doi:10.3969/j.issn.1000-436x.2014.z2.009

权限分离的属性基加密数据共享方案

朱辉，雷婉，黄容，李晖，刘西蒙
(西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071)

摘 要：属性基加密(ABE, attribute-based encryption)用于提供细粒度访问控制及一对多加密，现已被广泛应用于分布式环境下数据共享方案以提供隐私保护。然而，现有的属性基加密数据共享方案均允许数据拥有者任意修改数据，导致数据真实性无法保证，经常难以满足一些实际应用需求，如个人电子病例、审核系统、考勤系统等。为此，提出一种能保证数据真实可靠且访问控制灵活的数据共享方案。首先，基于 RSA 代理加密技术实现读写权限分离机制以保证数据真实可靠；其次，使用属性基加密机制提供灵活的访问控制策略；最后，利用关键字检索技术实现支持密钥更新的高效撤销机制。详细的安全性分析表明本方案能提供数据机密性以实现隐私保护，且性能分析和仿真表明本方案具有较高效率，能有效满足实际应用需求。
关键词：属性基加密；访问控制；权限分离；隐私保护；数据共享
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0053-10

Privilege separation of data sharing scheme using attribute-based encryption

ZHU Hui, LEI Wan, HUANG Rong, LI Hui, LIU Xi-meng
(State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China)

Abstract: Attribute-based encryption (ABE), which can provide fine-grained access control and flexible one-to-many encryption, has been envisioned as an important data sharing approach to achieve privacy preserving in the distributed environment. However, the flourish of the data sharing approach using attribute-based encryption still hinges upon how to fully understand and manage the challenges facing in the distributed environment, especially the veracity of the data. In fact, all of the existing data sharing schemes allow data owner to modify data without restrictions, in which the veracity of the data has been questioned and that cannot satisfy the demands of practical application sometimes, such as personal electronic medical records or assessment systems. A data sharing scheme with privilege separation is presented, in which the veracity of the data can be ensured and the flexible access control can be provided. Based on RSA-based proxy encryption, a new efficient privilege separation mechanism is introduced to ensure the veracity of the data; exploiting attribute-based encryption, the data owner can define the access policy to achieve fine-grained access control. Detailed security analysis shows that the proposed data sharing scheme can provide the data confidentiality to achieve privacy preserving. In addition, the performance analysis demonstrates the scheme's effectiveness in terms of the computation costs.
Key words: attribute-based encryption; access control; privilege separation; privacy preserving; data sharing

1 引言

随着云计算迅速发展，分布式环境下对数据共享的需求越来越普遍，进而数据外包技术持续高速发展。数据外包存储能给人们提供许多便利，如节省成本，加快处理速度等，但同时也带来一系列安

收稿日期：2014-07-02
基金项目：国家自然科学基金资助项目（61303218, 61272457）；中央高校基本科研业务费基金资助项目（K5051301017）；国家移动通信重大专项基金资助项目（2012ZX03002003-002）；高等学校学科创新引智计划基金资助项目（B08038）
Foundation Items: The National Natural Science Foundation of China (61303218, 61272457); Fundamental Research Foundations for the Central Universities of China (K5051301017); The National Mobile Communication Major Project (2012ZX03002003-002); 111 Project (B08038)

全挑战[1,2]。为了保证数据机密性，数据文件往往被数据拥有者在本地加密后才外包给服务器，但这又引起效率、灵活性等问题。因此，如何设计既能提供隐私保护[3~5]，又能灵活访问控制的数据共享机制已成为近年来的研究热点。

2005 年，Sahai 和 Waters 等[6]在基于身份加密(IBE, identity-based encryption)基础上，首次提出属性基加密(ABE, attribute-based encryption)的概念，将密文和用户密钥都与属性相关，规定仅拥有足够多属性的用户才能解密密文，但基本的 ABE 无法支持灵活的访问控制策略。随后文献[7]又提出密文策略属性基加密(CP-ABE, cipher-text-policy attribute-based encryption)，即密钥和属性集相关，密文与访问控制策略关联，且允许数据拥有者定义访问控制策略，进而为数据访问提供了极灵活的访问控制机制。此外，CP-ABE 也属于一对多加密机制，与传统一对一加密机制相比，极大地降低了数据加密开销，非常适合于分布式环境下数据共享，因而被广泛地应用于数据外包存储等场景中[8~11]。然而，由于 ABE 机制自身的复杂性，过于繁杂的属性撤销过程[12,13]已成为阻碍其进一步推广的关键所在。值得一提的是，Hur 等人[14]通过引入双重加密和分发路径密钥机制，使属性撤销仅需服务器进行重加密操作，极大降低了数据拥有者的负担，但该方案无法支持密钥更新操作。

综上所述，现有属性基加密数据共享方案均存在一个共同应用缺陷，即允许数据拥有者任意修改数据，导致数据真实性无法保证。事实上，在实际应用中，经常需要一种能提供灵活的访问控制策略且保证数据真实可靠的数据共享方案。如个人电子病历，为提供隐私保护，一方面应该让病人控制对病历数据可读性授权，经过病人授权读的用户才能解密密文；另一方面，为保证病历数据真实有效，应当仅医生才能写病历，即病人不应对自己病历数据任意修改。再如个人档案记录系统，档案当事人应当能够控制其他用户对其个人档案数据读的授权，但为确保档案数据真实可靠，档案当事人无权对自己档案数据进行写操作。

为解决上述问题，本文提出一种能保证数据真实可靠且访问控制灵活的数据共享方案。首先，基于 RSA 代理加密技术[15]构造读写权限分离机制以保证数据真实可靠；然后，利用属性基加密机制提供灵活的访问控制策略；最后，通过引入关键字检索技术[16]，提供一种支持密钥更新且更加高效的撤销机制。

2 预备知识

2.1 双线性对

令 G 和 G_T 是 2 个阶为大素数 p 的循环群，g 是 G 的生成元。假设 $e: G\times G\rightarrow G_T$ 为满足以下性质的一个映射：

1) 双线性：对于任意的 $u, v\in G$ 和 $a, b\in Z_p^*$，有 $e(u^a, v^b) = e(u, v)^{ab}$；

2) 非退化性：$e(g, g)\neq 1_T$, $1_T \in G_T$；

3) 可计算性：对于任意的 $u, v \in G$，存在有效的算法计算 $e(u, v)$。

则称这样的映射为双线性对映射。

2.2 Bilinear Diffie-Hellman(BDH)假设

定义 1 (BDH 假设) 给定四元组 $g, g^a, g^b, g^c \in G$，其中 $a, b, c \in Z_p^*$ 未知，对于任意一个概率多项式时间算法 A，进行如下计算

$$Adv_{BDH}(A) = \Pr[A(g, g^a, g^b, g^c) = e(g, g)^{abc}]$$

得到的概率优势 $Adv_{BDH}(A)$ 是可忽略的，则称 BDH 假设在(G, G_T)上是成立的。

2.3 系统模型

为实现数据共享时，数据真实可靠、访问灵活可控，定义如图 1 所示的系统模型，具体包括数据服务器、授权中心、数据拥有者、数据修改者及数据阅读者 5 部分。

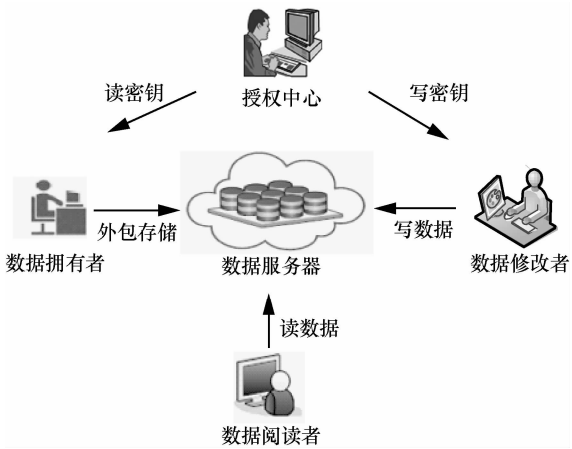

图 1 系统模型

1) 数据服务器。半可信，主要职责是存储数据、响应用户请求及提供相应服务。它既忠实地执行所

有被委派任务，又对加密数据内容感兴趣。另外，它和攻击者有区别，不会发起主动攻击，如服务器—用户合谋。

2) 授权中心。完全可信，被系统中所有参与方信任，其主要职责是分发读、写密钥。

3) 数据拥有者。唯一能够对数据读操作进行授权的用户，它持有读密钥，但不具备写操作权限，其主要职责是定义访问控制策略、加密读密钥、建立密文索引及分发查询密钥。

4) 数据修改者。唯一能够对数据进行写操作的用户，拥有写密钥。另外，经数据拥有者授权后，还可以读数据。

5) 数据阅读者。最普通的用户，经数据拥有者授权后，仅能读数据。

2.4 安全性需求

为实现具有隐私保护的权限分离，必须满足 2 个核心要求。

1) 为保证用户隐私，数据拥有者必须完全控制对数据访问的授权；

2) 为确保数据真实可靠，读写操作权限必须被分离，仅数据修改者能对数据进行写操作。

此外，为提高系统灵活性和安全性，细粒度访问控制及按需撤销也应该被满足。因此，定义如下安全性需求。

1) 数据机密性，未经授权的非法用户或者所持属性不够的合法用户，应当均不能恢复明文，且方案可以抵抗用户合谋攻击。

2) 权限分离，数据拥有者能够完全控制对数据读权限的授权，但仅数据修改者才能对数据进行写操作以确保数据真实可靠。

3) 按需撤销，包括用户撤销和属性撤销。用户撤销，即该用户不再合法，必须撤销他的全部属性。属性撤销，即该用户权限有所降低，必须确保该属性不能再解密之后的数据。

4) 细粒度访问控制，数据拥有者定义访问控制策略，且不同用户被授权访问不同的数据。

3 权限分离的属性基加密数据共享方案

首先定义一些符号来方便所提数据共享方案的表述，具体如表 1 所示。其中，$U=\{u_1,\cdots,u_n\}$和 $\Lambda=\{att_1,\cdots,att_p\}$分别表示用户集和属性集；而拥有某个属性的所有用户的集合称作属性群。

表 1　符号定义

符号	语义
u_t	用户 t 的身份标识
att_i	属性 i
G_i	属性 att_i 所对应的属性群
Λ	属性集
KEK_j	节点 j 所对应的 KEK
PK_t	u_t 的路径密钥
F_j	文件 j
$(k_{u_t}ck_{u_t})$	u_t 所对应的查询密钥对
(e_{i1}, e_{i2})	u_i 所对应的写密钥对
(d_{j1}, d_{j2})	F_j 所对应的读密钥对
$E_{ABE}(d_{j1})$	F_j 所对应的读密钥密文
C	消息密文

3.1 系统初始化

本方案的系统初始化过程包含密钥分发、初始化加密及初始化重加密 3 部分，涉及 ACGen，OwnGen 和 SerGen 3 个算法，具体说明如下。

3.1.1 密钥分发

密钥分发流程如图 2 所示。首先，授权中心运行 ACGen 算法生成文件的读写密钥。其中，写密钥被发送给数据修改者，读密钥被发送给数据拥有者，因此，数据拥有者可以完全控制读操作授权，而仅数据修改者才有写操作权限， 即读写权限被分离，既提供隐私保护，又确保数据真实可靠。然后，数据拥有者执行 OwnGen 算法为数据修改者或者数据阅读者生成属性密钥和查询密钥。其中，查询密钥被用来生成关键字陷门供数据服务器进行密文检索，而属性密钥被用来解密读密钥密文。最后，数据服务器运行 SerGen 算法生成路径密钥[13]，然后分发给数据修改者及数据阅读者。具体算法描述如下。

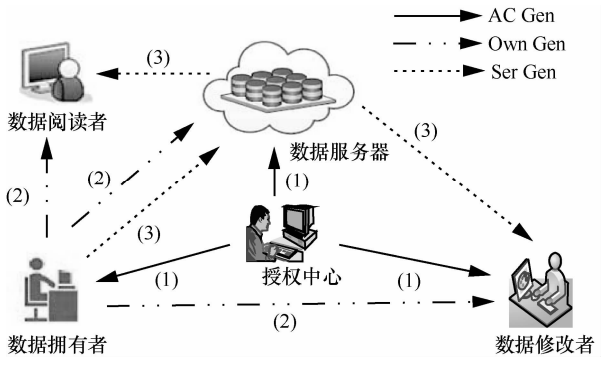

图 2　密钥分发流程

(1) ACGen 算法

授权中心首先运行标准的 RSA 密钥生成算法，输出参数 $(p, q, n, e, d, \Phi(n))$，且 n 是唯一公开参数。然后按照如图 3 所示方式分发读写密钥，具体说明如下。

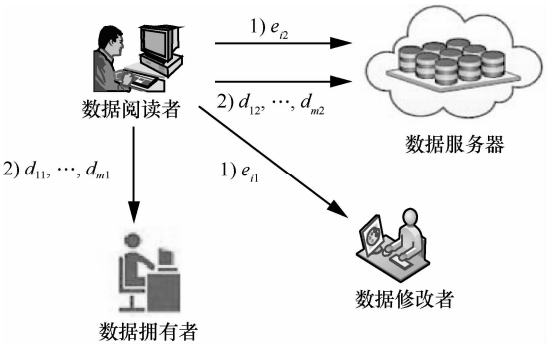

图 3 ACGen 算法流程

1) 授权中心为数据修改者分发写密钥。随机选取 e_{i1} 和 e_{i2}，且 $e_{i1}e_{i2} \equiv e \bmod \Phi(n)$。然后 e_{i1} 被发送给数据修改者，而对应的 e_{i2} 被发送给数据服务器。

2) 授权中心为数据拥有者分发读密钥。假设数据拥有者有 m 个文件，则$(d_{11}, d_{21}, \cdots, d_{m1})$被发送给数据拥有者，而$(d_{12}, d_{22}, \cdots, d_{m2})$被数据服务器保存。同样地，对于每个密钥对$(d_{j1}, d_{j2})$，要求其必须满足 $d_{j1}d_{j2} \equiv d \bmod \Phi(n)$。

(2) OwnGen 算法

令 G 和 G_T 是以素数 p 为阶的循环群，且 g 是 G 的生成元，H 和 H_w 为 $\{0,1\}^* \rightarrow G$ 的散列函数，H_e 为 $G_T \rightarrow Z_p^*$ 的散列函数。随机选取 $\alpha, \beta \in Z_p^*$ 和 k_{mask}，生成主密钥 $MK=(k_{mask}, \beta, g^{\alpha})$，公开参数 $PK=(G, g, h=g^{\beta}, e(g,g)^{\alpha}, H, H_w, H_e)$。然后按照图 4 所示流程分发密钥，具体说明如下。

1) 根据用户提交的用户属性，数据拥有者运行 CP-ABE 密钥生成算法，为 U 中的每个用户生成属性密钥

$$SK = (D = g^{(\alpha+r)/\beta}, \forall att_j \in \Lambda:$$

$$D_j = g^r H(att_j)^{r_j}, D_j^* = g^{r_j})$$

其中，$r, r_j \in Z_p^*$ 为随机选取。

2) 数据拥有者为 U 中的每个用户随机选取 $k_{u_t} \in Z_p^*$ 作为查询密钥，然后发送给用户。

3) 数据拥有者计算互补密钥 $ck_{u_t} = g^{k_{mask}/k_{u_t}}$，然后发送给数据服务器。

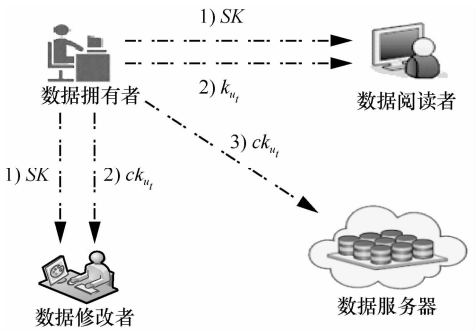

图 4 OwnGen 算法流程

(3) SerGen 算法

数据服务器首先执行 KEKGen 算法[13]给每个用户生成对应的密钥加密密钥（KEK, key encrypting key），然后如图 5 所示流程进行密钥分发，具体说明如下。

1) 数据拥有者将所有的属性群 G_i 发送给数据服务器。

2) 数据服务器根据属性群信息构造如图 6 所示的 KEK 二叉树，并给每个用户分发路径密钥 PK_t。其中，构造二叉树时，每个用户必须被唯一分配一个叶子节点，即叶子节点与用户身份一一对应。

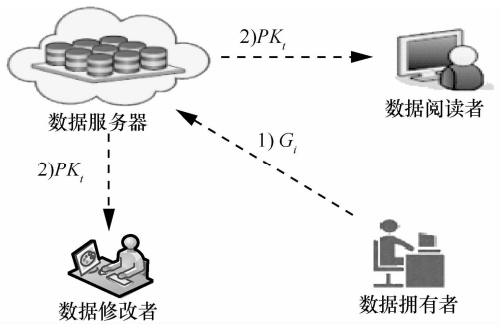

图 5 SerGen 算法流程

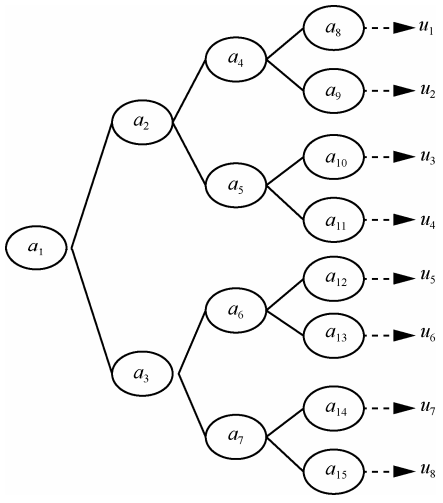

图 6 KEK 二叉树

二叉树的每个节点（包括内部节点和叶子节点）均被分配一个随机密钥 *KEK*。例如节点 a_j 对应的随机密钥为 KEK_j。

服务器给每个用户分发路径密钥 PK_t 为从叶子节点到根节点的所有 *KEK* 的集合。例如，用户 u_3 所存储的路径密钥 $PK_3=\{KEK_{10}, KEK_5, KEK_2, KEK_1\}$。

3.1.2 初始化加密

为了实现细粒度的访问控制，数据拥有者建立密文索引，并且使用 CP-ABE 机制加密读密钥，然后将密文索引及读数据密钥的密文发送给数据服务器。

1) 建立密文索引。数据拥有者随机选取 $R\in Z_p^*$，并且计算 $I(w)=e(H_w(w),g)^{k_{mask}}$ 和 $I(w)^*=[R, HMAC_k(R)]$，其中，$k=H_e(I(w))$，w 表示关键字，$I(w)^*$ 为密文索引。

2) 加密读密钥。数据拥有者运行 CP-ABE 加密算法，对每个文件的读密钥进行加密，然后得到读密钥密文。

$$E_{ABE}(d_{j1})=\{T, C_1=Me(g,g)^{\alpha s}, C_2=h^s$$
$$\forall y\in\phi: C_y=g^{q_y(0)},\ C_y^*=H(att_y)^{q_y(0)}\}$$

其中，随机选取 $s\in Z_p^*$，ϕ 为叶子节点集合。

3.1.3 初始化重加密

为了减少数据拥有者的撤销开销负担，数据服务器对读密钥密文做重加密操作。具体地说，数据服务器随机选取 $K_{att_y}\in Z_p^*$，计算并输出

$$E_{ABE}^*(d_{j1})=\{T, C_1=Me(g,g)^{\alpha s}, C_2=h^s$$
$$\forall y\in\phi: C_y=g^{q_y(0)},\ C_y^*=(H(att_y)^{q_{y(0)}})^{K_{att_y}}\}$$
$$Hdr=(\forall y\in\phi:\{E_K(K_{att_y})\}_{K\in KEK(G_y)})$$

其中，$E_K(M)$表示使用对称密钥 K 加密消息 M，$KEK(G_i)$表示属性群 G_i 的最小覆盖集合，仅在 G_i 的用户才持有相对应的 *KEK*，从而解密 K_{att_y}。例如，在图 6 所示二叉树中，若 $G_j=\{u_1, u_2, u_3, u_4, u_5, u_7\}$，则 $KEK(G_j)=\{KEK_2, KEK_{12}, KEK_{14}\}$，用户 u_3 持有 KEK_2（$KEK_2\in PK_2\cap KEK(G_j)$）。

3.2 数据查询

当用户 u_i 需要检索关键字为 w^* 的文件时，用户首先使用查询密钥计算陷门 $Q(w^*)=H_w(w^*)^{k_{u_i}}$，然后将其发送给数据服务器。

数据服务器接收查询消息后，首先计算 $Q(w^*)=e(Q(w^*), ck_{u_i})$ 和 $k'=H_e(Q^*(w^*))$，然后进行关键字检索。如果存在索引满足 $HMAC_k(R)=HMAC_{k'}(R)$，那么相对应的密文就被添加到检索结果中。

3.3 写数据操作

因写数据密钥仅被数据修改者所持有，故只有经授权的数据修改者才能进行写操作。

数据修改者首先从密钥空间随机选取密钥 k_x 作为对称密钥，然后使用对称加密算法 *E* 加密消息 *M*，得到密文 $C_{i1}=E_{k_x}(M)$，再使用写密钥 e_{i1} 加密对称密钥 k_x，得到密文 $C_{i2}=(k_x)^{e_{i1}}$，最后将消息密文 $C=(C_{i1}, C_{i2})$ 发送给数据服务器。

数据服务器接收到消息后，使用对应的写密钥 e_{i2} 对密文 C_{i2} 进行重加密操作，最后得到 $C_{i2}^*=C_{i2}^{e_{i2}}=(k_x)^{e_{i1}e_{i2}}=(k_x)^e$。

3.4 读数据操作

在将检索到的密文发送给用户之前，数据服务器首先使用相对应的文件读密钥对密文 C_{i2}^* 进行解密，得到密文 $\tilde{C}_{i2}=(C_{i2}^*)^{d_{j2}}=(k_x)^{ed_{j2}}$；然后，将消息密文 $\overline{C}=(C_{11}, \tilde{C}_{12}, \cdots, C_{i1}, \tilde{C}_{i2})$、读密钥密文 $E_{ABE}^*(d_{j1})$ 以及 *Hdr* 发送给用户 u_i。

用户的解密操作包括解密属性群密钥 K_{att_j}，对称密钥 k_x 及消息 *M*。

1) 用户 u_i 先解密 *Hdr* 以获取属性群密钥 K_{att_j}（如果 u_i 在属性群 G_j 中），再更新属性密钥

$$SK=(D=g^{(\alpha+r)/\beta}, \forall att_j\in\Lambda: D_j=g^r H(att_j)^{r_j},$$
$$D_j^*=(g^{r_j})^{1/K_{att_j}})$$

2) 用户使用 CP-ABE 方案解密读密钥密文 $E_{ABE}^*(d_{j1})$，获取读密钥 d_{j1}。再解密对称密钥

$$k_x=(\tilde{C}_{i2})^{d_{j1}}=(k_x)^{ed_{j2}d_{j1}}=(k_x)^{ed}$$

3) 用户使用 k_x 恢复出消息 $M=D_{k_x}(E_{k_x}(M))$。其中，符号 *D* 表示对称解密算法。

值得注意的是，数据拥有者是一种特殊的用户，不需要执行 CP-ABE 方案就能恢复出消息。

3.5 撤销操作

在本方案中，撤销操作包括用户撤销和属性撤销。其中，用户撤销是指当用户不再合法时需要撤销该用户的所有属性；属性撤销是指用户的读权限有所降低，数据拥有者必须为相对应的文件，向授权中心重新请求读密钥。具体操作过程如下。

1) 用户撤销

数据拥有者首先通知数据服务器用户 u_t 已经是非法用户。

数据服务器将移除该用户的所有信息，更新用户列表 L: $L=L\backslash< k_{u_t}, ck_{u_t} >$ 和属性群 G_i: $G_i=G_i\backslash u_t$，此后该用户将不再能访问数据服务器。

2) 属性撤销

数据拥有者首先为相应的文件，向授权中心重新请求读密钥。然后，数据拥有者和数据服务器再对读密钥密文进行更新，具体的更新步骤如下。

数据拥有者随机选取 $s^* \in Z_p^*$，更新

$$E_{ABE}(d_{j1}) = \{T, C_1 = M^* e(g,g)^{\alpha(s+s^*)}, C_2 = h^{s+s^*}, \forall y \in \phi, C_y = g^{q_y(0)+s^*}, C_y^* = (H(att_y)^{q_y(0)+s^*})\}$$

数据服务器随机选取 $K_{att_i}^* \in Z_p^*$，更新

$$E_{ABE}^*(d_{j1}) = \{T, C_1 = M^* e(g,g)^{\alpha(s+s^*)}, \ C_2 = h^{s+s^*}, C_i = g^{q_i(0)+s^*}, C_i^* = (H(att_i)^{q_i(0)+s^*})^{K_{att_i}^*}, \ \forall y \in \phi \backslash \{i\}: C_y = g^{q_y(0)+s^*}, \ C_y^* = (H(att_y)^{q_y(0)+s^*})^{K_{att_y}}\}$$

而没有被属性撤销所影响的其他属性群无需更新 K_{att_y}。

数据服务器重新计算最小覆盖集合 $KEK(G_i)$，更新

$$Hdr = (\{E_K(K_{att_i}^*)\}_{K \in KEK(G_i)}, \forall y \in \phi \backslash \{i\}: \{E_K(K_{att_y})\}_{K \in KEK(G_y)})$$

4 安全性分析

4.1 用户读、写授权的正确性

定理 1 （用户读授权的正确性）如果数据拥有者将加密存储的数据的读权限正确授权给数据修改者和数据阅读者，则他们能够正确解密并读取正确的数据。

证明 首先，数据拥有者将数据的读密钥和关键字加密存储到数据服务器，数据服务器重加密后以$(I(w)^* = [R, HMAC_k(R)], E^*_{ABE}(d_{j1}), Hdr)$的形式存储在本地。数据修改者将修改的文件以 $C = (C_{i1} = E_{k_x}(M), C_{i2} = (k_x)^{e_{i1}})$ 形式加密存储在数据服务器上，服务器然后用修改者的写密钥 e_{i2} 对密文 C_{i2} 进行重加密操作，得到最终密文 $(C_{i1} = E_{k_x}(M), C_{i2}^* = C_{i2}^{e_{i2}} = (k_x)^e)$。

当用户需要检索关键字为 w^* 的密文时，先发送检索请求 $Q(w^*) = H_w(w^*)^{k_{u_i}}$。数据服务器收到请求后，先计算 $Q^*(w^*) = e(Q(w^*), ck_{u_i}) = e(H_w(w^*)^{k_{u_i}}, g^{k_{mask}/k_{u_i}}) = e(H_w(w^*), g)^{k_{mask}}$，然后计算 $k' = H_e(Q^*(w^*)) = H_e(e(H_w(w^*), g)^{k_{mask}})$。因为 $k = H_e(I(w)) = H_e(e(H_w(w^*), g)^{k_{mask}})$，所以如果 $HMAC_k(R) = HMAC_{k'}(R)$，则证明检索用户拥有正确的查询密钥，是合法用户。

然后，数据服务器使用相对应的文件读密钥对密文 C_{i2}^* 进行解密，得到密文 $\tilde{C}_{i2} = (C_{i2}^*)^{d_{j2}} = (k_x)^{ed_{j2}}$；并将密文 $(\bar{C} = (C_{11}, \tilde{C}_{12}, \cdots, C_{i1}, \tilde{C}_{i2}), E^*_{ABE}(d_{j1}), Hdr)$ 发送给用户。

用户得到密文后，遍历自己的路径密钥作为对称密钥 K 解出属性群密钥：$K_{att_y} = D_K(E_K(K_{att_y}))_{K \in KEK(G_y)}$。如果该用户拥有必需的属性，则能正确解出 K_{att_y}，进而更新属性密钥 $SK = (D = g^{(\alpha+r)/\beta}, \forall att_j \in \Lambda: D_j = g^r H(att_j)^{r_j}, D_j^* = (g^{r_j})^{1/K_{att_j}})$。

接下来，用户对 $E^*_{ABE}(d_{j1})$ 进行解密。首先定义一个递归算法 $DecryptNode(E^*_{ABE}(d_{j1}), SK, x)$，$x$ 是访问控制树 T 的节点，算法输出群 G 的元素域 $\perp$。如果 x 是叶子节点，且 $K_{att_j} \in \Lambda$，则

$$DecryptNode(E^*_{ABE}(d_{j1}), SK, x) = \frac{e(D_x, C_x)}{e(D'_x, C'_x)} = \frac{e(g^r H(att_x)^{r_x}, g^{q_x(0)})}{e((g^{r_x})^{1/K_{att_x}}, (H(att_x)^{q_x(0)})^{K_{att_x}})} = e(g,g)^{rq_x(0)}$$

如果 x 是非叶子节点，对于节点 x 的所有孩子节点 z，调用算法 $DecryptNode(E^*_{ABE}(d_{j1}), SK, x)$，$S_x$ 是一个任意长度的孩子节点 z 的集合，计算

$$F_x = \prod_{z \in S_x} F_z^{\Delta_{i,S_x'}(0)}, i = index(z), S_x' = \{index(z): z \in S_x\}$$

$$= \prod_{z \in S_x} (e(g,g)^{rq_z(0)})^{\Delta_{i,S_x'}(0)}$$

$$= \prod_{z \in S_x} (e(g,g)^{rq_{P(z)}(index(z))})^{\Delta_{i,S_x'}(0)}$$

$$= \prod_{z \in S_x} e(g,g)^{rq_x(i)\Delta_{i,S_x'}(0)}$$

$$= e(g,g)^{rq_x(0)}$$

当算法递归到根节点 R 时，$DecryptNode(E^*_{ABE}(d_{j1}), SK, R) = e(g,g)^{rs}$，然后计算 $C_1/(e(C, D)/A) = d_{j1} e(g,g)^{\alpha s}/(e(h^s, g^{(a+r)/\beta})/e(g, g)^{rs}) = d_{j1}$ 得到读密钥 d_{j1}。

接下来计算对称密钥 $(\tilde{C}_{i2})^{d_{j1}}=(k_x)^{ed_{j2}d_{j1}}=(k_x)^{ed}=k_x$，并解密文件 $M=D_{k_x}(E_{k_x}(M))$。

由此得证，数据修改者和数据阅读者可以正确读文件，即数据拥有者的读授权是正确的。

定理 2　（用户写授权的正确性）如果数据修改者修改的数据能够被数据服务器正确验证并接收，则他们能够正确写数据。

证明　数据修改者将修改后的新数据 M 用对称算法 E 和对称密钥 k_x 进行加密，再用写密钥 e_{i1} 加密 k_x，将消息密文 $C=(C_{i1}=E_{k_x}(M),C_{i2}=(k_x)^{e_{i1}})$ 发送给数据服务器。

如果数据修改者是一个合法的用户，则数据服务器能够找到一个与之对应的写密钥 e_{i2} 对密文 C_{i2} 进行重加密操作，然后得到 $(C_{i1}=E_{k_x}(M),C_{i2}^{*}=C_{i2}^{e_{i2}}=(k_x)^{e})$ 存储在本地；否则，服务器直接抛弃数据。

由此得证，数据修改者能够提供正确的数据，即数据修改者的写权限是正确的。

4.2　读写权限分离

定理 3　如果 RSA 假设安全，则没有多项式时间的敌手能够破坏权限分离机制。

证明　本方案中的读写权限分离机制是基于 RSA 代理加密技术实现的，所以，只需要证明代理加密在 RSA 假设下是安全的即可。同时考虑到在整个系统中，数据服务器是获取信息最多的参与方，包括公开参数 n，中间过程密文，最终密文以及数据服务器的所有密钥。因此，必须证明数据服务器不能恢复消息。

初始化　挑战者 $\mathcal{C}$ 运行密钥生成算法，产生秘密值(e, d, p, q)和系统参数 n，$\mathcal{C}$ 保存秘密值，并将系统参数 n 发送给攻击者 $\mathcal{A}$。注意到 $\mathcal{A}$ 仅知道系统参数 n。

阶段 1　攻击者 $\mathcal{A}$ 执行多项式次数的适应性询问, 即每次询问可以依赖于以前询问的结果, 这些询问包括以下几项。

私钥询问　当攻击者 $\mathcal{A}$ 进行部分私钥询问的时候，挑战者 $\mathcal{C}$ 随机选取与 $\Phi(n)$互素的素数对$(e_B, d_B)_i$，并将 $(e_B, d_B)_i$ 发送给攻击者 $\mathcal{A}$；

加密询问　攻击者随机选择一个明文，挑战者运行加密算法产生密文 $c=m^e$，并将结果 c 返回给攻击者 $\mathcal{A}$；

解密询问　攻击者随机选择一个密文 $c=m^e$，挑战者运行解密算法，最后返回明文 m 或符号“⊥”表示解密失败；

挑战　攻击者 $\mathcal{A}$ 决定结束第一阶段的询问，生成两个相同长度的明文 m_0 和 m_1。挑战者 $\mathcal{C}$ 随机选择 $b\in\{0, 1\}$，计算 $c=(m_b)^e$，并将结果 c 发送给攻击者 $\mathcal{A}$。

阶段 2　与阶段 1 相同。

猜测　攻击者 $\mathcal{A}$ 最终输出他的猜测 b'，若 $b=b'$，则攻击者 $\mathcal{A}$ 赢得游戏。

攻击者 $\mathcal{A}$ 通过不断在发起私钥询问，可以获取知识$(e_B, d_B)_i$, i=1, 2, …, x。发起加密查询，可以获取知识 $c_1=c^{e_{B1}}$ 和 $c_2=(c_1)^{d_{B1}}$。如果攻击者 $\mathcal{A}$ 能够以不可忽略的概率恢复出消息 m_b，那么它就必须找到一个 d' 满足$(c_2)^{d'}=m_b$。这就意味着 $ee_{B1}d_{B1}d'\equiv 1 \bmod \Phi(n)$是可以计算的，即攻击者 $\mathcal{A}$ 是可以解决任何 RSA 问题，这与 RSA 问题相矛盾。

证毕。

4.3　按需撤销

定理 4　假定 BDH 假设成立，则没有多项式时间的敌手能够破坏撤销机制。

证明　对于用户撤销，由于当某个用户撤销时，数据拥有者会通知数据服务器移除该用户的所有信息，并更新用户列表 L: $L=L\backslash<u_t, ck_{u_t}>$和属性群 G_i: $G_i=G_i\backslash u_t$。故即使该用户还能生成关键字陷门 $H(w^*)^{k_{u_t}}$，但是由于数据服务器没有相对应的密钥 ck_{u_t}，使其不能计算 $Q^*(w^*)=e(H(w^*)^{k_{u_t}},ck_{u_t})$，所以该用户是无法执行关键字检索，从而不能继续访问文件。因此，本方案中用户撤销的安全性是显而易见的。

下面给出属性撤销安全性的详细证明。

在整个系统中，属性被撤销的用户是获取信息最多的参与方，故接下来将证明该用户不能恢复出当前消息。

初始化　挑战者 $\mathcal{C}$ 运行初始化算法，产生主密钥 $MK=(k_{mask}, \beta, g^{\alpha})$和系统参数 $PK=(G, g, e(g, g)^{\alpha}, h=g^{\beta})$。挑战者 $\mathcal{C}$ 秘密保存主密钥，并将系统参数 PK 发送给攻击者 $\mathcal{A}$。注意到 $\mathcal{A}$ 仅知道系统参数 PK。

阶段 1　攻击者 $\mathcal{A}$ 执行多项式次数的适应性询问, 即每次询问可以依赖于以前询问的结果, 这些询问包括以下几项。

加密询问　攻击者若是第一次发起加密询问，挑战者 $\mathcal{C}$ 运行加密算法产生密文 $C_1=Me(g, g)^{\alpha s}$ 和 $C_2=h^s$，并将结果 $C=\{C_1, C_2\}$返回给攻击者 $\mathcal{A}$。

之后若攻击者再发起加密询问，挑战者将随机选取 s^*，产生密文 $C_1 = M^* e(g, g)^{\alpha(s+s^*)}$ 和 $C_2 = h^{s+s^*}$，且要求 $M \neq M^*$。

解密询问 攻击者随机选择一个密文 C，挑战者运行解密算法，最后返回明文 M 或符号“⊥”表示解密失败。

挑战 攻击者 $\mathcal{A}$ 决定结束第一阶段的询问，生成两个相同长度的明文 M_0 和 M_1。挑战者 $\mathcal{C}$ 随机选择 $b \in \{0,1\}$，计算 $C_1 = M_b e(g, g)^{\alpha(s+s^*)}$ 和 $C_2 = h^{s+s^*}$，并将结果 C 发送给攻击者 $\mathcal{A}$。

阶段 2 与阶段 1 相同。

猜测 攻击者 $\mathcal{A}$ 最终输出他的猜测 b'，若 $b = b'$，则攻击者 $\mathcal{A}$ 赢得游戏。

攻击者 $\mathcal{A}$ 通过发起加密查询，可以获取知识 $C_1 = Me(g, g)^{\alpha s}$ 和 $C_2 = h^s$。如果攻击者 $\mathcal{A}$ 能够以不可忽略的概率恢复出消息 M_b，那么它就必须能够由 $\{g, e(g, g)^{\alpha}, h, e(g, g)^{\alpha s}, h^s, h^{s+s^*}\}$ 计算出 $e(g, g)^{\alpha(s+s^*)}$。这就意味着 DH 问题和 BDH 问题是可以解决的，这与实际情况相矛盾。

证毕。

5 性能分析

本节将针对所提方案在初始化、写操作及读数据方面的计算开销进行性能评估。在本方案中，每个数据拥有者可以完全控制对数据读的授权，定义灵活的访问控制策略及实现有效的撤销。所有这些性能的实现都是基于 RSA 代理加密、CP-ABE 以及关键字检索等技术。此外，由于关键字检索的开销主要是一些对运算操作，因此，利用 PBC[17]、OpenssL[18]及 CP-ABE 工具箱[19]等工具来测试一些基本运算操作，来评估所提方案的计算开销。测试环境为一台 2.4 GHz 双核处理器和 4 GB 内存的计算机。

在参数选取方面。首先选取 2 048 bit 主密钥，1 024 bit 读写密钥来测试 RSA 代理加密的速度；然后，使用 20 个属性生成属性密钥，并选取 10 个叶子节点的访问树作为访问策略来测试 CP-ABE 的系统建立、密钥产生、加密及解密的时间开销；同时，由于在本方案中，CP-ABE 和 RSA 分别用来加密读密钥和对称密钥，故针对这 2 种方案的加解密，采用大小为 1 KB 的密钥文件进行测试，而选取 256 bit 的 AES 算法作为对称加密算法来加密 1 MB 的数据文件；此外，为测试椭圆曲线的相关计算开销，在 512 bit 的有限域上的 $y^2 = x^3 + x$ 曲线上选取一个 160 bit 长的循环群。通过 10 万次测试取平均值的方法，可得测试环境下的基本运算参考时间，具体如表 2 所示。 此外，对运算为 1.389 ms，G 和 G_T 群上的幂运算分别为 1.994 ms 和 0.187 ms；SHA-1 对 20 byte 进行散列运算的时间为 0.000 94 ms，HMAC 运算时间为 0.003 ms。

表 2 基本操作开销

方案	操作	时间/s
RSA	主密钥(2048 bit)	0.406
	密钥对(1 024 bit)	0.981×10^{-3}
	加密(1 KB)	0.003
	解密(1 KB)	0.054
CP-ABE	系统建立	0.092
	生成密钥	0.436
	加密(1 KB)	0.234
	解密(1 KB)	0.092
AES	加密(1 MB)	0.028
	解密(1 MB)	0.039

在本方案中，授权中心只需要运行 RSA 方案生成主密钥和读写密钥；数据拥有者需要运行 CP-ABE 方案生成属性密钥和加密读密钥，以及建立密文索引。因此，假设每个数据拥有者有 10 个文件，基于表 2 测试时间，可以描述出授权中心的计算开销随着数据拥有者及数据修改者数量增多而变化的情况，具体如图 7 所示。显然，随着用户数量的增加，授权中心的计算开销呈线性增长，具体来说，对于每增加一个数据修改者，授权中心只需要找到满足 $e_{i1}e_{i2} \equiv e \bmod \Phi(n)$ 的一个密钥对即可，因此，随着数据修改者数量的增加，授权中心的仅需要增加极小的计算开销。

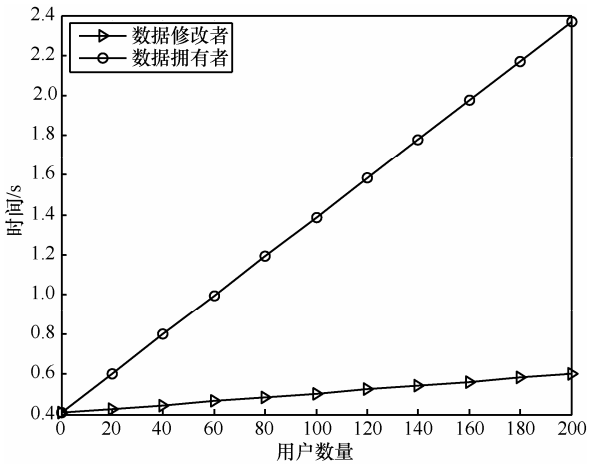

图 7 授权中心初始化计算开销

为了实现写操作，数据拥有者需要执行 AES 及 RSA 加密算法，数据服务器需要执行 RSA 重加密操作及关键字检索；而为了实现读操作，数据服务器需要先执行 RSA 重解密及关键字检索，然后用户运行 CP-ABE、RSA 及 AES 解密算法。因此，选取 1 MB 大小的数据文件在网络速率为 100 Mbit/s 的局域网平台上进行测试，测试结果如图 8 所示。显然，本方案读写操作的效率很高，且其计算开销随着关键字数量的增加是可忽略的。

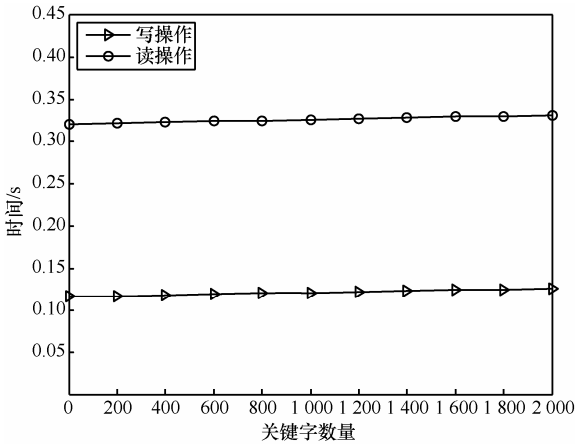

图 8　读写操作开销

针对属性撤销，对其计算代价进行了评估。为实现每个文件的撤销操作，仅需数据拥有者和数据服务器维护，其他用户不受影响。数据拥有者的计算开销与撤销属性的数量无关系，仅与叶子节点的数量成正比；而数据服务器的开销与撤销属性的数量及最小覆盖集合中 *KEK* 的数量成正比。令 a 和 b 分别表示 G 和 G_T 群上的幂运算代价，c 表示对称加密算法代价，且假设叶子节点的数量为 l，撤销属性的数量为 n，最小覆盖集合中 *KEK* 的数量为 m，则数据拥有者的计算开销为 $b+(2l+1)a$，数据服务器的开销为 $na+nmc$。在实验中，假设叶子节点的数量为 20，撤销属性的数量为 10，平均每个最小覆盖集合中 *KEK* 的数量为 10。另外，测试 AES-256 加密 256 byte 的时间开销作为对称加密算法代价，通过测试 10 万次取平均所得结果为 1.825 μs。由图 9 可知，本方案的属性撤销是非常高效的。

综上所述，本方案在满足特定安全需求的前提下，且有着计算及资源开销很少的优点，非常适合实际环境中应用。

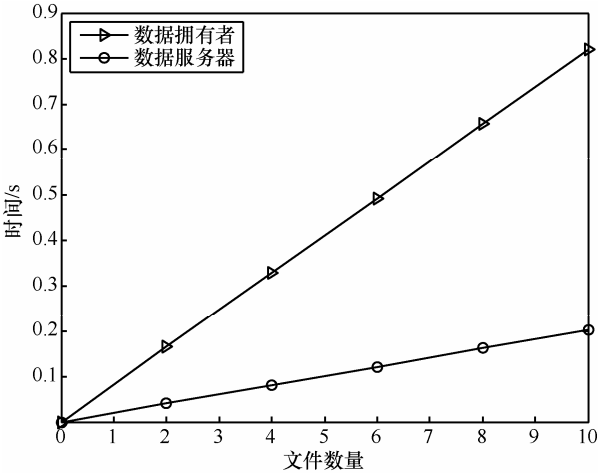

图 9　属性撤销操作开销

6　结束语

本文提出一种能保证数据真实可靠且访问控制灵活的权限分离数据共享方案。首先，通过基于 RSA 代理加密技术，实现文件读写权限分离的机制以保证数据真实可靠；然后，利用属性基加密机制，为所提方案提供灵活的访问控制策略；最后，利用关键字检索技术，实现支持密钥更新的高效撤销机制。此外，详细安全性分析和性能分析表明本方案能够高效地提供数据机密性来实现用户隐私保护。另外，在下一步工作中，将针对具体应用场景优化权限分离机制，进一步提高方案的性能。

参考文献：

[1] ARMBRUST M, FOX A, GRIFFITH R, *et al*. A view of cloud computing [J]. Communications of the ACM, 2010, 53(4): 50-58.

[2] 冯登国, 张敏, 张妍等. 云计算安全研究[J]. 软件学报, 2011, 22 (1): 71-83.
FENG D G, ZHANG M, ZHANG Y, *et al*. Study on cloud computing security[J]. Journal of Software, 2011, 22 (1): 71-83.

[3] 朱辉,李晖,苏万力等. 基于身份的匿名无线认证方案[J]. 通信学报, 2009,30(4):130-136.
ZHU H, LI H, SU W L, *et al*. ID-based wireless authentication scheme with anonymity[J]. Journal on Communications, 2009,30(4):130-136.

[4] AGRAWAL R, SRIKANT R. Privacy-preserving data mining [J]. ACM Sigmod Record, 2000, 29(2): 439-450.

[5] ZHU H, LIU T T, Wei G H, *et al*. PPAS: privacy protection authentication scheme for VANET [J]. Cluster Computing, 2013,16 (4): 873-886.

[6] SAHAI A, WATERS B. Fuzzy identity-based encryption[M]. Advances in Cryptology–EUROCRYPT 2005. Springer Berlin Heidelberg, 2005.

[7] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[A]. Security and Privacy, SP'07[C]. 2007. 321-334.

[8] YU S, WANG C, REN K, *et al*. Achieving secure, scalable, and fine-grained data access control in cloud computing[A]. INFOCOM, 2010 Proceedings IEEE[C]. 2010.1-9.

[9] LI M, YU S, ZHENG Y, *et al*. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption [J]. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(1): 131-143.

[10] AKINYELE J A, PAGANO M W, GREEN M D, *et al*. Securing electronic medical records using attribute-based encryption on mobile devices[A]. Proceedings of the 1st ACM workshop on Security and Privacy in Smartphones and Mobile devices[C]. ACM. 2011.75-86.

[11] NARAYAN S, GAGNE M, SAFAVI-NANINI R. Privacy preserving EHR system using attribute-based infrastructure[A]. Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop[C]. ACM.2010. 47-52.

[12] JAHID S, MITTAL P, BORISOV N. EASIER: Encryption-based access control in social networks with efficient revocation[A]. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security[C]. ACM. 2011. 411-415.

[13] XU Z, MARTIN K M. Dynamic user revocation and key refreshing for attribute-based encryption in cloud storage[A]. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications[C]. 2012.844-849.

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

[15] DONG C, RUSSELLO G, DULAY N. Shared and searchable encrypted data for untrusted servers[M]. Data and Applications Security XXII. Springer Berlin Heidelberg, 2008.

[16] YANG Y, LU H, WENG J. Multi-user private keyword search for cloud computing[A]. 2011 IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom)[C]. IEEE. 2011. 264-271.

[17] BEN L. PBC library[EB/OL]. http://crypto.stanford.edu/pbc/, 2013.

[18] Openssl Team OpenSSL: The open source toolkit for SSL/TLS [EB/OL]. http://www.openssl.org, 2013.

[19] BETHENCOURT J, SAHAI A, WATERS B. The cpabe toolkit[EB/OL]. http://acsc.csl.sri.com /cpabe/, 2013.

作者简介：

朱辉（1981-），男，河南周口人，博士，西安电子科技大学副教授，主要研究方向为信息安全和隐私保护。

雷婉（1991-），女，陕西渭南人，西安电子科技大学硕士生，主要研究方向为基于属性加密和信息安全。

黄容（1989-），女，湖南衡阳人，西安电子科技大学硕士生，主要研究方向为基于属性加密和云计算安全。

李晖（1969-），男，河南灵宝人，博士，西安电子科技大学教授，主要研究方向为密码学、无线网络安全、信息论和网络编码。

刘西蒙（1988-），男，陕西西安人，西安电子科技大学博士生，主要研究方向为公钥密码学、信息安全、安全网络编码及其应用。