面向移动云的属性基密文访问控制优化方法

刘建，鲜明，王会梅，荣宏
（国防科技大学电子科学学院，湖南 长沙 410073）

摘 要：针对移动云数据安全共享与访问控制问题，综合考虑当前密文访问控制机制的不足以及移动终端资源受限、网络带宽较低等特点，提出了一种面向移动云的属性基密文访问控制优化方法。通过引入属性基加密运算分割和双重加密机制，并结合多秘密共享技术进行改进，实现了移动用户数据发布和权限管理开销的大幅优化。理论和实验分析表明，所提方案在安全性、计算和网络开销等方面均能够满足移动云中的访问控制需求，具有良好的应用前景。

关键词：移动云；访问控制；双重加密；属性基加密；优化
中图分类号：TP309.2
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2018112

Optimization method for attribute-based cryptographic access control in mobile cloud computing

LIU Jian, XIAN Ming, WANG Huimei, RONG Hong
College of Electronic Science, National University of Defense Technology, Changsha 410073, China

Abstract: For the problem of secure data sharing and access control in mobile cloud, the drawback of traditional cryptographic access control schemes was deeply analyzed. Considering the truth that mobile devices were usually equipped with limited resources, an optimized attribute-based cryptographic access control scheme was proposed in this study. In the proposed scheme, a third party proxy was introduced into the system model, and the two-layer encryption method was applied. Combining traditional attribute-based encryption (ABE) algorithm with multi-secret sharing and split measurement of ABE encryption, the scheme could greatly reduce the cost of mobile users in terms of data publish and access management. Theoretical and experimental analysis shows that the contribution can well meet the requirements of mobile cloud in terms of security, computational complexity and communication cost, which means that it is promising for future applications.

Key words: mobile cloud, access control, two-layer encryption, attribute-based encryption, optimization

1 引言

移动云计算作为移动互联网与云计算融合发展的最新形态，不仅继承了传统云计算资源规模大、动态可扩展、多用户共享和可靠性高等优势，还具有移动互联、灵活接入和实时在线等特点，因而具有广阔的发展前景。然而，在移动云环境中的数据安全与隐私等同时也面临着巨大挑战：一方面，用户通常采用无线网络接入，其天然的开放特性可能导致攻击者非授权接入；另一方面，移动终端小型化易丢失和安全防护能力不足等特点也可能导致信息被窃取或丢失。因此，设计满足移动用户需求的轻量级安全解决方案，实现其数据安全防护与访问控制等已经成为学术界和产业界关注的一个重要方向[1-3]。

实际上，移动云的部署和实现方式决定了用户数据将存储在远程云端服务器，而该服务器不在用户的可信与可控范围之内，因而传统的依赖于服务

收稿日期：2017−09−05；**修回日期**：2018−04−04
通信作者：刘建，ljabc730@nudt.edu.cn

器 ACL 的访问控制方法无法满足用户对其数据安全的防护需求[4]。针对该问题，人们提出了基于密文的访问控制模型，在该模型中，云端存储的是用户加密后的数据，而数据拥有者通过对数据访问者解密能力的控制，来保证其数据明文不会被非法访问和窃取。在不同的密文访问控制模型中，本文选择属性基加密（ABE, attribute-based encryption）算法作为基础加解密模块，这是因为：1)属性基加密算法具有一方加密多方解密的特性，使数据在初始加密时不需要得知所有的合法解密用户的列表，因而对于移动云环境下用户集合不固定的场景尤其适用；2)相比传统的 PKI 密文访问控制方案，属性基密文访问控制方案能够有效降低用户密钥的管理开销和数据存储开销[5]。

属性基加密方案最早起源于 Sahai 等[6]提出的模糊身份基加密，依据访问策略的嵌入位置不同可以分为 2 类，密钥策略的属性基加密（KP-ABE）和密文策略的属性基加密（CP-ABE）。其中，KP-ABE[7]从数据对象提取属性集合，并由授权机构制定访问策略后嵌入用户的密钥分片中，当且仅当密钥中的访问策略与数据对象属性相匹配时，用户可以成功解密数据；而在 CP-ABE[8-9]中，属性集对应于用户描述，数据拥有者在执行数据加密的过程中制定访问策略，并将其嵌入在密文中，当且仅当该策略与访问用户的属性相匹配时，才能够正确地解密获得明文数据。可见 CP-ABE 更加接近传统的角色基访问控制（role-based access control）方案[10]，因而更具实用性。由于属性基加密方案具有良好的可扩展性，且支持细粒度、灵活多样的访问控制策略，因此当前很多研究工作围绕属性基加密算法以及基于属性的密文访问控制方案（简称属性基密文访问控制方案）展开[11-22]。

实际上，将属性基加密技术应用于移动云环境下的数据访问控制面临着 2 个主要问题：1) 其加解密过程包含大量的模指数与双线性映射运算，计算代价高且该开销随着属性集的增大而快速增加；2) 权限撤销的效率和通信开销有待优化。由于移动终端资源有限，这 2 个问题都可能导致系统瓶颈的出现。对于此，研究者已经进行了部分研究。文献[12-16]重点研究了属性基加密方案中的用户权限撤销问题，并提出了一系列支持属性撤销和细粒度权限控制的密文访问控制方案，其中，文献[15]将属性基加密与密钥封装机制（KEM, key encapsulation mechanism）相结合，一方面，避免用户使用属性基加密算法直接处理数据而引入大量运算，另一方面，进一步地利用替代重加密思想可以有效优化权限撤消的效率。文献[18]提出了支持在线/离线的属性基加密方案，要求设备在离线阶段自动完成大量加密预处理工作，保证其上线之后可以快速完成数据加密，一定程度上降低了用户执行属性基加密的运算开销，提高了密文生成效率。文献[19-20]借助半可信的第三方代理将属性基密文转化为 ElGamal 密文，大幅降低了用户执行解密的计算开销。

本文针对移动云环境下的数据访问控制优化问题，综合考虑移动终端计算、带宽资源有限等因素，设计了一种基于第三方代理的轻量级、高效、灵活的属性基密文访问控制方案，以 Rouselakis 等[11]提出的“广域空间（large universe）”CP-ABE 算法为基础进行优化构造：采用属性基加密运算分割技术[18]，保证移动用户在数据上传过程中仅需要执行少量运算，而大部分加密运算则委托由代理执行；引入双重加密与多秘密共享思想，使权限变更（主要涉及数据重加密）过程中用户的计算和带宽成本大幅降低，提高了变更效率。

2 预备知识

2.1 访问结构

定义 1[18,23] 假设属性集合的全集为 $\mathcal{U}$，定义 $\mathbb{A}\subseteq 2^{\mathcal{U}}\setminus\{\varnothing\}$ 为访问控制结构。$\mathbb{A}$ 中的任意元素均表示一个属性集合，称为授权或合法属性集，不在 $\mathbb{A}$ 属性集合中的则称为非授权属性集。另外，当满足如下条件时：对于 $\forall B,C\in 2^{\mathcal{U}}\setminus\{\varnothing\}$，当 $B\in\mathbb{A}$ 且 $B\subseteq C$ 时，均可得 $C\in\mathbb{A}$，称访问结构是单调的。

在 CP-ABE 体制中，属性集合 $\mathcal{U}$ 用来描述用户信息，当且仅当用户所拥有的属性集为授权属性集时，才能够获得数据密文，反之无法解密。另外，本文在设计方案时仅考虑了单调的访问结构，在实际中则可以参考文献[18]中的方法将之扩展为通用访问结构。

2.2 线性多秘密共享方案

在属性基加密算法的构造过程中，使用了线性秘密共享机制来保护数据安全，通常情况下，方案中需要分享的秘密值为有限域中的一个元素，将其称为线性单秘密共享。本文为了实现双重加密条件下的高效权限变更，引入多秘密共享机制。参照多目标单调张成方案（multi-target monotone span

program）[24]的形式化描述，给出该机制的形式化定义如下。

定义 2　定义线性多秘密共享方案 Π 为四元组 $(\mathbb{Z}_p, \boldsymbol{M}, \rho, \boldsymbol{V})$，其中，$\mathbb{Z}_p$ 为 p 阶有限域（p 取素数），$\boldsymbol{M} \in \mathbb{Z}_p^{\ell \times n}$ 为定义在该域上与访问结构 $\mathbb{A}$ 相关联的 $\ell \times n$ 阶矩阵，又称秘密生成矩阵，取 $\mathcal{U}$ 为属性全集，则 $\rho \in \mathcal{F}(|\ell| \to \mathcal{U})$ 为一个从矩阵 $\boldsymbol{M}$ 行索引 $\{1,2,\cdots,\ell\}$ 到 $\mathcal{U}$ 的映射，$\boldsymbol{V} = (\vec{\boldsymbol{e}}_1, \vec{\boldsymbol{e}}_2, \cdots, \vec{\boldsymbol{e}}_c)(1 \leqslant c < n)$ 为定义在有限域 $\mathbb{Z}_p$ 的单位向量集合。

1) 秘密分享算法：令 $s_1, s_2, \cdots, s_c (s_i \in \mathbb{Z}_p)$ 为需要分享的秘密值，$r_{c+1}, r_{c+2}, \cdots, r_n$ 为在相应有限域上选取的 $n-c$ 个随机值，2 个部分共同组成一个 n 维向量 $\vec{\boldsymbol{v}} = (s_1, s_2, \cdots, s_c, r_{c+1}, \cdots, r_n)^{\mathrm{T}} \in \mathbb{Z}_p^{n \times 1}$。$\rho(i)$ 为矩阵第 i 行对应的属性值，该属性值对应的秘密分片为 $\lambda_i = \vec{\boldsymbol{M}}_i \vec{\boldsymbol{v}}$，其中，$\vec{\boldsymbol{M}}_i$ 为矩阵 $\boldsymbol{M}$ 第 i 行对应的向量。

2)秘密恢复算法：针对某属性集 $S \in 2^{\mathcal{U}} \setminus \{\varnothing\}$，取索引集合 $I = \{i \,|\, i \in [\ell] \wedge \rho(i) \in S\}$，则 $\boldsymbol{M}_S$ 为矩阵 $\boldsymbol{M}$ 的子矩阵，且其行号 $i \in I$。若 $\boldsymbol{V} = (\vec{\boldsymbol{e}}_1, \vec{\boldsymbol{e}}_2, \cdots, \vec{\boldsymbol{e}}_c)$ 中的每个单位向量可以由 $\boldsymbol{M}_S$ 行向量线性表示，称属性集 S 为授权属性集，即 $S \in \mathbb{A}$。此时，针对 $\boldsymbol{V}$ 中的每个单位向量 $\vec{\boldsymbol{e}}_\tau$，存在一组随机系数 $\omega_{i,\tau}$，使 $s_\tau = \sum_{i \in I} (\omega_{i,\tau} \lambda_i)$，且该系数可以在多项式时间内计算得出。

在本文的访问控制方案中，为了更好地兼容双重加密机制，将 CP-ABE 加密过程中所分享的秘密值设定为 2，分别为 s_1、s_2。因此，上述定义中访问结构 $\mathbb{A}$ 可简化为 $(\boldsymbol{M}, \rho)$，此时授权属性集合 S 对应的子矩阵 $\boldsymbol{M}_S$ 行向量的张成子空间内存在单位向量(1,0,⋯,0)和(0,1,0,⋯,0)。显然，存在多项式时间算法可以计算出系数 $\{\omega_i\}_{i \in I}$ 使 $s_1 = \sum_{i \in I} (\omega_i \lambda_i)$ 以及 $\{\mu_i\}_{i \in I}$ 使 $s_2 = \sum_{i \in I} (\mu_i \lambda_i)$。

3　系统模型与算法描述

3.1　系统模型

本文采用的系统模型如图 1 所示，共包含 5 个参与方：数据拥有者（DO, data owner）、授权机构（AA, authorized agency）、云端服务器（CS, cloud server）、代理方（PA, proxy agency）以及云服务其他用户（CU, cloud user）。

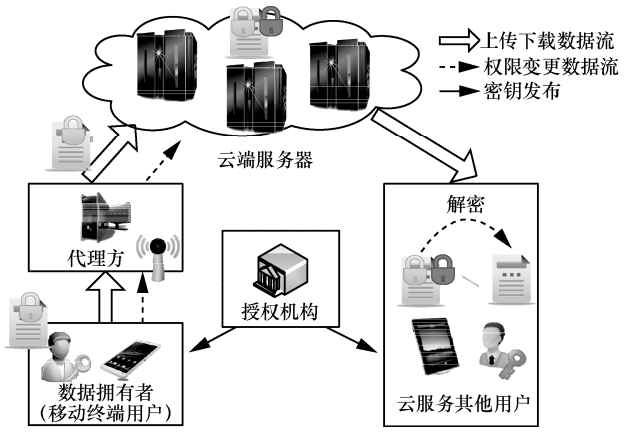


图 1　移动云环境下的属性基密文访问控制系统模型

数据拥有者即移动终端用户，其设备仅具备有限的计算、存储能力，并通过无线网络（3G/4G 移动通信网、Wi-Fi 等）访问远程云服务。在访问控制模型中，DO 主要负责在数据发布过程中定义访问结构、执行第一重对称加密生成中间密文以及执行权限变更过程中的部分运算等操作。

授权机构主要负责用户属性的注册管理，并根据用户属性集合生成相应的密钥分片。

云端服务器由云服务供应商（CSP）管理，通常具有强大的计算、存储和网络通信能力，其掌握的资源量远大于其他参与方。在本文中，CS 除了担任数据持久化存储之外，还需要在数据发布过程中执行第二重对称加密以及权限变更过程的密钥更换和密文更新等操作。

代理方作为移动终端用户（DO）访问云端服务的网关代理，其主要作用在于降低 DO 在执行属性基加密及权限变更过程中的开销。在数据发布过程中，PA 接收 DO 生成的中间密文，并进行转换使最终密文结构符合 CP-ABE 解密规范；在权限变更过程中，PA 对 DO 上传的部分策略变更信息处理后发送给云端服务器 CS。

云服务其他用户通过移动互联网或传统互联网访问 CS 中的共享文件。假设每个 CU 拥有特定的属性集合，并利用自己从 AA 获得的密钥分片执行属性基解密过程，当且仅当其属性集满足 DO 指定的访问结构时，才能够正确执行属性基解密操作，并最终获得数据明文。

显然，本文模型相比传统模型新引入了第三方代理 PA 以降低数据拥有者的开销。在实际的环境中，PA 可以直接由 CSP 管理运维，即 PA 和 CS 可以采用同一个云服务商甚至同一台云服务器来实

现。这种简化的模型可以降低方案的通信总成本，提高运行效率，且对于系统的安全性并没有造成影响（具体分析见 5.1 节）。然而，为了使所提方案描述得更加清晰，下面依然将 PA 和 CS 作为独立的参与者，分别执行协议中的不同算法模块。

3.2 算法描述

本文方案主要包括 4 个过程：方案初始化、数据发布、数据访问以及访问策略变更，每个过程包含了多个多项式时间算法。

1) 方案初始化

$Setup(1^{\lambda})\rightarrow(pk,msk)$：该算法由 AA 执行，输入 1^{λ} 作为系统的安全参数，并为整体访问控制方案生成所需的公共参数 pk 以及系统主密钥 msk。

$KeyGen(msk,S)\rightarrow sk$：该算法由 AA 执行，输入用户的属性集合 S 及系统主密钥 msk，为系统模型中 DO、CU 等所有的注册用户生成与其属性集合相匹配的密钥 sk。

2) 数据发布

$PriEncrypt(m,\mathbb{A})\rightarrow ICT$：该算法由 DO 执行，输入访问控制策略 $\mathbb{A}$ 以及数据明文 m，并基于 KEM 机制构造出中间密文 ICT，该中间密文不仅包含数据的第一重对称加密所得的密文，还包含第一重对称密钥利用属性基加密生成的中间信息。

$TransEncrypt(ICT,pk)\rightarrow CT$：该算法由 PA 执行，输入系统的公共参数 pk 以及 DO 提交的中间密文 ICT，生成符合 CP-ABE 解密规范的密文数据，并将其上传到远程的 CS 服务器。

$SecEncrypt(CT)\rightarrow CT$：该算法由 CS 执行，负责选定第二重对称密钥并对数据密文执行第二重加密操作。

3) 数据访问

$Decrypt(CT,sk)\rightarrow(k_{\text{in}},k_{\text{out}})$：该算法由 CU 执行，输入数据密文以及用户密钥分片，当用户属性集能够满足密文中嵌入的访问结构，它就可以正确执行属性基解密获得 2 层对称密钥 $(k_{\text{in}},k_{\text{out}})$，进一步执行 2 次对称解密可以获取明文。

4) 访问策略变更

$PolicyUpdate(CT,\mathbb{A}')\rightarrow CT'$：该算法在访问策略变更时由 DO、PA 和 CS 三方协作完成，输入变更后的访问结构 $\mathbb{A}'$ 以及原始数据密文 CT，将 CT 转换为新策略 $\mathbb{A}'$ 下的密文 CT'，以确保被撤销权限的用户不再具有数据解密能力，即便其缓存了之前曾经使用过的相关密钥。

4 方案详细设计

根据第 3 节所描述的系统模型及算法构成，从以下 4 个过程详细介绍本文的访问控制方案。

4.1 方案初始化

该过程主要的参与者为授权机构（AA），负责属性基访问控制方案中所涉及的代数结构（如有限域、循环群和双线性映射等）的初始化，并生成系统的主密钥和公共参数。此外，AA 还要为注册用户生成与其属性集合相匹配的密钥。该过程涉及的主要算法包括以下 2 个。

1) $Setup(1^{\lambda})\rightarrow(pk,msk)$

该算法输入 1^{λ} 作为安全参数，首先由授权机构（AA）选定一个安全的大素数 p，并构建有限域 $\mathbb{Z}_p$；进一步构建双线性映射 $e:G\times G\rightarrow G_T$，其中，$G$ 和 G_T 均为 p 阶乘法循环群；取 $\mathcal{K}$ 为对称加密算法的密钥空间，$H:G_T\rightarrow\mathcal{K}$ 为一个安全的散列函数，$\mathcal{U}=\mathbb{Z}_p$ 表示属性全集。

AA 从生成的循环群 G 以及有限域 $\mathbb{Z}_p$ 中分别选取随机元素 $g,h,u,v,w\xleftarrow{R}G$ 以及 $\alpha\xleftarrow{R}\mathbb{Z}_p$，并生成系统主密钥

$$msk=\alpha \tag{1}$$

之后，生成系统参数的公共部分

$$pk=(H,G,G_T,g,h,u,v,w,e(g,g)^{\alpha}) \tag{2}$$

最后，AA 将 pk 公共参数广播发布，并在本地安全地保存主密钥 msk。

2) $KeyGen(msk,S)\rightarrow sk$

授权机构（AA）为包含 DO 和 CU 等角色在内的所有注册用户生成密钥分片。具体地，令 $S=\{a_1,a_2,\cdots,a_k\}\subseteq\mathbb{Z}_p$ 表示某用户所拥有的属性集，AA 随机选择 $r_i\xleftarrow{R}\mathbb{Z}_p(1\leqslant i\leqslant k)$，选取 $r\xleftarrow{R}\mathbb{Z}_p$，并生成密钥为

$$\begin{aligned}&K_0=g^{\alpha}w^{r},K_1=g^{r},\\&\{K_{i,2}=g^{r_i},K_{i,3}=(u^{a_i}h)^{r_i}v^{-r}\}_{i\in[k]}\end{aligned} \tag{3}$$

最终，所得用户密钥为 $sk=(S,K_0,K_1,\{K_{i,2},K_{i,3}\}_{i\in[k]})$。

4.2 数据发布

该过程基于密钥封装机制，引入双重加密和 ABE 加密运算分割思想，主要完成数据加密、密

钥加密和数据上传操作。具体包括 3 个子过程：数据拥有者（DO）执行数据预加密、代理方（PA）执行密文转换和云端服务器（CS）执行第二重加密。

1) $PriEncrypt(m,\mathbb{A}=(\boldsymbol{M},\rho))\rightarrow ICT$

假设一个数据文件 m 具有唯一的标识 ID_f，DO 首先随机选取属性基加密过程分享的第一个秘密值 $s_1 \xleftarrow{R} \mathbb{Z}_p$，那么 KEM 所使用的第一重对称加密密钥为

$$k_{\text{in}} = H(e(g,g)^{\alpha s_1}) \in \mathcal{K} \tag{4}$$

之后，DO 利用 k_{in} 对数据 m 执行对称加密（如 AES、3DES 等）操作得到密文 C'_m，接下来 DO 随机产生 $n-2$ 个随机数 $y_3,y_4,\cdots,y_n \xleftarrow{R} \mathbb{Z}_p$，构造随机向量 $\vec{\boldsymbol{y}}=(s_1,0,y_3,\cdots,y_n)^{\mathrm{T}} \in \mathbb{Z}_p^{n\times 1}$，依据访问结构 $\mathbb{A}$ 执行秘密分享算法得 $\vec{\boldsymbol{\lambda}}=(\lambda_1,\lambda_2,\cdots,\lambda_\ell)^{\mathrm{T}}=\boldsymbol{M}\vec{\boldsymbol{y}}$。进一步地，令 $\delta_1,\delta_2 \xleftarrow{R} \mathbb{Z}_p$，DO 对于所有的 $j\in[\ell]$ 计算

$$\begin{aligned} &C'_0 = g^{s_1}, C'_1 = w^{\delta_1}, C'_2 = u^{\delta_2}, \\ &\{C'_{j,3} = \lambda_j - \delta_1, C'_{j,4} = \rho(j) + \delta_2\}_{j\in[\ell]} \end{aligned} \tag{5}$$

最后，DO 将中间密文 $ICT=(ID_f,C'_m,C'_0,C'_1,C'_2,\{C'_{j,3},C'_{j,4}\}_{j\in[\ell]})$ 以及访问结构 $\mathbb{A}$ 发送给 PA，并在本地安全地存储秘密值 s_1。

2) $TransEncrypt(ICT,pk)\rightarrow CT$

输入中间密文 ICT，由 PA 执行本算法对其进行转换，使转换后的密文符合 CP-ABE 解密规范。具体地，PA 选取随机数 $t_j,\theta_j,\varphi_j \xleftarrow{R} \mathbb{Z}_p$，其中 $j\in[\ell]$。最终，得到如下密文

$$\begin{aligned} &C_0 = C'_0 = g^{s_1}, C_1 = C'_1 = w^{\delta_1}, \{C_{j,2} = (C'_2)^{t_j} = u^{t_j\delta_2}, \\ &C_{j,3} = w^{\theta_j} v^{t_j}, C_{j,4} = (u^{\varphi_j} h)^{-t_j}, C_{j,5} = g^{t_j}, \\ &C_{j,6} = C'_{j,3} - \theta_j = \lambda_j - \delta_1 - \theta_j, \\ &C_{j,7} = -t_j(C'_{j,4} - \varphi_j) = -t_j(\rho(j) + \delta_2 - \varphi_j)\}_{j\in[\ell]} \end{aligned} \tag{6}$$

然后，PA 将访问结构 $\mathbb{A}$ 和密文 $CT=(C'_m,C_0,C_1,\{C_{j,2},C_{j,3},C_{j,4},C_{j,5},C_{j,6},C_{j,7}\}_{j\in[\ell]})$ 发送给远程的 CS 服务器。

另外，在本文方案中，PA 还需要维护一个列表 ParamList，其每一项为

$$(ID_f,t_1,\cdots,t_\ell,\theta_1,\cdots,\theta_\ell,\varphi_1,\cdots,\varphi_\ell) \tag{7}$$

3) $SecEncrypt(CT)\rightarrow CT_o$

云端服务器（CS）输入 PA 上传的密文 CT，对其中的数据密文 C'_m 执行第二重对称加密。另外，为了将此次使用的密钥嵌入属性基密文中，CS 还需要修正 CT 中部分的属性基密文分片。上述过程的详细步骤如下：CS 随机取值 $s_2 \xleftarrow{R} \mathbb{Z}_p$，并取第二重对称加密的密钥值为

$$k_{\text{out}} = H(e(g,g)^{\alpha s_2}) \in \mathcal{K} \tag{8}$$

然后利用密钥 k_{out} 对密文 C'_m 执行一次对称加密操作获得新密文 C_m。

此外，为了将 s_2 作为属性基加密过程需要分享的第二个秘密值，则需要进一步修正属性基的密文分片，具体过程为，首先选取修正向量

$$\vec{\boldsymbol{y}}_c = (0,s_2,0,\cdots,0)^{\mathrm{T}} \in Z_p^{n\times 1} \tag{9}$$

并计算

$$\vec{\boldsymbol{v}}_c = (v_1,v_2,\cdots,v_\ell)^{\mathrm{T}} = \boldsymbol{M}\vec{\boldsymbol{y}}_c \tag{10}$$

对属性基密文分片进行如下修正（其中，$j\in[\ell]$）

$$C_{j,6} = C_{j,6} + v_j = (\lambda_j + v_j) - \delta_1 - \theta_j \tag{11}$$

最后，CS 计算 $C_8 = g^{s_2}$ 并将 s_2 安全地存放在本地，最终所得密文结果为

$$CT = (C_m, C_0, C_1, \{C_{j,2}, C_{j,3}, C_{j,4}, C_{j,5}, C_{j,6}, C_{j,7}\}_{j\in[\ell]}, C_8) \tag{12}$$

4.3　数据访问

该过程主要是云服务用户（CU）通过网络访问共享文件，要求只有已授权合法用户才可以成功提取明文数据。

$Decrypt(CT,sk)\rightarrow(k_{\text{in}},k_{\text{out}})$：用户（CU）从云端服务器（CS）下载密文 CT 及其访问控制结构 $\mathbb{A}=(\boldsymbol{M},\rho)$ 后，首先依据如下步骤判定其属性集是否满足访问控制策略：根据其属性集合 S 中的元素，生成行号集合 $I=\{i\,|\,i\in[\ell]\wedge\rho(i)\in S\}$，并提取 $\boldsymbol{M}$ 中与相应的行组成子矩阵 $\boldsymbol{M}_S$，计算(1,0,⋯,0)和(0,1,0,⋯,0)是否存在于 $\boldsymbol{M}_S$ 的行空间中。若否，则 $S\notin\mathbb{A}$，即 S 为非授权属性基，CU 输出错误信息，反之，依据如下过程完成解密。

通过求解线性方程组，用户（CU）计算得出系数集合 $\{\omega_i\}_{i\in I}$ 和 $\{\mu_i\}_{i\in I}$，使如下 2 个等式（其中，$\vec{\boldsymbol{M}}_i$ 为矩阵 $\boldsymbol{M}$ 的第 i 个行向量）成立。

$$\sum_{i\in I}\omega_i\vec{\boldsymbol{M}}_i=(1,0,\cdots,0) \tag{13}$$

$$\sum_{i\in I}\mu_i\vec{\boldsymbol{M}}_i=(0,1,0,\cdots,0) \tag{14}$$

易得，$\sum_{i\in I}(\omega_i(\lambda_i+v_i))=s_1$ 及 $\sum_{i\in I}(\mu_i(\lambda_i+v_i))=s_2$，那么 CU 可以利用自己的密钥分片 $sk=(S,K_0,K_1,\{K_{i,2},K_{i,3}\}_{i\in[k]})$ 通过下面计算式计算出对称密钥 k_{in} 和 k_{out}。

首先，计算

$$\begin{aligned}AUX_{\text{in}}&=\prod_{i\in I}\Big(e(C_{i,3}w^{C_{i,6}}C_1,K_1)\cdot\\&\quad e(C_{i,4}u^{C_{i,7}}C_{i,2},K_{j,2})e(C_{i,5},K_{j,3})\Big)^{\omega_i}\\&=\prod_{i\in I}\Big(e(w,g)^{(\lambda_i+v_i)r}\Big)^{\omega_i}\\&=e(w,g)^{s_1r}\end{aligned} \tag{15}$$

$$\begin{aligned}AUX_{\text{out}}&=\prod_{i\in I}\Big(e(C_{i,3}w^{C_{i,6}}C_1,K_1)\cdot\\&\quad e(C_{i,4}u^{C_{i,7}}C_{i,2},K_{j,2})e(C_{i,5},K_{j,3})\Big)^{\mu_i}\\&=\prod_{i\in I}\Big(e(w,g)^{(\lambda_i+v_i)r}\Big)^{\mu_i}\\&=e(w,g)^{s_2r}\end{aligned} \tag{16}$$

进一步地，CU 可以得出

$$\begin{aligned}k_{\text{in}}&=H\left(\frac{e(C_0,K_0)}{AUX_{\text{in}}}\right)=H\left(\frac{e(g^{s_1},g^{\alpha}w^{r})}{e(w,g)^{s_1r}}\right)\\&=H\left(e(g,g)^{\alpha s_1}\right)\in\mathcal{K}\end{aligned} \tag{17}$$

$$\begin{aligned}k_{\text{out}}&=H\left(\frac{e(C_8,K_0)}{AUX_{\text{out}}}\right)=H\left(\frac{e(g^{s_2},g^{\alpha}w^{r})}{e(w,g)^{s_2r}}\right)\\&=H\left(e(g,g)^{\alpha s_2}\right)\in\mathcal{K}\end{aligned} \tag{18}$$

随后，用户分别使用 k_{in} 和 k_{out} 即可执行 2 次解密操作获得数据明文。

4.4 访问策略变更

在本文方案中，完成访问策略的变更需要数据拥有者（DO）、代理（PA）和云端服务器（CS）三方协作共同完成。显然，在 KEM 模式的密文访问控制模型中，有效的权限变更（尤其是权限撤销）肯定要涉及密文的重新加密。相比传统方案，所提方案大幅降低了 DO 将原始密文转换为新访问结构下的密文所产生的开销，针对其优化性能以及安全性能的分析将在本文后续章节进行详细介绍。

$PolicyUpdate(CT,\mathbb{A}')\to CT'$：该算法由 DO 发起执行，以实现对某用户针对数据文件 ID_f 的访问权限的授予或撤销。授权过程简单直接，这里主要描述对已授权用户的访问权限的撤销。在下面的描述中，仅考虑单调的访问结构，方案中没有使用负值属性，因而可以合理地假设 $\ell'\leqslant\ell$。

1) DO 构建新的访问结构 $\mathbb{A}'=(\boldsymbol{M}',\rho')$，其中，$\boldsymbol{M}'$ 为 $\ell'\times n'$ 阶矩阵，重新随机选取 $n-2$ 个有限域元素 $y_3',y_4',\cdots,y_{n'}'$，组成向量 $\vec{\boldsymbol{y}}'=(s_1,0,y_3',y_4',\cdots,y_{n'}')^{\mathrm{T}}\in\mathbb{Z}_p^{n'\times1}$。那么可得 $\vec{\boldsymbol{\lambda}}'=(\lambda_1',\lambda_2',\cdots,\lambda_{\ell'}')^{\mathrm{T}}=\boldsymbol{M}'\vec{\boldsymbol{y}}'$，进一步地，计算

$$\begin{aligned}C_{j,3}'&=\lambda_j'-\delta_1\\C_{j,4}'&=\rho'(j)+\delta_2\end{aligned} \tag{19}$$

随后 DO 将 $C_{j,3}'$、$C_{j,4}'$ 这 2 个元素发送至代理（PA）。

2) 接收到权限变更请求后，PA 查询 ParamList 获取 ID_f 对应的列表项，利用其中的参数值对所有的 $j\in[\ell']$ 执行运算

$$\begin{aligned}\hat{C}_{j,6}&=C_{j,3}'-\theta_j=\lambda_j'-\delta_1-\theta_j\\\hat{C}_{j,7}&=t_j(C_{j,4}'-\varphi_j)=-t_j(\rho'(j)+\delta_2-\varphi_j)\end{aligned} \tag{20}$$

之后 PA 将分片 $\{\hat{C}_{j,6},\hat{C}_{j,7}\}_{j\in[\ell']}$ 发送至云端 CS。

3) CS 在接收到权限撤销请求后，针对 PA 发送过来的密文分片 $\{\hat{C}_{j,6},\hat{C}_{j,7}\}_{j\in[\ell']}$，进行第二重密钥更换和密文更新操作：首先利用原密钥 $k_{\text{out}}=H\left(e(g,g)^{\alpha s_2}\right)$ 对数据密文 C_m 进行解密得 $\tilde{C}_m$，之后随机选择新的秘密值 s_2'，计算新的密钥 $k_{\text{out}}'=H\left(e(g,g)^{\alpha s_2'}\right)$，并利用该密钥对 $\tilde{C}_m$ 进行重新加密得到 $\hat{C}_m$。

随后，CS 还需要依据新的访问结构 $\mathbb{A}'$ 对密文进行修正：取向量 $\vec{\boldsymbol{y}}_c=(0,s_2',0,\cdots,0)^{\mathrm{T}}\in Z_p^{n\times1}$，计算 $\vec{\boldsymbol{v}}_c=(v_1,v_2,\cdots,v_{\ell'})^{\mathrm{T}}=\boldsymbol{M}\vec{\boldsymbol{y}}_c$。针对所有的 $j\in[\ell']$，修正原始密文分片为

$$\hat{C}_{j,6}=\lambda_j'-\delta_1-\theta_j+v_j=(\lambda_j'+v_j)-\delta_1-\theta_j \tag{21}$$

此外，取

$$\hat{C}_8=g^{s_2'} \tag{22}$$

此时，云服务器 CS 将原始的 $C_m,\{C_{j,6},C_{j,7}\}_{j\in[\ell']},C_8$ 替换为 $\hat{C}_m$，$\{\hat{C}_{j,6},\hat{C}_{j,7}\}_{j\in[\ell']}$，$\hat{C}_8$，并将新的秘密值 s_2' 安全地保存在本地，删除原秘密值 s_2。

至此，完成了一次有效的权限撤销操作。

5　安全性与性能分析

5.1　安全性分析

依据攻击者的能力不同，本文将方案可能面临的攻击者模型分为 4 类：L_1 攻击者，仅能够获取用户存储在云服务器（CS）上的密文信息，但不能控制 CS 执行任意指定操作；L_2 攻击者，完全控制云服务器（CS），不仅能够获取其上存储的数据，还能够控制其执行包括加解密在内的任意操作；L_3 攻击者，同时掌握云服务器（CS）和代理方（PA）的控制权，能够发起 CS 与 PA 的合谋攻击；L_4 攻击者，通常为被撤销访问权限的用户，该类型攻击者在 L_1 能力的基础上，还缓存了之前使用过的所有对称加密密钥。下面分别讨论这 4 种攻击模型对方案安全性的影响。

首先，讨论 L_1 攻击者情况。本文方案采用了 KEM 机制，即对数据部分由对称加密算法保护，而对称密钥则由 CP-ABE 加密保护，L_1 攻击者将获得如式(12)所示结构的密文。通常假设对称加密算法为计算安全的，因而此时攻击者能否获得数据明文的关键在于所采用的 CP-ABE 算法是否能够有效保护对称密钥的安全。实际上，本文所采用的 CP-ABE 方案是基于 Rouselakis 等[11]的成果（简称 RW 方案），并借鉴文献[18]（简称 HW 方案）的思想对 RW 方案的加密过程进行了分割处理，以降低 DO 的数据发布成本。从密文结构上看，本文方案与 HW 方案是类似的，均包含了 2 个组成部分：随机密文部分和修正值部分，如表 1 所示。其中，随机密文部分是相对正常的属性基加密而言的，指的是利用随机值替代属性值而生成的密文；修正值部分是指为了保证随机密文能够被符合属性约束的用户正常解密而添加的偏移数值，这些偏移数值与属性相关。

表 1　本文方案与 HW 方案密文结构对比

方案	随机密文部分	修正值部分
本文方案	$C_0,\{C_{j,3},C_{j,4},C_{j,5}\}_{j\in[\ell]},C_8$	$C_1,\{C_{j,2},C_{j,6},C_{j,7}\}_{j\in[\ell]}$
HW 方案	$C_0,\{C_{j,1},C_{j,2},C_{j,3}\}_{j\in[\ell]}$	$\{C_{j,4},C_{j,5}\}_{j\in[\ell]}$

参照文献[18]中定理 2 证明方法，本文方案安全性依赖于 RW 方案[11]的安全性，因而易证得本文所采用的 CP-ABE 算法在 L_1 攻击者模型下是 CPA 安全的。此时攻击者只能通过暴力穷举的方法破解对称密文，因此本文方案在面对 L_1 型攻击者时是计算安全的。

接下来，讨论 L_2 攻击者情况。此时，攻击者可以控制云服务器（CS），利用第二重对称密钥 k_{out} 执行解密操作得到第一重密文 C'_m，并执行式(11)的逆向操作。然而，即便如此攻击者所获得的密文结构本质上与 L_1 攻击者所得到的密文分片是类似的。那么，与 L_1 攻击者模型下的安全性证明类似，易证 L_2 攻击模型下 ABE 算法依然是 CPA 安全的，因而此时访问控制系统整体仍是计算安全的。

进一步地，讨论 L_3 攻击者情况。此时，攻击者通过控制 PA 与 CS 实现合谋攻击。由于本文方案中数据密文经过了两重对称加密，第一重由数据拥有者（DO）执行，第二重由云端服务器（CS）执行，此时即便 CS、PA 合谋，仍需要获得第一重加密密钥 k_{in} 才可以完成数据明文的提取。即 L_3 类型攻击者需要获得一定数目的秘密 $\lambda_j(j\in[\ell])$ 以重构 k_{in}。根据第 4 节数据发布过程的描述可知，攻击者仅能获得盲化后的随机值 $\lambda_j-\delta_1$ 和 w^{δ_1}。由于离散对数难题，攻击者无法得到 δ_1 的值，也就无法获取足够数目的 λ_j，从而无法提取出密钥 $k_{\text{in}}=H\left(e(g,g)^{\alpha s_1}\right)$。显然，本文方案在 L_3 类型的攻击者模型下依然能够保障用户数据不被泄露。

最后，讨论 L_4 攻击者情况。此时，攻击者是被撤销访问权限的一类用户，它可以利用之前缓存的密钥等信息发起攻击。研究者的部分权限撤销方案[13,25]并没有更新秘密值 s，导致已被撤销的用户仍然可以利用之前缓存的一些信息（如 $e(g,g)^{\alpha s}$ 等）完成解密获得明文。显然，一个有效的权限撤销必须保证被撤销权限的用户无法成功解密数据获得明文。在本文方案中，CS 更新了秘密值 s'_2，并将 $k'_{\text{out}}=H\left(e(g,g)^{\alpha s'_2}\right)$ 作为新的对称密钥，重新对数据进行加密，这就避免了攻击者利用缓存的密钥实施密文破解，保证了用户数据在面对 L_4 攻击者时仍然是安全的。

5.2　性能评估

接下来，对本文所设计的属性基密文访问控制方案性能进行综合评估，主要从用户移动终端的计算时间开销和网络通信开销 2 个方面展开。另外，前面曾经提到本文方案基于 KEM 模式工作，因此，

将所对比的几类方案也实现为 KEM 的模式。

在本文的实验中，代码使用 Python 语言（编译器版本 2.7.3）编写，基于 JHU 大学的 Charm 框架[26]实现。该框架核心代码利用 C 语言编写，具有较好的计算性能。由于 Charm 包含了大量的基础密码库（对称加密、公钥密码、散列函数、数字签名等），且提供了 LSSS 访问结构的相关支持代码，大幅减轻了本文所提属性基密文访问控制方案的实现成本。实验中，选取对称加密算法为 AES-256，利用桌面 PC（Intel Core i5-2450 2.5 GHz 处理器、8 GB DDR3 内存、OpenSUSE-12.2 操作系统）模拟方案中的各个参与方。为提高测试结果的准确性，所有实验工作在单线程模式，且每个结果取 10 次实验的平均值。

1) 计算时间开销

前面指出，本文通过引入第三方代理 PA 对属性基加密运算进行分割，从而避免可能出现的系统瓶颈。下面，将设计实验对该优化效果进行评估。

首先评估 DO 在数据发布阶段的时间开销。这里主要对比本文方案和直接采用 RW 方案的情况（即将 RW 方案[11]直接与一般双重加密思想[21]结合）。共设计了 2 组实验：实验 1 中，取访问结构中的属性数目为 10 个，DO 需要发布的文件大小为变量，取值为 50~200 MB；实验 2 中，取 DO 需要发布的文件大小为 100 MB，访问结构相关属性数目为变量，取值为 10~50 个。由于 2 个方案中均必须由 DO 执行一次对称加密运算，且该部分计算开销并非本文讨论的重点，因此，在取实验结果时仅统计了 DO 执行属性基加密（ABE）运算的时间开销，其结果分别如图 2 和图 3 所示。

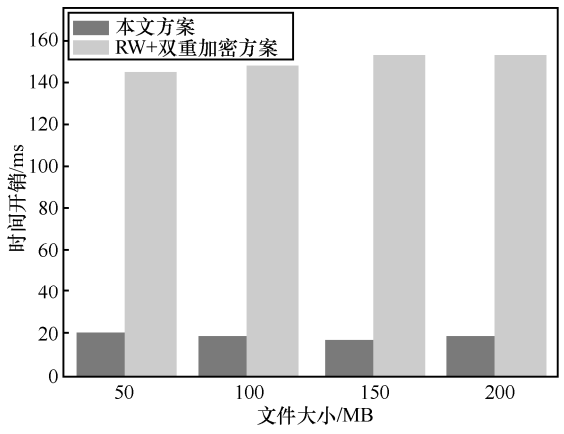


图 2 不同文件大小情况下 DO 数据发布时间开销（仅 ABE）

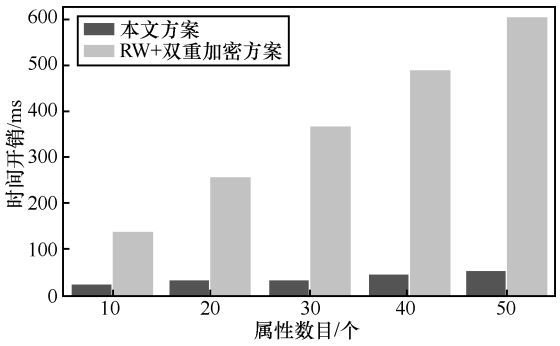


图 3 不同属性数目情况下 DO 数据发布时间开销（仅 ABE）

从图 2 和图 3 可以看出，一方面，本文方案中 DO 在数据发布时的计算开销明显优于 RW+双重加密的访问控制方案（在属性数目为 10 时，DO 执行 ABE 部分的开销仅为另一方案的 14.2%）；另一方面，随着访问结构中属性数目的增多，本文方案相对于 RW+双重加密方案在 DO 计算开销方面的优化效果越好。这是由于本文方案中 DO 在数据发布阶段仅需要执行一次对称加密、一次秘密分享和有限次数（且与访问结构大小 ℓ 无关）的指数运算，而大部分的有限域指数运算和乘法运算则分割给了第三方代理 PA 执行，从而大幅降低了数据拥有者的计算开销，且属性数目越多（此时 ℓ 增大），委托给 PA 执行的运算越多，也就表现出更好的优化效果。

接下来，评估权限撤销过程中 DO 的计算开销。这里主要将本文方案与 RW+双重加密方案[21]、RW+替代重加密方案[15]这 2 个方案进行了对比。参数选取与实验 1 类似，图 4 显示了访问结构中的属性数目固定为 10 个，文件大小从 50~200 MB 变化的情况下，权限撤销过程中 DO 的运算时间开销。图 5 显示了文件大小固定为 100 MB，而属性数目从 10~50 个变化的情况下，权限撤销过程中 DO 的时间开销。

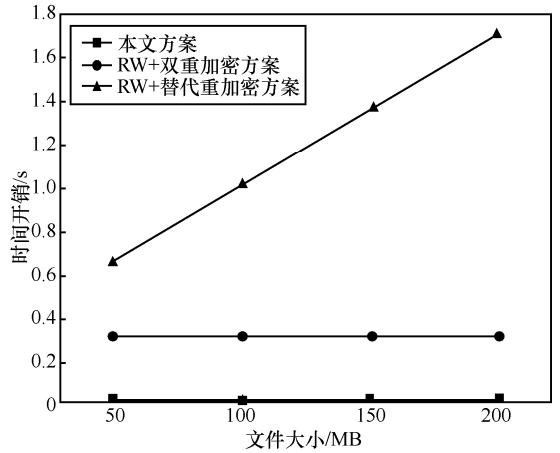


图 4 不同文件大小情况下权限撤销 DO 时间开销

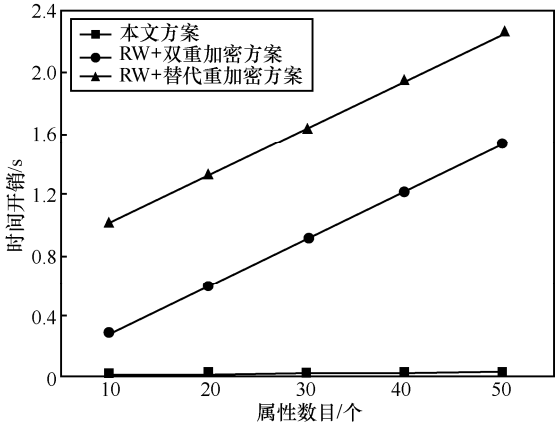


图 5　不同属性数目情况下权限撤销 DO 时间开销

从图 4 和图 5 可以看出：① 本文方案对于降低 DO 在权限撤销过程中的计算开销是极为有效的，其时间开销相比于其他 2 种方案几乎是可以忽略的，这是由于在一般双重加密或替代重加密方案中，两重对称密钥是先进行比特串拼接（$k_{\text{in}} \| k_{\text{out}}$）后才进行属性基加密的，而每一次有效的权限撤销需要更换第二重密钥 k_{out}，这就要求 DO 分别执行一次完整的属性基解密与加密算法，显然会引入较高的计算开销；本文将多秘密共享的思想引入了属性基访问控制方案中，将两重密钥分别关联到秘密值 s_1 和 s_2，而后将 2 个秘密值依据访问结构 $\mathbb{A}$ 嵌入一套属性基密文中，该方法实现了每个秘密值可以独立更新而不需要先执行解密恢复，因此，本文方案在权限撤销中不需要 DO 执行完整的属性基加解密过程，而只需要依据新的访问结构执行一次秘密共享即可（具体见 4.4 节），其计算开销大幅降低；② 当文件大小变化而属性数目保持不变时，本文方案与 RW+双重加密方案中 DO 的计算开销并不变化，这是因为 2 种方案中 DO 的计算开销仅涉及属性基加解密部分，而该部分运算仅与属性数目相关。

2) 网络通信开销

这里主要对方案的网络开销进行全面评估。具体地，对数据发布与权限撤销 2 个过程中 DO、PA 与 CS 三方所产生的数据通信开销进行理论分析，并与 RW 方案[11]、RW+双重加密方案[21]以及 RW+替代重加密方案[15]等类似方案进行对比。

首先，讨论数据发布与权限撤销过程中 DO 的网络开销，如表 2 所示。其中，$|p|$ 表示方案所采用的循环群中的元素长度，$|m|$ 表示整个数据文件的长度（这里假设对称加密后的数据大小不变），$|m_s|$ 表示其中一个分片的长度。由表 2 可以看出，在数据发布过程中，对于所有的方案而言，DO 上传 $|m|$ 大小的数据密文是不可避免的，因此，只能考虑降低属性基密文分片长度，本文方案需要上传的属性基密文分片大小为 $(2\ell+3)|p|$，优于其他 3 种方案；在权限撤销过程中，结合双重加密或替代重加密的方法都可以有效降低数据拥有者 DO 的网络开销，而本文方案在该过程中不需要数据拥有者下载任何的数据，而仅需要向 PA 发送少量（$2\ell|p|$）的修正分片，相比其他 3 种方案更加节省带宽。

其次，讨论数据发布与权限撤销过程中，PA 与 CS 两者间的网络开销。1) 数据发布过程：本文方案中，PA 从 DO 接收数据，并执行 *TransEncrypt*(*ICT*, *pk*)→*CT* 操作后将数据发送给云端，由式(6)可得，该过程中 PA 与云端通信的数据量为 $|m|+(6\ell+2)|p|$，而其他方案中云端接收的数据量为 $|m|+(3\ell+1)|p|$（此时，云端接收的数据量与 DO 发布数据的网络开销一致。因为在 RW+双重加密方案以及 RW+替代重加密方案中不涉及 PA 对数据的处理，所以可以合理假设在这 2 个方案中 PA 与 DO 为同一实体，下同。）。显然，本文方案开销稍高，这是因为本文方案为了实现属性基加密运算分割而添加了部分随机分片，导致属性基密文部分长度增加，在一定程度上增大了通信开销。2) 权限撤销过程：由 4.4 节的描述可得，本文方案中，PA 与云端的通信数据量（含上传与下载，下同）为 $2\ell|p|$，而 RW+双重加密方案为 $(6\ell+2)|p|$，RW+

表 2　　**本文方案与其他方案在数据发布和权限撤销过程中的网络开销对比**

方案	数据发布过程中 DO 网络开销	权限撤销过程中 DO 网络开销	
		下载	上传
RW 方案	$\|m\|+(3\ell+1)\|p\|$	$\|m\|+(3\ell+1)\|p\|$	$\|m\|+(3\ell+1)\|p\|$
RW+双重加密方案	$\|m\|+(3\ell+1)\|p\|$	$(3\ell+1)\|p\|$	$(3\ell+1)\|p\|$
RW+替代重加密方案	$\|m\|+(3\ell+1)\|p\|$	$(3\ell+1)\|p\|+2\|m_s\|$	$(3\ell+1)\|p\|+2\|m_s\|$
本文方案	$\|m\|+(2\ell+3)\|p\|$	0	$2\ell\|p\|$

替代重加密方案为 $(6\ell+2)|p|+4|m_s|$，显然本文方案在该过程具有最小的通信数据量，这是因为本文方案在双重加密基础上引入了多秘密共享，由云端独立完成第二重密文的重新加密，并仅需要较少的辅助信息便能够实现属性基密文中共享秘密值的高效更新。

由此可见，本文方案在降低数据发布过程中的 DO 通信开销、权限变更过程中的 DO 通信开销及云端通信开销方面效果明显。虽然数据发布过程中 PA 与云端 CS 间传输的密文长度有所增加，但是由于两者通常具有比较充足的计算和网络带宽，很难形成系统瓶颈，这在现实环境下是完全可以接受的。另外，根据前面对于 PA 安全性的分析，可以将 PA 与 CS 部署在同一个云服务供应商而不会引入新的安全风险，这种简化的系统模型有助于解决数据发布过程中二者之间通信开销大的问题。

6 结束语

随着云计算技术边缘的不断拓展，面向移动终端的云服务模式逐渐获得广泛应用。如何设计满足移动用户需求的轻量级数据安全保障机制是当前的热点问题。针对移动云环境下终端资源少、通信带宽受限等问题，本文提出了一种高效、灵活的属性基访问控制优化方案。该方案在传统 CP-ABE 访问控制模型的基础上引入第三方代理，并借鉴在线/离线属性基加密思想，将大部分的加密运算任务委托给代理方执行，大幅减轻了数据发布过程中移动终端的计算开销。此外，利用多秘密共享对属性基加密算法进行改进，并结合双重加密机制，使云端可以独立完成第二重密钥的更换以及数据密文的更新操作，以最大程度减少了权限变更过程中移动终端的计算和网络开销。实验验证与理论分析表明，本文所提密文访问控制方案不仅可以有效实现细粒度的数据安全访问控制，而且大幅优化了数据拥有者的数据发布和权限管理开销，且随着访问结构相关属性数目的增加具有更加明显的优化效果，有效避免了移动终端资源受限可能导致的系统瓶颈问题，具有良好的应用前景。

参考文献：

[1] 李瑞轩, 董新华, 辜希武, 等. 移动云服务的数据安全与隐私保护综述[J]. 通信学报, 2013, 34(12): 158-166.
LI R X, DONG X H, GU X W, et al. Overview of the data security and privacy-preserving of mobile cloud services[J]. Journal on Communications, 2013, 34(12): 158-166.

[2] 苏铓, 史振国, 谢绒娜, 等. 面向移动云计算的多要素代理重加密方案[J]. 通信学报, 2015, 36(11): 73-79.
SU M, SHI Z G, XIE R N, et al. Multi-element based on proxy re-encryption scheme for mobile cloud computing[J]. Journal on Communications, 2015, 36(11): 73-79.

[3] 崔勇, 宋健, 缪葱葱, 等. 移动云计算研究进展与趋势[J]. 计算机学报, 2017, 40(2): 273-295.
CUI Y, SONG J, MIAO C C, et al. Mobile cloud computing research progress and trends[J]. Chinese Journal of Computers, 2017, 40(2): 273-295.

[4] 王于丁, 杨家海, 徐聪, 等. 云计算访问控制技术研究综述[J]. 软件学报, 2015, 26(5): 1129-1150.
WANG Y D, YANG J H, XU C, et al. Survey on access control technologies for cloud computing[J]. Journal of Software, 2015, 26(5): 1129-1150.

[5] DONG C, RUSSELLO G, DULAY N. Shared and searchable encrypted data for untrusted servers[J]. Journal of Computer Security, 2011, 19(3):367-397.

[6] SAHAI A, WATERS B. Fuzzy identity-based encryption[M]. Advances in Cryptology–EUROCRYPT, 2005: 457-473.

[7] 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 Communications Security. 2006:89-98.

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

[9] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[M]. Public Key Cryptography–PKC, 2011: 53-70.

[10] ZHOU L, VARADHARAJAN V, HITCHENS M. Achieving secure role-based access control on encrypted data in cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(12): 1947-1960.

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

[12] LIANG X, CAO Z, LIN H, et al. Attribute based proxy re-encryption with delegating capabilities[C]//The 4th International Symposium on Information, Computer, and Communications Security. 2009: 276-286.

[13] YU S, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//The 29th Conference on Information Communications. 2010: 534-542.

[14] YANG K, JIA X, REN K. Secure and verifiable policy update outsourcing for big data access control in the cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2015, 26(12): 3461-3470.

[15] CHENG Y, WANG Z Y, MA J, et al. Efficient revocation in

ciphertext-policy attribute-based encryption based cryptographic cloud storage[J]. Frontiers of Information Technology & Electronic Engineering, 2013, 14(2): 85-97.

[16] YANG K, JIA X, REN K, et al. DAC-MACS: effective data access control for multi-authority cloud storage systems[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(11): 1790-1801.

[17] HAN J, SUSILO W, MU Y, et al. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(3): 665-678.

[18] HOHENBERGER S, WATERS B. Online/offline attribute-based encryption[M]. Public-Key Cryptography, 2014: 293-310.

[19] GREEN M, HOHENBERGER S, WATERS B. Outsourcing the decryption of ABE ciphertexts[C]//The 20th USENIX Conference on Security. 2011: 34.

[20] LIN S, ZHANG R, MA H, et al. Revisiting attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2015, 10(10): 2119-2130.

[21] SABRINA D C, SARA F, SUSHIL J, et al. Over-encryption: management of access control evolution on outsourced data[C]//The 33rd International Conference on Very Large Data Bases. 2007: 123-134.

[22] 洪澄, 张敏, 冯登国. 面向云存储的高效动态密文访问控制方法[J]. 通信学报, 2011, 32(7): 125-132.
HONG C, ZHANG M, FENG D G. Achieving efficient dynamic cryptographic access control in cloud storage[J]. Journal on Communications, 2011, 32(7): 125-132.

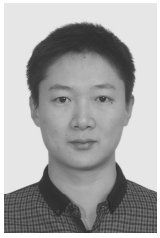
[23] BEIMEL A. Secure schemes for secret sharing and key distribution[M]. Technion-Israel Institute of Technology, Faculty of Computer Science, 1996.

[24] BEIMEL A. Secret-sharing schemes: a survey[M]. Coding and cryptology, 2011: 11-46.

[25] YU S, WANG C, REN K, et al. Attribute based data sharing with attribute revocation[C]//The 5th ACM Symposium on Information, Computer and Communications Security. 2010: 261-270.

[26] AKINYELE J A, GARMAN C, MIERS I, et al. Charm: a framework for rapidly prototyping cryptosystems[J]. Journal of Cryptographic Engineering, 2013, 3(2): 111-128.

[作者简介]



刘建（1986−），男，山东泰安人，博士，国防科技大学讲师，主要研究方向为通信网信息安全、云计算与大数据安全、隐私保护等。

鲜明（1970−），男，四川南充人，博士，国防科技大学研究员，主要研究方向为网络安全评估、云计算系统安全与数据安全、数据挖掘及隐私保护技术等。

王会梅（1981−），女，河北行唐人，博士，国防科技大学讲师，主要研究方向为网络安全评估、云计算与大数据安全等。

荣宏（1988−），男，山西大同人，国防科技大学博士生，主要研究方向为数据挖掘及隐私保护技术。