可公开定责的密文策略属性基加密方案

马潇潇[1] 于 刚[2,3]
(郑州信息科技职业学院 郑州 450046)[1]
(中国人民解放军信息工程大学数学工程与先进计算国家重点实验室 郑州 450001)[2]
(华东师范大学计算机科学与软件工程学院 上海 200062)[3]

摘 要 属性基加密利用属性集和访问结构之间的匹配关系实现用户解密权限的控制,从功能上高效灵活地解决了"一对多"的密数据共享问题,在云计算、物联网、大数据等细粒度访问控制和隐私保护领域有光明的应用前景。然而,在属性基加密系统中(以密文策略属性基加密为例),一个属性集合会同时被多个用户拥有,即一个解密私钥会对应多个用户,因此用户敢于共享其解密私钥以非法获利。此外,半可信的中心存在为未授权用户非法颁发私钥的可能。针对属性基加密系统中存在的两类私钥滥用问题,通过用户和中心分别对私钥进行签名的方式,提出一个密文策略属性基加密方案。该方案支持追踪性和公开定责性,任何第三方可以对泄露私钥的原始持有者的身份进行追踪,审计中心可以利用公开参数验证私钥是用户泄露的还是半可信中心非法颁发的。最后,可以证明方案的安全性基于其依赖的加密方案、签名方案。

关键词 属性基加密,可追踪性,可公开定责性,不可否认性
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2017.05.028

Publicly Accountable Ciphertext-policy Attribute-based Encryption Scheme

MA Xiao-xiao[1] YU Gang[2,3]
(Zhengzhou Vocational University of Information and Technology, Zhengzhou 450046, China)[1]
(State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450001, China)[2]
(School of Computer Science and Software Engineering, East China Normal University, Shanghai 200062, China)[3]

Abstract Ciphertext-policy attribute-based encryption (ABE) enables fine-grained access control of decryption privilege by using the matching relation between the attribute set and the access structure, and is a promising one-to-many encryption primitive which has a bright application prospect in cloud computing, big data etc. However, an attribute set may be owned by many users in ABE, i.e. one decryption key may belong to many users. Thus, malicious users dare to leak their decryption privileges to others for profits. Furthermore, a semi-trust authority may illegally generate decryption keys to unauthorized users. To solve these two kinds of key abuses in ABE, we proposed a publicly accountable ciphertext-policy attribute-based encryption scheme by embedding both signatures of user and authority into the secret key. The proposed scheme can achieve traceability and accountability, in which anybody can trace the identity of a leaked decryption key, and an auditor can verify whether the leaked key is shared by a malicious user or is illegally generated by a semi-trust authority. At last, the security of the proposed scheme can be proved based on the security of its atomic encryption and signature schemes.

Keywords Attribute-based encryption, Traceability, Public accountability, Nonrepudiation

1 引言

随着云计算、物联网、大数据等新型网络服务的快速发展,越来越多的用户将数据存放到第三方数据服务机构,以便进行远程数据分享、外包计算等。用户在享受新型网络服务带来的巨大便利的同时,也越来越关注外包数据隐私保护等问题。因此,数据在进行外包之前,用户有必要对数据进行加密操作。然而,传统"一对一"的加密模式下,数据拥有者需要针对每个数据为每个意定解密用户颁发解密私钥。当系统中数据和解密用户数量巨大时,密钥管理将成为系统的瓶颈。

到稿日期:2016-03-28 返修日期:2016-08-14 本文受国家自然科学基金(61371083),中国博士后科学基金(2016M591629),河南省高等学校重点科研项目(16A420006)资助。

马潇潇(1984—),女,博士,讲师,主要研究方向为信息安全、信息提取,E-mail:mxx1010@126.com;于 刚(1984—),男,博士,讲师,主要研究方向为密码学。

结合访问控制和数据加密技术，Waters[1] 于 2005 年提出了属性基加密(ABE)的思想，将属性集(或访问结构)嵌入到解密私钥中，对应地将访问结构(或属性集)嵌入到密文中，由属性集和访问结构之间的匹配关系确定用户的解密能力。因此，ABE 可以通过灵活的访问策略实现细粒度的数据解密权限控制。

然而，不同于“一对一”加密系统中一个密文只能由一个意定接收者解密，ABE 系统中(以密文策略 ABE 为例)，属性集合满足密文中访问结构的所有用户都可以解密。用户的解密能力不再是独有的，因此用户之间存在共享私钥以获得非法利益的动机。另外，一个属性集合可能对应多个不同用户，这也意味着这些用户具有相同的解密私钥。此外，ABE“一对多”灵活加密的设计目标，使得私钥以及密文中不能含有任何关于用户身份的信息，这使得即使解密私钥被恶意共享，也很难准确找到泄露私钥的恶意用户。因此，系统中的用户会非常乐意与其他用户共享解密私钥以非法获利。另一方面，私钥生成中心并不是完全可信的，中心存在给未授权用户非法颁发解密私钥的可能，这种可能性也会导致即使追踪到泄露私钥用户的身份，用户也可以声称是半可信中心非法颁发的，从而进行抵赖。

举一个简单的例子：一个出版集团因业务拓展需要，租用某云平台以存储其巨大的电子数据库。为了保护版权，在存储前，有必要先对电子资源进行加密，使得只有获得授权的用户才可以解密。为了灵活地实现解密权限的控制，出版集团可以使用密文策略的 ABE 加密系统。出版集团首先根据用户的购买情况，对每个用户赋予不同的属性集合，例如用户 A{论文，报刊}，用户 B{杂志，图书}，私钥生成中心根据用户的属性集合为用户颁发相应的解密私钥，忠实的用户只能解密其属性集合满足访问结构的资源。但是，为了非法获利，用户 A 可能将其对应{论文，图书}的解密权限分享给用户 B；另一方面，半可信中心可能为没有购买的用户 C 非法颁发{论文，报刊，杂志}的解密私钥。这两种情况的密钥滥用都会使得该出版集团损失惨重。

两类私钥滥用问题极大地限制了 ABE 系统从理论走向实际应用，单纯的属性基加密已经不能满足实际需求。因此，ABE 系统应该提供对泄露私钥身份的可追踪性以及公开定责性。

1.1　主要工作

针对 ABE 系统中存在的两类私钥滥用问题，提出一种支持可公开定责的密文策略属性基加密方案，记为 CP-AABE，其主要优势如下：

(1)可追踪性。CP-AABE 方案中，解密私钥显式地包含了用户的身份，用户的身份作为解密私钥的一部分必须参与解密操作，否则无法恢复明文。因此，任何第三方可以根据泄露的私钥直接追踪到私钥拥有者的身份，且中心不需要任何列表来存储身份与私钥的信息。

(2)公开验证性。CP-AABE 方案通过中心对用户身份进行签名并将签名嵌入到私钥的方式，实现了公开验证性。任何第三方追踪到私钥拥有者的身份后，可以根据公开参数验证身份的正确性。

(3)不可否认性。一方面，CP-AABE 方案支持中心的不可否认性，由于正确的私钥中会嵌入中心的签名，基于签名的不可伪造性，中心无法否认一个正确的私钥；另一方面，CP-AABE 方案支持用户的不可否认性，用户的签名同样被嵌入到私钥中，基于签名的不可伪造性，用户也无法否认一个正确的私钥。因此，审计中心可以公开判定泄露私钥是用户进行了恶意共享还是中心非法颁发给未授权用户，从而实现公开定责。

(4)强表达能力以及低存储。CP-AABE 方案支持线性秘密共享方案可实现的任意单调访问结构。并且，实现公开验证时除了公开参数，不需要任何额外的存储代价。

1.2　相关研究

ABE 在云计算、物联网、大数据等领域均有广泛应用，围绕效率、安全性、访问结构等指标，许多 ABE 方案被提出[2-15]。

针对用户恶意分享解密私钥的问题，Hinek 等[16] 于 2008 年提出了一个密钥可追踪的 ABE 系统，但解密者需与第三方机构进行交互后才能解密；Yu 等[17] 于 2009 年将每一位身份信息作为一个属性嵌入到访问策略中，提出了一个可追踪的密钥策略 ABE 方案；Li 等[18] 提出了一个可公开验证的支持“与门”的可定责 ABE 方案，但该方案不能提供不可否认性，而且经过分析发现其不能实现可追踪性；Katz 等[19] 于 2011 年提出了一个可追踪的内积谓词加密方案；Liu 等[20] 于 2013 年提出了一个支持任意单调访问结构的可追踪 ABE 方案；Ning 等[21] 于 2015 年提出了一个支持可追踪的大属性 ABE 方案。此外，针对中心的密钥托管问题，Zhang 等[22] 提出了一个可以阻止第二类私钥滥用的 ABE 方案。虽然文献[20-21]给出的可追踪方案支持强表达能力，但由于追踪到的是与用户对应的随机数，随机数与用户身份没有可公开验证的联系，而文献[22]则无法阻止第一类私钥滥用，因此文献[20-22]无法实现公开定责。

1.3　文章结构

第 2 节给出本文需要的预备知识；第 3 节给出 CP-AABE 的定义及其安全模型；第 4 节给出一个 CP-AABE 的具体构造；第 5 节给出 CP-AABE 方案的安全分析和效能分析；最后总结全文。

2　预备知识

2.1　线性秘密共享方案

设 $\mathcal{P}=\{P_1,\cdots,P_k\}$ 表示参与者的集合，$(\mathbf{W},\rho)$ 表示一个访问结构，其中 $\mathbf{W}$ 是一个 l 行 k 列的矩阵，ρ 是从 $\{1,2,\cdots,l\}$ 到 $\mathcal{P}$ 的映射。一个线性秘密共享方案(LSSS)包含以下两个算法：

1)秘密分发。假设 $s\in\mathbf{Z}_p$ 是待共享的秘密值，算法随机选取 $v_2,\cdots,v_k\in_R\mathbf{Z}_p^*$，构造向量 $\vec{v}=(s,v_2,\cdots,v_n)$，则 $\rho(i)$ 分享的子秘密值为 $\lambda_i=W_i\cdot\vec{v}$，其中 W_i 为矩阵 $\mathbf{W}$ 的第 i 行。

2)秘密重构。对于任一授权集 S，令 $I=\{i:\rho(i)\in S\}$，存在多项式时间算法可以计算得到系数 $\{w_i\in\mathbf{Z}_p\}_{i\in I}$，其中 $\{w_i\in\mathbf{Z}_p\}_{i\in I}$ 满足 $\sum_{i\in I}w_iW_i=(1,0,\cdots,0)$，因此可以恢复秘密 $s=\sum_{i\in I}w_iW_i\cdot\vec{v}=\sum_{i\in I}w_i\lambda_i$。

2.2　双线性对

假设 G，G_T 是 p 阶乘法循环群，其中 p 是大素数，g 是群

G 的一个生成元。$e:G\times G\to G_T$ 称为一个双线性映射，如果 e 满足以下 3 条性质：

1)双线性。对于任意的 $a,b\in Z_p$，都有 $e(g^a,g^b)=e(g^b,g^a)=e(g,g)^{ab}$。

2)非退化性。如果 $e(g^a,g^b)=1$ 当且仅当 $ab=0(\mathrm{mod}\ p)$。

3)有效性。对任意 $P,Q\in G$，存在多项式时间算法计算 $e(P,Q)$。

2.3 困难假设

假设 G，G_T 是 p 阶乘法循环群，p 是大素数，$e:G\times G\to G_T$ 为双线性映射，g 是群 G 的一个生成元。

计算性 Diffie-Hellman 假设(CDH)：输入 $(g,g^a,g^b)\in G^3$，其中 $a,b\in_R Z_p^*$，称 CDH 假设在群 G 成立，如果不存在一个多项式时间算法能够在多项式时间内以不可忽略的概率计算 g^{ab} 的值。

判定性 q 次并行双线性 Diffie-Hellman 指数假设(q-PBDHE)如下。

给定以下多元组：

$$(g^s,g^a,g^{a^2},\cdots,g^{a^q},g^{a^{q+2}},\cdots,g^{a^{2q}})$$

$$\forall 1\leqslant j\leqslant q:(g^{sb_j},g^{a/b_j},\cdots,g^{a^q/b_j},g^{a^{q+2}/b_j},\cdots,g^{a^{2q}/b_j})$$

$$\forall 1\leqslant j,k\leqslant q,j\neq k:(g^{asb_k/b_j},\cdots,g^{a^qsb_k/b_j})$$

其中，$s,a,b_1,\cdots,b_q\in_R Z_p^*$ 均未知，如果不存在一个多项式时间算法能够在多项式时间内以相对安全参数不可忽略的概率区分 $e(g,g)^{a^{q+1}}$ 和 G_T 中的随机元素，则称判定性 q-PBDHE 假设成立。

3 定义和安全模型

3.1 定义

一个 CP-AABE 方案包含以下算法。

系统初始化算法：输入安全参数 λ，输出系统主密钥 MSK 和系统公开参数 PP。

签名密钥生成算法：输入系统公开参数 PP，输出用户的签名私钥 k_{ID} 和公钥 P_{ID}。

解密私钥生成算法：用户向私钥生成中心(CA)提交身份 ID、公钥 P_{ID}、加密属性集 $w\subseteq U$。1)CA 利用系统公开参数 PP、主密钥 MSK 生成部分解密私钥 L，并秘密发送给用户 ID；2)用户 ID 利用签名私钥 k_{ID} 对部分解密私钥 L 进行短签名，将短签名 σ 发送给 CA；3)CA 验证 σ 的合法性，并计算剩余解密私钥 L'，并输出解密私钥 $SK_{ID,w}=(L,L',\sigma)$。

加密算法：输入系统公开参数 PP、加密访问结构 A、消息 M，输出相应的密文 CT。

解密算法：输入公开参数 PP、私钥 $SK_{ID,w}$、密文 CT，输出消息 M 或解密失败符号 $\perp$。

公开验证算法：输入系统公开参数 PP、私钥 $SK_{ID,w}$、公钥 P_{ID}，输出无效符号 $\perp$ 或身份 ID。

审计算法：输入系统公开参数 PP、私钥 $SK_{ID,w}$(包含签名 σ)、公钥 P_{ID}，输出无效符号 $\perp$ 或有效符号 $\top$。

3.2 安全模型

3.2.1 机密性

相比一般 ABE 方案，CP-AABE 方案增加了 3 个算法：签名私钥生成算法、公开验证算法、审计算法。其中公开验证算法以及审计算法都可以公开进行，对 CP-AABE 方案的机密性没有影响。而针对签名私钥生成算法，安全模型假设敌手 $\mathcal{A}$ 可以腐化部分用户，但是要求 $\mathcal{A}$ 在接收到系统的公开参数后，将腐化用户集合 C 发送给挑战者 $\mathcal{C}$，并且 $\mathcal{A}$ 不能对腐化的用户进行签名私钥提取询问。而对于未腐化的用户，其签名私钥提取询问由 $\mathcal{C}$ 进行模拟。CP-AABE 在选择模型下的适应性安全(IND-s-CCA2)可以由敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的游戏来刻画。

承诺：$\mathcal{A}$ 选择一个挑战访问结构 $\mathbb{W}^*$，并将 $\mathbb{W}^*$ 发送给 $\mathcal{C}$。

系统建立：$\mathcal{C}$ 运行系统初始化算法，生成系统主密钥 MSK 和公开参数 PP，秘密保存主密钥 MSK，将公开参数 PP 发送给 $\mathcal{A}$。$\mathcal{A}$ 将腐化用户集合 C 发送给 $\mathcal{C}$。

询问阶段 1：$\mathcal{A}$ 适应性地进行多项式次数的以下询问。

1)签名密钥提取询问：$\mathcal{A}$ 选择身份 $ID'\notin C$，$\mathcal{C}$ 输出签名私钥 $k_{ID'}$。

2)解密私钥提取询问：$\mathcal{A}$ 选择身份 ID'、公钥 $P_{ID'}$、加密属性集 $w'\subseteq U$，$\mathcal{C}$ 输出 $SK_{ID',w'}$。

3)解密询问：$\mathcal{A}$ 选择访问结构 $\mathbb{W}'$、密文 CT'，$\mathcal{C}$ 输出明文消息 M' 或失败符号 $\perp$。

挑战阶段：$\mathcal{A}$ 向 $\mathcal{C}$ 提交两个等长的消息 (M_0,M_1) 以及挑战访问结构 $\mathbb{W}^*$，其中要求已经执行解密私钥提取询问的加密属性集合 w' 都不能满足访问结构 $\mathbb{W}^*$。$\mathcal{C}$ 随机选择 $\beta\in\{0,1\}$，对访问结构 $\mathbb{W}^*$、消息 M_β 生成挑战密文 CT^*，并发送给 $\mathcal{A}$。

询问阶段 2：$\mathcal{A}$ 继续执行多项式次的解密私钥提取询问和解密询问，但是不能对满足访问结构 $\mathbb{W}^*$ 的任意属性集合 w' 执行解密私钥提取询问，也不能对挑战密文 CT^* 执行解密询问。

猜测：最后，$\mathcal{A}$ 输出对随机比特 $\beta\in\{0,1\}$ 的猜测值 β'。如果 $\mathcal{A}$ 给出了正确的猜测值，即 $\beta'=\beta$，则称 $\mathcal{A}$ 赢得了游戏。

$\mathcal{A}$ 的优势定义为：$Adv(\mathcal{A})=|\Pr[\beta'=\beta]-\frac{1}{2}|$。

3.2.2 可追踪性

私钥拥有者身份的可追踪性是基于私钥中对身份签名的不可伪造性，其安全模型可以由敌手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的一系列游戏来刻画。

系统建立：$\mathcal{C}$ 运行系统初始化算法，得到系统主密钥 MSK 和公开参数 PP，秘密保存主密钥 MSK，将公开参数 PP 发送给 $\mathcal{A}$。

询问阶段 1：$\mathcal{A}$ 适应性地进行多项式次数的解密私钥提取询问，$\mathcal{A}$ 任意选择身份 ID'、公钥 $P_{ID'}$、加密属性集 $w'\subseteq U$，C 输出解密私钥 $SK_{ID',w'}$。

伪造阶段：$\mathcal{A}$ 输出属性集 w^*、身份 ID^*、公钥 P_{ID^*}、私钥 SK_{ID^*,w^*}，其中要求不能对 w^* 和 ID^* 执行解密私钥提取询问。如果 SK_{ID^*,w^*} 可以通过公开验证算法，则 $\mathcal{A}$ 赢得游戏。

敌手 $\mathcal{A}$ 的优势定义为 $Adv(\mathcal{A})=\Pr[\mathcal{A}\ \mathrm{wins}]$。

3.2.3 公开定责性

公开定责性是基于可追踪性以及解密私钥中用户对部分解密私钥签名的不可伪造性，而签名的不可伪造性可以由敌

手 $\mathcal{A}$ 和挑战者 $\mathcal{C}$ 之间的一系列游戏来刻画。

系统建立：$\mathcal{C}$ 运行系统初始化算法，得到系统主密钥 MSK 和公开参数 PP，秘密保存主密钥 MSK，将公开参数 PP 发送给 $\mathcal{A}$。

询问阶段 1：$\mathcal{A}$ 适应性地进行多项式次数的签名私钥提取询问。$\mathcal{A}$ 任意选择身份 ID'，$\mathcal{C}$ 输出用户的签名私钥 $k_{ID'}$。

伪造阶段：$\mathcal{A}$ 输出加密属性集 w^*、身份 ID^*、公钥 $P_{ID}{}^*$、私钥 SK_{ID^*,w^*}，其中要求不能对 $P_{ID}{}^*$，ID^* 执行签名私钥提取询问。如果 SK_{ID^*,w^*} 可以通过审计算法，则 $\mathcal{A}$ 赢得游戏。

敌手 $\mathcal{A}$ 的优势定义为 $Adv(\mathcal{A})=\Pr[\mathcal{A}\ \text{wins}]$。

4　具体方案

基于 Waters[7] 的密文策略 ABE 方案、Boneh[23] 的短签名方案，本文给出一个可公开定责的属性基加密方案，记为 CP-AABE。

(1)系统初始化：CA 选取素数 p 阶的乘法循环群 (G, G_T)，随机选取群 G 的一个生成元 g，选取一个双线性映射 $e: G\times G\to G_T$，以及两个密码学上安全的 Hash 函数 $H:\{0,1\}^*\to Z_p^*$，$G:\{0,1\}^*\to G$；对属性空间 $U=\{att_1,\cdots,att_\ell\}$，$\ell\in Z_p^*$ 中的每一个属性 $att_i\in U$，随机选取 $x_i\in_R Z_p^*$，并计算 $T_i=g^{x_i}$；随机选取 $g_1\in_R G$，$\alpha,a\in_R Z_p^*$。系统主密钥 $MSK=g_1^\alpha$，公开参数 $PP=(G, G_T, g, e, g_1, e(g_1,g)^a, g^a, \{T_i\}_{att_i\in U}, U, G, H)$。

(2)签名密钥生成：用户 ID 随机选取私钥 $k_{ID}\in Z_p^*$，计算公钥 $P_{ID}=g^{k_{ID}}$。

(3)解密私钥生成：给定用户的身份 ID、公钥 P_{ID} 及加密属性集 $w=\{att_1,\cdots,att_t\}\subset U$，生成用户私钥 $SK_{ID,w}=(ID, \sigma, L, K, \{K_i:\forall att_i\in w\})$。

①CA 随机选取 $\tau\in Z_p^*$，计算部分解密私钥 $L=g^\tau$，将 L 秘密发送给用户(为了实现不可否认性，CA 需要检查对一个用户 ID，不能重复使用两次 $L=g^\tau$)。

②用户 ID 对 L 进行短签名 $\sigma=G(L)^{k_{ID}}$，并将短签名 σ 公开发送给 CA。

③CA 验证等式 $e(\sigma,g)=e(G(L),P_{ID})$ 是否成立，如果成立，则计算其余解密私钥 $K=g_1^{\alpha h}g^{a\tau}$，$K_i=T_i^\tau$，$\forall att_i\in w$，其中 $h=H(L, ID, \sigma, P_{ID})$。

(4)加密：给定消息 M 以及访问结构 $(\mathbf{W},\rho)$，其中 $\mathbf{W}$ 为 $l\times k$ 规模的矩阵，如下生成密文 $CT_{(\mathbf{W},\rho)}=(C, C', C_1,\cdots,C_l, D_1,\cdots,D_l)$。

①随机选取向量 $\vec{v}=(s, y_2,\cdots,y_k)\in(Z_p^*)^k$，对 $i=1,\cdots,l$，计算 $\lambda_{\rho(i)}=\vec{v}\cdot W_i$，其中 W_i 为 $\mathbf{W}$ 的第 i 行；

②随机选取 $r_1,\cdots,r_l\in Z_p^*$，计算：

$C=M\cdot e(g_1,g)^{\alpha s}$，$C'=g^s$

$C_1=g^{a\lambda(1)}T_{\rho(1)}^{-r_1}$，$D_1=g^{r_1}$

$\cdots$

$C_l=g^{a\lambda(l)}T_{\rho(l)}^{-r_l}$，$D_l=g^{r_l}$

(5)解密：给定密文 $CT_{(\mathbf{W},\rho)}$，如果 w 满足解密访问结构 $(\mathbf{W},\rho)$，令 $I=\{i: att_{\rho(i)}\in w\}$，通过秘密重构算法计算 $\{\omega_i\in Z_p\}_{i\in I}$ 使得 $\sum_{i\in I}\omega_i W_i=(1,0,\cdots,0)$，然后计算：$M=C\Big(\frac{(\prod_{i\in I}e(C_i,L)e(D_i,K_{\rho(i)}))^{\omega_i}}{e(C',K)}\Big)^{\frac{1}{h}}$，其中 $h=H(L, ID, \sigma, P_{ID})$。

(6)公开验证：给定用户私钥 $SK_{ID,w}=(ID,\sigma,L,K,\{K_i:\forall att_i\in w\})$，首先验证等式 $e(K,g)=e(g_1,g)^{ah}e(g^a,L)$ 是否成立，若不成立，则返回无效符号 $\perp$；否则验证是否存在 $att_i\in w$，使得等式 $e(K_i,g)=e(L,T_i)$ 成立(这是因为用户可能只泄露部分解密私钥)，若不存在，则输出无效符号 $\perp$，否则输出 ID，即私钥属于用户 ID。

(7)审计：如果用户 ID 否认泄露 $SK_{ID,w}$，第三方审计机构首先对 $SK_{ID,w}$ 进行公开验证，若公开验证不通过，则输出无效符号 $\perp$，验证终止；否则审计机构验证等式 $e(\sigma,g)=e(G(L),P_{ID})$ 是否成立，若成立，则输出有效符号 $\top$，否则输出无效符号 $\perp$。

5　效能分析

5.1　安全分析

定理 1　在判定 q-PBDHE 假设下，CP-AABE 方案在选择模型下是 IND-s-CCA2 安全的。

证明：CP-AABE 方案的机密性可以规约到 Waters[7] 提出的属性基加密方案(记作 W-ABE 方案)的机密性。CP-AABE方案中，为了实现解密私钥身份的公开验证性，在 Waters[7] 的属性基加密方案的基础上进行了一些适应性改变：1)密文中 $C=M\cdot e(g,g)^{\alpha s}$ 用 $C=M\cdot e(g_1,g)^{\alpha s}$ 代替，其中 $g, g_1\in_R G$；2)在密钥部分 $K=g^\alpha g^{a\tau}$ 用 $K=g_1^{ah}g^{a\tau}$ 代替，其中 $h=H(L, ID, \sigma, P_{ID})$。

可以证明如果存在敌手 $\mathcal{A}$ 可以攻破 CP-AABE 方案，那么敌手 $\mathcal{A}$ 可以攻破 W-ABE 方案。定义游戏 0：$\mathcal{A}$ 进行真实的 CP-AABE 方案的机密性游戏；定义游戏 1：除了将密文中 $C=M\cdot e(g_1,g)^{\alpha s}$ 替换为 $C=M\cdot e(g,g)^{\alpha s}$，其余的同游戏 0 相同；定义游戏 2：除了将 $K=g_1^{ah}g^{a\tau}$ 替换为 $K=g^\alpha g^{a\tau}$，其余与游戏 1 相同。易知此时，游戏 2 实际模拟的是 W-ABE 方案的机密性游戏。

由于 $g, g_1\in_R G$ 是随机的生成元，$C=M\cdot e(g_1,g)^{\alpha s}$ 和 $C=M\cdot e(g,g)^{\alpha s}$ 在分布上对 $\mathcal{A}$ 来说是多项式时间不可区分的。因此对 $\mathcal{A}$ 来说游戏 0 和游戏 1 是不可区分的；而又因为 $\tau\in Z_p^*$ 是随机选取的，$K=g_1^{ah}g^{a\tau}=g^{a\tau+s\alpha h}$ 和 $K=g^\alpha g^{a\tau}$ 在随机数 τ 的掩盖下对 A 来说同样是多项式时间不可区分的。因此对 $\mathcal{A}$ 来说游戏 1 和游戏 2 是不可区分的。

因此，如果 W-ABE 是 IND-s-CCA2 安全，那么 CP-AABE 也是 IND-s-CCA2 安全。

定理 2　在 CDH 假设下，AABE 方案中解密私钥的身份满足公开验证性。

证明：CP-AABE 方案中，身份直接作为解密私钥的一部分，可以显示地实现对身份的追踪。此外，CA 对解密私钥中的用户身份进行了签名，解密私钥身份的公开验证性可以由签名的不可伪造性保证。下面证明私钥中对身份的签名在随机预言模型下满足适应性选择消息的存在性不可伪造。

假设 g^b, g^c，其中 $b, c\in_R Z_p^*$，是一个 CDH 实例。挑战者 $\mathcal{C}$ 如下模拟攻击游戏。

系统建立：$\mathcal{C}$ 令 $g_1=g^b$，其他参数正常选取，额外保存 x_i，其中 $i\in 1,\cdots,l$。设置公开参数 $(G, G_T g, e, g_1, e(g_1,g^c),$

g^c,$\{T_x, att_x \in \mathbb{U}\}$,$G$,$H$),其中隐式定义 $MSK=g^{bc}$,$\mathscr{C}$ 也不知道 MSK 的具体值。$\mathscr{C}$ 将公开参数 PP 发送给 $\mathscr{A}$。

询问阶段 1:$\mathscr{C}$ 如下回答 $\mathscr{A}$ 的 Hash 询问、适应性解密私钥提取私钥提取询问。

1)签名密钥生成算法:敌手任意选择身份 ID',$\mathscr{C}$ 随机选取私钥 $k_{ID} \in \mathbb{Z}_p^*$,返回 k_{ID}。

2)Hash 询问:对于第 i 次 $h=H(L, ID, \sigma, P_{ID})$ 询问,$\mathscr{C}$ 随机选择 $h_i \in_R \mathbb{Z}_p^*$,返回 h_i,为了保持回答的一致性,$\mathscr{C}$ 将这些值存储在列表里。

3)解密私钥提取询问:对于第 i 次 ID,P_{ID},$w=\{att_1, \cdots, att_t\}$ 私钥提取询问,$\mathscr{C}$ 随机选取 $\tau_i' \in \mathbb{Z}_p^*$,计算 $L_i=g^{\tau_i'}(g^b)^{-h_i}$,$\mathscr{C}$ 利用签名私钥 k_{ID} 生成 L_i 的签名 σ_i,并计算 $K_i=g^{c\tau_i'}$,$K_{i,j}=g^{x_j\tau_i'}(g^b)^{-x_jh_i}$,$\forall att_j \in w$,其中 h_i 来自 Hash 询问,返回解密私钥 $SK_{ID,w}^i$。解密私钥 $SK_{ID,w}^i$ 相当于设置 $\tau_i=\tau_i'-bh_i$,在敌手看来其与正常生成的私钥分布是不可区分的,且这样生成的解密私钥在形式上是正确的:

$$e(g_1,g)^{ch}e(g^c,L_i)=e(g_1,g)^{ch}e(g^c,g^{\tau_i}(g^b)^{-h_i})$$
$$=e(g^{c\tau_i},g)=e(K_i,g)$$
$$e(K_{i,j},g)=e(g^{x_j\tau_i}(g^b)^{-x_jh_i},g)$$
$$=e(L_i,T_j),\forall att_j \in w$$

伪造阶段:根据分叉引理[24],如果存在适应性选择消息攻击者 $\mathscr{A}$ 以概率 ϵ 伪造合法的签名,那么 $\mathscr{C}$ 可以得到 ID,L,σ,P_{ID},h_1 和 ID,L,σ,P_{ID},h_2,其中 $h_1 \neq h_2$,满足:

$$e(K,g)=e(g_1,g)^{ch_1}e(g^c,L)$$
$$e(K',g)=e(g_1,g)^{ch_2}e(g^c,L)$$

那么有:

$$e(K(K')^{-1},g)e(g_1^{ch_2-ch_1},g)=1$$
$$\Rightarrow K(K')^{-1}g_1^{ch_2-ch_1}=\mathcal{O}$$
$$\Rightarrow g^{bc}=(K^{-1}(K'))^{h_1-h_2}$$

这意味着 $\mathscr{C}$ 可以求解 CDHP。

定理 3 在 CDH 假设下,CP-AABE 方案可以提供用户对拥有解密私钥的不可否认性。

证明:审计中心首先可以通过公开验证算法验证解密私钥 $SK_{ID,w}=(ID,\sigma,L,K,\{K_i:\forall att_i \in w\})$ 是与用户身份 ID 的绑定,并且由定理 2 可知该私钥是 CA 生成。下面只需证明该解密私钥 $SK_{ID,w}$ 不是 CA 非法生成即可。如果 ID 否认,ID 需要提交其私钥 $SK'_{ID,w}=(ID,\sigma,L,K',\{K_i':\forall att_i \in w\})$ 给审计中心进行验证,如果验证成立,由 CA 对身份 ID 的签名及定理 2 证明的不可伪造性,可以判定用户的合法私钥为 $SK'_{ID,w}$,并且可以判定泄露私钥 $SK_{ID,w}$ 不是用户 ID 泄露的而是 CA 非法生成的。这是因为一个部分解密私钥 L,CA 对于每个用户仅使用一次。如果 ID 无法提供其合法私钥,由于其对 L 的短签名以及短签名[23]在 CDH 假设下是存在性不可伪造的,因此用户无法否认该解密私钥是其唯一拥有的。

5.2 效率分析

本小节中,对已有的可追踪的 ABE[20-21]、可定责属性基加密[18]与本文提出的 CP-AABE 方案进行了比较。其中在文献[18]的方案中,恶意用户可以对解密私钥进行变换后再进行非法共享,此时无法追踪到真实的私钥身份,具体变换如下。

文献[18]中解密私钥 d_0,d_1,d_2,d_3,形如:

$d_0=g_2^a(u_0^{ID}u_0^{H(L_1)}\cdots u_0^{H(L_n)}g_3)^r$,$d_1=g^r$,

$d_2=ID$,$d_3=[L_1,\cdots,L_n]$

变换后的解密私钥 d_0',d_1',d_2',d_3',形如:

$d_0'=g_2^a(u_0^{ID+ID'}u_0^{H(L_1)}\cdots u_0^{H(L_n)}g_3)^r$,$d_1'=g^r$,

$d_2'=ID+ID'$,$d_3'=[L_1,\cdots,L_n]$

可以验证变换的私钥是可以通过验证的:

$e(d_0',g)=e(g_2,g_1)e(u_0^{d_2'}u_0^{H(L_1)}\cdots u_0^{H(L_n)}g_3,d_1')$

而变换后的身份是 $d_2'=ID+ID'$,因此无法实现可追踪与定责。

从表 1 可以看出,CP-AABE 方案同时可以实现可追踪性、公开验证性和不可否认性。

表 1 特征比较

方案	白盒可追踪	公开验证性	不可否认性	访问结构
文献[18]	×*	×*	×	AND Gate
文献[20]	√	×	×	LSSS
文献[21]	√	×	×	LSSS
CP-AABE	√	√	√	LSSS

表 2 对可以实现可追踪的 ABE[20-21] 与本文提出的 CP-AABE 方案进行了存储和计算两方面代价的比较。表 2 中,存储代价用群中元素个数表示,计算代价只考虑双线性对运算的个数,其中 WT 表示可踪阶段,PV 代表公开验证阶段,NR 代表审计阶段,$|s|$ 代表私钥相关的属性个数,$|l|$ 代表访问结构矩阵行数,$|I|$ 代表参与解密的属性个数。CP-AABE 方案由于身份嵌入在解密私钥中可以直接实现可追踪,公开验证性也只需要 $2|s|+2$ 次对运算,不可否认性只需要 2 次对运算,而且不需要保存列表[20]或者对称加密私钥[21]等额外的存储代价。

表 2 效率比较

方案	密钥长度	密文长度	解密	WT	PV	NR
文献[20]	$\|s\|+4$	$2\|l\|+3$	$2\|I\|+1$	$2\|s\|+4$	—	—
文献[21]	$2\|s\|+4$	$3\|l\|+3$	$3\|I\|+1$	$4\|s\|+4$	—	—
CP-AABE	$\|s\|+4$	$2\|l\|+2$	$2\|I\|+1$	0	$2\|s\|+2$	2

结束语 针对 ABE 系统中存在的两类私钥滥用问题,提出一个支持任意单调访问结构的密文策略属性基加密方案。该方案可以提供可追踪性,任何第三方可以根据泄露的私钥直接追踪到私钥拥有者的身份;而且,方案可以提供公开定责性,审计中心可以公开判定私钥是用户进行了恶意共享还是中心非法颁发给未授权用户;此外,与可追踪的 ABE 方案[20-21]相比,该方案具有较高的效率。在判定 q-parallel BDHE 困难的假设下,可以证明该方案在选择安全模型下满足 IND-s-CCA2 安全。

参 考 文 献

[1] SAHAI A, WATERS B. Fuzzy identity based encryption [C]// Advances in Cryptology-EUROCRYPT 2005, LNCS 3494. Springer-Verlag, 2005: 457-473.

[2] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data [C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006: 89-98.

[3] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures [C] // Proceedings of ACM Conference on Computer and Communication Security-CCS 2007. ACM Press, 2007: 195-203.

[4] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption [C] // Advances in Cryptology-EUROCRYPT 2010, LNCS 6110. Springer-Verlag, 2010: 62-91.

[5] OKAMOTO T, TAKASHIMA K. Fully secure functional encryption with general relations from the decisional linear assumption [C] // Advances in Cryptology-CRYPTO 2010. Springer-Verlag, 2010: 191-208.

[6] HERRANZ J, LAGUILLAUMIE F, RAFOLS C. Constant-size ciphertext in threshold attribute-based encryption [C] // Proceedings of Public Key Cryptology-PKC 2010, LNCS 6056. Springer-Verlag, 2010: 19-34.

[7] WATERS B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization [C] // Public Key Cryptography- PKC 2011. Springer Berlin Heidelberg, 2011: 53-70.

[8] YAMADA S, ATTRAPADUNG N, HANAOKA G, et al. Generic constructions for chosen ciphertext secure attribute based encryption [C] // Proceedings of Public Key Cryptology- PKC 2011, LNCS 6571. Springer-Verlag, 2011: 71-89.

[9] LEWKO A, WATERS B. New proof methods for attribute-based encryption: achieving full security through selective techniques [C] // Advances in Cryptology-CRYPTO 2012, LNCS 7417. Springer-Verlag, 2012: 180-198.

[10] HOHENBERGER S, WATERS B. Attribute based encryption: with fast decryption [C] // Proceedings of Public Key Cryptology-PKC 2013. Springer-Verlag, 2013: 162-179.

[11] ROUSELAKIS Y, WATERS B. Practical constructions and new proof methods for large universe attribute-based encryption [C] // Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security. ACM, 2013: 463-474.

[12] NARUSE T, MOHRI M, SHIRAISHI Y. Attribute-based encryption with attribute revocation and grant function using proxy re-encryption and attribute key for updating [M] // Future Information Technology. 2014: 119-125.

[13] QIAN H, LI J, ZHANG Y, et al. Privacy Preserving Personal Health Record Using Multi-Authority Attribute-Based Encryption with Revocation [J]. International Journal of Information Security, 2015, 14(6): 487-497.

[14] ZHANG K, GONG J, TANG S, et al. Practical and Efficient Attribute-Based Encryption with Constant-Size Ciphertexts in Outsourced Verifiable Computation [C] // Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016: 269-279.

[15] SHI Y, ZHENG Q, LIU J, et al. Directly revocable key-policy attribute-based encryption with verifiable ciphertext delegation [J]. Information Sciences, 2015, 295: 221-231.

[16] HINEK M J, JIANG S, SAFAVI-NAINI R, et al. Attribute-based encryption with key cloning protection [J]. Bulltein of the Korean Mathematical Society, 2008, 2008(4): 803-819.

[17] YU S, REN K, LOU W, et al. Defending against key abuse attacks in KP-ABE enabled broadcast systems [C] // Security and Privacy in Communication Networks. Springer Berlin Heidelberg, 2009: 311-329.

[18] LI J, REN K, KIM K. A2BE: Accountable attribute-based encryption for abuse free access control [EB/OL]. [2009-03-11]. http://eprint.iacr.org/2009/118.

[19] KATZ J, SCHRODER D. Tracing insider attacks in the context of predicate encryption schemes [EB/ OL]. https:// www.usukita.org/node/1779.

[20] LIU Z, CAO Z, WONG D S. White-box traceable ciphertext-policy attribute-based encryption supporting any monotone access structures [J]. IEEE Transactions on Information Forensics and Security, 2013, 8(1): 76-88.

[21] NING J, DONG X, CAO Z, et al. White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Flexible Attributes [J]. IEEE Transactions on Information Forensics and Security, 2015, 10(6): 1274-1288.

[22] ZHANG X, JIN C, WEN Z, et al. Attribute-Based Encryption without Key Escrow [C] // Cloud Computing and Security 2015, LNCS 9483. Springer-Verlag, 2015: 74-87.

[23] BONEH D, LYNN B, SHACHAM H. Short signatures from the Weil pairing [C] // Advances in Cryptology—ASIACRYPT 2001. Springer Berlin Heidelberg, 2001: 514-532.

[24] POINTCHEVAL D, STERN J. Security arguments for digital signatures and blind signature [J]. Journal of Cryptology, 2000, 13(3): 361-396.

（上接第 124 页）

[9] SWEENEY L. Achieving k-anonymity privacy protection using generalization and suppression [J]. International Journal on Uncertaint, Fuzziness and Knowledge-based Systems, 2002, 10(5): 571-588.

[10] LU W T, MIKLAU G, GUPTA V. Generating private Synthetic Databases for Untrusted System Evaluation [C] // Proceedings of the 30th International Conference on Data Engineerin (ICDE). Washington, USA, 2014: 654-663.

[11] DWORK C. Differential privacy in new settings [C] // Proc. Symposium on Discrete Algorithms (SODA), Society for Industrial and Applied Mathematics. 2010: 174-183.

[12] DWORK C. A firm foundation for private data analysis [J]. Communications of the ACM, 2011, 54(1): 86-95.

[13] XIAO X K, WANG G Z, GCHRKE J. Differential privacy via wavelet transforms [J]. IEEE Transactions on Knowledge and Data Engincering, 2011, 23(8): 1200-1214.

[14] NERGIZ M E, CLIFTON C, NERGIZ A E. Multirelational k-anonymity [J]. IEEE Trans on Knowledge and Data Engineering, 2009, 21(8): 1104-1117.

[15] Releasing Differentially Private DataCubes for Health Information [C] // Proceedings of the 28th International Conference on Data Engineerin (ICDE). Washington, USA, 2012: 1305-1308.

[16] HECKERMAN D. MSNBC [EB/OL]. (1999-09-28). http://archive.ics.uci.edu/ml/datasets.

[17] Frequent itemset mining dataset repository [OL]. http://fimi.ua.ac.be/data.