可高效撤销的属性基加密方案

李学俊，张丹，李晖
（西安电子科技大学网络与信息安全学院，陕西 西安 710071）

摘 要：在现有的解决方案中，基于时间的方案难以实现即时撤销，基于第三方的方案往往需要重加密运算，计算量大，不适用于海量密文数据。针对该问题，提出了一种高效的支持用户和属性级别的即时撤销方案，所提方案基于经典的 LSSS 型访问结构的 CP-ABE，引入了 RSA 密钥管理机制和属性认证思想，借助半可信第三方，在解密之前对用户进行属性认证。与现有的撤销方案对比，所提方案只需半可信第三方更新 RSA 属性认证密钥，不需要用户更新密钥且不需要重加密密文，极大地减少了撤销带来的计算量和通信量，同时保证了抗串谋攻击和前后向安全性。安全性分析和实验仿真证明，所提方案具有更高的撤销效率。

关键词：密文−策略属性基加密机制；属性撤销；RSA 密钥管理；多机构；计算开销小
中图分类号：TN918
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019150

Efficient revocable attribute-based encryption scheme

LI Xuejun, ZHANG Dan,LI Hui
School of Cyber Engineering, Xidian University, Xi’an 710071,China

Abstract: In the existing solutions, the time-based scheme is difficult to achieve immediate revocation, and the third-party-based scheme often requires re-encryption, which needs large amount of calculation and doesn’t apply to massive data. To solve the problem, an efficient and immediate CP-ABE scheme was proposed to support user and attribute levels revocation. The scheme was based on the classic LSSS access structure, introducing RSA key management mechanism and attribute authentication. By means of a semi-trusted third party, the user could be authenticated before decryption. Compared with the existing revocation schemes, The proposed scheme didn’t need the user to update the key or re-encrypt the ciphertext. The semi-trusted third party wasn’t required to update the RSA attribute authentication key. The scheme greatly reduced the amount of computation and traffic caused by revocation, while ensuring anti-collusion attacks and forward and backward security. Finally, the security analysis and experimental simulation show that the scheme has higher revocation efficiency.

Key words: CP-ABE, attribute revocation, RSA key management, multi-authority, less computation

1 引言

随着社会与科技的发展，人们越来越多地希望能跨平台、跨地理位置地访问或修改数据，对外部数据云存储的需求前所未有的高涨。然而，将具有不同敏感级别的数据，存储在外部云存储服务器上，为人们带来便利好处的同时，也带来了安全问题[1]。

首先，大量数据托管存储在第三方营运的大型云端数据中心，而云端服务器并不完全可信，且数据的敏感程度不同，因此需要使用属性基加密 ABE（attribute-based encryption）方案加密数据，实现高

收稿日期：2019–03–22；修回日期：2019–05–02
基金项目：国家重点研发计划基金资助项目（No. 2018YFB0804701）；国家自然科学基金资助项目（No.61572460）
Foundation Items: The National Key Research and Development Project of China(No. 2018YFB0804701), The National Natural Science Foundation of China(No. 61572460)

效的细粒度访问控制[2]。其次，对敏感数据的访问并非一成不变，比如接入云端存储服务器的各类设备数量众多，计算能力弱，且往往因随机动态变化引起属性频繁的变化，因此需要实现高效的属性撤销机制，并尽可能减少终端的计算量。

2011 年，Waters[3]首次提出基于线性秘密共享方案（LSSS, linear secret sharing scheme）型访问结构的 CP-ABE 方案(ciphertext-policy ABE)。相较于树型访问结构，LSSS 型访问结构更灵活，且解密效率更高。但该方案只有一个可信中央机构 CA(central authority)，由其管理所有用户的属性和密钥分发工作，工作量巨大，影响系统效率。

在属性基加密方案中，用户和属性往往是一对多或多对一的关系，复杂度较高，这增加了属性撤销机制的研究难度。为了实现属性撤销，一些可撤销的 ABE 方案被提出[4]，但这些方案均未能实现属性的即时撤销。Luan 等[5]引入属性撤销列表和在线第三方，第一次实现了属性的即时撤销。现有的基于第三方的属性撤销都能实现即时撤销，主要方法有以下几种：基于版本号和代理重加密[6-10]、基于属性群和 KEK（key encryption key）树[11-12]、基于中国剩余定理[13]等。Wu 等[7]通过版本号和代理重加密技术实现属性撤销，利用版本号记录系统主密钥的演化过程，并将此版本号和系统密钥、用户密钥和重加密密文进行关联，撤销操作发生后，授权机构将系统版本号加 1，可信第三方需更新所有与版本号相关的密钥和密文。Li 等[12]通过改进 Hur[11]的方案，基于属性群和 KEK 树及半可信第三方为每个属性生成相应的属性群密钥，对密文进行重加密，并生成头部信息发送给用户，撤销用户由于不能恢复属性群密钥，不能正确解密。但该方案中 KEK 树的总节点会随着用户数量的增多而增多，高度的增长也会导致用户路径密钥的增长。同时该方案仍需更新撤销属性的属性群密钥，需要重加密密文。强衡畅等[13]引入中国剩余定理求解同余式方程组的方法，替换了求解 KEK 树上包含属性群所有用户的最小子树，使得密 KEK 的时间复杂度降到常数阶。但该方案仍需更新属性群密钥，重加密密文。

综上所述，基于可信或半可信第三方实现 CP-ABE 方案的撤销机制，大多数工作集中在密钥更新和撤销信息通过重加密嵌入到密文中。面对海量数据如何降低计算量，有学者[14-15]通过引入多项式秘密共享和广播撤销技术实现撤销。由于多项式的阶是固定的，限制了每个属性的撤销用户上限，同时秘密值的求解时间也与多项式的选取有关。

本文将构造一种基于半可信第三方、可高效撤销的属性基加密方案（以下简称本文方案），该方案不需要用户更新密钥和重加密密文，能够实现用户属性撤销及用户撤销。本文主要工作与创新点如下：1) 构造了一种基于半可信第三方的多机构 CP-ABE 方案，方案中使用云存储服务器兼任半可信第三方，可降低系统通信开销；2)引入 RSA 密钥管理机制实现属性认证，为每个属性分配一对 RSA 密钥。用户在撤销某个属性或撤销用户时，只需要更新 RSA 属性认证密钥即可，不需要更新密文，且密钥更新的计算量很少，极大地降低了撤销引起的计算量；3) 在实现撤销机制的同时，保证了与文献[3]同样的安全程度，并基于判定性 q 阶双线 DH 指数（q-BDHE, decisional q-parallel Bilinear Diffie Hellman exponent）假设证明了安全性，同时保证了抗串谋攻击和前后向安全性。

2　相关知识

2.1　线性秘密共享方案

假设有共享方案$\prod$，包含 P 个实体用户，若方案$\prod$满足下列条件，则称其是线性秘密共享方案[16]。

1) 域 Z_P 中的向量可以表示每个实体所拥有的秘密份额。

2) 对于每个共享方案$\prod$，都存在一个 l 行 n 列的共享生成矩阵 $\boldsymbol{M}$。$\rho(i)$ 表示将矩阵的第 i 行映射为某一实体，$i=1,2,\cdots,l$。随机选取 $s,r_2,\cdots,r_n\in Z_P$，共享，构造向量 $\boldsymbol{v}=(s,r_2,\cdots,r_n)$，那么实体用户拥有的秘密定义为 $\lambda_i=(\boldsymbol{Mv})_i$。

上述定义的线性秘密共享方案满足线性重构性质，设有一种 LSSS 方案$\prod$，S 为合法的授权集。定义 $I=\{i:\rho(i)\in S\}$ 且 $I\subset\{1,2,\cdots,l\}$，即表示 $\boldsymbol{M}$ 中与属性有关的行。假设 $\{\lambda_i\}$ 能有效分享 s，那么最终一定能够找到常数集合 $\{w_i\}$ 满足 $\sum w_i\lambda_i=s$。

2.2　密钥管理

令 Z_N 为模 $N=pq$ 的等价类，其中 p 和 q 是大素数，且 $p\neq q$。对任意非零元素 $a\in Z_N$，gcd(a,N)=1 成立，当且仅当 a 存在一个乘法逆元 b，即 $ab\equiv1(\bmod N)$。

首先为系统属性集中的每个属性 x_i 选择安全

的素数 $p_i, i=1,2,\cdots,N$，并且满足 $\gcd(p_i,\varphi(N))=1$，然后计算 q_i 使 $p_i q_i \equiv 1(\mathrm{mod}\varphi(N))$。假设 $\{N,p_1,p_2,\cdots,p_N\}$ 是公开参数，$\{\varphi(N),q_1,q_2,\cdots,q_N\}$ 是私有参数。

选择随机数 h 满足 $2<h<N-1$，并且 $\gcd(h,N)=1$。计算 $K_A=h^{d_A}(\mathrm{mod}\,N)$ 与用户的属性集 A 相关，计算 $K_P=h^{d_P}(\mathrm{mod}\,N)$ 与访问结构中的属性集 P 相关。其中，$d_A=\prod_{i=1}^{N}q_i^{a_i}$，当 $x_i\in A$ 时，$a_i=1$；当 $x_i\notin A$ 时 $a_i=0$。同样，$d_P=\prod_{i=1}^{N}q_i^{b_i}$，当 $x_i\in P$ 时，$b_i=1$；当 $x_i\notin P$ 时 $b_i=0$。

属性集 A 包含访问结构中的属性集 P，当且仅当 $\frac{e_A}{e_P}$ 是一个整数[17]，其中，$e_A=\prod_{i=1}^{N}p_i^{a_i}$，$e_P=\prod_{i=1}^{N}p_i^{b_i}$，且有 $K_P=K_A^{\frac{e_A}{e_P}}(\mathrm{mod}\,N)$。

3 方案描述

3.1 方案背景与系统框架

本文将物联网技术与车辆维修管理相结合，构造了一个车辆维修管理系统[18]。传统维修过程中，车辆在维修时，由于维修本身所具有的私密性，无法保证车主对维修人员的相关行为实施监督，因此营运车辆维修质量得不到充分的保障。本文构造的车辆维修管理系统首先记录车辆的车牌号、车主等基本信息及维修类别和接车员。车辆进入维修区域后，系统使用无线射频技术收集维修数据，记录现场维修人员和负责人的信息及维修工作。维修完成后进行车辆性能检测，记录检测信息，形成车辆电子维修档案。因此车主、交通运输管理部门、维修企业、检测机构均可共享车辆维修信息，车主还可在线监督维修过程，维修人员可提供远程维修指导等，极大地方便了生活。

实现上述系统必须解决以下问题[19]：1) 系统中的电子维修档案存储在云端服务器，但云服务器一般是不可信的，且数据的敏感程度不同，因此需要使用 ABE 加密数据；2)物联网具有实时性、动态性等特点，终端节点会频繁动态地变化，且用户共享属性。如果一个用户撤销了某个属性，其他用户对撤销属性的使用也会受到影响， 因此必须实现高效的属性撤销机制。

如图 1 所示，车辆维修管理系统共有 6 个实体，分别如下。

1) 可信中央授权机构 CA，负责为系统中的用户发布唯一的身份标识 uid，为 AA（attribute authority）发布唯一的身份标识 aid；生成系统公共参数，完全可信。

2) k 个属性授权机构 AA，负责生成用户的属性私钥，部分 AA 可能被腐化。

3) 云存储服务器 CSS（cloud storage server），负责存储 TU（terminal user）上传的数据密文。CSS 是半可信的，它有可能会窥探用户数据，但是会严格执行 CA 分发的工作。

4) 半可信第三方 SM（semi-trusted mediator），负责用户的属性认证。用户访问密文时，SM 首先认证用户是否拥有访问结构中的全部属性，方案中使用 CSS 兼任半可信第三方。

5) 终端用户 TU，表示系统接入设备，其加密消息会上传至 CSS。

6) 数据用户 DU（data user），当且仅当在 SM 处认证通过并满足访问结构的用户才能得到预解密密钥。

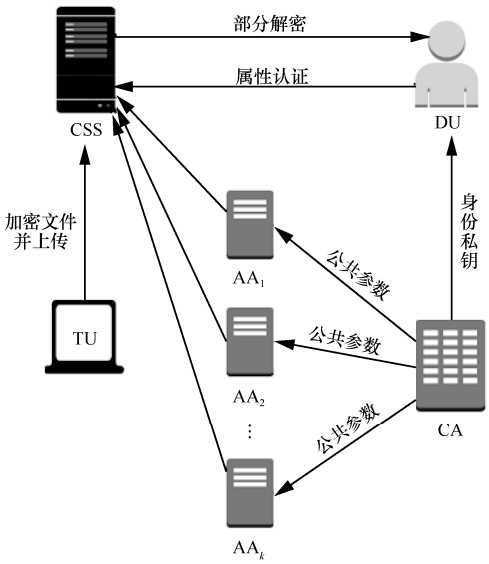

图 1 车辆维修管理系统框架

3.2 方案概述

设 G 和 G_T 为阶为素数 p 的双线性群，e 为双线性映射 $e:G\times G\to G_T$，g 为生成元，$H:\{0,1\}^*\to G$ 为安全的散列函数。用户集用 $U=\{u_1,u_2,\cdots,u_T\}$ 表示，系统属性集用 $A=\{x_1,x_2,\cdots,x_N\}$ 表示，每个用户的属性空间为 $\Lambda=\{x_1,x_2,\cdots,x_n\}$。设共有 k 个属性

管理中心，属性集合中的属性分 k 个不相交的集合。

1) 系统建立阶段

$\mathrm{CASetup}(\lambda)\to\{\mathrm{Pk},\mathrm{MK},\mathrm{uid},\mathrm{aid}\}$。CA 给每个授权机构分发唯一的身份标识 aid，给每个用户唯一的身份标识 uid。CA 选择素数 p 且 $p\neq q$，计算 $N=pq$，为每个属性选择随机数 p_i 使 $(p_i,\varphi(N))=1$，计算 q_i 满足 $p_iq_i\equiv1(\mathrm{mod}\ \varphi(N))$，$i=1,2,\cdots,N$。选择随机数 h 使 $2<h<N-1$，且满足 $\gcd(h,N)=1$。CA 再随机选择 $\alpha,\beta,a\in Z_P$ 作为主密钥，生成系统公私钥对，如式(1)和式(2)所示。

$$\mathrm{MK}=(\alpha,\beta,a,p,q,q_1,q_2,\cdots,q_N,h) \tag{1}$$

$$\mathrm{PK}=\left(g,g^a,e(g,g)^{\alpha},N,p_1,p_2,\cdots,p_N\right) \tag{2}$$

2) 用户身份私钥生成阶段

$\mathrm{IDKeyGen}(\mathrm{MK},\mathrm{uid})\to\mathrm{SK}_{\mathrm{uid}}$。CA 为每个用户选择随机数 $t_u\in Z_P$，根据每个用户拥有的属性计算 $D_{\mathrm{uid}}=h^{d_{\mathrm{uid}}}$，$d_{\mathrm{uid}}=\prod_{x_i\in\Lambda}q_i$。CA 根据系统属性计算 $D_A=h^{d_A}$，$d_A=\prod_{x_i\in A}q_i$。输出用户身份私钥

$$\mathrm{SK}_{\mathrm{uid}}=(S_0=t_u,S_1=g^{\frac{\alpha}{t_u}}g^{\frac{\alpha\beta}{t_u}},S_2=g^{\frac{\beta}{t_u}},D_{\mathrm{uid}},D_A) \tag{3}$$

3) 用户属性私钥生成阶段

$\mathrm{AttrKeyGen}(\mathrm{MK},\mathrm{aid},\mathrm{uid},\mathrm{SK}_{\mathrm{uid}},\Lambda)\to\mathrm{SK}_{\mathrm{aid,uid}}$。每个 AA 运行该算法，对每个用户拥有的属性 x_i 判断其是否为 $\mathrm{AA}_{\mathrm{aid}}$ 管理，生成用户属性私钥，用 $\mathrm{SK}_{\mathrm{aid,uid}}$ 表示 $\mathrm{AA}_{\mathrm{aid}}$ 中拥有用户 u_{uid} 的属性，则

$$\mathrm{SK}_{\mathrm{aid,uid}}=\{\forall x_i\in S_{\mathrm{aid,uid}}:K_{x_i,\mathrm{uid}}=H(x_i)^{\frac{\beta}{t_u}}\} \tag{4}$$

CA 通过安全通道将 S_0 发给每个用户，将 S_1、S_2、D_A 和每个用户的 D_{uid} 发给云存储服务器，每个 AA 将 $\mathrm{SK}_{\mathrm{aid,uid}}$ 也发给云存储服务器用于部分解密。

4) 加密明文

$\mathrm{Encrypt}(\mathrm{PK},(M,\rho),m)\to\mathrm{CT}$。终端对明文 m 随机选取一对对称密钥 k_m，用 k_m 和安全的对称加密算法加密 m 得到 $C_m=E_{k_m}(m)$。

设访问结构 LSSS 矩阵 $(\boldsymbol{M},\rho(i))$，$\boldsymbol{M}$ 是 $l\times n$ 矩阵，其中，l 代表属性数量，函数 $\rho(i)$ 是第 i 行与相应属性的映射函数。随机选择一个加密的秘密 $s\in Z_P$，随机向量 $\boldsymbol{v}=(s,y_2,y_3,\cdots,y_n)\in Z_P^n$，其中 $y_2,y_3,\cdots,y_n$ 用来分享秘密 s。对于 $i=1,2,\cdots,l$，计算 $\lambda_i=\boldsymbol{v}\boldsymbol{M}_i$，其中 $\boldsymbol{M}_i$ 是矩阵 $\boldsymbol{M}$ 的第 i 行。然后随机选择 $r_1,r_2,\cdots,r_l\in Z_P$，输入 PK，利用 $(\boldsymbol{M},\rho(i))$ 加密 k_m 得到密文（设访问结构中用到的属性集记为 P），如式(5)所示。

$$\mathrm{CT}=\begin{cases}(\boldsymbol{M},\rho(i)),C=k_me(g,g)^{\alpha s},C'=g^s\\ e_P=\prod_{x_i\in P}p_i\\ (C_i=g^{a\lambda_i}H(\rho(i))^{-r_i},D_i=g^{r_i})_{i=1,2,\cdots,l}\end{cases} \tag{5}$$

5) 属性认证

$\mathrm{IDAuth}(\mathrm{uid},\Lambda)$。用户发送自己的身份标识 uid 和属性列表即 (uid,Λ) 给云存储服务器进行属性认证。

服务器用从 CA 处得到的用户私钥 D_{uid} 和密文中的 e_P 及用户发送的属性列表为用户计算 K_{uid} 值，即

$$K_{\mathrm{uid}}=(D_{\mathrm{uid}})^{\frac{e_{\mathrm{uid}}}{e_P}}=h^{d_{\mathrm{uid}}\cdot\frac{e_{\mathrm{uid}}}{e_P}}=h^{d_p}$$

其中，$d_{\mathrm{uid}}=\prod_{x_i\in\Lambda}q_i$，$e_{\mathrm{uid}}=\prod_{x_i\in\Lambda}p_i$，$e_P=\prod_{x_i\in P}p_i$，$d_P=\prod_{x_i\in P}q_i$。

服务器再用从 CA 处得到的 D_A 和密文中的 e_P 及系统所有属性集 A 进行如下计算。

$$K_A=D_A^{\frac{e_A}{e_P}}=h^{d_A\cdot\frac{e_A}{e_P}}=h^{d_P}$$

其中，$d_A=\prod_{x_i\in A}q_i$，$e_A=\prod_{x_i\in A}p_i$。

服务器将 2 次计算的结果进行比较，若相等说明用户拥有访问结构中的所有属性，则使用 uid 的属性私钥为用户进行部分解密；若不相等则输出 $\perp$。

6) 预解密

$\mathrm{ProxyDec}(\mathrm{CT},S_1,S_2,K_{x_i,\mathrm{uid}})\to A$。用户认证成功后，云存储服务器为用户进行预解密。定义 $I=\{i:\rho(i)\in S\}$，服务器选择一组常量 $w_i\in Z_P$ 使 $\sum_{i\in I}w_i\lambda_i=s$，其中 λ_i 是根据访问结构 $\boldsymbol{M}$ 计算出的。

$$A=\frac{e(C',S_1)}{\prod_{i\in I}\left(e(C_i,S_2)e(D_i,K_{x_i,\mathrm{uid}})\right)^{w_i}}=e(g,g)^{\frac{\alpha s}{t_u}} \tag{6}$$

7) 用户解密

$\mathrm{UserDec}(\mathrm{CT},A,S_0,C_{\boldsymbol{M}})$。用户计算 $k_m=\frac{C}{A^{t_u}}$，再用 k_m 解密 $C_{\boldsymbol{M}}=E_{k_m}(m)$ 即可得到明文 m。

8) 用户撤销

$\mathrm{UserRev}(\mathrm{uid},L_{K_{x_i,\mathrm{uid}}})\to L'_{K_{x_i,\mathrm{uid}}}$。若要撤销某个

用户 uid，不需要更新其他用户的密钥和密文，只需要删除该用户在云存储服务器上的属性密钥即可。一旦 uid 的属性私钥被删除，服务器就不能为该用户进行部分解密工作，该用户也不能解密得到明文。

9) 属性撤销

$\mathrm{AttrRev}\left(x_j\right)\rightarrow\left(q_j^{'},D_A^{'},D_{\mathrm{uid}}^{'}\right)$。当用户 uid 撤销或添加某一属性 x_j 时，CA 更新用户 uid 的属性并发送给用户，为该属性计算新的 $q_j^{'}$，然后重新计算

$$D_A^{'}=h^{d_A^{'}},d_A^{'}=\prod_{x_i\in A,i\neq j}q_iq_j^{'}$$

CA 为该用户和其他拥有该属性但未撤销的用户重新计算 $D_{\mathrm{uid}}^{'}=h^{d_{\mathrm{uid}}^{'}}$，$d_{\mathrm{uid}}^{'}=\prod_{x_i\in\Lambda,i\neq j}=q_iq_j^{'}$ 发给云存储服务器。

用户 uid 在属性认证时，若云存储服务器用新的 $D_{\mathrm{uid}}^{'}$ 和 $D_A^{'}$ 的计算结果不相等，则不能认证成功，其他未撤销属性 x_j 的用户则可以认证通过，从而得到预解密密钥。

4 安全性分析

4.1 选择明文安全性

定理 1 假定 q-BDHE 问题是困难的，敌手的挑战访问结构是 $\left(\boldsymbol{M}^*,\rho^*\right)$，$\boldsymbol{M}^*$ 是 $l^*\times n^*$ 的矩阵且 l^*、$n^*\leqslant q$，则不存在多项式时间的敌手能选择明文攻破本方案。

证明 采用反证法，假设存在概率多项式时间（PPT, probabilistic polynomial time）的敌手 $\mathcal{A}$，能够在安全模型下以不可忽略的优势 $\varepsilon=\mathrm{Adv}\left(\mathcal{A}\right)$ 攻破方案，假设敌手$\mathcal{A}$选择一个行列数都不超过 q 的矩阵 $\boldsymbol{M}^*$，构造一个模拟器 $\mathcal{B}$ 以不可忽略的优势解决 q-BDHE 问题。

建立 模拟器 $\mathcal{B}$ 随机选取 $\alpha'\in Z_p$，对每个属性 x_i选择一个随机数 z_x，模拟器 $\mathcal{B}$ 按如下规则设计 H。

如果 $X\neq\phi$，$H\left(x\right)=g^{z_x}\prod_{i\in X}g^{\frac{aM_{i,1}^*}{b_i}}g^{\frac{a^2M_{i,2}^*}{b_i}}\cdots g^{\frac{a^{n^*}M_{i,n^*}^*}{b_i}}$；如果 $X=\phi$，$H\left(x\right)=g^{z_x}$。

阶段 1 在该阶段模拟器 $\mathcal{B}$ 响应敌手$\mathcal{A}$的密钥询问。敌手$\mathcal{A}$发送(uid,s_{aid})给模拟器 $\mathcal{B}$ 进行询问，模拟器 $\mathcal{B}$ 选择随机数 $r\in Z_p$，计算 $S_2=g^{\frac{t}{r}}\prod_{i=1,\cdots,n^*}(g^{a^{q+1-i}})^{\frac{t}{w_i}}=g^{\frac{t}{\beta}}$；$S_1=g^{\frac{\alpha'}{t}}g^{\frac{a\beta}{t}}\prod_{i=2,\cdots,n^*}(g^{a^{q+2-i}})^{\frac{t}{w_i}}$。

如果属性在访问结构中没有用到，则令 $K_x=S_2^{z_x}$。对于访问结构中出现的属性，计算 K_x 如式(7)所示。

$$K_x=S_2^{z_x}\prod_{i\in X}\prod_{j=1,\cdots,n^*}\left(g^{\left(\frac{a^j}{b_i}\right)\beta}\prod_{k=1,\cdots,n^*,k\neq j}\left(g^{\frac{a^{q+1+j-k}}{b_i}}\right)^{w_k}\right)^{\frac{M_{i,j}^*}{t}}\tag{7}$$

挑战 敌手$\mathcal{A}$给模拟器模拟器 $\mathcal{B}$ 提供 2 个等长的消息 m_0和m_1，模拟器 $\mathcal{B}$ 掷一枚硬币查看结果 $b\in\{0,1\}$，返回对消息 m_b 的加密密文，如式(8)所示。

$$C=m_bTe\left(g^s,g^{\alpha'}\right),C'=g^s,\ D_i=g^{-r_i^{'}}g^{-sb_i}$$

$$C_i=H(\rho^*(i))^{r_i^{'}}*\left(\prod_{j=2,\cdots,n^*}(g^a)^{M_{i,j}^*y_j^{'}}\right)(g^{b_iS})^{-z_{\rho^*(i)}}\cdot\left(\prod_{k\in R_i}\prod_{j=1,\cdots,n^*}(g^{\frac{a^jsb_i}{b_k}})^{M_{k,j}^*}\right)\tag{8}$$

阶段 2 重复阶段 1。

猜测 敌手$\mathcal{A}$提交对 b 的猜测 b'。如果 T 是有效的元组，那么模拟器 $\mathcal{B}$ 做出了准确模拟，则式(9)所示的等式成立。

$$\Pr\left[\mathcal{B}\left(\vec{y},T=e\left(g,g\right)^{a^{q+1}s}\right)=0\right]=\frac{1}{2}+\mathrm{Adv}\left(\mathcal{A}\right)\tag{9}$$

如果 T 是群 G_T 中的一个随机元素，则称消息 m_b 对敌手是隐藏的，并且有 $\Pr[\mathcal{B}\left(\vec{y},T=R\right)=0]=\frac{1}{2}$，故有

$$\left|\Pr\left[\mathcal{B}\left(\vec{y},T=e\left(g,g\right)^{a^{q+1}s}\right)=0\right]-\Pr\left[\mathcal{B}\left(\vec{y},T=R\right)=0\right]\right|=\varepsilon\tag{10}$$

即模拟器 $\mathcal{B}$ 能够以一个不可忽略的优势解决 q-BDHE 问题，但是这一问题已被证明是困难的，所以假设不成立，从而证明方案达到了选择明文安全性，证毕。

4.2 抗串谋攻击

本文方案中为每个用户分配一个唯一的身份标识 uid，从不同属性管理中心获得的属性私钥通过该 uid 绑定。当多个用户合谋攻击时，即使属性集满足访问结构，若不同用户的身份标识不同，服务器只寻找认证用户的 uid 的私钥进行部分解密，因此多个用户共谋也不能得到预解密密文。

4.3 前向安全性和后向安全性

当撤销/添加用户，或用户撤销/添加某个属性时，方案保证了前向安全性和后向安全性。当某一用户的属性被撤销时，CA 为该属性计算新的 q_j，并为该用户和其他拥有该属性但未撤销的用户更新 D_{uid} 发给服务器。因此撤销属性的用户在下一次进行属性认证时，服务器用更新后的 D_{uid} 进行计算，若与 D_A 计算的结果不相等则不能认证成功，从而撤销属性的用户不能解密密文，因此前向安全性得到保证。另一方面，当系统新加入用户或者用户添加某个属性，服务器利用更新的 D_{uid} 计算的结果能通过身份认证，从而用户可以得到部分解密结果进而解密得到密文，因此后向安全性得到保证。

5 性能分析

方案性能评估从理论分析和实验仿真两方面进行[20]。理论分析方面，将本文方案与经典的撤销方法版本号、KEK 树和中国剩余定理进行对比，分析各方案的存储开销、通信开销和计算开销，得到结果列表；实验仿真方面，在相同环境中进行实验仿真，分析密文密钥更新时间随着撤销属性个数增长所需要的时间，得到结果图。

在进行性能评估时，$|G|$ 和 $|G_T|$ 分别代表群 G 和 G_T 中数据元素长度；$|P|$ 代表域 Z_p 中数据元素长度；$|C_K|$ 代表 KEK 密钥长度；n_a 代表系统中的属性个数；n_c 代表密文中的属性个数；n_r 代表撤销属性的个数；$n_{a,u}$ 代表用户拥有的属性个数；E 和 E_T 分别代表模指数和双线性对运算；E_N 代表模乘运算。

5.1 理论分析

比较各方案的功能、存储开销、通信开销和计算开销时，由于存储开销与用户的私钥长度有关，通信开销与密文长度有关，只需要对比各方案的密文长度和私钥长度；计算开销主要对比因撤销引起的密文密钥更新的计算量。由于用户使用移动终端资源有限，因此方案用户私钥应越短越好，又由于在海量数据环境下，撤销引起的更新计算量也应越小越好。

从表 1 可以看出，在存储开销方面，上述对比方案的用户私钥长度都与用户属性个数相关。文献[11]方案和文献[12]方案使用 KEK 树方法实现撤销，因此需要存储额外的 KEK 密钥长度 $|C_K|$。文献[17]方案和文献[19]方案使用版本号实现撤销，文献[13]方案使用中国剩余定理失效撤销由于这些私钥需要在用户本地存储，因此会给用户带来巨大的存储开销，不适合移动终端的使用环境。与上述方案不同，本文方案中引入半可信第三方，通过外包解密将用户的一部分私钥委托给第三方保存并解密，用户本地只需存储一个|P|长度的私钥，极大地减轻了用户存储的负担。在通信开销方面，本文方案在密文长度上比文献[7]方案、文献[12]方案小了 n_c 个 $|G|$ 群元素长度，与文献[11]方案、文献[13]方案相比只增加了一个可以忽略不计的整数项便实现了高效的属性撤销，因此本文方案在实现撤销功能的同时并没有增加通信开销。

表 1　存储开销和通信开销性能对比

方案	存储开销	通信开销
NEDAC-MACS[7]	$(n_{a,u}+2)\|G\|+\|P\|$	$\|G_T\|+(3n_c+2)\|G\|$
UR-CP-ABE[9]	$(2n_{a,u}+4)\|G\|+2\|P\|$	$\|G_T\|+(2n_c+4)\|G\|$
KEK-CP-ABE[11]	$(2n_{a,u}+1)\|G\|+\|C_K\|$	$\|G_T\|+(2n_c+1)\|G\|$
AR-CP-ABE[12]	$(3n_{a,u}+1)\|G\|+\|C_K\|$	$\|G_T\|+(3n_c+1)\|G\|$
CRT-CP-ABE[13]	$(2n_{a,u}+1)\|G\|+3$	$\|G_T\|+(2n_c+1)\|G\|$
本文方案	$\|P\|$	$\|G_T\|+(2n_c+1)\|G\|+1$

在比较计算开销时，由于群 G 和 G_T 上模乘运算开销远远小于模指数运算和双线性对运算开销，因此计算开销主要考虑群 G 和 G_T 上的模指数和双线性对运算。由于方案重点在于实现属性撤销功能，以下主要对比属性撤销后，密钥更新和密文更新这两阶段的计算开销。

由表 2 可看出，文献[7]方案和文献[9]方案使用版本号实现撤销，当有属性撤销时，AA 为该属性选择新的版本号，因此需要更新用版本号标记的所有相关密钥。文献[7]方案密文只需要更新撤销属性的部分密文即可，而文献[9]方案密文更新阶段相当于重新进行一次属性基加密。文献[11]方案和文献[12]方案使用 KEK 树实现撤销，因此除了更新撤销属性相关的密钥外，还需要寻找能重新覆盖撤销属性所对应的新属性群的所有用户的最小子集，更新所有的密文需要的时间复杂度为 $O(n)$。文献[13]引入中国剩余定理虽然减少了密钥更新时间，但是密文更新阶段相当于进行一次属性基加密，运算量大。本文方案在密文更新时的计算开销为零，在密钥更新时的计算量为撤销属性的模乘运算，即更新 RSA 部分私钥，其计算量可忽略不计。综上所述，

本文方案具有更高的撤销效率。

表 2 撤销引起的计算开销性能对比

方案	密钥更新	密文更新
NEDAC-MACS[7]	$(2n_r+3)E$	$3n_rE$
UR-CP-ABE[9]	$(2n_r+4)E$	$(n_r+n_c+4)E+E_T$
KEK-CP-ABE[11]	$n_rE+O(n)$	$(n_r+n_c+1)E+E_T$
AR-CP-ABE[12]	$3n_rE+O(n)$	$(n_r+n_c+1)E+E_T$
CRT-CP-ABE[13]	$3n_rE_N$	$(n_r+n_c+1)E+E_T$
本文方案	n_rE_N	0

5.2 效率分析

本节实验仿真对本方案和文献[7]方案和文献[12]方案在属性撤销后密钥和密文的更新时间进行评估。实验环境配置：Intel(R) Core(TM) i5-7400 CPU @3.00GHz，四核，8.00 GB RAM，Windows 10 操作系统。仿真程序基于 JPBC 库，采用 Java 语言。撤销属性数目选取 2、4、6、8、10 共 5 个参考点，并编写时间测量函数测量这些参考点的密钥和密文的更新时间。具体仿真结果如图 2 和图 3 所示。

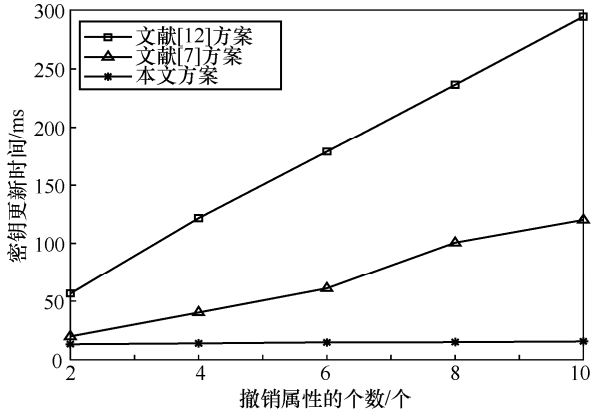

图 2 密钥更新时间

图 2 和图 3 描述的是属性撤销后，随着撤销属性个数的增长，更新密钥和密文所需要的时间变化情况。由图可看出，本方案的密钥更新时间比文献[7]方案和文献[12]方案的时间大大减少，只需要更新 RSA 部分私钥即可。文献[12]方案由于引入 KEK 树密钥，因此比文献[7]方案的版本号密钥需要更多的计算量。在密文更新方面，本文方案不需要更新密文，文献[7]更新撤销属性部分密文，文献[12]方案全部更新，因此从 3 图可看出文献[12]方案密文更新时间更长。综上所述，本文提出的撤销方案相比较现有的版本号和 KEK 重加密方案具有更高的效率。

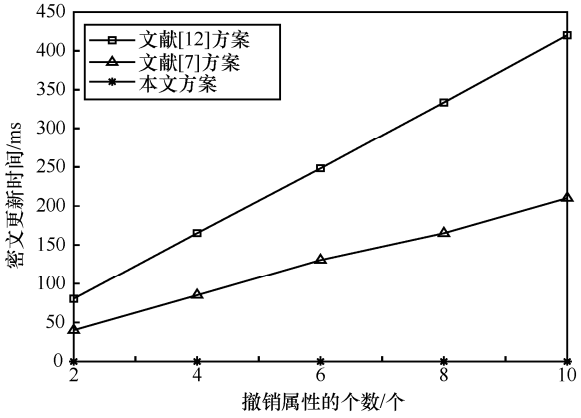

图 3 密文更新时间

6 结束语

海量数据托管存储在第三方营运的大型云端数据中心，带来便利的同时，也带来安全问题。针对这个问题，本文构造了一种基于半可信第三方的高效撤销的属性基加密方案，实现了撤销用户和用户属性级别的撤销。所提方案的特点是引入 RSA 属性认证，不需要用户更新密钥，也不需要重加密密文，适用于属性变更频繁的海量数据的网络环境。撤销权限由 CA 控制，属性认证由半可信第三方执行。属性撤销后，CA 只需更新 RSA 属性认证部分密钥即可，极大地减少了撤销带来的计算量，用户不需要参与密钥更新，因此也减少了接入设备的计算量，同时保证了前后向安全性和抗串谋攻击。最后给出了所提方案的理论分析和实验分析，说明了本文提出的撤销方法更适用于海量数据环境。

参考文献：

[1] RIVERA D, GARCÍA A, MARTÍN-RUÍZ M L, et al. Secure communications and protected data for a Internet of things smart toyplatform[J]. IEEE Internet of Things Journal, 2019,6(2):3785-3795.

[2] SAHAIA, WATERS B. Fuzzy identity-based encryption[C]//Annual International Conference on Theory and Applications of Cryptographic Tchniques. Springer, 2005:457-473.

[3] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//International Workshop on Public Key Cryptography. Springer, 2008:321-334.

[4] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE symposium on Security and Privacy.IEEE, 2007:321-334.

[5] LUAN I, PETKOVIC M, NIKOVA S, et al. Mediated ciphertext-policy attribute-based encryption and its application[C]// Information Security Applications, 10th International Workshop. 2009: 309-323.

[6] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]//TheInternational Symposium on ACM Symposium on Information,Computer and communications security. ACM, 2010:261-270.

[7] WU X, JIANG R, BHARGAVA B. On the security of data access control for multiauthority cloud storage systems[J]. IEEE Transactions on Services Computing, 2015, 10(2):285-272.

[8] FAN K, WANG J, WANG X, et al. Secure, efficient and revocable data sharing scheme for vehicular fogs[J]. Peer-to-Peer Networking and Applications, 2018, 11(4):766-777.

[9] LI J, YAO W, ZHANG Y, et al. Flexible and fine-grained attribute-based data storage in cloud computing[J]. IEEE Transactions on Services Computing, 2016,10(5):785-796.

[10] FAN K, WANG J, WANG X, et al. Proxy-assisted access control scheme of cloud data for smart cities[J]. Personal & Ubiquitous Computing, 2017, 21(5):937-947.

[11] HUR J, NOH D K. Attribute-based access control with efficient revocation in data outsourcing systems[J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(7):1214-1221.

[12] LI J, YAO W, HAN J, et al. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage[J]. IEEE Systems Journal, 2017, 12(2): 1767-1777.

[13] 强衡畅, 王晓明. 一种高效细粒度云存储访问控制方案[J]. 计算机与数字工程, 2014, 42(9):1673-1677.
QIANG H C, WANG X M. Fine-grained access control with efficient revocation in cloud storage[J]. Computer and Digital .Engineering, 2014, 42(19): 1673-1677.

[14] 林娟. 可撤销的属性基加密技术的研究[D]. 上海:上海交通大学,2014.
LIN J. Research on revocable attribute based encryption technology[D]. Shanghai: Shanghai Jiaotong University, 2014.

[15] IMINE Y, LOUNIS A,BOUABDALLAH A. Revocable attribute-based access control in mutli-autority systems[J].Journal of Network and Computer Applications, 2018, 122: 61-76.

[16] BEIMEL A. Secure schemes for secret sharing and key distribution[J]. International Journal of Pure & Applied Mathematics, 1996.

[17] ODELU V, DAS A K, KHURRAM KHAN M, et al. Expressive CP-ABE scheme for mobile devices in IOT satisfying constant-size keys and ciphertexts[J]. IEEE Access, 2017(5):3273-3283.

[18] 王一兵. 物联网技术在营运车辆安全监管中的应用[J]. 计算机时代, 2018(3): 35-37.
WANG Y B. Application of Internet of things technology in safety supervision of operation vehicles[J]. Journal of Computer, 2018(3): 35-37.

[19] YANG Y, ZHONG M, YAO H, et al. Internet of things for smart ports: technologies and challenges[J]. IEEE Instrumentation and Measurement Magazine, 2018, 21(1):34-43.

[20] VAANCHIG N, CHEN W, QIN Z. Ciphertext-policy attribute-based access control with effective user revocation for cloud data sharing system[C]// International Conference on Advanced Cloud & Big Data. IEEE, 2017: 186-193.

[作者简介]

李学俊（1969− ），女，山西浮山人，博士，西安电子科技大学副教授，主要研究方向为物联网数据安全、安全方案及协议设计、无线网络安全。

张丹（1994− ），女，陕西咸阳人，西安电子科技大学硕士生，主要研究方向为属性基加密、物联网安全。

李晖（1968− ），男，河南灵宝人，博士，西安电子科技大学教授、博士生导师，主要研究方向为密码学、无线网络安全、云计算安全、信息论与编码理论。