 素数子群判定假设,采用双系统加密方法[6]证明该 GWABE 方案在标准模型下是完全安全的. 然后,我们利用完全子树构架将该 GWABE 转化成 ABTR 方案,并证明该 ABTR 方案是完全安全的,且用户私钥长度是固定的.

第 2 节给出本文所使用的预备知识;第 3 节给出 GWABE 的定义及其安全性模型,提出一个具体的 GWABE 方案,并证明其相应的安全性;第 4 节采用完全子树构架将第 3 节的 GWABE 转化成 ABTR 方案,并证明该 ABTR 方案是完全安全的,随后将该方案与相关方案在性能方面进行比较;第 5 节给出全文的总结.

2 预备知识

2.1 符号说明

本文中,Z 表示整数环,对于正整数 p,Z_p 表示模为 p 的整数环. 符号 $x \xleftarrow{R} Z_p$ 表示在 Z_p 中随机选取元素 x. 当 $\mathcal{A}$ 表示某个算法时,符号 $\mathcal{A}(a_1, a_2, \cdots,$

$a_n)\to b_1,\cdots,b_m$ 表示算法 $\mathcal{A}$ 以 $a_1,a_2,\cdots,a_n$ 为输入，输出 $b_1,\cdots,b_m$.

2.2　访问结构和线性秘密共享方案(LSSS)

定义 1(访问结构[6]).　设 $\mathcal{P}=\{\mathcal{P}_1,\mathcal{P}_2,\cdots,\mathcal{P}_n\}$ 是 n 个参与者的集合，集族 $\mathbb{A}\subseteq 2^{\mathcal{P}}$ 称为单调的，如果对任意集合 B、C，都有：若 $B\in\mathbb{A}$ 且 $B\subseteq C$，则 $C\in\mathbb{A}$. 访问结构(或单调访问结构)是 $\mathcal{P}$ 的某些非空子集构成的集族 $\mathbb{A}$(或单调集族)，即 $\mathbb{A}\subseteq 2^{\mathcal{P}}\setminus\varnothing$，$\mathbb{A}$ 中的集合称为授权集，不在 $\mathbb{A}$ 中的集合称为非授权集.

定义 2(LSSS[6]).　称参与者集合 $\mathcal{P}=\{\mathcal{P}_1,\mathcal{P}_2,\cdots,\mathcal{P}_n\}$ 上的一个秘密共享方案 Π 是线性的，如果①参与者的秘密分享值构成 Z_p 上的一个向量；②对于 Π，存在一个秘密份额生成矩阵 $\boldsymbol{A}_{l\times h}$ 和行标号函数 $\rho:\{1,\cdots,\ell\}\to\mathcal{P}$，设 $s\in Z_p$ 是待共享的秘密值，随机选择 $r_2,\cdots,r_h\in Z_p$，构成向量 $\boldsymbol{v}=(s,r_2,\cdots,r_h)$，令 $\boldsymbol{v}'$ 为 $\boldsymbol{v}$ 的转置，则 $\boldsymbol{A}\cdot\boldsymbol{v}'$ 是 ℓ 个秘密份额构成的向量，根据标号函数将秘密份额 $\lambda_i=(\boldsymbol{Av})_i$ $(1\le i\le\ell)$ 分配给参与者 $\rho(i)$.

LSSS 的线性重构性质：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 $I=\{i:\rho(i)\in S\}\subseteq\{1,\cdots,\ell\}$，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 $\{\lambda_i\}_{i\in\{1,\cdots,\ell\}}$，满足 $\Sigma_{i\in I}c_i\lambda_i=s$.

将 LSSS 引入到本文的方案中，参与者为属性，访问结构包含所有的授权属性集.

2.3　合数阶双线性群和复杂性假设

文献[6]提出合数阶双线性群的概念，本文利用一个群生成器算法 $\mathcal{G}$ 对其定义. 该算法输入系统的安全参数 λ，输出一个对双线性群 G 的描述，即 $\mathcal{G}$ 输出一个元组 (p_1,p_2,p_3,G,G_T,e)，其中 p_1,p_2,p_3 为 3 个不同素数，G 和 G_T 是 $N=p_1p_2p_3$ 阶循环群，映射 $e:G\times G\to G_T$ 满足：(1) 双线性. $\forall u,v\in G;a,b\in Z_N;e(u^a,v^b)=e(u,v)^{ab}$. (2) 非退化性. $\exists g\in G$ 使得 $e(g,g)$ 在 G_T 中的阶为 N. (3) 可计算性. G 和 G_T 中的运算以及双线性映射 e 都是在多项式时间内可计算的.

令 G_{p_1},G_{p_2},G_{p_3} 分别表示群 G 的 p_1,p_2,p_3 阶子群，当 $h_i\in G_{p_i},h_j\in G_{p_j}$，且 $i\ne j$ 时，$e(h_i,h_j)$ 为 G_T 的单位元. 子群 G_{p_1}，G_{p_2} 和 G_{p_3} 之间的正交性[6]是本文构造方案的一个主要工具.

下面，我们给出用于证明本文方案安全性的复杂性假设. 本文中的 3 个 3 素数子群判定假设是在文献[6]中被提出的，在这些假设中，令 $G_{p_1p_2}$ 等表示群 G 的 p_1p_2 阶子群，Pr 是概率函数.

假设 1.　给定群生成器 $\mathcal{G}$，我们定义如下分布：$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G}(\lambda),g\xleftarrow{R}G_{p_1},X_3\xleftarrow{R}G_{p_3},D=(\mathbb{G},g,X_3),T_1\xleftarrow{R}G_{p_1p_2},T_2\xleftarrow{R}G_{p_1}$. 我们定义敌手 $\mathcal{A}$ 攻破假设 1 的优势为

$$Adv1_{\mathcal{G},\mathcal{A}}(\lambda):=|Pr(\mathcal{A}(D,T_1)=1)-Pr(\mathcal{A}(D,T_2)=1)|.$$

假设 2.　给定群生成器 $\mathcal{G}$，我们定义如下分布：$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G}(\lambda)$，$g\xleftarrow{R}G_{p_1}$；$X_2,Y_2\xleftarrow{R}G_{p_2}$；$X_3,Y_3\xleftarrow{R}G_{p_3}$，$D=(\mathbb{G},g,X_1X_2,X_3,Y_2Y_3),T_1\xleftarrow{R}G,T_2\xleftarrow{R}G_{p_1p_3}$. 我们定义敌手 $\mathcal{A}$ 攻破假设 2 的优势为

$$Adv2_{\mathcal{G},\mathcal{A}}(\lambda):=|Pr(\mathcal{A}(D,T_1)=1)-Pr(\mathcal{A}(D,T_2)=1)|.$$

假设 3.　给定群生成器 $\mathcal{G}$，我们定义如下分布：$\mathbb{G}=(N=p_1p_2p_3,G,G_T,e)\xleftarrow{R}\mathcal{G}(\lambda),\alpha,t\xleftarrow{R}Z_N$，$g\xleftarrow{R}G_{p_1}$；$X_2,Y_2,Z_2\xleftarrow{R}G_{p_2}$，$X_3\xleftarrow{R}G_{p_3}$，$D=(\mathbb{G},g,g^{\alpha}X_2,X_3,g^tY_2,Z_2)$，$T_1\xleftarrow{R}e(g,g)^{\alpha t}$，$T_2\xleftarrow{R}G_T$.

我们定义敌手 $\mathcal{A}$ 攻破假设 3 的优势为

$$Adv3_{\mathcal{G},\mathcal{A}}(\lambda):=|Pr(\mathcal{A}(D,T_1)=1)-Pr(\mathcal{A}(D,T_2)=1)|.$$

定义 3.　如果对于任意多项式时间的敌手 $\mathcal{A}$，$Adv1_{\mathcal{G},\mathcal{A}}(\lambda)$，$Adv2_{\mathcal{G},\mathcal{A}}(\lambda)$，$Adv3_{\mathcal{G},\mathcal{A}}(\lambda)$ 都是可忽略的，我们就说群生成器 $\mathcal{G}$ 满足假设 1,2,3，即假设 1,2,3 均成立.

2.4　子集覆盖构架和完全子树构架

令 $\mathcal{N}$ 表示全体用户的集合，$\mathcal{R}$ 表示撤销用户的集合，$\mathcal{N}\setminus\mathcal{R}$ 表示未撤销用户集合. 子集覆盖构架[18]将每个用户与二叉树的一个叶子节点相对应，由 Subset 算法和 Cover 算法组成. Subset 算法定义一个子集的集合 $(S_1,S_2,\cdots,S_w)$，每个子集 $S_i\subset\mathcal{N}$ $(1\le i\le w)$ 具有一个身份模式 P_i，S_i 中的每个用户都能解密在模式 P_i 下加密的密文. 当有用户子集 $\mathcal{R}$ 被系统撤销时，Cover 算法将未撤销用户集合 $\mathcal{N}\setminus\mathcal{R}$ 划分成若干个互不相交的集合 $(S_{i1},S_{i2},\cdots,S_{im})$，使得 $S_{i1}\cup S_{i2}\cup\cdots\cup S_{im}=\mathcal{N}\setminus\mathcal{R}$.

完全子树构架是对子集覆盖构架的一个具体实现，基于完全子树构架定义的加密系统由 3 个算法组成：(1) 初始化算法. 给每个合法用户指定秘密信息，用于解密消息. (2) 加密算法. 给定消息 M 和撤销用户集合 $\mathcal{R}$，系统利用 Cover 算法将未撤销用户集合 $\mathcal{N}\setminus\mathcal{R}$ 划分成 $(S_{i1},S_{i2},\cdots,S_{im})$，随后选择会话密钥 K，分别用这些子集对应的身份模式 P_{ij} $(1\le$

$j \leq m$)对会话密钥 K 进行公钥加密,而用 K 对消息 M 进行对称加密,密文形如 $\{[i_1, i_2, \cdots, i_m, Enc_{P_{i1}}(K), \cdots, Enc_{P_{im}}(K)], E_K(M)\}$,其中,$Enc$ 为公钥加密算法,为了提高效率减少带宽,E 采用快速的对称加密算法,例如 M 和 K 的异或运算. (3)解密算法. 未撤销用户 $u \in \mathcal{N} \backslash \mathcal{R}$ 首先找到 j 使得 $u \in S_{ij}$,利用自己的秘密信息解密 $Enc_{P_{ij}}(K)$,得到会话密钥 K,计算 $D_K(E_K(M))$,得到消息 M.

3 具有扩展通配符的 ABE 方案(GWABE)

为了将 ABE 和完全子树构架相结合实现用户的撤销,本节基于 LW 的 KP-ABE 方案[6]提出具有扩展通配符的属性基加密方案(GWABE),GWABE 本质上是 ABE 的一种变形.

为了更好地理解 GWABE 的定义,我们首先给出身份模式(或模式)和匹配的概念. 身份模式 P 是由长度为 n 的位串来表示,其中可能包含一个通配符 $*$,通配符 $*$ 由其开始位置和终止位置决定,例如,长度为 9 的身份模式 $P=$"101 $*$101",其中,通配符 $*$ 的长度为 3,开始位置为 4,终止位置为 6. 如果 P 中确实包含一个通配符,则称 P 为扩展通配符. 每个身份模式可记为 $P = P_{ip} \| * \| P_{is}$,其中,$P_{ip}$,$P_{is}$ 分别是长度为 ip, is 的位串($1 \leq ip, is \leq n$),通配符 $*$ 的长度为 $n-ip-is$,开始位置为 $ip+1$,终止位置为 $n-is$. 给定用户的身份 id 和身份模式 P,如果 $id = P$ 或者 id 和 P 的形式为 $P = P_{ip} \| * \| P_{is}$ 且 $id = P_{ip} \| id_* \| P_{is}$,其中 id_* 是长度为 $n-ip-is$ 的位串,称 id 和 P 相匹配,记作 $id \in {}_*P$.

在 GWABE 方案中,用户是由一个元组 $(id, (\boldsymbol{A}, \rho))$来标识,$id$ 是一个长度为 n 的位串,表示用户的身份,$(\boldsymbol{A}, \rho)$是用户的访问结构. 用户的私钥与身份 id 和访问结构 $(\boldsymbol{A}, \rho)$相关,密文与身份模式 P 和属性集 ω 相关,当且仅当 $id \in {}_*P$ 且 ω 满足访问结构 $(\boldsymbol{A}, \rho)$时,用户 $(id, (\boldsymbol{A}, \rho))$才能解密密文.

3.1 GWABE 的定义和安全性模型

一个 GWABE 方案由 4 个算法组成:初始化(Setup),密钥生成(KeyGen),加密(Enc),解密(Dec).

$\text{Setup}(\lambda) \rightarrow PK, MSK$. 初始化算法输入系统安全参数 λ,输出系统公钥 PK 和主密钥 MSK.

$\text{KeyGen}(id, (\boldsymbol{A}, \rho), MSK) \rightarrow d_{id,(\boldsymbol{A},\rho)}$. 密钥生成算法输入用户的身份 id、访问结构 $(\boldsymbol{A}, \rho)$、主密钥 MSK,输出用户私钥 $d_{id,(\boldsymbol{A},\rho)}$.

$\text{Enc}(M, \omega, P, PK) \rightarrow CT$. 加密算法输入消息 M、属性集 ω、身份模式 P 和公钥 PK,输出密文 CT.

$\text{Dec}(d_{id,(\boldsymbol{A},\rho)}, CT) \rightarrow M$. 解密算法输入用户私钥 $d_{id,(\boldsymbol{A},\rho)}$ 和在 ω 和 P 下加密的密文 CT,仅当 $id \in {}_*P$ 且 ω 满足访问结构 $(\boldsymbol{A}, \rho)$时,用户 $(id, (\boldsymbol{A}, \rho))$才能解密密文,否则,解密失败.

正确性. 系统运行初始化算法生成 PK 和 MSK,对于所有消息 $M \in \{0,1\}^*$,$id \in \{0,1\}^n$,身份模式 P,当 ω 满足 $(\boldsymbol{A}, \rho)$且 $id \in {}_*P$ 时,$\text{Dec}(\text{KeyGen}(id, (\boldsymbol{A}, \rho), MSK), \text{Enc}(M, \omega, P, PK)) = M$ 的概率为 1.

下面,我们通过挑战者 $\mathcal{S}$ 和敌手 $\mathcal{A}$ 之间的交互性游戏定义 GWABE 的完全安全性.

(1)初始化. 挑战者 $\mathcal{S}$ 运行系统初始化算法,生成公钥 PK 和主密钥 MSK,并将 PK 发送给敌手 $\mathcal{A}$.

(2)阶段 1. 敌手 $\mathcal{A}$ 适应性地询问用户 $(id, (\boldsymbol{A}, \rho))$的私钥,挑战者生成私钥并其发送给敌手 $\mathcal{A}$,敌手可以重复多次询问私钥.

(3)挑战. 敌手 $\mathcal{A}$ 向挑战者 $\mathcal{S}$ 提交等长消息 M_0、M_1、挑战属性集 ω^* 和挑战身份模式 P^*,挑战者抛掷一枚公平硬币 $b \in \{0,1\}$,计算 $CT^* = \text{Enc}(M_b, \omega^*, P^*, PK)$,并将 CT^* 发送给敌手.

(4)阶段 2. 重复执行阶段 1.

(5)猜测. 敌手 $\mathcal{A}$ 输出对密文 CT^* 的一个猜测值 $b' \in \{0,1\}$.

若 $b' = b$,且敌手从未询问这类用户 $(id, (\boldsymbol{A}, \rho))$的私钥,其中 $id \in {}_*P^*$,且 ω^* 满足 $(\boldsymbol{A}, \rho)$,则称敌手赢得这个游戏. 敌手在上述游戏中获胜的优势定义为 $Adv_{\mathcal{A}} = |Pr[b' = b] - 1/2|$.

定义 4. 如果任意多项式时间敌手 $\mathcal{A}$ 赢得上述游戏的优势都是可以忽略的,则称这个 GWABE 方案是完全安全的.

3.2 GWABE 方案

我们首先解释本小节中所使用的标号. $j \in id$ 表示变量 j 取遍位串 id 中所有是 1 的位置,定义 Waters 散列函数为 $F(id) = u_0 \Pi_{j \in id} u_j$,其中,$u_j$ 是系统公钥 PK 中的元素. 对于一个模式 $P = P_{ip} \| * \| P_{is}$,定义 $F(P_{ip} \| * \| P_{is}) = F(P_{ip} \| 0 \cdots 0 \| P_{is})$,其中,0 的个数为 $n-ip-is$. 注意:如果已知所有的 u_j^t ($j = ip+1, \cdots, n-is$),则对任意长度为 $n-ip-is$ 的位串 id_*,我们可以使用 $F(id_{ip} \| * \| id_{is})^t$ 计算 $F(id_{ip} \| id_* \| id_{is})^t$,即

$$F(id_{ip} \| id_* \| id_{is})^t = F(id_{ip} \| * \| id_{is})^t \cdot \Pi_{j \in id_*} u_j^t.$$

利用上述特性,如果密文中包含与通配符相应的元素 u_j^t,解密者可以组合与自己身份相应的 u_j^t 进行解密.

令 G, G_T 是阶为 $N = p_1 p_2 p_3$ 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_{p_i} 是群 G 的阶为 p_i 的子群. $\mathcal{N}$ 为全体用户的集合，$|\mathcal{N}|$ 是 $\mathcal{N}$ 中的用户个数，$n = \log_2 |\mathcal{N}|$.

Setup(λ) $\to PK, MSK$. 可信授权机构输入安全参数 λ，随机选择 $\alpha \in Z_N, g, u_0, \cdots, u_n \in G_{p_1}$ 和 G_{p_3} 的生成元 X_3. 对每个属性 i，选择一个随机数 $s_i \in Z_N$，计算 $T_i = g^{s_i}\ \forall i$. 定义 Waters 散列函数 $F: \{0,1\}^n \to G_{p_1}^*$ 为 $F(id) = u_0 \prod_{j \in id} u_j$. 输出系统公钥 $PK = \{N, g, e(g,g)^\alpha, T_i\ \forall i, u_0, \cdots, u_n\}$，主密钥 $MSK = \{\alpha, X_3\}$.

KeyGen($MSK, id, (\boldsymbol{A}, \rho)$) $\to d_{id,(\boldsymbol{A},\rho)}$. 授权机构随机选择 $v_2, \cdots, v_h \in Z_N$，构成向量 $\boldsymbol{v} = (\alpha, v_2, \cdots, v_h)$. 对矩阵 $\boldsymbol{A}$ 的每个行向量 $\boldsymbol{A}_x$，随机选择 $r_x, r'_x \in Z_N, U_x, V_x, W_x \in G_{p_3}$，计算 $d_{id,(\boldsymbol{A},\rho)}$ 为

$$K_x^1 = g^{\boldsymbol{A}_x \cdot \boldsymbol{v}} T_{\rho(x)}^{r_x} F(id)^{r'_x} W_x,$$
$$K_x^2 = g^{r_x} V_x,\ K_x^3 = g^{r'_x} U_x.$$

Enc(M, ω, P, PK) $\to CT$. 加密算法输入消息 M、属性集合 ω、模式 $P = P_{ip} \| * \| P_{is}$ 和公钥 PK. 随机选择 $t \in Z_N$，计算密文 CT 如下：

$$C_1 = M \cdot e(g,g)^{\alpha t},\ C_2 = g^t,\ C_{3,i} = T_i^t\ \forall i \in \omega,$$
$$C_4 = (C_{4,ip,is} = F(P_{ip} \| 0 \cdots 0 \| P_{is})^t,$$
$$(C_{4,j} = u_j^t)_{j=ip+1,\cdots,n-is}).$$

其中，位串 $P_{ip} \| 0 \cdots 0 \| P_{is}$ 的长度为 n，0 的个数为 $n-ip-is$，即用 $n-ip-is$ 个 0 替代 P 中的通配符.

Dec($d_{id,(\boldsymbol{A},\rho)}, CT, PK$) $\to M$. 解密算法收到在 P 和 ω 下加密的密文 CT 时，如果 $id \in {}_*P$ 且 ω 满足 $(\boldsymbol{A}, \rho)$，首先计算：

$$C'_4 = F(id)^t = C_{4,ip,is} \prod_{j \in id, j=ip+1,\cdots,n-is} C_{4,j}.$$

然后，计算常量 c_x 使得 $\sum_{\rho(x) \in \omega} c_x \boldsymbol{A}_x = (1,0,\cdots,0)$，并计算

$$\prod_{\rho(x) \in \omega} \left[\frac{e(C_2, K_x^1)}{e(C_{3,\rho(x)}, K_x^2) e(C'_4, K_x^3)} \right]^{c_x}$$
$$= \prod_{\rho(x) \in \omega} \left[\frac{e(g^t, g^{\boldsymbol{A}_x \cdot \boldsymbol{v}}) e(g^t, T_{\rho(x)}^{r_x}) e(g^t, F(id)^{r'_x})}{e(C_{3,\rho(x)}, K_x^2) e(C'_4, K_x^3)} \right]^{c_x}$$
$$= e(g,g)^{t \sum_{\rho(x) \in \omega} c_x \boldsymbol{A}_x \cdot \boldsymbol{v}} = e(g,g)^{t\alpha},$$

最后，恢复消息 $M = C_1 / M e(g,g)^{t\alpha}$.

3.3　安全性证明

为了证明 GWABE 方案是完全安全的，我们需要首先定义半功能密文和半功能私钥. 令 $\boldsymbol{1} = (1,0,\cdots,0)$，$g_2$ 为子群 G_{p_2} 的生成元.

半功能密文. 加密算法首先计算消息 M 的正规密文，然后，选择随机数 $c \in Z_N$，对每个属性 $i \in \omega$，选择随机数 $z_i \in Z_N$，为矩阵 $\boldsymbol{A}$ 的每个行向量 $\boldsymbol{A}_x$，随机选择 $R_x, R'_x \in G_{p_2}$，计算半功能密文为

$$C_1 = M \cdot e(g,g)^{\alpha t},\ C_2 = g^t g_2^c,\ C_{3,i} = T_i^t g_2^{c z_i}\ \forall i \in \omega,$$
$$C_4 = (C_{4,ip,is} = F(P_{ip} \| 0 \cdots 0 \| P_{is})^t R_x,$$
$$(C_{4,j} = u_j^t R'_x)_{j=ip+1,\cdots,n-is}).$$

半功能私钥. 密钥生成算法首先为用户 $(id, (\boldsymbol{A}, \rho))$ 生成正规密钥，选择随机向量 $\boldsymbol{v}' \in Z_N^h$，随机数 $\gamma_x \in Z_N$，令 $\delta_x = \boldsymbol{A}_x \cdot \boldsymbol{v}'$，计算 I 型半功能私钥为

$$K_x^1 = g^{\boldsymbol{A}_x \cdot \boldsymbol{v}} T_{\rho(x)}^{r_x} F(id)^{r'_x} W_x g_2^{\delta_x + \gamma_x z_{\rho(x)}},$$
$$K_x^2 = g^{r_x} V_x g_2^{\gamma_x},\ K_x^3 = g^{r'_x} U_x.$$

II 型半功能私钥为

$$K_x^1 = g^{\boldsymbol{A}_x \cdot \boldsymbol{v}} T_{\rho(x)}^{r_x} F(id)^{r'_x} W_x g_2^{\delta_x},$$
$$K_x^2 = g^{r_x} V_x,\ K_x^3 = g^{r'_x} U_x.$$

注意：当密文的属性满足访问结构且用户身份匹配密文中的模式时，正规私钥可以解密半功能密文，半功能私钥也可以解密正规密文，但半功能私钥不能解密半功能密文，因为存在一个多余项

$$e(g_2, g_2)^{\sum_{\rho(x) \in \omega} c \cdot c_x \cdot \boldsymbol{A}_x \cdot \boldsymbol{v}'} = e(g_2, g_2)^{c \cdot \boldsymbol{v}' \cdot \boldsymbol{1}}.$$

若 $\boldsymbol{v}' \cdot \boldsymbol{1} = 0$ 且 $id \in {}_*P$，我们称 I 型半功能私钥为 I 型名义半功能私钥，注意：I 型名义半功能私钥可以解密相应的半功能密文.

该 GWABE 方案的安全性依赖于 2.3 节中给出的假设 1～3，我们利用混合争论技术，借助一系列相邻游戏（$\text{Game}_{\text{Real}}$, Game_0, $\text{Game}_{1,1}$, $\text{Game}_{1,2}$, …, $\text{Game}_{k-1,2}$, $\text{Game}_{k,1}$, $\text{Game}_{k,2}$, …, $\text{Game}_{q-1,2}$, $\text{Game}_{q,1}$, $\text{Game}_{q,2}$, $\text{Game}_{\text{Final}}$）的不可区分性证明该方案的安全性，其中，$q$ 是敌手询问密钥的最大次数.

$\text{Game}_{\text{Real}}$：一个真实的 GWABE 系统的安全性游戏，私钥和密文都是正规的.

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

$\text{Game}_{k,1}$：与 Game_0 类似，除了前 $k-1$ 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，剩余的私钥是正规的.

$\text{Game}_{k,2}$：与 Game_0 类似，除了前 k 次询问的私钥是 II 型半功能的，剩余的私钥是正规的.

$\text{Game}_{\text{Final}}$：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. 如果存在一个多项式时间（PPT）算法 $\mathcal{A}$（敌手）使得 $\text{Game}_{\text{Real}} Adv_{\mathcal{A}} - \text{Game}_0 Adv_{\mathcal{A}} = \varepsilon$，那么我们可以构造一个 PPT 算法 $\mathcal{S}$ 以 ε 的优势攻破假设 1.

证明.　挑战者 $\mathcal{S}$ 接收到假设 1 的条件 $\{g, X_3, T\}$，能够模拟 $\text{Game}_{\text{Real}}$ 或 Game_0. $\mathcal{S}$ 设置公共参数如下：随机选择 $\alpha, s_i \in Z_N\ (\forall i)$，向量 $\boldsymbol{\tau} = (\tau_y)_{y=0,\cdots,n} \in Z_N^{n+1}$，计算 $\boldsymbol{u} = (u_y = g^{\tau_y})_{y=0,\cdots,n}$，生成公钥 $PK = \{N, g, \boldsymbol{u}, e(g,g)^\alpha, T_i = g^{s_i}\ \forall i\}$ 并将其发送给敌手 $\mathcal{A}$，

保存主密钥 $MSK=\{\alpha,X_3\}$. 当 $\mathcal{A}$ 询问私钥时，$\mathcal{S}$ 利用 MSK 和密钥生成算法给 $\mathcal{A}$ 颁发正规私钥.

$\mathcal{S}$ 用属性集 ω 和身份模式 $P=P_{ip}\|*\|P_{is}$ 对消息 M_b 进行加密，令 T 的 G_{p_1} 部分为 g^t，生成挑战密文为

$$C_1=M_b\cdot e(g,T)^{\alpha},\ C_2=T,\ C_{3,i}=T^{s_i}\ \forall i\in\omega,$$

$$C_4=(C_{4,ip,is}=T^{\tau_0+\sum_{j\in P_{ip}\|P_{is}}\tau_j},(C_{4,j}=T^{\tau_j})_{j=ip+1,\cdots,n-is}).$$

注意：挑战密文隐式的设置 $z_i=s_i$，但是，由中国剩余定理可知，$s_i \bmod p_1$ 与 $z_i \bmod p_2$ 是无关的. 如果 $T=g^t\in G_{p_1}$，上述密文是一个均匀分布的正规密文；如果 $T=g^tX_2\in G_{p_1p_2}$，上述密文是一个均匀分布的半功能密文. 因此，$\mathcal{S}$ 可以根据 $\mathcal{A}$ 的输出以 ε 优势攻破假设 1.

引理 2. 如果存在一个 PPT 算法 $\mathcal{A}$（敌手）使得 $\mathrm{Game}_{k-1,2}\,Adv_{\mathcal{A}}-\mathrm{Game}_{k,1}\,Adv_{\mathcal{A}}=\varepsilon$，那么我们可以构造一个 PPT 算法 $\mathcal{S}$ 以几乎为 ε 的优势攻破假设 2.

证明. 挑战者 $\mathcal{S}$ 接收到假设 2 的条件 $\{g,X_3,g^tX_2,Y_2Y_3,T\}$，能够模拟 $\mathrm{Game}_{k-1,2}$ 或 $\mathrm{Game}_{k,1}$. $\mathcal{S}$ 设置公共参数如下：随机选择 $\alpha,s_i\in Z_N(\forall i)$，向量 $\boldsymbol{\tau}=(\tau_y)_{y=0,\cdots,n}\in Z_N^{n+1}$，计算 $\boldsymbol{u}=(u_y=g^{\tau_y})_{y=0,\cdots,n}$，生成公钥 $PK=\{N,g,\boldsymbol{u},e(g,g)^{\alpha},T_i=g^{s_i}\ \forall i\}$ 并发送给敌手 $\mathcal{A}$，保存主密钥 $MSK=\{\alpha,X_3\}$.

$\mathcal{S}$ 用属性集 ω 和身份模式 $P=P_{ip}\|*\|P_{is}$ 对明文 M_b 进行加密，生成挑战密文为

$$C_1=M_b\cdot e(g,g)^{\alpha t}=M_b\cdot e(g,g^tX_2)^{\alpha},$$

$$C_2=g^tX_2,\ C_{3,i}=(g^tX_2)^{s_i}\ \forall i\in\omega,$$

$$C_4=(C_{4,ip,is}=(g^tX_2)^{\tau_0+\sum_{j\in P_{ip}\|P_{is}}\tau_j},$$
$$(C_{4,j}=(g^tX_2)^{\tau_j})_{j=ip+1,\cdots,n-is}).$$

挑战密文隐式的设置 $z_i=s_i$，但是 $s_i \bmod p_1$ 与 $z_i \bmod p_2$ 是无关的. 下面，我们将私钥询问分为 3 部分.

(1) 当 $\mathcal{A}$ 询问私钥次数大于 k 时，$\mathcal{S}$ 利用 MSK 和私钥生成算法给 $\mathcal{A}$ 颁发相应的正规私钥.

(2) 当 $\mathcal{A}$ 询问私钥次数小于 k 时，$\mathcal{S}$ 选择随机向量 $\boldsymbol{v},\boldsymbol{v}_2'\in Z_N^h$，使得 $\boldsymbol{v}\cdot\boldsymbol{1}=\alpha$，随机选择 $r_x,r_x'\in Z_N$，$W_x,V_x,U_x\in G_{p_3}$，计算 II 型半功能私钥为

$$K_x^1=g^{\boldsymbol{A}_x\cdot\boldsymbol{v}}T_{\rho(x)}^{r_x}F(id)^{r_x'}W_x(Y_2Y_3)^{\boldsymbol{A}_x\cdot\boldsymbol{v}_2'},$$

$$K_x^2=g^{r_x}V_x,\ K_x^3=g^{r_x'}U_x.$$

注意：若 $Y_2=g_2^c$，则上述 II 型半功能私钥中的 $\boldsymbol{v}'=c\boldsymbol{v}_2'$.

(3) 当 $\mathcal{A}$ 进行第 k 次私钥询问时，$\mathcal{S}$ 选择随机向量 $\boldsymbol{u}',\boldsymbol{u}''\in Z_N^h$，使得 $\boldsymbol{u}'\cdot\boldsymbol{1}=0,\boldsymbol{u}''\cdot\boldsymbol{1}=\alpha$. 令 T 的 G_{p_1} 部分为 g^r，$\mathcal{S}$ 隐式的设置 $\boldsymbol{v}=r\boldsymbol{u}'+\boldsymbol{u}''$，随机选择 $\gamma_x,r_x'\in Z_N,W_x,V_x,U_x\in G_{p_3}$，计算

$$K_x^1=g^{\boldsymbol{A}_x\cdot\boldsymbol{u}''}T^{\boldsymbol{A}_x\cdot\boldsymbol{u}'}T^{\gamma_x\cdot s_{\rho(x)}}F(id)^{r_x'}W_x,$$

$$K_x^2=T^{\gamma_x}V_x,\ K_x^3=g^{r_x'}U_x.$$

注意：在这个私钥中，$r_x=r\cdot\gamma_x$，但是 $r_x \bmod p_1$ 与 $\gamma_x \bmod p_2$ 是无关的. 当 $T\in G_{p_1p_3}$，这个私钥是正规私钥；当 $T\in G$，这个私钥是 I 型半功能私钥，此时，若 $id\in_*P$，这个私钥是 I 型名义半功能私钥.

下面我们证明，当 $\mathcal{A}$ 的第 k 个询问私钥不能解密挑战密文时，$\mathcal{A}$ 无法区分第 k 个私钥是 I 型名义半功能私钥还是 I 型半功能私钥. 注意：在访问结构 $(\boldsymbol{A},\rho)$ 中，每个属性在 ρ 中至多出现一次. 当属性 $i\notin\omega$ 时，由于除了第 k 个以外的半功能私钥都是 II 型的，所以 z_i 仅可能在第 k 个私钥中出现. 由安全性模型可知，第 k 个询问私钥无法解密挑战密文，所以当 $id\in_*P$，$\boldsymbol{A}$ 中 $\rho(x)\in\omega$ 的所有行 x 生成的行空间 $\boldsymbol{R}$ 不包含 $\boldsymbol{1}$. 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 $\boldsymbol{1}$，即 $\boldsymbol{1}\cdot\boldsymbol{w}\neq0$. 我们固定一个包含 $\boldsymbol{w}$ 的基，则存在 $f\in Z_N$，使得 $\boldsymbol{u}'=f\boldsymbol{w}+\boldsymbol{u}_1' \bmod p_2$，其中 $\boldsymbol{u}_1'$ 属于除 $\boldsymbol{w}$ 外的基向量扩张的空间中，注意到 $\boldsymbol{u}_1'$ 是均匀分布的，且无法揭露 f 的任何信息. 由于 $\boldsymbol{u}'\cdot\boldsymbol{1}=f\cdot\boldsymbol{1}\cdot\boldsymbol{w}+\boldsymbol{1}\cdot\boldsymbol{u}_1'$，且 $\boldsymbol{1}\cdot\boldsymbol{w}\neq0$，所以 $\boldsymbol{u}'\cdot\boldsymbol{1}$ 与 f 相关.

当 $\rho(x)\in\omega$ 时，$\boldsymbol{A}_x\cdot\boldsymbol{u}'=\boldsymbol{A}_x\cdot(f\cdot\boldsymbol{w}+\boldsymbol{u}_1')=\boldsymbol{A}_x\cdot\boldsymbol{u}_1'$，与 f 无关. 当 $\rho(x)\notin\omega$ 时，$f\cdot\boldsymbol{w}$ 仅出现在 $\boldsymbol{A}_x\cdot\boldsymbol{u}'+\gamma_xz_{\rho(x)}$ 中，当 $\gamma_x\neq0 \bmod p_2$ 时，每项 $\boldsymbol{A}_x\cdot\boldsymbol{u}'+\gamma_xz_{\rho(x)}$ 都引入一个新的未知量 $z_{\rho(x)}$，且 $z_{\rho(x)}$ 不出现在其它项中，因此，$\mathcal{A}$ 无法从这些项中得知 f 的任何信息. 准确地说，无论 $\boldsymbol{u}'$ 的第一个分量为何值，上述方程都有相同个数的解，因此，当所有的 $\gamma_x \bmod p_2$ 都不为 0 时，在 $\mathcal{A}$ 看来，挑战密文和第 k 个私钥以几乎为 1 的概率均匀分布.

因此，当 $T\in G_{p_1p_3}$，$\mathcal{S}$ 完美仿真 $\mathrm{Game}_{k-1,2}$；当 $T\in G$；$\mathcal{S}$ 以几乎为 1 的概率完美仿真 $\mathrm{Game}_{k,1}$，所以，$\mathcal{S}$ 可以根据 $\mathcal{A}$ 的输出以几乎为 ε 的概率攻破假设 2.

引理 3. 如果存在一个 PPT 算法 $\mathcal{A}$ 使得 $\mathrm{Game}_{k,1}\,Adv_{\mathcal{A}}-\mathrm{Game}_{k,2}\,Adv_{\mathcal{A}}=\varepsilon$，那么我们可以构造一个 PPT 算法 $\mathcal{S}$ 以 ε 的优势攻破假设 2.

证明. 挑战者 $\mathcal{S}$ 接收到假设 2 的条件 $\{g,X_3,g^tX_2,Y_2Y_3,T\}$，能够模拟 $\mathrm{Game}_{k,1}$ 或 $\mathrm{Game}_{k,2}$. $\mathcal{S}$ 设置公共参数如下：随机选择 $\alpha,s_i\in Z_N(\forall i)$，向量 $\boldsymbol{\tau}=(\tau_y)_{y=0,\cdots,n}\in Z_N^{n+1}$，计算 $\boldsymbol{u}=(u_y=g^{\tau_y})_{y=0,\cdots,n}$，生成公钥 $PK=\{N,g,\boldsymbol{u},e(g,g)^{\alpha},T_i=g^{s_i}\ \forall i\}$ 并将其发送给敌手 $\mathcal{A}$，保存主密钥 $MSK=\{\alpha,X_3\}$.

挑战密文、前 $k-1$ 个 II 型半功能私钥和询问次数大于 k 的所有正规私钥的构造方法与引理 2 相同. 当 $\mathcal{A}$ 进行第 k 次私钥询问时，$\mathcal{S}$ 选择随机向量 $\boldsymbol{v}$，

$\boldsymbol{v}'\in Z_N^h$，使得 $\boldsymbol{v}\cdot\mathbf{1}=\alpha$. 随机选择 $\gamma_x, r_x'\in Z_N, U_x, V_x, W_x\in G_{p_3}$，计算

$$K_x^1=g^{\boldsymbol{A}_x\cdot\boldsymbol{v}}T^{\gamma_x s_{\rho(x)}}F(id)^{r_x'}W_x(Y_2Y_3)^{\boldsymbol{A}_x\cdot\boldsymbol{v}'},$$

$$K_x^2=T^{\gamma_x}V_x,\ K_x^3=g^{r_x'}U_x.$$

注意：若 T 的 G_{p_1} 部分为 g^r，则 $r_x=r\cdot\gamma_x$. 如果 $T\in G$，则这个私钥是均匀分布的 I 型半功能私钥；如果 $T\in G_{p_1p_3}$，则这个私钥是均匀分布的 II 型半功能私钥.

因此，$\mathcal{S}$将根据$\mathcal{A}$的输出以 ε 的概率攻破假设 2.

引理 4.　如果存在一个 PPT 算法$\mathcal{A}$使得 $\mathrm{Game}_{q,2}Adv_{\mathcal{A}}-\mathrm{Game}_{\mathrm{Final}}Adv_{\mathcal{A}}=\varepsilon$，那么我们可以构造一个 PPT 算法$\mathcal{S}$以 ε 的优势攻破假设 3.

证明.　挑战者$\mathcal{S}$接收到假设 3 的条件$\{g, X_3, g^{\alpha}X_2, g^{t}Y_2, Z_2, T\}$，能够模拟 $\mathrm{Game}_{q,2}$ 或 $\mathrm{Game}_{\mathrm{Final}}$. $\mathcal{S}$设置公共参数如下：随机选择 $s_i\in Z_N(\forall i)$，向量 $\boldsymbol{\tau}=(\tau_y)_{y=0,\cdots,n}\in Z_N^{n+1}$，计算 $\boldsymbol{u}=(u_y=g^{\tau_y})_{y=0,\cdots,n}$，生成公钥 $PK=\{N, g, \boldsymbol{u}, e(g,g^{\alpha}X_2), T_i=g^{s_i}\ \forall i\}$并将其发送给敌手$\mathcal{A}$，注意：$\mathcal{S}$不知道主密钥中的 α.

$\mathcal{S}$用属性集 ω 和身份模式 $P=P_{ip}\|*\|P_{is}$ 生成挑战密文为

$$C_1=M_bT, C_2=g^tX_2,\ C_{3,i}=(g^tX_2)^{s_i}\ \forall i\in\omega,$$

$$C_4=((g^tX_2)^{\tau_0+\sum_{j\in P_{ip}\|P_{is}}\tau_j}, ((g^tX_2)^{\tau_j})_{j=ip+1,\cdots,n-is}).$$

如果 $T=e(g,g)^{\alpha t}$，上述密文为 M_b的半功能密文，如果 T 是 G_T中的随机元素，上述密文为随机消息的半功能密文，此时$\mathcal{A}$无法获知 b 的任何信息.

为了给用户$(id,(\boldsymbol{A},\rho))$生成 II 型半功能私钥，$\mathcal{S}$隐式的选择向量 $\boldsymbol{v}=(\alpha, v_2, \cdots, v_h)$，其中，$v_2, \cdots, v_h\xleftarrow{R}Z_N$，然后，随机选择向量 $\boldsymbol{v}'\in Z_N^h, U_x, V_x, W_x\in G_{p_3}, r_x, r_x'\in Z_N$，计算

$$K_x^1=(g^{\alpha}X_2)^{\boldsymbol{A}_{x,1}}g^{\sum_{i=2}^{h}\boldsymbol{A}_{x,i}\cdot v_i}g^{s_{\rho(x)}r_x}Z_2^{\boldsymbol{A}_x\cdot\boldsymbol{v}'}F(id)^{r_x'}W_x,$$

$$K_x^2=g^{r_x}V_x,\ K_x^3=g^{r_x'}U_x.$$

注意：若 $X_2=g_2^c, Z_2=g_2^d$，K_x^1的 G_{p_2} 部分是 $g_2^{\delta_x}$，则 $\delta_x=\boldsymbol{A}_x\cdot\boldsymbol{v}_2'$，其中 $\boldsymbol{v}_2'=d\boldsymbol{v}'+(c,0,\cdots,0)$，从而可得上述 II 型半功能私钥是均匀分布的. 综上所述，$\mathcal{S}$可以根据$\mathcal{A}$的输出以 ε 的概率攻破假设 3.

定理 1.　如果假设 1～3 均成立，则该 GWABE 方案是完全安全的.

证明.　根据上述 4 个引理可知，如果假设 1～3 成立，则真实游戏 $\mathrm{Game}_{\mathrm{Real}}$ 和 $\mathrm{Game}_{\mathrm{Final}}$ 是不可区分的，又因为在信息论意义上 $\mathrm{Game}_{\mathrm{Final}}$ 中的 b 对敌手是隐藏的，所以敌手在 $\mathrm{Game}_{\mathrm{Final}}$ 中的优势为 0，从而可得敌手在真实游戏中的优势是可忽略的.　证毕.

4　可追踪并撤销叛徒的 ABE 方案(ABTR)

本节利用完全子树构架将第 3 节的 GWABE 转化成 ABTR 方案. 在该 ABTR 方案中，令$\mathcal{N}$表示所有用户的集合，$|\mathcal{N}|$是$\mathcal{N}$中用户的个数，$n=\log_2^{|\mathcal{N}|}$，$\mathcal{R}$为撤销用户的集合. 我们首先构造一棵深度为 n 的完全二叉树，在该树的每一层上，左分支对应 0，右分支对应 1. 与 GWABE 方案相同，每个用户由一个元组$(id,(\boldsymbol{A},\rho))$来标识，用户的身份 $id\in\{0,1\}^n$ 被指定到二叉树的一个叶子节点. 如果用 GWABE 在节点 S 和属性集 ω 下加密消息，我们将用通配符来替代 S 以下的层次，当密文中的属性满足用户的访问结构，且该用户为以 S 为根节点的子树中的用户时才能解密密文. 如图 1 所示，叶子节点对应用户，$S_{i1}, \cdots, S_{i4}$是未撤销用户的一个覆盖，使用 GWABE 在属性集 ω 和子集 $S_{ij}(1\le j\le 4)$的身份模式下对 K 进行加密，以 S_4 为例，我们用 GWABE.Enc$(K,\omega,$"11$*$",$PK)$加密 K. ABTR 对消息 M 的加密生成的密文为$\{\omega,[i_1,i_2,i_3,i_4,$ GWABE.Enc$(K,\omega,$"00$*$",$PK)$,$\cdots$,GWABE.Enc$(K,\omega,$"11$*$",$PK)$],$E_K(M)\}$，其中，K 为会话密钥，E 为对称加密算法.

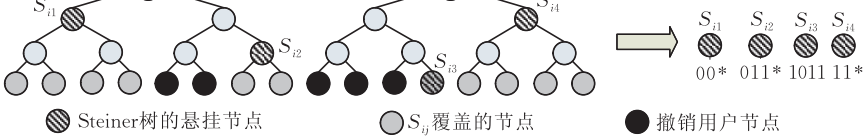

图 1　基于完全子树构架和 GWABE 的 ABTR 方案

ABTR 的目标是追踪所有叛徒的身份，并将其从系统中撤销，使得盗版解密设备无效，即允许任何用户在 ω 和$\mathcal{R}$下加密消息，使得用户是未撤销用户，且密文中 ω 满足该用户的访问结构，才能解密密文. 同时，$\mathcal{R}$中的所有用户联合起来也无法解密密文.

4.1　ABTR 的定义和安全性模型

一个 ABTR 方案由 5 个算法构成：初始化(Setup)，密钥生成(KeyGen)，加密(Enc)，解密(Dec)，叛徒追踪(Trace).

Setup(λ)$\rightarrow PK, MSK$. 初始化算法输入系统安全参数λ,输出系统公钥PK和主密钥MSK.

KeyGen($id,(\boldsymbol{A},\rho),MSK$)$\rightarrow d_{id,(\boldsymbol{A},\rho)}$. 密钥生成算法输入用户的身份$id$、访问结构$(\boldsymbol{A},\rho)$、主密钥$MSK$,输出用户私钥$d_{id,(\boldsymbol{A},\rho)}$.

Enc($M,\omega,\mathcal{R},PK$)$\rightarrow CT$. 加密算法输入消息M、属性集ω、撤销列表$\mathcal{R}$和公钥PK,输出密文CT.

Dec($d_{id,(\boldsymbol{A},\rho)},CT$)$\rightarrow M$. 解密算法输入密钥$d_{id,(\boldsymbol{A},\rho)}$和密文$CT$,仅当用户的身份$id\in\mathcal{N}\backslash\mathcal{R}$且密文中的$\omega$满足用户的访问结构$(\boldsymbol{A},\rho)$时,输出消息$M$,否则,解密失败.

Trace$^{\mathbb{D}}$($MSK,\omega,\mathcal{R}$). 叛徒追踪算法输入主密钥MSK、属性集合ω、撤销列表$\mathcal{R}$、盗版解码器$\mathbb{D}$,输出用户身份的集合(称此类用户为"叛徒").

正确性. 系统运行初始化算法生成PK和MSK,对于所有消息$M\in\{0,1\}^*$,$id\in\{0,1\}^n$,撤销列表$\mathcal{R}$,属性集ω,当ω满足$(\boldsymbol{A},\rho)$且$id\in\mathcal{N}\backslash\mathcal{R}$时,Dec(KeyGen($id,(\boldsymbol{A},\rho),MSK$),Enc($M,\omega,\mathcal{R},PK$))$=M$的概率为1.

注意:本文的叛徒追踪算法基于子集追踪过程,用户只能用叶子节点的私钥解密密文,而叶子节点的私钥直接暴露用户的身份,因此,叛徒追踪算法可以追查到所有叛徒.该算法还要求所有盗版解密设备可以重置,即在两次解密之间不保留状态信息,特别的,盗版设备不能自毁.

ABTR的完全安全模型通过挑战者$\mathcal{S}$和敌手$\mathcal{A}$之间的攻击性游戏来定义.

(1)初始化. 挑战者$\mathcal{S}$运行Setup算法,生成系统公钥PK和主密钥MSK,并将PK发送给敌手$\mathcal{A}$.

(2)阶段1. 敌手向挑战者询问任意用户(id,$(\boldsymbol{A},\rho)$)的私钥,挑战者运行密钥生成算法,将$d_{id,(\boldsymbol{A},\rho)}$返回给敌手,并将$id$添加到撤销列表$\mathcal{R}$($\mathcal{R}$初始化为空).

(3)挑战. 敌手提交等长消息M_0,M_1和挑战属性集ω^*.挑战者随机选取一个比特$b\in\{0,1\}$,利用ω^*和$\mathcal{R}$对M_b加密,生成挑战密文CT^*,并将CT^*发送给敌手.

(4)阶段2. 重复执行阶段1,但敌手不能询问这类用户($id,(\boldsymbol{A},\rho)$)的私钥,其中ω^*满足$(\boldsymbol{A},\rho)$且$id\in\mathcal{N}\backslash\mathcal{R}$.

(5)猜测. 敌手输出一个猜测值$b'\in\{0,1\}$.

若$b'=b$,则称敌手$\mathcal{A}$赢得这个游戏.敌手$\mathcal{A}$在上述游戏中的优势$Adv_{\mathcal{A},\mathrm{ABTR}}$定义为$|Pr[b'=b]-1/2|$.如果任意多项式时间敌手$\mathcal{A}$赢得上述游戏的优势都是可以忽略的,则称ABTR方案是完全安全的.

4.2 ABTR方案

Setup(λ)$\rightarrow PK, MSK$. 可信授权机构执行初始化算法,选择一个阶为$N=p_1p_2p_3$(3个互不相同的素数)的双线性群G.令G_{p_i}表示群G的p_i阶子群.该算法随机选择$\alpha\in Z_N, g, u_0,\cdots,u_n\in G_{p_1}, G_{p_3}$的生成元$X_3$.对每个属性$i$,选择一个随机数$s_i\in Z_N$,计算$T_i=g^{s_i}$.定义Waters散列函数$F:\{0,1\}^n\rightarrow G_{p_1}^*$为$F(id)=u_0\prod_{y\in id}u_y$.输出系统公钥$PK=\{N,g,e(g,g)^\alpha,T_i\ \forall i,u_0,\cdots,u_n\}$,主密钥$MSK=\{\alpha,X_3\}$.此外,初始化算法还定义了一个对称加密方案$(E_K,D_K)$来加密消息.

KeyGen(MSK,$id,(\boldsymbol{A},\rho)$)$\rightarrow d_{id,(\boldsymbol{A},\rho)}$. 授权机构随机选择$v_2,\cdots,v_h\in Z_N$,构成向量$\boldsymbol{v}=(\alpha,v_2,\cdots,v_h)$.对$\boldsymbol{A}$的每一行$\boldsymbol{A}_x$,随机选择$r_x,r'_x\in Z_N$,$U_x$,$V_x,W_x\in G_{p_3}$,计算$d_{id,(\boldsymbol{A},\rho)}$为

$$K_x^1=g^{\boldsymbol{A}_x\cdot\boldsymbol{v}}T_{\rho(x)}^{r_x}F(id)^{r'_x}W_x,$$

$$K_x^2=g^{r_x}V_x,\ K_x^3=g^{r'_x}U_x.$$

Enc($M,\omega,\mathcal{R},PK$)$\rightarrow CT$. 加密算法输入消息M,属性集ω,用户撤销列表$\mathcal{R}$和公钥PK.该算法运行完全子树构架,将未撤销用户$\mathcal{N}\backslash\mathcal{R}$划分成不相交子集$S_{i1},\cdots,S_{im}$,每个子集$S_{ij}$($1\leq j\leq m$)对应一个身份模式$P_{ij}=id_{ij}\|*$,其中$id_{ij}=id_{ij,1}\,id_{ij,2}\cdots id_{ij,ip}$是从根节点到节点$S_{ij}$的道路,$id_{ij}$的长度是$ip$.然后,加密算法随机选择一个会话密钥$K$,用GWABE在每个子集的身份模式$P_{ij}$和$\omega$下对$K$进行$m$次加密.最后,利用会话密钥$K$对消息$M$进行对称加密,即$E_K(M)$.

下面,我们详细介绍如何用GWABE在模式P_{ij}($1\leq j\leq m$)和ω下对K进行加密.GWABE的加密算法选择一个随机数$t\in Z_N$,计算$C^j=(P_{ij},C_1^j,C_2^j,C_{3,i}^j,C_4^j)$如下:

$$C_1^j=Ke(g,g)^{\alpha t},\ C_2^j=g^t,\ C_{3,i}^j=T_i^t\ \forall i\in\omega,$$

$$C_4^j=(C_{4,ip,n}^j=F(id_{ij}\|0\cdots0)^t,(C_{4,z}^j=u_z^t)_{z=ip+1,\cdots,n}),$$

输出密文$CT=\{\omega,[i_1,\cdots,i_m,C^1,\cdots,C^m],E_K(M)\}$.

Decrypt($d_{id,(\boldsymbol{A},\rho)},CT,PK$)$\rightarrow M$. 用户($id,(\boldsymbol{A},\rho)$)收到用$\omega$和$\mathcal{R}$加密的密文$CT$,如果$\omega$满足$(\boldsymbol{A},\rho)$且$id\in\mathcal{N}\backslash\mathcal{R}$,用户首先找到$j$使得$id\in{}_*P_{ij}$,并计算常量$c_x$使得$\sum_{\rho(x)\in\omega}c_x\boldsymbol{A}_x=(1,0,\cdots,0)$.然后,用私钥$d_{id,(\boldsymbol{A},\rho)}$解密$C^j$得到$K$.最后,计算$D_K(E_K(M))$得到消息$M$.

下面,我们解释如何解密C^j得到K,计算

$$C_4'^j=F(id)^t=C_{4,ip,n}^j\Pi_{z\in id,z=ip+1,\cdots,n}C_{4,z}^j,$$

$$C_1^j\prod_{\rho(x)\in\omega}\left(\frac{e(C_{3,\rho(x)}^j,K_x^2)e(C_4'^j,K_x^3)}{e(C_2^j,K_x^1)}\right)^{c_x}=K.$$

$\mathrm{Trace}^{\mathbb{D}}(MSK,\omega,\mathcal{R})$. 可信授权机构执行叛徒追踪算法，该算法得到一个盗版解码器$\mathbb{D}$，它能以大于门限值q的概率p解密在ω和$\mathcal{R}$下加密的密文. 当$\mathbb{D}$中包含t个叛徒的密钥，追踪算法执行以下子集追踪过程$t\log_2|\mathcal{N}|$次，追查到所有叛徒的确切身份，并将其添加到撤销列表$\mathcal{R}$.

(1) 追踪算法用撤销列表$\mathcal{R}$生成一个划分$\mathcal{N}\backslash\mathcal{R}=S_{i1}\cup\cdots\cup S_{im}$，令$p_j(0\leq j\leq m)$表示$\mathbb{D}$正确解密追踪密文

$$\{\omega,[i_1,i_2,\cdots,i_m,\mathrm{GWABE.Enc}(R_K,\omega,P_{i1},PK),\cdots,\mathrm{GWABE.Enc}(R_K,\omega,P_{ij},PK),\mathrm{GWABE.Enc}(K,\omega,P_{i(j+1)},PK),\cdots,\mathrm{GWABE.Enc}(K,\omega,P_{im},PK)],E_K(M)\}$$

的概率，其中R_K是一个与会话密钥K等长的随机位串，注意：$p_0=p$，$p_m=0$.

(2) 追踪算法对当前划分使用子集追踪过程，子集追踪过程使用类似二分查找法找到索引j使得$|p_{j-1}-p_j|\geq p/m$. 初始搜索区间为$[0,m]$，子集追踪过程递归地执行搜索过程将区间缩短到$[a,b]$. 在每次递归执行时，计算中值$c=\lceil(a+b)/2\rceil$和p_c，如果$|p_c-p_a|\geq|p_b-p_c|$，将搜索区间折半到$[a,c]$，否则，区间折半到$[c,b]$. 经过$\lceil\log_2 m\rceil$次递归执行，当$a=b-1$时，子集追踪过程结束并将b返回给索引j，输出叛徒所在子集S_{ij}[18].

(3) 如果S_{ij}中用户个数大于1，将S_{ij}分割为2个大小相同的子集$S_{ij,1}$，$S_{ij,2}$，得到一个新的划分$S_{i1},\cdots,S_{i(j-1)},S_{ij,1},S_{ij,2},S_{i(j+1)},\cdots,S_{im}$，追踪算法对新的划分继续使用二分查找法搜索包含叛徒的子集. 如果S_{ij}中仅包含一个用户，该用户一定是叛徒并将其撤销，得到一个新的撤销列表，则当前划分为$S_{i1},\cdots,S_{i(j-1)},S_{i(j+1)},\cdots,S_{im}$. 此时，追踪算法在该划分下检测解码器$\mathbb{D}$解密密文的概率$p$，当$p$大于门限值$q$时，追踪算法对此划分继续使用二分查找法搜索包含叛徒的子集. 否则，追踪算法结束，并输出所有叛徒.

4.3 安全性证明

该ABTR的安全性依赖于GWABE的安全性. 我们利用混合争论技术，借助一系列相邻游戏$(\mathrm{TRGame}^0,\mathrm{TRGame}^1,\cdots,\mathrm{TRGame}^m)$的不可区分性证明ABTR的安全性，其中，$m$是$\mathcal{N}\backslash\mathcal{R}$的划分中子集的个数.

TRGame^0：是真实ABTR的安全性游戏. $\mathcal{A}$接收到PK后，询问用户$(id,(\boldsymbol{A},\rho))$的私钥，挑战者$\mathcal{S}$使用密钥生成算法$\mathrm{ABTR.KeyGen}(MSK,id,(\boldsymbol{A},\rho))$生成私钥$d_{id,(\boldsymbol{A},\rho)}$，并将其发送给$\mathcal{A}$，$\mathcal{S}$将$id$添加到$\mathcal{R}$中. $\mathcal{A}$提交等长的消息M_0、M_1和挑战属性集ω^*，$\mathcal{S}$随机选择$b\in\{0,1\}$，计算挑战密文$CT^*=\mathrm{ABTR.Enc}(M_b,\omega,\mathcal{R},MSK)$，并将其发送给$\mathcal{A}$. $\mathcal{A}$输出猜测值$b'\in\{0,1\}$，如果$b=b'$，称$\mathcal{A}$赢得这个游戏. 定义$\mathcal{A}$赢得这个游戏的优势$\mathrm{TRGame}^0 Adv_{\mathcal{A}}$为

$$|Pr[\mathcal{A}(\mathrm{ABTR.Enc}(M_1,\omega,\mathcal{R},MSK))=1]-Pr[\mathcal{A}(\mathrm{ABTR.Enc}(M_0,\omega,\mathcal{R},MSK))=1]|.$$

如果这个优势是不可忽略的，我们称$\mathcal{A}$可以攻破ABTR的完全安全性.

我们构造ABTR的密文如下：

$$\mathrm{ABTR.Enc}(M,\omega,\mathcal{R},MSK)=(\mathrm{GWABE.Enc}(M,\omega,P_{i1},PK),\cdots,\mathrm{GWABE.Enc}(M,\omega,P_{im},PK)),$$

其中，$\mathcal{N}\backslash\mathcal{R}$被划分成$m$个子集$S_{i1},\cdots,S_{im}$，每个子集$S_{ij}$对应身份模式$P_{ij}$.

在后面的游戏中，我们逐步修改挑战密文，定义修改后的加密算法$\mathrm{ABTR.Enc}^k$为

$$\mathrm{ABTR.Enc}^k(M,\omega,\mathcal{R},MSK)=(\mathrm{GWABE.Enc}(M_0,\omega,P_{i1},\mathrm{PK}),\cdots,\mathrm{GWABE.Enc}(M_0,\omega,P_{ik},PK),\mathrm{GWABE.Enc}(M,\omega,P_{i(k+1)},PK),\cdots,\mathrm{GWABE.Enc}(M,\omega,P_{im},PK)).$$

注意：

$\mathrm{ABTR.Enc}^0(\cdot)=\mathrm{ABTR.Enc}(\cdot)$，

$\mathrm{ABTR.Enc}^k(M_0,\omega,\mathcal{R},PK)=\mathrm{ABTR.Enc}(M_0,\omega,\mathcal{R},PK)$，$0\leq k\leq m$，

$\mathrm{ABTR.Enc}^m(M,\omega,\mathcal{R},PK)=\mathrm{ABTR.Enc}(M_0,\omega,\mathcal{R},PK)$，其中$M$为任意消息.

$\mathrm{TRGame}^k(k=1,2,\cdots,m)$：与$\mathrm{TRGame}^{k-1}$相同，除了挑战者用$\mathrm{ABTR.Enc}^k(\cdot)$替代$\mathrm{ABTR.Enc}^{k-1}(\cdot)$. 我们用$\mathrm{TRGame}^k Adv_{\mathcal{A}}$表示敌手$\mathcal{A}$在$\mathrm{TRGame}^k$中的优势. 注意：在最后一个游戏$\mathrm{TRGame}^m$中，挑战密文总是对消息$M_0$的加密，因此，$\mathcal{A}$在该游戏中的优势为0.

引理5. 如果存在一个PPT算法$\mathcal{A}$使得$\mathrm{TRGame}^k Adv_{\mathcal{A}}-\mathrm{TRGame}^{k-1} Adv_{\mathcal{A}}=\varepsilon$，那么我们可以构造一个PPT算法$\mathcal{A}'$以$\varepsilon$的优势攻破GWABE安全性.

证明. $\mathcal{A}'$的挑战者运行GWABE的初始化算法，生成PK,MSK，并将PK发送给$\mathcal{A}'$，$\mathcal{A}'$收到GWABE的公钥PK，能够模拟TRGame^k或TRGame^{k-1}. 由于GWABE和ABTR具有相同的公钥，$\mathcal{A}'$将PK作为ABTR的公钥发送给$\mathcal{A}$.

当$\mathcal{A}$询问用户$(id,(\boldsymbol{A},\rho))$的私钥时，$\mathcal{A}'$向其挑战者询问$(id,(\boldsymbol{A},\rho))$的私钥，$\mathcal{A}'$得到$d_{id,(\boldsymbol{A},\rho)}$并将其

发送给$\mathcal{A}$.由于GWABE方案和ABTR方案的密钥生成算法是相同的,所以$\mathcal{A}'$可以确保给$\mathcal{A}$的私钥是正确的.当敌手$\mathcal{A}$询问用户$(id,(\boldsymbol{A},\rho))$的私钥后,$\mathcal{A}'$将$id$添加到撤销列表$\mathcal{R}$中($\mathcal{R}$初始为空集).

$\mathcal{A}'$将$\mathcal{N}\backslash\mathcal{R}$划分成$S_{i1},S_{i2},\cdots,S_{im}$,提交等长消息$M_0$、$M_1$、模式$P_{ik}$和挑战属性集$\omega^*$给其挑战者,该挑战者生成GWABE的挑战密文$CT_b=$GWABE.Enc$(M_b,\omega^*,P_{ik},PK)$并将其发送给$\mathcal{A}'$.$\mathcal{A}'$计算ABTR的挑战密文

$$\begin{aligned}CT^*=(&\text{GWABE.Enc}(M_0,\omega^*,P_{i1},PK),\cdots,\\&\text{GWABE.Enc}(M_0,\omega^*,P_{i(k-1)},PK),CT_b,\\&\text{GWABE.Enc}(M_1,\omega^*,P_{i(k+1)},PK),\cdots,\\&\text{GWABE.Enc}(M_1,\omega^*,P_{im},PK)),\end{aligned}$$

并将其发送给$\mathcal{A}$.

$\mathcal{A}$接收到CT^*后,可以继续询问用户的私钥,注意:$\mathcal{A}$此时不能询问这类用户$(id,(\boldsymbol{A},\rho))$的私钥,其中,$\omega^*$满足$(\boldsymbol{A},\rho)$且$id\in\mathcal{N}\backslash\mathcal{R}$.

当$\mathcal{A}$输出它的猜测值后,$\mathcal{A}'$将输出相应的猜测值.由ABTR挑战密文的构造可知,当$b=0$,$\mathcal{A}'$模拟的游戏是TRGame^k;当$b=1$,$\mathcal{A}'$模拟的游戏是TRGame^{k-1}.因此,$\mathcal{A}'$能够以ε的优势攻破GWABE的安全性.

定理2. 如果GWABE是完全安全的,则ABTR是完全安全的.

证明. 由引理5可知,如果GWABE是IND-CPA安全的,则相邻游戏TRGame^k和TRGame^{k-1}($k=1,2,\cdots,m$)是不可区分的.因此,TRGame^0和TRGame^m是不可区分的,由于敌手$\mathcal{A}$在TRGame^m中的优势为0,所以,敌手$\mathcal{A}$在TRGame^0中的优势是可以忽略的,即定理2成立. 证毕.

4.4 性能比较

表1将本文ABTR方案和相关方案在效率和安全模型方面进行了详细比较,其中ABTT[10]方案需要在系统初始化前设置叛徒的最大个数c,且追踪算法出错的概率为ε.r表示撤销用户的个数,$|\mathcal{N}|$表示全体用户的个数.

表1 本文ABTR方案与相关方案的性能对比

方案	私钥长度	公钥长度	密文长度	加密时间	解密时间	安全模型
NNL[18]	$O(\log\|\mathcal{N}\|)$	0	$O(r\log(\|\mathcal{N}\|/r))$	$O(r\log(\|\mathcal{N}\|/r))$	$O(1)$	完全安全
IDTR[19]	$O(1)$	$O(\log\|\mathcal{N}\|)$	$O(r\log(\|\mathcal{N}\|/r)\cdot\log\|\mathcal{N}\|)$	$O(r\log(\|\mathcal{N}\|/r)\cdot\log\|\mathcal{N}\|)$	$O(\log\|\mathcal{N}\|)$	完全安全
ABTT[10]	$O(1)$	$O(c^2\log(\|\mathcal{N}\|/r)+\log(1/\varepsilon))$	$O(c^2\log(\|\mathcal{N}\|/r)+\log(1/\varepsilon))$	$O(c^2\log(\|\mathcal{N}\|/r)+\log(1/\varepsilon))$	$O(\log\|\mathcal{N}\|)$	选择安全
本文的ABTR	$O(1)$	$O(\log\|\mathcal{N}\|)$	$O(r\log(\|\mathcal{N}\|/r)\cdot\log\|\mathcal{N}\|)$	$O(r\log(\|\mathcal{N}\|/r)\cdot\log\|\mathcal{N}\|)$	$O(\log\|\mathcal{N}\|)$	完全安全

与ABTT方案[10]相比,本文的ABTR方案同时支持叛徒的追踪和撤销,且当叛徒个数较大时,该ABTR方案的效率高于ABTT方案.与NNL[18]和IDTR[19]方案相比,该ABTR方案支持加密数据的细粒度访问控制,且用户的私钥长度是固定的.

5 结 论

本文首先提出一个具有扩展通配符的ABE方案(GWABE),然后,将GWABE和完全子树构架[18]相结合,提出一个可追踪并撤销叛徒的属性基加密方案(ABTR),并证明该ABTR方案是完全安全的,且用户私钥长度是固定的.本文的主要贡献有3个方面:

(1)该ABTR方案同时支持属性基加密系统的叛徒追踪和用户撤销两种功能.

(2)该ABTR方案能够在标准模型下证明其完全安全性,而此前可追踪叛徒的ABE方案仅满足选择安全性.

(3)我们提出了一个GWABE方案,并证明其完全安全性.GWABE可以用来设计可撤销的ABE方案,可能具有独立的学术价值.

本文基于完全子树构架采用撤销列表的方法撤销用户.事实上,还存在其它的撤销方法,例如周期性更新用户私钥[13]和引入半可信的仲裁者[20]等撤销方法,如何将这些撤销方法和叛徒追踪算法有机结合起来,生成效率更高的ABTR方案,是我们未来重点的研究工作.

致 谢 在此,我们向对本文提出宝贵修改意见的匿名审稿老师表示衷心的感谢!

参 考 文 献

[1] Sahai A, Waters B. Fuzzy identity based encryption//Proceedings of the EUROCRYPT 2005. Aarhus, Denmark, 2005: 457-473

[2] Goyal V, Pandey O, Sahai A, Waters B. Attribute-based encryption for fine-grained access control of encrypted data//Proceedings of the 13th ACM Conference on Computer and Communication Security. Alexandria, VA, USA, 2006: 89-98

[3] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption//Proceedings of the 2007 IEEE Symposium on Security and Privacy. Washington, USA, 2007: 321-334

[4] Traynor P, Butler K, Enck W, Mcdaniel P. Realizing massive-scale conditional access systems through attribute-based cryptosystems//Proceedings of the 15th NDSS 2008. San Diego, USENIX Association, 2008: 1-13

[5] Yu S C, Ren K, Lou W J. Attribute-based content distribution with hidden policy//Proceedings of the 4th Workshop on Secure Network Protocols. Orlando, 2008: 39-44

[6] Lewko A, Okamoto T, Sahai A, Takashima K, Waters B. Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption//Proceedings of the EUROCRYPT 2010. Monaco, 2010: 62-91

[7] Hinek M J, Jiang S, Safavi-Naini R, Shahandashti S F. Attribute-based encryption with key cloning protection. Cryptology ePrint Archive: Report 2008/478, 2008

[8] Yu S C, Ren K, Lou W J, Li J. Defending against key abuse attacks in KP-ABE enabled broadcast system//Proceedings of the Security and Privacy in Communication Networks. Athens, Greece, 2009: 311-329

[9] Li J, Ren K, Zhu B, Wan Z G. Privacy-aware attribute-based encryption with user accountability//Proceedings of the Information Security Conference 2009. 2009: 347-362

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

[11] Boneh D, Shaw J. Collusion-secure fingerprinting for digital data//Proceedings of the CRYPTO 1995. Santa Barbara, California, USA, 1995: 452-465

[12] Abdalla M, Dent A W, Malone-Lee J, Neven G, Phan D H, Smart N P. Identity-based traitor tracing//Proceedings of the Public Key Cryptography. Beijing, China, 2007: 298-314

[13] Pirretti M, Traynor P, Mcdaniel P, Waters B. Secure attribute-based systems//Proceedings of the 13th ACM Conference on Computer and Communication Security. Alexandria, VA, USA, 2006: 99-112

[14] Ostrovsky R, Sahai A, Waters B. Attribute-based encryption with non-monotonic access structures//Proceedings of the 14th ACM Conference on Computer and Communication Security. Alexandria, New York, USA, 2007: 195-203

[15] Attrapadung N, Imai H, Conjunctive broadcast and attribute-based encryption//Proceedings of the Pairing-Based Cryptography-Pairing 2009. Palo Alto, USA, 2009: 248-265

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

[17] Su Jin-Shu, Cao Dan, Wang Xiao-Feng, Sun Yi-Pin, Hu Qiao-Lin. Attribute-based encryption schemes. Journal of Software, 2011, 22(6): 1299-1315(in Chinese)
(苏金树，曹丹，王小峰，孙一品，胡乔林. 属性基加密机制，软件学报，2011, 22(6): 1299-1315)

[18] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers//Proceedings of the CRYPTO 2001. Santa Barbara, California, USA, 2001: 41-62

[19] Phan D H, Trinh V C. Identity-based trace and revoke schemes//Proceedings of the ProvSec'11. Xi'an, China, 2011: 204-221

[20] Cheung L, Newport C. Provably secure ciphertext policy ABE//Proceedings of the ACM Conference on Computer and Communication Security. Alexandria, Virginia, USA, 2007: 456-465

MA Hai-Ying, born in 1977, Ph. D. candidate, lecturer. Her research interests focus on public key cryptography and network security.

ZENG Guo-Sun, born in 1964, Ph. D., professor, Ph. D. supervisor. His research interests include information security, parallel computing.

Background

Secure data storage and sharing service becomes more and more attractive, and it is a hot research topic in the field of information security. The attribute-based encryption (ABE) technology is considered as one of the most efficient methods to implement secure data storage and sharing, and it is a new branch of information security. Recently, many ABE schemes have been proposed. In ABE schemes, users' access rights are related to their private keys. This leads to a problem that the system's access control policy will be breached if malicious users leak their private keys to illegitimate users. Although many schemes proposed several methods to mitigate this key leakage problem, they aim only at tracing traitors who leaked their keys to illegal users, and can not revoke them as to render their keys invalid. Actually, if traitors can not be revoked, their leaked keys still threaten the security of ABE systems. Thus, it is an important research work to explore a new solution to trace traitors and revoke them from the ABE systems.

This paper proposes an ABE scheme for traitor tracing and revocation together (ABTR). We first introduce an ABE scheme with generalized wildcards (GWABE). Then we integrate the GWABE with complete subtree framework to yield an ABTR scheme and prove it is adaptively secure. However, the existing ABE schemes for traitor tracing can only be proved selectively secure.

This research is supported by the National High Technology Research and Development Program (863 Program) of China under Grant No. 2009AA012201; the National Natural Science Foundation of China under Grant No. 61103068; the joint of NSFC and Microsoft Asia Research under Grant No. 60970155; the Program of Shanghai Subject Chief Scientist under Grant No. 10XD1404400; the Ph. D. Programs Foundation of Ministry of Education under Grant No. 20090072110035; the special Fund for Fast Sharing of Science Paper in Net Era by CSTD under Grant No. 20110740001.