doi:10.11959/j.issn.1000-436x.2016009

适应性安全的可追踪叛徒的基于属性加密方案

马海英[1]，曾国荪[2]，陈建平[1]，王金华[3]，王占君[3]

(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. 南通大学理学院，江苏 南通 226007)

摘 要：针对基于属性加密(ABE, attribute-base encryption)机制存在的密钥滥用问题，为每个用户增加唯一的身份标识符，将联合安全编码和叛徒追踪机制引入到 ABE 方案中，给出适应性安全的可追踪叛徒 ABE 的定义、安全模型和可追踪模型，提出一种适应性安全的可追踪叛徒的 ABTT 方案，该方案允许适应性追踪指定策略盗版解码器中的叛徒。基于合数阶群上的子群判定假设和 DDH 假设，证明所提方案是适应性安全和适应性可追踪的。因此，所提方案不仅可以适应性追查指定策略盗版解码器中的叛徒，而且进一步增强了 ABE 系统的安全性，具有一定的理论和应用价值。

关键词：基于属性加密；叛徒追踪；双系统加密；适应性安全；联合安全编码

中图分类号：TP309 **文献标识码**：A

Adaptively secure attribute-based encryption for traitor tracing

MA Hai-ying[1], ZENG Guo-sun[2], CHEN Jian-ping[1], WANG Jin-hua[3], WANG Zhan-jun[3]

(1. College of Computer Science and Technology, Nantong University, Nantong 226019, China;
2. Department of Computer Science and Technology, Tongji University, Shanghai 201804, China;
3. School of Science, Nantong University, Nantong 226007, China)

Abstract: For the key abuse problem in attribute-based encryption (ABE), each user was identified by his unique identity, and the collusion secure codes and the traitor tracing mechanism were introduced to the ABE scheme. The definition, security model and tracing model for adaptively secure attribute-based encryption for traitor tracing (ABTT)were formalized, and an adaptively secure ABTT scheme was proposed, which may trace traitors in policy-specific pirate decorders. Under these subgroup decision assumptions in composite groups and the DDH assumption, adaptively secure and can adaptively trace traitors were proved. Therefore, the scheme not only was capable of tracing adaptively traitors in policy-specific pirate decorders, but also further strengthens the security of ABE system, which has theoretical and practical values.

Key words: attribute-based encryption, traitor tracing, dual system encryption, adaptive security, collusion secure code

1 引言

基于属性加密(ABE, attribute-base encryption)机制作为一种新型的一对多的公钥加密机制，实现了对加密数据的细粒度访问控制[1,2]。然而，在 ABE 系统中，用户的访问权限与其私钥直接关联[3,4]。一个密文可以被满足访问策略的多个用户解密，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被打破[5,6]。特别的，用户私钥仅与其属性相关，不同用

收稿日期：2014-12-20；**修回日期**：2015-03-19

基金项目：国家自然科学基金资助项目(No.61402244, No.61272424, No.61202006, No.61272107, No.61202173, No.61103068)；NSFC-微软亚洲研究院联合基金资助项目(No.60970155)；上海市优秀学科带头人计划基金资助项目(No.10XD1404400)；教育部博士点基金资助项目(No.20090072110035)；上海自然科学基金资助项目(No.13ZR1443100)；南通大学校级自然科学基金资助项目(No.15Z06)

Foundation Items: The National Natural Science Foundation of China (No.61402244, No.61272424, No.61202006, No.61272107, No.61202173, No.61103068), The Joint of NSFC and Microsoft Asia Research (No.60970155), The Program of Shanghai Subject Chief Scientist(No.10XD1404400), The Ph.D Programs Foundation of Ministry of Education China(No.20090072110035), Shanghai Natural Science Foundation Program(No.13ZR1443100), The Natural Science Foundation of Nan tong University(No.15Z06)

户可能会有相同属性，而与用户的任何特定信息(如身份)无关，即使盗版密钥被发现，也无法将其与任何合法用户相关联。因此，恶意用户可以轻易地与他人共享自己的私钥而不用担心被追究责任[5]，称这些恶意用户为叛徒。

针对基于属性加密中的密钥滥用问题，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[3]提出一种基于标号的 ABE 方案。在该方案中，当用户需要解密密文时，利用在线的可信第三方，如果恶意用户拷贝或代理生成私钥，并分发给他人时，则将会导致该用户的个人隐私信息被泄露。该方案有效地抵制了 ABE 中密钥拷贝或密钥代理攻击，对预防密钥滥用起到威慑作用。但是，该方案不能追究密钥滥用者的责任。2009 年，Yu 等[7]和 Li 等[6]基于 DBDH 和 D-Linear 假设分别提出了防密钥滥用密钥策略 ABE 方案和可追责的匿名密文策略 ABE 方案，可追查到叛徒的真实身份，解决了 ABE 中叛徒非法行为的责任追究问题。2011 年，Wang 等[5]将联合安全编码[8]和叛徒追踪技术[9]引入到 ABE 机制中，提出了基于属性的叛徒追踪方案。然而，上述方案仅满足较弱的选择安全模型，即攻击者必须在生成系统公钥之前选择攻击目标。在实际应用的 ABE 系统中，系统公钥生成之后，攻击者可以适应性地选择攻击目标，构造盗版解码设备。因此，上述方案均不能满足实际密码系统对适应性安全的应用需求。同时，Wang 等[5]将如何构建适应性安全的基于属性加密的叛徒追踪方案作为一个公开问题被提出。2013 年，Liu 等[10]提出了适应性安全的可追踪叛徒的密文策略 ABE 方案，将盗版解码器分为 2 种：1) 类密钥盗版解码器，显式地给出一个属性集，并将相应的私钥固化在盗版设备中，只要该属性集满足密文中访问策略，就能以不可忽略的概率解密密文；2) 指定策略盗版解密器，明确给出一个访问策略，该盗版解码器能以不可忽略的概率解密在该访问策略下加密的密文。该方案能够适应性追踪类密钥盗版解码器，但仅能选择性追踪指定策略盗版解密器。

为了构造出可适应性追踪指定策略盗版解密器中叛徒的 ABE 方案，本文需要解决以下 2 个问题。1) 由于在 ABE 机制中，可能存在多个用户具有相同属性集合，所以，ABE 机制不能根据属性集合来严格区分用户。然而，叛徒追踪方案要求必须能够严格区分每一个用户。因此，每个用户除了拥有一个属性集合 $?$，还引入一个身份信息 ID，即采用一对值$(ID, ?)$来标识每个用户。此外，为了使用户身份 ID 具有唯一性，本文利用联合安全编码[9]技术，将每个用户身份 ID 映射到一个码字。2) 授权中心根据用户的身份属性对$(ID, ?)$生成相应私钥，该私钥必定包含与身份 ID 对应的成分。为了保证本方案仍然是 ABE 方案，还需要解决另一个问题，即解密能否成功仅与用户拥有的属性集合相关，而与用户身份 ID 无关。本文在密文中引入一个向量，通过合理设计解密算法，使解密时能将密文和用户私钥中的身份信息相互抵销，不影响解密的前提条件。

本文通过修改 Lewko 等[11]提出的适应性安全的密文策略 ABE 方案，采用非对称的双线性对技术，将联合安全编码技术和 Abdalla 等[9]提出的叛徒追踪算法引入到该密文策略 ABE 方案中，提出一种适应性安全的可追踪叛徒的 ABE 方案。基于合数阶群上的子群判定假设和 DDH 假设，利用双系统加密技术[12]，通过一系列混合讨论，证明本方案是适应性安全和适应性追踪指定策略盗版解密器中的叛徒。因此，本方案不仅可以适应性追查叛徒，而且进一步增强了 ABE 系统的安全性，具有一定的理论和应用价值。

2　预备知识

2.1　联合安全编码

本节将简述联合安全编码的相关概念和结论，结合本文所提方案，采用文献[9]的符号来描述其定义。一个联合安全编码可以用$(ß, \mathrm{N}, e)$-联合安全码来表示，其中，$ß$ 表示叛徒追踪算法可允许的串谋用户的最大取值，N表示系统中用户的最大数目，e 表示追踪算法出错的概率值，这样的一个联合安全码可以由长度为 $l = O(ß^2(\log(\mathrm{N})+\log(\frac{1}{e})))$的码字和一个长度 $|\Sigma|=2$ 的字母表来生成。

令 S 表示一个长度为 $|\Sigma| = |S|$的符号字母表。假定 $x = x_1 \cdots x_l \in S^l$ 是一个长度为 l 的符号串，$I = \{1 \le i_1 < i_2 \cdots < i_n \le l\}$是一个索引集合，$x|_I$ 表示一个子串 $x_{i_1} \cdots x_{i_n}$，该子串仅包含字符串 x 在位置 I 上的这些符号。令 $W = \{ w_1, \cdots, w_ß \in S^l \}$表示一个符号串的集合，$I$ 表示 W 中符号串在对应位置相等的索引集合，即 I 是满足 $w_{1|I} = w_{2|I} = \cdots = w_{ß|I}$ 的最大集合。给出可行集合 W 的定义为 $FS(W) = \{ x \in S^l : x|_I = w_{1|I} =$

$w_{2|I}$ = ??? = $w_{ß|I}$ }。

一个字母表为 S，**长度为** l **的联合安全编码由一个集合**C**和一个追踪算法**T_C**组成。集合**C= { $w_r^{(i)}$| 1 ≤ i ≤ N, r∈{0,1}^{l} }，**记作编码本，其中，**r **是长度为**l**的** 0 **和** 1 **的字符串，对** $1 \le i \le \mathsf{N}$, $w_r^{(i)}$**是索引的码字。对于最多为** ß **个串谋用户集合**C ⊆{1, ???, N}，W = { $w_r^{(i)}$, i ∈ C }，**和所有的多项式时间算法** A，**联合安全码满足** $\Pr[\mathsf{T}_C(x, r) \in \mathsf{C} \mid x \in FS(W); x \xleftarrow{R} \mathsf{A}(W); r \xleftarrow{R} \{0,1\}^l] > 1 - e$。

这个概率值是由随机数 r、**随机算法**A**和追踪算法**T_C**来决定的，**$x \xleftarrow{R} \mathsf{A}(W)$**表示当随机算法**A**在输入集合** W **时，把输出结果赋值给** x；$r \xleftarrow{R} \{0,1\}^l$ **表示根据均匀分布选择的随机值** $r \in \{0,1\}^l$。**联合安全编码的详细资料可以参考文献**[9]。

2.2 非对称合数阶双线性群和困难问题假设

下面给出非对称合数阶群上的困难问题假设，假设给定一个群生成器G，**输入系统安全参数** ?，**输出非对称合数阶双线性群的描述**($N = p_1p_2p_3, G_1, G_2, G_T, \hat{e}$)，**其中，**$G_1, G_2, G_T$ **均是阶为** $N = p_1p_2p_3$ **的循环群，双线性映射** $\hat{e}$：$G_1 \times G_2$? G_T **满足下列条件。**1) **双线性：** $\forall g_1 \in G_1, h_1 \in G_2; a, b \in Z_N; \hat{e}(g_1^a, h_1^b) = \hat{e}(g_1, h_1)^{ab}$。2)**非退化性：**$\exists g_1 \in G_1, h_1 \in G_2$ **使** $\hat{e}(g_1, h_1)$**在** G_T **中的阶为** N。3)**可计算性：群** G_1, G_2, G_T **中的运算以及双线性映射** $\hat{e}$ **都是在多项式时间内可计算的。**4)**正交性：令** G_{1, p_i} **表示群** G_1 **的** p_i **阶子群，**G_{2, p_j} **表示群** G_2 **的** p_j **阶子群**(i = 1, 2, 3; j = 1, 2, 3)，**如果** $g_i \in G_{1, p_i}, h_j \in G_{2, p_j}$, **且** $i \neq j$ **时，**$\hat{e}(g_i, h_j)$ =1 **为** G_T **的单位元，则称其为群** G_1 **和** G_2 **上的正交性。令** G_{1, p_ip_j} **和** G_{2, p_ip_j} **分别表示群** G_1 **和群** G_2 **的** p_ip_j **阶子群，下面给出非对称合数阶群上子群判定困难问题假设。**

假设 1 给定非对称合数阶双线性群 E =($N = p_1p_2p_3, G_1, G_2, G_T, \hat{e}$)，**随机选择** $h_1 \in G_{2, p_1}, X_3 \in G_{2, p_3}$，**令** D= (E , h_1, X_3), **随机选择** $T_1 \in G_{2, p_1p_2}, T_2 \in G_{2, p1}$，**任意概率多项式时间的攻击者**A**区分元组**(D, T_1)**和元组**(D, T_2)**的优势是可以忽略的。**

假设 2 给定非对称合数阶双线性群 E =($N = p_1p_2p_3, G_1, G_2, G_T, \hat{e}$)，**随机选择** $h_1, X_1 \in G_{2, p_1}, X_2, Y_2 \in G_{2, p_2}, X_3, Y_3 \in G_{2, p_3}$，**令** D = (E , h_1, X_1X_2, X_3, Y_2Y_3), **随机选择** $T_1 \in G_2$, $T_2 \in G_{2, p_1p_3}$，**任意概率多项式时间的攻击者**A**区分元组**(D, T_1)**和元组**(D, T_2)**的优势都是可忽略的。**

假设 3 给定非对称合数阶双线性群 E =($N = p_1p_2p_3, G_1, G_2, G_T, \hat{e}$)，**随机选择** $a, s \in Z_N, h_1 \in G_{2, p_1}, X_2, Y_2, Z_2 \in G_{2, p_2}, X_3 \in G_{2, p_3}$，**令** D = (E , h_1, $h_1^a X_2$, X_3, $h_1^s Y_2$,Z_2), **随机选择** $T_1 \in \hat{e}(f(h_1), h_1)^{as}, T_2 \in G_T$，**任意概率多项式时间的攻击者**A**区分元组**(D, T_1)**和元组**(D, T_2)**的优势都是可忽略的。**

假设 4 给定非对称合数阶双线性群 E = ($N = p_1p_2p_3, G_1, G_2, G_T, \hat{e}$)，**随机选择** $a, s \in Z_N, h_1 \in G_{2, p_1}, X_2, Y_2, Z_2 \in G_{2, p_2}, X_3 \in G_{2, p_3}$，**令** D = (E , h_1, $h_1^a X_2$, X_3, $h_1^s Y_2$,Z_2), **任意概率多项式时间的攻击者**A**利用已知条件** D **计算出** $\hat{e}(f(h_1), h_1)^{as}$ **的优势都是可忽略的。**

假设 5 给定非对称合数阶双线性群 E = ($N = p_1p_2p_3, G_1, G_2, G_T, \hat{e}$)，**随机选择** $a, b \in Z_N, g_1 \in G_{1, p_1}$，**令** D =(E , g_1^a , g_1^b),**任意概率多项式时间的攻击者**A**打破** G_{1, p_1}**上的**DDH**假设的优势都是可忽略的。**

2.3 访问结构和线性秘密共享方案(LSSS)

定义 1 (**访问结构**[11])。**假定**P ={$\mathsf{P}_1, \mathsf{P}_2, \mathsf{P}_3, \cdots, \mathsf{P}_n$}**是** n **个参与者的集合，由**P**的某些非空子集构成的集族** A **，称其为访问结构，其中，集族**$A \subseteq 2^{\mathsf{P}} \setminus \phi$，**且** A **是单调的，即对任意集合** B, C，**均有：如果** $B \in A$ **且** $B \subseteq C$，**那么** $C \in A$ 。A **中的所有集合称为授权集，不在** A **中的集合称为非授权集。**

定义 2 (LSSS[11])。**在参与者集合**P={$\mathsf{P}_1, \mathsf{P}_2, \cdots, \mathsf{P}_n$}**上构造一个秘密共享方案** ? **是线性的，如果有：**1)**将** Z_p **上的一个向量构造成参与者的秘密分享值；**2)**对于这个秘密共享方案** ? **，存在一个** $n_1 \times n_2$ **的秘密份额生成矩阵** $\boldsymbol{A}$ **和行标号函数** ?: {1, ⋯, n_1}? P，**假定** $s \in Z_p$ **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** $\boldsymbol{v}$ = ($s, r_2, \cdots, r_{n_2}$)，**设** $\boldsymbol{v}'$**为** $\boldsymbol{v}$ **的转置，则** $\boldsymbol{Av}'$**是** n_1 **个秘密份额构成的向量，根据标号函数将秘密份额** $?_i = (\boldsymbol{Av})_i (1 \le i \le n_1)$**分配给参与者** $?(i)$。

LSSS **的可重构性。假定** ? **是访问结构** A **的线性秘密共享方案，令** $S \in A$ **是授权集，定义** $I = \{i: ?(i) \in S\} \subseteq \{1, \cdots, n_1\}$，**则存在多项式时间算法计算** $\{c_i \in Z_p\}_{i \in I}$，**使对于秘密共享值** s **的任意有效份额** $\{?_i\}_{i \in \{1, \cdots, n1\}}$，**满足** $\Sigma_{i \in I} c_i l_i = s$ 。

将 LSSS **引入到本文所提方案中，将属性作为参与者，则所有的授权属性集均包含在访问结构。**

3　适应性安全 ABTT 定义和安全模型

本节描述适应性安全的可追踪叛徒的基于属性加密(ABTT, adaptively secure attribute-based encryption for traitor tracing)的形式化定义、安全模型和可追踪模型。在本方案中，每个用户使用一个对(ID, $?$)来标识，其中，ID 表示用户的身份，$?$ 表示用户拥有的属性集合，且不同用户可以具有相同的属性集合。

3.1　适应性安全 ABTT 的定义

一个可追踪叛徒的基于属性加密方案形式上可以由以下 5 个概率多项式时间算法来构成。

1) 初始化算法。该算法输入安全参数 $?$ 和系统全部属性集合 W，输出系统公钥 PK 和主密钥 MSK。

2) 私钥生成算法。该算法输入主密钥 MSK 和用户的身份属性对(ID, $?$)，输出该用户的私钥 $SK_{ID,?}$。

3) 加密算法。该算法输入消息 M、访问结构($\boldsymbol{A}$, $?$)和系统公钥 PK，输出一个密文 CT。

4) 解密算法。该算法输入一个密文 CT、一个用户私钥 $SK_{ID,?}$ 和公钥 PK，仅当私钥中的属性集合能够满足密文中的访问结构时，输出明文 M；否则，输出 ^ 表示解密失败。

5) 叛徒追踪算法。针对访问结构($\boldsymbol{A}$, $?$)的盗版解密设备 D，该算法拥有对该设备的访问权限，输出一组用户的身份，与这些身份对应的用户被认为是叛徒。

注意。本文定义的所有盗版解密设备 D 均是可复位的[5]，这意味着盗版解密设备只能解密，不能自毁且没有其他状态。上述叛徒追踪算法定义的盗版解密设备 D 是针对某个访问结构($\boldsymbol{A}$, $?$)的，这表明 D 能以不可忽略的优势解密在该访问结构($\boldsymbol{A}$, $?$)下加密生成的随机密文。

本方案的正确性可以描述为。系统运行初始化算法生成 PK 和 MSK，对于所有消息 $M\in\{0,1\}^*$，用户身份 ID，当 $?$ 满足($\boldsymbol{A}$, $?$)时，$\mathrm{Dec}(\mathrm{KeyGen}(ID, ?, MSK), \mathrm{Enc}(M, (\boldsymbol{A}, ?), PK)) = M$ 的概率为 1。

3.2　安全模型

本方案的适应性安全模型是通过挑战者S和攻击者A之间的交互性游戏来定义的。

1) 初始化：挑战者S运行本方案的初始化算法，并将生成的公钥 PK 发送给攻击者A。

step1　A适应性地询问用户(ID, $?$)的私钥，挑战者生成私钥并其发送给A，A可以重复多次询问私钥。

2) 挑战阶段：A向挑战者S提交访问结构($\boldsymbol{A}$, $?$)、等长消息 M_0 和 M_1，S抛掷一枚公平硬币 $b\in\{0,1\}$，计算 $CT=\mathrm{Enc}(M_b, (\boldsymbol{A}, ?), PK)$，并将 CT 发送给A。

step2　重复执行 step1。

3) 猜测阶段：A输出对挑战密文 CT 的一个猜测值 $b'\in\{0,1\}$。

若 $b'=b$，且攻击者A在 step1 和 step2 中从未询问这类用户(id, $?$)的私钥，其中，$?$ 满足挑战访问结构($\boldsymbol{A}$, $?$)，则称A赢得了这个游戏。攻击者A在上述游戏中获胜的优势定义为：$\mathrm{Adv}_A=|\Pr[b'=b]-\frac{1}{2}|$。

定义 3　如果任意多项式时间攻击者A赢得上述游戏的优势都是可以忽略的，则称这个可追踪叛徒的基于属性加密方案是适应性安全的。

3.3　可追踪模型

本节将构造出一种适应性安全的可追踪模型。在该模型下，攻击者可以自适应的选择挑战访问结构，且拥有一个针对该访问结构的盗版解密设备的访问权限。令 $?$, $ß$ 表示相关的 2 个安全参数，可追踪模型可以通过挑战者S和攻击者A之间的交互性游戏进行如下描述。

1) 初始化。挑战者S运行本方案的初始化算法，将生成的公钥发送给攻击者A。

2) 私钥生成询问。A可以多次询问属性身份对($?_j$, ID_j)的解密私钥，其中，下标 j 表示第 j 次询问。

3) 生成盗版解密设备。A构造一个针对挑战访问结构($\boldsymbol{A}$, $?$)的盗版解密设备 D，D 是一个概率电路的描述，当向 D 输入随机密文时，输出消息。

4) 叛徒追踪。S在黑盒测试 D 的情况下，运行本文的叛徒追踪算法，获得一组用户身份集合Q。

注意。在上述可追踪模型中，假定所有盗版解密设备 D 是可复位的[9]，这就要求这些解密设备 D 在任意次解密之间不保留任何中间状态，且不能自毁。

令T表示攻击者A提交的私钥询问的用户身份集合，且要求在该集合中的任意身份 ID_j 对应的属性集合 $?_j$ 满足挑战访问结构($\boldsymbol{A}$, $?$)，如果同时满足如下 3 个条件，则说攻击者A在可追踪游戏中获胜。

1) 盗版解密设备 D 能以不可忽略的优势解密

在访问结构($\boldsymbol{A}$, $?$)下加密的随机密文，即 D 可以解密在访问结构($\boldsymbol{A}$, $?$)下加密的随机密文的一部分。

2) Q =Æ或QËT。

3) 攻击者A提交的所有私钥生成询问中最多有 ß 个不同用户的身份，且与这些身份一起询问的属性集合满足挑战访问结构($\boldsymbol{A}$, $?$)。对于不满足挑战访问结构($\boldsymbol{A}$, $?$)的属性集合，攻击者的私钥生成询问次数不需要限制。

攻击者A在上述游戏中获胜的概率可定义为A打破本方案可追踪性的优势。如果任意多项式时间的攻击者A在上述追踪游戏中的优势是关于 $?$ 的可忽略函数，那么可追踪叛徒的基于属性加密方案是 ß-TT-CPA 安全的。

4 适应性安全 ABTT 方案

本方案采用非对称双线性对技术来构建，即 $\hat{e}$：$G_1 \times G_2$? G_T, 存在一个可有效计算的同构映射 f：G_2 ? G_1，且要求该同构映射是不可逆的。本方案利用 Z_N^* 中的部分元素来表示系统所有属性的集合 O，假定 $GID = \{ID_1, ID_2, \cdots, ID_N\}$ 表示所有用户的集合，s 表示符号字母表的大小，用长度为 l 的字符串来表示一个码字，选择一个集合{1, 2, ···, N}上的随机置换 p。可信授权中心维持从用户 ID_j 到码字 $w_r^{p(j)}$ 的映射，其中，r 是联合安全编码的随机串。对于非二进制的字母表，可以使用一个长度为 $n = \lceil \mathrm{lb} s \rceil l$ 的位串表示一个码字，$cw \in \{0,1\}^n$ 表示一个码字的位串编码，cw_j 表示 cw 中的第 j 位。选择一个长度为(n +1)的向量 $\boldsymbol{F}$= (f_0, f_1, ···, f_n)， 其中，$f_j \in G_{2, p_1}$，令 $f(f_j) = e_j$，向量 $\boldsymbol{E}$ = (e_0, e_1, ···, e_n)是同构映射 f 作用在向量 F 上的映像。设 $f_i = h_1^{k_i}$ (i= 0,1, ···, n), 则 $e_i = f(f_j) = g_1^{k_i}$。利用向量 $\boldsymbol{E}$ 和 $\boldsymbol{F}$ 定义 Waters 散列函数[5,8]

$$H(cw) = f_0 \prod_{j \in B} f_j \quad , \quad \tilde{H}(cw) = e_0 \prod_{j \in B} e_j$$

其中，B 是满足 cw_j=1 的所有 j 的集合。

Setup($?$, O)? (PK, MSK)该初始化算法根据系统安全参数 $?$ 生成阶 $N=p_1p_2p_3$ 的乘法循环群 G_1、G_2 和 G_T, 令 G_{1, p_1} 和 G_{2, p_1} 分别是群 G_1 和 G_2 的 p_1 阶子群，g_1, h_1, X_3 分别是 G_{1,p_1}, G_{2,p_1}, G_{2,p_3} 的生成元，且满足 $g_1 = f(h_1)$。可信授权中心(TA)随机选择 a, $a \in Z_N$，对每个属性 $i \in O$，随机选择 $s_i \in Z_N$。此外，TA 生成如上所述的 2 个向量 $\boldsymbol{E}$ 和 $\boldsymbol{F}$，选择秘密随机置换 p 和用于联合安全编码的秘密值 $r \in \{0,1\}^l$，将每个用户的 ID 映射到各自的码字 cw，生成系统公钥 PK 和主密钥 MSK 为

$$PK = \{N, g_1, g_1^a, \$(g_1, h_1)^a, T_i = g_1^{s_i}, \forall i \in W$$
$$E = (e_0, e_1, \mathrm{L}, e_n)\}$$
$$MSK = \{a, h_1, h_1^a, S_i = h_1^{s_i}, \forall i \in W$$
$$X_3, p, r, F = (f_0, f_1, \mathrm{L}, f_n)\}$$

KeyGen(MSK, ID, $?$) ? $SK_{ID, ?}$ 假定用户拥有身份 ID 和属性集合 $?$，该私钥生成算法随机选择 $t, t' \in Z_N$，$R_0, R_0', R_0'' \in G_{2, p_3}$，对每一个属性 $i \in ?$，随机选择 $R_i \in G_{2,p_3}$，令 ID 对应的码字为 cw，计算用户私钥 $SK_{ID, ?}$ 为

$$SK_{ID,w} = \{w, cw, K_1 = h_1^a h_1^{at} H(cw)^{t'} R_0$$
$$K_2 = h_1^t R_0', K_{3,i} = S_i^t R_i, \forall i \in w, K_4 = h_1^{t'} R_0'' \}$$

Enc(($\boldsymbol{A}$, $?$), PK, M) ? CT 该加密算法利用访问结构($\boldsymbol{A}$, $?$)和公钥 PK 对消息 M 进行加密，其中，$\boldsymbol{A}$ 是一个 $n_1 \times n_2$ 的矩阵，$?$ 是一个从 $\boldsymbol{A}$ 的每一行 $\boldsymbol{A}_x$ 到一个属性 $?(x)$的映射。该算法随机选择 s, v_2, ···, $v_{n2} \in Z_N$，组成随机向量 $\boldsymbol{v}$ = (s, v_2, ···, v_{n2})。对矩阵 $\boldsymbol{A}$ 的每个行向量 $\boldsymbol{A}_x$，随机选择 $r_x \in Z_N$, 计算密文如下

$$C_0 = M \$(g_1, h_1)^{as}, C_1 = g_1^s, C_{2,x} = g_1^{a\boldsymbol{A}_x \boldsymbol{v}} T_{r(x)}^{-r_x}$$
$$C_{3,x} = g_1^{r_x}, \forall x, C_4 = (e_j^s)_{j=0,1,\mathrm{L},n}$$

Dec(CT, $SK_{ID, ?}$, PK) ? M 假定密文 CT 中的访问结构是($\boldsymbol{A}$, $?$)，仅当用户私钥 $SK_{ID, ?}$ 中的属性集合 $?$ 满足($\boldsymbol{A}$, $?$)时，该解密算法可以成功解密密文，否则，解密失败。解密密文需要执行如下过程，首先计算 $C_4' = C_4^0 \prod_{j \in B} C_4^{(j)} = \tilde{H}(cw)^s$ 其中，B 是使 cw_j=1 的所有 j 的集合。然后，计算一组常量 $c_x \in Z_N$，使得 $\sum_{r(x) \in w} c_x \boldsymbol{A}_x = (1,0,\mathrm{L},0)$。计算

$$\frac{\$(C_1, K_1)}{\prod_{r(x) \in w} (\$(C_{2,x}, K_2) \$(C_{3,x}, K_{3,r(x)}))^{c_x} \$(C_4', K_4)} = \$(g_1, h_1)^{as}$$

$$M = \frac{C_0}{\$(g_1, h_1)^{as}}$$

$\mathsf{T}_C((\boldsymbol{A}, ?), D)$? Q可信授权中心执行该叛徒追踪算法，该算法拥有一个对访问结构($\boldsymbol{A}$, $?$)的盗版解密设备 D 的访问权限。令 d ($?$)表示关于 $?$ 的一个不

可忽略函数，D能以概率$d(?)$成功解密在$(\boldsymbol{A}, ?)$下加密的密文。令$C_4^{(i,j)}$表示C_4中的第$(\lceil \mathrm{lb}\, l \rceil (i-1)+j)$个元素。对每一个$1 \le i \le l$和$1 \le j \le \lceil \mathrm{lb} s \rceil$，该算法初始化计数器$ctr_{i,j}=0$，执行$\frac{16l}{d(l)}$次下面的测试过程。

1) 选择一个随机消息M。

2) 用访问结构$(\boldsymbol{A}, ?)$加密消息M，并生成一个密文$CT=((\boldsymbol{A}, ?), C_0, C_1, C_{2,x}, C_{3,x}, C_4, "x)$。

3) 从G_1中随机选择一个元素代替$C_4^{(i,j)}$。

4) 使用替换后的密文CT访问D。

5) 若D输出M，则计数器的值$ctr_{i,j}$? $ctr_{i,j}$+1。

完成以上循环，位串cw'可以按如下规则重新构成，让cw'_{ij}表示cw'的第$\lceil \mathrm{lbs} \rceil (i-1)+j$位，如果$ctr_{i,j} \le 4$?则$cw'_{i,j}=1$，否则$cw'_{i,j}=0$。然后，把位串$cw'$解码为长度是$l$的符号串$x$，最后利用联合安全编码的追踪算法计算$\mathrm{Q} \xleftarrow{\$} \mathrm{T_C}(x, r)$，并输出叛徒的身份的集合$ID_{p^{-1}}(\mathrm{Q})$。

上述方案的正确性计算过程如下

$$\frac{\hat{e}(C_1, K_1)}{\prod_{r(x)\in w} (\hat{e}(C_{2,x}, K_2)\hat{e}(C_{3,x}, K_{3,r(x)}))^{c_x}\hat{e}(C_4', K_4)}$$

$$= \frac{\hat{e}(g_1^s, h_1^a h_1^{at} H(cw)^{t'} R_0)}{\prod_{r(x)\in w} (\hat{e}(g_1^{a\boldsymbol{A}_x \boldsymbol{v}} T_{r(x)}^{-r_x}, h_1^t R_0')\hat{e}(g_1^{r_x}, S_{r(x)}^t R_{r(x)}))^{c_x}\hat{e}(\tilde{H}(cw)^s, h_1^{t'} R_0'')}$$

$$= \frac{\hat{e}(g_1^s, h_1^a)\hat{e}(g_1^s, h_1^{at})\hat{e}(g_1^s, H(cw)^{t'})}{\prod_{r(x)\in w} (\hat{e}(g_1^{a\boldsymbol{A}_x \boldsymbol{v}} T_{r(x)}^{-r_x}, h_1^t R_0')\hat{e}(g_1^{r_x}, S_{r(x)}^t R_{r(x)}))^{c_x}\hat{e}(\tilde{H}(cw)^s, h_1^{t'})}$$

$$= \frac{\hat{e}(g_1^s, h_1^a)\hat{e}(g_1^s, h_1^{at})\hat{e}(g_1^s, H(cw)^{t'})}{\prod_{r(x)\in w} (\hat{e}(g_1^{a\boldsymbol{A}_x \boldsymbol{v}} T_{r(x)}^{-r_x}, h_1^t)\hat{e}(g_1^{r_x}, S_{r(x)}^t))^{c_x}\hat{e}(\tilde{H}(cw)^s, h_1^{t'})}$$

$$= \frac{\hat{e}(g_1^s, h_1^a)\hat{e}(g_1^s, h_1^{at})\hat{e}(g_1^s, h_1^{(k_0+\sum_{j\in B} k_j)t'})}{\prod_{r(x)\in w} (\hat{e}(g_1^{a\boldsymbol{A}_x \boldsymbol{v}}, h_1^t))^{c_x}\hat{e}(g_1^{(k_0+\sum_{j\in B} k_j)s}, h_1^{t'})}$$

$$= \frac{\hat{e}(g_1^s, h_1^a)\hat{e}(g_1^s, h_1^{at})}{\hat{e}(g_1^{as}, h_1^t)}$$

$$= \hat{e}(g_1, h_1)^{as}$$

5　安全性和追踪性证明

为了证明本方案的安全性和追踪性，需要首先定义半功能密文和半功能私钥，然后将半功能私钥进一步分为 1 型半功能私钥和 2 型半功能私钥，但它们不会被应用在真实的系统中。为了构造半功能密文和半功能私钥，需要选择一些共用的参数$h_2 \in G_{2,p2}$，$g_2 = f(h_2)$，对每个属性$i \in O$，随机选择$z_i \in Z_N$。对$j = 0, 1, \cdots, n$，随机选择$d_j \in Z_N$。

半功能密文：半功能密文算法首先利用加密算法生成正常密文$CT=((\boldsymbol{A}, ?), C_0, C_1, C_{2,x}, C_{3,x}, C_4, "x)$，选择随机值$c \in Z_N$和随机向量$\boldsymbol{u} \in Z_N^{n_2}$，对访问矩阵$\boldsymbol{A}$的每一行$\boldsymbol{A}_x$，随机选择$?_x \in Z_N$，计算半功能密文如下

$$C_0 = M\hat{e}(g_1, h_1)^{as}, C_1' = C_1 g_2^c = g_1^s g_2^c$$

$$C_{2,x}' = C_{2,x} g_2^{\boldsymbol{A}_x \boldsymbol{u} + g_x z_{r(x)}} = g_1^{a\boldsymbol{A}_x \boldsymbol{v}} T_{r(x)}^{-r_x} g_2^{\boldsymbol{A}_x \boldsymbol{u} + g_x z_{r(x)}}$$

$$C_{3,x}' = C_{3,x} g_2^{-g_x} = g_1^{r_x} g_2^{-g_x}, C_4 = (e_j^s g_2^{d_j c})_{j=0,1,\cdots,n}, \forall x$$

1 型半功能私钥：该算法随机选择$t, d, b, t' \in Z_N$, $R_0, R_0', R_0'', R_i \in G_{2,p3}$，计算 1 型半功能私钥为

$$K_1 = h_1^a h_1^{at} H(cw)^{t'} R_0 h_2^d, K_2 = h_1^t R_0' h_2^b,$$

$$K_{3,i} = S_i^t R_i h_2^{bz_i}, K_4 = h_1^{t'} R_0'', \forall i \in w$$

2 型半功能私钥：该算法随机选择$t, d, t' \in Z_N$, R_0, R_0', R_0'', $R_i \in G_{2,p3}$，选择子群$G_{2,p2}$的生成元h_2，计算 2 型半功能私钥为

$$K_1 = h_1^a h_1^{at} H(cw)^{t'} R_0 h_2^d, K_2 = h_1^t R_0',$$

$$K_{3,i} = S_i^t R_i, K_4 = h_1^{t'} R_0'', \forall i \in w$$

值得注意的是，2 型半功能私钥相当于将 1 型半功能私钥的指数$b = 0$。当使用半功能私钥解密半功能密文时，得到多余项为$\hat{e}(g_2, h_2)^{cd-bu_1}$，其中，$u_1$是向量$\boldsymbol{u}$的第一个分量，即$<1, 0, \cdots, 0>\boldsymbol{u}$。此时，半功能密文和 1 型半功能私钥中的$z_i$是相同的，当用半功能私钥解密半功能密文时，这些$z_i$值将会被消掉，从而不影响解密。相反地，这些$z_i$是用来隐藏半功能密文在子群$G_{1,p_2}$中被共享$u_1$的值。这里要求访问结构中的每个属性只能使用一次，当攻击者有一个不能解密挑战密文的 1 型半功能私钥时，根据信息理论可知，它能获知关于z_i的信息是可忽略的。如果在访问结构中每个属性可以多次使用，则z_i的值将会多次暴露给攻击者。在下列定义的每个游戏中，1 型半功能私钥至多出现一次，其他半功能私钥都是 2 型的，这样就可以避免多次泄露z_i的值。

如果$cd - bu_1 = 0$，则称该 1 型半功能私钥是名义

半功能私钥，即名义半功能私钥可以成功解密相应的半功能密文。

5.1 安全性分析

本文所提方案是通过修改文献[11]的密文策略 ABE 方案而构造的，本文方案的安全性证明过程与这个密文策略 ABE 方案类似，基于假设 1～假设 3，可以证明本文方案是适应性安全的。由于篇幅有限，本文不做详细说明，其具体安全性证明过程可以参考文献[11]。

5.2 可追踪性证明

基于子群 $G_{1,\ p_1}$ 上的 DDH 假设和合数阶群 G_2 上的静态假设 1、2、4、5，利用混合争论技术，借助一系列相邻游戏 ($\mathrm{Trace}_{\mathrm{Real}}$, Trace_0, $\mathrm{Trace}_{1,1}$, $\mathrm{Trace}_{1,2}$,…, $\mathrm{Trace}_{k-1,2}$, $\mathrm{Trace}_{k,1}$, $\mathrm{Trace}_{k,2}$,…, $\mathrm{Trace}_{q-1,2}$, $\mathrm{Trace}_{q,1}$, $\mathrm{Trace}_{q,2}$)的不可区分性，证明本文方案的可追踪性，其中，q 是攻击者询问私钥的最大次数。

$\mathrm{Trace}_{\mathrm{Real}}$：一个真实的本方案的可追踪性游戏，私钥和密文都是正常的。

Trace_0：与 $\mathrm{Trace}_{\mathrm{Real}}$ 类似，除了挑战者S生成半功能密文发送给盗版解码器 D 。

$\mathrm{Trace}_{k,1}$：与 Trace_0 类似，除了前 $k-1$ 次询问的私钥是 2 型半功能的，第 k 次询问私钥是 1 型半功能的，剩余的私钥是正常的。

$\mathrm{Trace}_{k,2}$：与 Trace_0 类似，除了前 k 次询问的私钥是 2 型半功能的，剩余的私钥是正常的。

$\mathrm{Trace}_{q,2}$：在这个可追踪性游戏中，所有询问私钥都是 2 型半功能的，且挑战者S生成半功能密文发送给盗版解码器 D 。

定理 1 如果所有串谋者C的码字中 $cw_{i',j'}=0$，那么 D 成功解密一个 (i', j') 位置被篡改的密文的优势为 p_0，有

$$p_0 \geq d(l) - \mathrm{Adv}^{\mathrm{XDDH}}_{\mathsf{S}_1, G_{1,p_1}}(l)$$

其中，S_1 是一个依赖于攻击者A的概率多项式时间算法。

证明 假设存在攻击者A构造了一个盗版解密设备 D ，它成功解密随机密文的优势为 $d(?)$，成功解密 $(i,\ j)$ 位置被替换密文的优势为 $p_0 \leq d(?)-?$，其中，$?>0$，可以构造一个算法 S_1 以 $?$ 的优势攻破 $G_{1,p1}$ 中 DDH 假设。

算法 S_1 接收到 DDH 假设的输入 $(g_1^{\mu},\ g_1^{?},\ Z)$，令 $k'=\lceil \mathrm{lb}_2 n \rceil (i'-1)+(j'-1)$。S随机选择 $a,\ a\in Z_N$，对每个属性 $i\in O$，随机选择 $s_i\in Z_N$。此外，对 $j=0,\ 1,\ \cdots,\ n$ 且 $j\neq k'$ 时，随机选择 $?_j\in Z_N$，计算 $e_j=g_1^{q_j}$, $f_j=h_1^{q_j}$ ；当 $j=k'$ 时，令 $e_{k'}=g_1^{\mu}$, $f_{k'}=\perp$。S_1 选择秘密随机置换 p 和用于联合安全编码的秘密值 $r\in\{0,1\}^l$，将每个用户的 ID 映射到各自的码字 cw，生成系统公钥 PK 和主密钥 MSK 为

$$PK=\{N, g_1, g_1^a, \hat{e}(g_1,h_1)^a, T_i=g_1^{s_i}, \forall i\in W, \boldsymbol{E}=(e_0,e_1,\perp,e_n)\}$$

$$MSK=\{a, h_1, h_1^a, S_i=h_1^{s_i}, \forall i\in W, X_3, p, r, \boldsymbol{F}=(f_0,f_1,\perp,f_n)\}$$

当A提交身份 ID 和属性集合 $?$ 时，S_1 随机选择 $t,\ t'\in Z_N$，$R_0,\ R_0',\ R_0''\in G_{2,p_3}$，对每一个属性 $i\in ?$，随机选择 $R_i\in G_{2,p_3}$，令 ID 对应的码字为 cw，计算用户私钥 $SK_{ID,?}$ 为

$$SK_{ID,w}=\{w, cw, K_1=h_1^a h_1^{at} H(cw)^{t'} R_0,$$
$$K_2=h_1^t R_0',\ K_{3,i}=S_i^t R_i,\ K_4=h_1^{t'} R_0'',\ \forall i\in w\}$$

注意：由条件 $cw_{k'}=0$，可知 $H(cw)$ 与 $f_{k'}$ 无关，所以 S_1 在不知道 f_k 的情况下仍然可以计算该用户的私钥。然后，攻击者A构造出一个针对挑战访问结构 $(A,\ ?)$ 的盗版解密设备 D。

S_1 产生一个随机消息 M，随机选择 $v_2',\ \cdots,\ v_{n2}'\in Z_N$，组成随机向量 $\boldsymbol{v}'=(1,\ v_2',\ \cdots,\ v_{n_2}')$，对访问矩阵 $\boldsymbol{A}$ 的每个行向量 $\boldsymbol{A}_x$，随机选择 $r_x\in Z_N$，计算密文如下

$$C_0=M\hat{e}(g_1^n,h_1)^a,\ C_1=g_1^n,$$
$$C_{2,x}=(g_1^n)^{\alpha \boldsymbol{A}_x \boldsymbol{v}'} T_{r(x)}^{-r_x},\ C_{3,x}=g_1^{r_x},\ \forall x,$$
$$C_4^{(j)}=\begin{cases}(g_1^n)^{q_j}, 0\leq j\leq n, j\neq k'\\ Z, j=k'\end{cases}$$

如果盗版解密设备 D 成功解密，那么算法 S_1 输出 1，否则输出 0。

如果 $Z=g_1^{\mu?}$，那么该密文是正确生成的随机密文，此时，D 正确解密密文的概率为 $d(?)$。如果 Z 是随机的，该密文是 C_4 中的第 k' 位被篡改的密文，那么 D 正确解密篡改密文的概率为 $d(?)-?$。所以算法 S_1 以

$$\mathrm{Adv}^{\mathrm{XDDH}}_{\mathsf{S}_1, G_{1,p_1}}(l) \geq d(l) - (d(l)-g) = g$$

的优势解决 G_{1,p_1} 中的 DDH 假设。

引理 1 当所有串谋者C的码字中 $cw_{i',j'}=1$ 时，

如果存在一个概率多项式时间攻击者A使$\mathrm{Trace}_{\mathrm{Real}}\mathrm{Adv}_{\mathrm{A}} - \mathrm{Trace}_{0}\mathrm{Adv}_{\mathrm{A}} = e$，那么可以构造一个概率多项式时间挑战者S，以$e$的优势攻破假设1。

证明　挑战者S接收到假设1的条件$\{h_1, X_3, T\}$，能够模拟$\mathrm{Trace}_{\mathrm{Real}}$或$\mathrm{Trace}_{0}$。S随机选择$a, a\in Z_N$，对每个属性$i\in O$，随机选择$s_i\in Z_N$。此外，对$j = 0, 1, \cdots, n$，随机选择$?_j\in Z_N$，计算$g_1=f(h_1)$，向量$\boldsymbol{E} = (g_1^{q_j})_{j=0,1,\cdots,n}$，向量$\boldsymbol{F}=(h_1^{q_j})_{j=0,1,\cdots,n}$，选择秘密随机置换$p$和用于联合安全编码的秘密值$r\in\{0,1\}^{l}$，将每个用户的$ID$映射到各自的码字$cw$，生成系统公钥$PK$和主密钥$MSK$为

$$PK=\{N, g_1, g_1^{a}, \hat{e}(g_1,h_1)^{a}, T_i=g_1^{s_i}, \forall i\in W, \boldsymbol{E}=(e_0,e_1,\cdots,e_n)\},$$

$$MSK=\{a, h_1, h_1^{a}, S_i=h_1^{s_i}, \forall i\in W, X_3, p, r, \boldsymbol{F}=(f_0,f_1,\cdots,f_n)\}$$

当A询问私钥时，S利用MSK和密钥生成算法给A颁发正规私钥。然后，攻击者A构造出一个针对挑战访问结构$(\boldsymbol{A}, ?)$的盗版解密设备D。

S产生一个随机消息M，随机选择$v_2', \cdots, v_{n_2}'\in Z_N$，组成随机向量$\boldsymbol{v}' = (1, v_2', \cdots, v_{n_2}')$，对访问矩阵$\boldsymbol{A}$的每个行向量$\boldsymbol{A}_x$，随机选择$r_x'\in Z_N$，利用挑战访问结构$(A^{*}, ?)$计算第$k'$位被篡改的密文如下。

$$C_1=M\hat{e}(g_1,T)^{a},\quad C_2=j(T),$$

$$C_3=j(T^{a\boldsymbol{A}_x\boldsymbol{v}'}T^{-r_x's_{r(x)}}),$$

$$C_4^{(j)}=\begin{cases} j(T^{q_j}), 0\le j\le n, j\ne k' \\ Z, \quad Z\leftarrow G_1, j=k' \end{cases}$$

其中，上述密文隐式的设置$\boldsymbol{v}=(s, sv_2', \cdots, sv_{n_2}')$，$r_x=sr_x'$，$\boldsymbol{v}$是随机向量，其第一个分量为$s$，且$r_x$是随机值。当$T\in G_{2,p_1}$时，$C_4^{(j)}=j(T^{q_j})=g_1^{sq_j}=e_j^{s}$，该密文是第$k'$位被篡改的正规密文。当$T\in G_{2,p_1p_2}$时，令$T=g_1^{s}g_2^{c}$，此时，该密文是半功能密文，其中，$u=cav'$，$?_x=-cr_x'$，$z_{?(x)}=s_{?(x)}$，$C_4^{(j)}=j(T^{q_j})=g_1^{sq_j}g_2^{cq_j}=e_j^{s}g_2^{cq_j}$，$d_j=?_j$。尽管半功能密文中重复使用了$G_{2,p1}$部分的值，但是，由中国剩余定理可知，$a, r_x', v_2', \cdots, v_{n_2}', s_{?(x)}, ?_j \bmod p_1$与$a, r_x', v_2', \cdots, v_{n_2}', s_{?(x)}, ?_j \bmod p_2$是无关的，上述密文是第$k'$位被篡改的半功能密文。因此，S可以根据A的输出，以e优势攻破假设1。

引理2　当所有串谋者C的码字中$cw_{i',j'}=1$时，如果存在一个概率多项式时间攻击者A使$\mathrm{Trace}_{k-1,2}\mathrm{Adv}_{\mathrm{A}}-\mathrm{Trace}_{k,1}\mathrm{Adv}_{\mathrm{A}}=e$，那么可以构造一个概率多项式时间挑战者S，以几乎为e的优势攻破假设2。

证明　挑战者S接收到假设2的条件$\{h_1, X_1X_2, X_3, Y_2Y_3, T\}$，能够模拟$\mathrm{Trace}_{k-1,2}$或$\mathrm{Trace}_{k,1}$。S随机选择$a, a\in Z_N$，对每个属性$i\in O$，随机选择$s_i\in Z_N$。此外，对$j = 0, 1, \cdots, n$，随机选择$?_j\in Z_N$，计算$g_1=f(h_1)$，向量$\boldsymbol{E} = (g_1^{q_j})_{j=0,1,\cdots,n}$，向量$\boldsymbol{F}=(h_1^{q_j})_{j=0,1,\cdots,n}$，选择秘密随机置换$p$和用于联合安全编码的秘密值$r\in\{0,1\}^{l}$，将每个用户的$ID$映射到各自的码字$cw$，生成系统公钥$PK$和主密钥$MSK$为

$$PK=\{N, g_1, g_1^{a}, \hat{e}(g_1,h_1)^{a}, T_i=g_1^{s_i}, \forall i\in W, \boldsymbol{E}=(e_0,e_1,\cdots,e_n)\},$$

$$MSK=\{a, h_1, h_1^{a}, S_i=h_1^{s_i}, \forall i\in W, X_3, p, r, \boldsymbol{F}=(f_0,f_1,\cdots,f_n)\}$$

下面将A的私钥询问分为以下3种情况：1)当A询问私钥次数大于k时，S利用MSK和私钥生成算法给A颁发相应正规私钥；2)当A询问私钥次数小于k时，S随机选择$t, t'\in Z_N, R_0, R_0', R_0'', R_i\in G_{2,p_3}$，计算2型半功能私钥为

$$K_1=h_1^{a}h_1^{at}H(cw)^{t'}R_0(Y_2Y_3)^{t}, K_2=h_1^{t}R_0',$$

$$K_{3,i}=S_i^{t}R_i, K_4=h_1^{t'}R_0'', \forall i\in w$$

其中，$t \bmod p_2$, $t \bmod p_3$和$t \bmod p_1$的值是不相关的，因此，该私钥是一个均匀分布的2型半功能私钥；3)当A进行第k次私钥询问时，令T的G_{p_1}部分为h_1^{t}，S随机选择$t'\in Z_N, R_0, R_0', R_0'', R_i\in G_{2,p_3}$，计算

$$K_1=h_1^{a}T^{a}H(cw)^{t'}R_0, K_2=TR_0',$$

$$K_{3,i}=T^{s_i}R_i, K_4=h_1^{t'}R_0'', \forall i\in w$$

其中，当$T\in G_{2,p_1p_3}$，这个私钥是正规私钥；当$T\in G_2$，这个私钥是1型半功能私钥，此时，该私钥隐式的设置$z_i=s_i$。如果T的G_{2,p_2}部分为h_2^{b}，则$d=ba \bmod p_2$，K_2的G_{2,p_2}部分为$h_2^{bz_i}$，$z_i \bmod p_2$和$s_i \bmod p_1$是不相关的。然后，攻击者A构造出一个针对挑战访问结构$(\boldsymbol{A}, ?)$的盗版解密设备D。

S产生一个随机消息M，隐式地设置$X_1=h_1^{s}$，$X_2=h_2^{c}$，随机选择$r_x', u_2, \cdots, u_{n_2}\in Z_N$，生成向量$\boldsymbol{u}'=(1,$

$u_2,\cdots, u_{n_2}$), 用挑战访问结构($\boldsymbol{A}$, ρ)对消息 M 进行加密，计算第 k'位被篡改的密文

$$C_0 = M\hat{e}(g^{(h_1)}, X_1X_2)^a = M\hat{e}(g^{(h_1)}, X_1)^a$$

$$C_1 = g^{(X_1X_2)}, C_{2,x} = g^{((X_1X_2)^{A_x\boldsymbol{u}'}(X_1X_2)^{-r_{x'}s_{\rho(x)}})}$$

$$C_{3,x} = g^{(X_1X_2)^{r_{x'}}}$$

$$C_4^{(j)} = \begin{cases} g^{(X_1X_2)^{q_j}}, 0 \le j \le n, j \ne k' \\ Z, \quad Z \leftarrow G_1, j = k' \end{cases}$$

其中，上述密文隐式地设置 $\boldsymbol{v} = s\alpha^{-1}\boldsymbol{u}'$, $\boldsymbol{u} = c\boldsymbol{u}'$, 因此，$s$ 是 G_{1,p_1} 部分被分享的值，$c\alpha$ 是 G_{1,p_2} 部分被分享的值，且 $r_x = sr_x'$, $\rho_x = -cr_x'$，$z_{\rho(x)} = s_{\rho(x)}$,此时，当第 k 个私钥是 1 型半功能时，$z_{\rho(x)}$在半功能密文和密钥中是一致的，$d_j = \rho_j$。

当第 k 个私钥是 1 型半功能时，K_1 与 $\alpha \bmod p_2$ 相关，密文中 $\boldsymbol{u}$ 的第一个分量为 $c\alpha$，$cd - bu_1 = cb\alpha - bc\alpha = 0 \bmod p_2$，此时该 1 型半功能私钥是名义半功能私钥。因此，第 k 个私钥可能是名义半功能的或正规的。

为了证明挑战密文 G_{1,p_2} 中被分享的值 $u_1 = c\alpha$ 在信息理论上是隐藏的，需要限制访问结构($\boldsymbol{A}$, ρ)中每个属性在 ρ 中至多出现一次。因为第 k 个私钥无法解密挑战密文，所以 $\boldsymbol{A}$ 中 $\rho(x) \in \rho$ 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 $\boldsymbol{w}$ 正交于 $\boldsymbol{R}$，但 $\boldsymbol{w}$ 不正交于 $\boldsymbol{1}$，即 $\boldsymbol{1}\cdot\boldsymbol{w} \ne 0$。固定一个包含 $\boldsymbol{w}$ 的基，则存在 $f \in Z_N$, 使 $\boldsymbol{u} = f\boldsymbol{w} + \boldsymbol{u}'' \bmod p_2$，其中，$\boldsymbol{u}''$属于除 $\boldsymbol{w}$ 外的基向量扩张的空间中，注意到 $\boldsymbol{u}''$是均匀分布的，且无法揭露 f 的任何信息。由于 $\boldsymbol{u}\cdot\boldsymbol{1} = f\cdot\boldsymbol{1}\cdot\boldsymbol{w} + \boldsymbol{1}\cdot\boldsymbol{u}''$，且 $\boldsymbol{1}\cdot\boldsymbol{w} \ne 0$，所以 $\boldsymbol{u}''\cdot\boldsymbol{1}$ 与 f 相关。

由于 $f\boldsymbol{w}$ 仅出现在 $\boldsymbol{A}_x^*\cdot\boldsymbol{u} + \rho_x z_{\rho(x)}$中，当 $\rho(x) \in \rho$ 时，$\boldsymbol{A}_x^*\cdot\boldsymbol{u} = \boldsymbol{A}_x^*\cdot(f\boldsymbol{w} + \boldsymbol{u}'') = \boldsymbol{A}_x^*\cdot\boldsymbol{u}''$，与 f 无关。当 $\rho(x) \notin \rho$ 时，若 $\rho_x \ne 0 \bmod p_2$，每项 $\boldsymbol{A}_x^*\cdot\boldsymbol{u}'' + \rho_x z_{\rho(x)}$都引入一个新的未知量 $z_{\rho(x)}$，且 $z_{\rho(x)}$不出现在其他项中，因此，A无法从这些项中得知 f 的任何信息。准确的说，无论 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 $\rho_x \bmod p_2$ 都不为 0 时，在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 $T \in G_{2,p_1p_3}$ 时，S完美仿真 $\mathrm{Trace}_{k-1,2}$；当 $T \in G_2$ 时，S以几乎为 1 的概率完美仿真 $\mathrm{Trace}_{k,1}$，所以，S可以根据A的输出，以几乎为 e 的概率攻破假设 2。

引理 3 当所有串谋者C的码字中 $cw_{i',j'} = 1$ 时，如果存在一个概率多项式时间攻击者A使 $\mathrm{Trace}_{k,1}\mathrm{Adv}_A - \mathrm{Trace}_{k,2}\mathrm{Adv}_A = e$，那么可以构造一个概率多项式时间挑战者S，以几乎为 e 优势攻破假设 2。

证明 挑战者S接收到假设 2 的条件$\{h_1, X_1X_2, X_3, Y_2Y_3, T\}$，能够模拟 $\mathrm{Trace}_{k,1}$ 或 $\mathrm{Trace}_{k,2}$。S随机选择 a, $a \in Z_N$，对每个属性 $i \in O$，随机选择 $s_i \in Z_N$。此外，对 $j = 0, 1, \cdots, n$, 随机选择 $\rho_j \in Z_N$，计算 $g_1 = f(h_1)$, 向量 $\boldsymbol{E} = (g_1^{q_j})_{j=0,1,\cdots,n}$, 向量 $\boldsymbol{F} = (h_1^{q_j})_{j=0,1,\cdots,n}$, 选择秘密随机置换 p 和用于联合安全编码的秘密值 $r \in \{0,1\}^l$，将每个用户的 ID 映射到各自的码字 cw，生成系统公钥 PK 和主密钥 MSK 为

$$PK = \{N, g_1, g_1^a, \hat{e}(g_1, h_1)^a, T_i = g_1^{s_i}, \forall i \in W, \boldsymbol{E} = (e_0, e_1, \cdots, e_n)\}$$

$$MSK = \{a, h_1, h_1^a, S_i = h_1^{s_i}, \forall i \in W, X_3, p, r, \boldsymbol{F} = (f_0, f_1, \cdots, f_n)\}$$

下面将A的私钥询问分为以下 3 种情况。1) 当A询问私钥次数大于 k 时，S利用 MSK 和私钥生成算法给A颁发相应的正规私钥。2)当A询问私钥次数小于 k 时，2 型半功能私钥与引理 2 的构造方法相同。3) 当A进行第 k 次私钥询问时，与引理 2 的构造方式类似，但需要增加一个随机值 $h \in ZN$，计算

$$K_1 = h_1^a T^a H(cw)^{t'}(Y_2Y_3)^h, K_2 = TR_0'$$

$$K_{3,i} = T^{s_i}R_i, K_4 = h_1^{t'}R_0'', \forall i \in w$$

唯一不同的是，K_1 中增加了一项$(Y_2Y_3)^h$，该项重新随机化了 K_1 的 G_{2,p_2} 部分。然后，攻击者A构造出一个针对挑战访问结构($\boldsymbol{A}$, ρ)的盗版解密设备 D。第 k'位被篡改的密文的构造方式与引理 2 相同，注意此时，第 k 次私钥不再是名义半功能的。如果用第 k 次私钥解密挑战密文，$cd - bu_1 \ne 0$，解密将会失败。

因此，当 $T \in G_{2,p_1p_3}$ 时，第 k 个私钥是 2 型半功能私钥，S完美仿真 $\mathrm{Trace}_{k,2}$；当 $T \in G_2$ 时，第 k 个私钥是 1 型半功能私钥，S完美仿真 $\mathrm{Trace}_{k,1}$，所以，S可以根据A的输出以 e 的优势攻破假设 2。

引理 4 当所有串谋者C的码字中 $cw_{i',j'} = 1$ 时，如果存在一个概率多项式时间攻击者A使

$\mathrm{Trace}_{q,2}\mathrm{Adv}_{\mathsf{A}}=e$，那么可以构造一个概率多项式时间算法S，以 e 的优势攻破假设 4。

证明　挑战者S接收到假设 4 的条件$\{\ h_1,\ h_1^a X_2,\ X_3,\ h_1^s Y_2,\ Z_2\ \}$，能够攻破 $\mathrm{Trace}_{q,2}$。S随机选择$a\in Z_N$，计算 h_1^a，对每个属性$i\in O$，随机选择$s_i\in Z_N$，计算$S_i=h_1^{s_i}$。此外，对 $j=0,1,\cdots,n$, 随机选择 $?_j\in Z_N$，计算 $g_1=f(h_1)$，向量 $\boldsymbol{E}=(g_1^{q_j})_{j=0,1,\cdots,n}$，向量 $\boldsymbol{F}=(h_1^{q_j})_{j=0,1,\cdots,n}$，选择秘密随机置换 p 和用于联合安全编码的秘密值$r\in\{0,1\}^l$，将每个用户的 ID 映射到各自的码字 cw，生成系统公钥 PK

$$PK=\{N,g_1,g_1^a,\hat{e}(g_1,h_1)^a=\hat{e}(g_1,h_1^a X_2)$$
$$T_i=g_1^{s_i},\forall i\in W,\boldsymbol{E}=(e_0,e_1,\cdots,e_n)\}$$

为了生成 2 型半功能私钥，S随机选择 $t, t'\in Z_N$, $R_0, R_0', R_0'', R_i\in G_{2,p3}$，计算

$$K_1=h_1^a X_2 h_1^{at} H(cw)^{t'} Z_2^t R_0,\ K_2=h_1^t R_0'$$
$$K_{3,i}=S_i^t R_i,\ K_4=h_1^{t'} R_0'',\forall i\in w$$

然后，攻击者A构造出一个针对挑战访问结构$(\boldsymbol{A},?)$的盗版解密设备D。

S产生一个随机消息 M，隐式的设置指数 s 来自于项 $h_1^s Y_2$，随机选择值 $r_x', u_2,\cdots,u_{n2}\in Z_N$, 生成向量$\boldsymbol{u}'=(a,u_2,\cdots,u_{n2})$, 用挑战访问结构$(\boldsymbol{A},?)$对消息 M 进行加密，计算第 k'位被篡改的密文

$$C_0=MT,C_1=j\ (h_1^s Y_2)$$
$$C_{2,x}=j\ ((h_1^s Y_2)^{A_x^*\boldsymbol{u}'}(h_1^s Y_2)^{-r_x' s_{r(x)}})$$
$$C_{3,x}=j\ (h_1^s Y_2)^{r_x'}$$
$$C_4^{(j)}=\begin{cases} j\ (h_1^s Y_2)^{q_j}, 0\le j\le n, j\ne k' \\ Z,\quad Z\leftarrow G_1, j=k' \end{cases}$$

其中，上述密文隐式设置 $\boldsymbol{v}=sa^{-1}\boldsymbol{u}'$, $\boldsymbol{u}=c\boldsymbol{u}'$，因此，$s$ 是 G_{1,p_1} 部分被分享的值，ca 是 G_{1,p_2} 部分被分享的值，且 $r_x=sr_x'$, $?_x=-cr_x'$，$z_{?(x)}=s_{?(x)}$, $d_j=?_j$。

如果盗版解密设备D成功解密上述密文的概率为 q_2，则算法S可以以相同的概率计算出 $\frac{C_0}{M}=\hat{e}(g_1,h_1)^{as}$ 作为假设 4 的解，所以 $q_1\le\mathrm{Adv4}_{\mathsf{G},\mathsf{A}}(?)$是可以忽略的。

定理 2　如果所有串谋者C的码字中 $cw_{i',j'}=1$，那么 D 成功解密一个(i',j')位置被篡改密文的优势 q_2 是可忽略的。

证明　如果假设 1、2、4、5 成立，根据引理 1~引理 4 可知，追踪性游戏 $\mathrm{Trace}_{\mathrm{Real}}$ 和 $\mathrm{Trace}_{q,2}$ 是不可区分的，由于在 $\mathrm{Trace}_{q,2}$ 中攻击者A成功解密一个(i',j')位置被篡改密文的优势是可忽略的，所以，在 $\mathrm{Trace}_{\mathrm{Real}}$ 中 D 成功解密一个(i',j')位置被篡改密文的优势 q_2 是可忽略的。

定理 3　本文适应性安全的 ABTT 方案满足 $ß$-TT-CPA 可追踪性，如果下面 3 个条件同时成立：1)本文方案采用的编码是字母表长度为 $\wp$、字符串长度为 l 的$(ß, N, e)$联合安全编码；2)DDH 假设在 G_{1,p_1} 上成立；3)假设 1~假设 4 在 G_2 上成立。即任意概率多项式时间的攻击者A生成一个不可追踪的盗版解密设备 D 的优势。$\mathrm{Adv}_{A,FABTT}^{\mathrm{trace-}CPA(b)}(l)\le e+l\lceil\mathrm{lb}\wp\rceil(q_2+\mathrm{e}^{-?})$。其中，$D$ 至多利用 $ß$ 个串谋者的私钥以 $d(?)$的概率成功解密密文，且

$$d(?)\ge 2\,\mathrm{Adv}_{\mathsf{S},G_{1,p_1}}^{DDH}(l)$$

证明　假定A是本方案可追踪性的攻击算法，输入系统公钥 PK，输出一个盗版解密设备D。利用A构造针对联合安全编码的攻击算法A'，输入 $ß$ 个随机代码字 $W=\{cw_1,\cdots,cw_ß\}$，输出一个字符串 x。下面证明，如果A能够以不可忽略的概率避免被追踪，那么A'能以不可忽略的概率输出一个不能被追踪的代码字 x。

A'随机选择 $i_1,\cdots,i_ß\in\{1,\cdots,\mathsf{N}\}$，设置串谋集合 $\mathsf{C}=\{i_1,\cdots,i_ß\}$，输入对应的码字

$$W=\{cw_r^{(i_j)},j=1,2,\cdots,ß\}$$

A'运行本方案的初始化算法，生成系统公钥

$$PK=\{N,g_1,g_1^a,\hat{e}(g_1,h_1)^a,T_i=g_1^{s_i},\forall i\in W$$
$$\boldsymbol{E}=(e_0,e_1,\cdots,e_n)\}$$

A至多进行 $ß$ 次私钥生成询问，设A第 j 次进行私钥询问时的输入为$(?,ID)$，A'用 $cw_r^{(i_j)}$ 为其生成相应的私钥。因为 W 包含随机串谋集C的代码字，因此 p 是一个随机置换，所以，A'返回给A的私钥是均匀分布的。然后，A构造出一个针对挑战访问结构$(\boldsymbol{A},?)$的盗版解密设备 D。A'运行本方案的追踪算法，输出字符串 x，根据定理 1、定理 2 和文献[8]中的 Chernoff 界，可知追踪算法输出的字符串 x 不属于可行集 $FS(W)$ 的概率，至多为 $\Pr[x\notin FS(W)]\le l\lceil\mathrm{lb}\wp\rceil(q_2+\mathrm{e}^{-?})$。由$(ß,N,e)$联合安全编码的性质可

知，定理 3 成立。

5.3 仿真实验的结果分析

为了验证本方案能够适应性追踪叛徒，基于双线性对程序库 PBCL，通过适当修改 libfenc 程序库[13]中密文策略 ABE 的部分代码，实现了本方案，并对其进行仿真实验。假定系统安全参数l =159，最多串谋叛徒个数b =2，用户总数为 1 024，追踪算法出错概率为 10^{-6}，则可以将联合安全码字长度取值为 60 位。一个具体的联合安全编码的构建是比较复杂的，由于篇幅有限，下面简单介绍联合安全编码工作原理，重点介绍本文叛徒追踪算法的实验结果。在本文方案中，有 1 024 个码字 $w_1, w_2, \cdots, w_{1\,024}$，并将其分配给所有用户。利用这些码字，任何 2 个用户均可定义一个可行集合，分别记为 $\mathrm{FS}_{1,2}$, $\mathrm{FS}_{1,3}$, …, $\mathrm{FS}_{1\,023,1\,024}$，此处 $\mathrm{FS}_{i,j}$ 表示由码字 w_i 和 w_j 定义的可行集合。令该实验中，2 个串谋用户的码字为 w_1 和 w_2，他们的可行集合为 $\mathrm{FS}_{1,2}$。根据本文叛徒追踪算法，对码字二进制串的每位运行 404 496 次测试，经过大量实验可得如下结果：1) 当所有叛徒位串的第(i, j)位 $cw_{i,j}$ 都是 1 时，从 G_1 中随机选择一个元素代替密文 C_4 中的第$(\lceil \mathrm{lb}\, n \rceil (i-1)+j)$个元素，此时解密成功的次数 ctr_{ij} 为 0 次或 1 次，远远小于 $4l$ =636 次，由追踪算法可知，其重构位的值是 1；2) 当所有叛徒位串的第(i, j)位 $cw_{i,j}$ 都是 0 时，从 G_1 中随机选择一个元素代替密文 C_4 中的第$(\lceil \mathrm{lb}\, n \rceil (i-1)+j)$个元素，此时解密成功的次数 ctr_{ij} 为 2 543 次，远远大于 636 次，由追踪算法可知，其重构位的值是 0；3) 当所有叛徒位串的第(i, j)位 $cw_{i,j}$ 不相同时，修改密文中相应位置的元素为随机值时，解密成功的次数将在 0~2 544 次随机取值，由追踪算法可知，该位可能被重构为 0 或 1，但这些位不影响叛徒码字的可行集合。由上述 3 种情况可以构造出叛徒码字的可行集 FS_{12}，利用联合安全编码的追踪算法，可追踪到叛徒的一组身份。总之，本文的追踪算法能够成功追查叛徒。

5.4 性能比较

表 1 列出本文 ABTT 方案和相关方案在效率和追踪性方面的详细比较，其中，n_1 表示密文中访问矩阵的行数，$|?|$表示集合 $?$ 中属性的个数，$|I|$表示解密钥中满足访问策略的属性个数，N表示系统中用户的最大数目，n 表示联合安全编码中一个码字的二进制位数。

表 1 本文 ABTT 方案与相关方案的性能比较

方案	密文长度	私钥长度	解密双线对个数	追踪性
LOS	$2n_1+2$	$\|w\|+2$	$2\|I\|+1$	否
LCW	$2n_1+17\sqrt{N}$	$\|w\|+4$	$2\|I\|+10$	适应性追踪类密钥盗版解码器，选择性追踪指定策略盗版解码器
本文	$2n_1+n+2$	$\|w\|+3$	$2\|I\|+2$	适应性追踪指定策略盗版解码器

与文献[11]的 LOS 方案相比，虽然密文长度增加了 n 个群 G 中的元素，但本方案实现了适应性叛徒追踪的功能。与文献[10]的 LCW 方案相比，尽管本方案只能容忍指定个数叛徒构造盗版解码器，但是实现了指定策略盗版解密器的适应性追踪。

6 结束语

为了增加可追踪叛徒的基于属性加密机制的安全性，本文修改了适应性安全的密文策略 ABE 方案[11]，将叛徒追踪机制和联合安全编码引入到该方案中，给出了适应性安全的 ABTT 的定义、安全模型和追踪模型，提出了一个适应性安全的 ABTT 方案。基于合数阶群上的静态假设和 DDH 假设，证明本方案是适应性安全和适应性可追踪的。因此，该方案不仅可以适应性追查指定策略盗版解码器中的叛徒，而且进一步增强了 ABE 系统的安全性，具有一定的理论和实用价值。

参考文献：

[1] SAHAI A, WATERS B. Fuzzy identity based encryption[C]//The EUROCRYPT. Aarhus, Denmark, c2005: 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//The 13th ACM Conference on Computer and Communication Security. Alexandria, Virginia, USA, c2006: 89-98.

[3] HINEK M J, JIANG S, SAFAVI-NAINI R, et al. Attribute-based encryption with key cloning protection[EB/OL]. http://eprint.iacr.org/2008/478.pdf.

[4] 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.
MA H Y, ZENG G S. An attribute-based encryption scheme for traitor tracing and revocation together[J]. Chinese Journal of Computers, 2012, 35(9):1845-1855.

[5] 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.

[6] LI J, REN K, KIM K. A^2BE: accountable attribute-based encryption for

abuse free access control[EB/OL]. http://eprint.iacr.org/2009/ 118.pdf.

[7] YU S C, REN K, LOU W J, et al. Defending against key abuse attacks in KP-ABE enabled broadcast system[C]//The Security and Privacy in Communication Networks. Athens, Greece, c2009: 311-329.

[8] BONEH D, SHAW J. Collusion-secure fingerprinting for digital data[C]//The CRYPTO'95. Santa Barbara, California, USA, c1995: 452-465.

[9] ABDALLA M, DENT A W, MALONE-LEE J, et al. Identity-based traitor tracing[C]//The public Key Cryptography. Beijing, China, c2007: 298-314.

[10] LIU Z, CAO Z, WONG D S. Blackbox traceable CP-ABE: how to catch people leaking their keys by selling decryption ices on eBay[C]//The 20th Conference on Computer and Communication Security. Berlin, Germany, c2013: 475-486.

[11] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[C]//The EUROCRYPT. c2010: 62-91.

[12] WATERS B. Dual system encryption: realizing fully secure ibe and hibe under simple assumptions[C]//The CRYPTO'09. Santa Barbara, California, USA, c2009: 619-636.

[13] GREEN M, AKINYELE A, RUSHANAN M. Libfenc: The Functional Encryption Library[EB/OL]. http://code.google.com/p/libfenc.

作者简介：

马海英（1977-），女，河南卫辉人，博士，南通大学副教授，主要研究方向为公钥密码学和网络安全。

曾国荪（1964-），男，江西吉安人，同济大学教授、博士生导师，主要研究方向为网格计算、可信软件。

陈建平（1960-），男，江苏南通人，南通大学教授、硕士生导师，主要研究方向为信息安全、数值计算等。

王金华（1963-），男，江苏南通人，博士，南通大学教授、博士生导师，主要研究方向为信息安全、组合数学等。

王占君（1978-），男，河南鹤壁人，南通大学讲师，主要研究方向为公钥密码学和 Hopf 代数。