doi:10.11959/j.issn.1000-436x.2017094

支持用户撤销的多关键字密文查询方案

伍祈应[1]，马建峰[1,2]，李辉[1]，张俊伟[1]，姜奇[1]，苗银宾[1]
（1. 西安电子科技大学网络与信息安全学院，陕西 西安 710071；2. 西安电子科技大学通信工程学院，陕西 西安 710071）

摘 要：在密文策略的属性加密技术上提出一种支持文件级别的访问授权和数据用户撤销的多关键字密文查询方案。该方案在多数据拥有者多数据用户的场景下不仅支持文件级别的访问授权，即数据用户能够获取不同数据拥有者用不同密钥加密的密文，而且该方案能实现数据用户撤销。该方案在随机预言模型下是抗选择关键字攻击的，且基于实际数据集的实验结果表明方案在实际应用中是可行的、高效的。

关键词：可搜索加密；文件级别的访问授权；用户撤销；多关键字；属性加密
中图分类号：TN918.4 **文献标识码**：A

Multi-keyword search over encrypted data with user revocation

WU Qi-ying[1], MA Jian-feng[1,2], LI Hui[1], ZHANG Jun-wei[1], JIANG Qi[1], MIAO Yin-bin[1]
(1. School of Cyber Engineering, Xidian University, Xi'an 710071, China;
2. School of Telecommunication Engineering, Xidian University, Xi'an 710071, China)

Abstract: A multi-keyword search over encrypted data was proposecl with file-level access authorization and data user revocation scheme through employing ciphertext-policy attribute-based encryption (CP-ABE). The scheme supports file-level access authorization in the multi-owner multi-user settings, which means that data users could only gain the authorized files encrypted by different data owners with different keys. Moreover, the scheme could achieve data user revocation. Formal security analysis shows that the proposed scheme could resist the chosen keyword attack in random oracle. Moreover, the experimental study over real-world dataset demonstrates its efficiency and feasibility in practice.

Key words: searchable encryption, file-level access authorization, user revocation, multi-keyword, attribute-based encryption

1 引言

随着云计算[1]的普及与应用，数据用户选择将本地数据存储在云服务器上以节省本地数据的管理和维护开销。然而，云计算在提供便利的存储和计算服务的同时也带来了数据安全隐患[2]。为保护数据安全和隐私，数据拥有者在数据外包给云服务器之前需要对其进行加密。当数据用户要获取感兴趣的文档时，将全部密文下载到本地再解密的方式极大地浪费了网络带宽资源，并且效率低。可搜索加密技术（SE, searchable encryption）[3,4]在不泄露敏感信息给云服务器的前提下实现了密文高效的检索。根据密码构造的不同，SE 大致可以分为：对称可搜索加密方案[3]和非对称可搜索加密方案[4]。其中，数据拥有者根据关键字建立安全索引，当数据用户查询含有某个关键字的密文时需要向云服务器提交陷门，云服务器通过匹配陷门和索引来返回所需的文档密文。但大多数的可搜索加密方案[5,6]只能支持单关键字检索，云服务器会返回很多不相关的密文，并占用了大量的计算和带宽资源。因此，为了快

收稿日期：2016-10-18；**修回日期**：2017-02-17
基金项目：国家高技术研究发展计划（“836”计划）基金资助项目（No.2015AA016007）；国家自然科学基金资助项目（No.61472310，No.61672413）；中央高校基本科研业务费专项基金资助项目（No.JBG161511）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA016007), The National Natural Science Foundation of China (No.61472310，No.61672413), The Fundamental Research Funds for the Central Universities (No.JBG161511)

速、精确地定位到所需文档，实用的可搜索加密方案[7,8]应允许数据用户在一次查询请求中可以提交多个关键字。

在云环境解密方不固定的场景下，数据拥有者希望只有满足属性条件的数据用户才能对密文进行搜索。现有的属性加密技术（ABE, attribute-based encryption）实现了对数据用户的安全访问控制。根据访问策略是嵌入密文还是密钥，分为密文策略的属性加密（CP-ABE, ciphertext-policy attribute-based encryption）[9]和密钥策略的属性加密（KP-ABE, key-policy attribute-based encryption）[10]。特别地，基于 CP-ABE 的加密方案允许数据拥有者制定访问策略决定哪些数据用户能够访问密文数据，在实际应用场景中更具可扩展性。为此，Zheng 等[11]分别构造了基于 CP-ABE 的可搜索加密方案和基于 KP-ABE 的可搜索加密方案，方案允许满足访问控制策略的数据用户发起基于关键字的查询请求。为了提供更灵活的查询语句，Liu 等[12] 利用 ABE 提出支持模糊关键字查询的方案，克服了大部分可搜索加密方案只能支持精确关键字查询的缺陷。然而单个云服务器可能产生单点失效威胁，影响云服务器访问的可靠性。为此，Miao 等[13]分别利用 KP-ABE 和 CP-ABE 提出了支持多云模型的可搜索加密方案，确保了云存储的可靠性和数据的可访问性。

然而，基于 ABE 的可搜索加密技术仍然存在局限性。例如，无法撤销属性集发生改变的数据用户的搜索权限，则非法的数据用户会获得私密数据，造成数据泄露。Qian 等[14]提出了支持属性撤销的数据共享方案，但该方案不能支持关键字查询。接着，Yang 等[15] 利用 ABE 提出了同时支持用户撤销和关键字查询的数据共享方案。然而，上述的方案只能实现对数据用户的安全访问控制，在多数据拥有者共享海量文件给多数据用户的场景中，希望满足访问控制策略的数据用户能够获取不同数据拥有者用不同密钥加密的密文，即文件级别的访问授权。Li 等[16]利用分层谓词加密技术提出了支持授权关键字的可搜索加密方案，实现了文件级别的授权和属性撤销。但是该方案只支持结构化数据，且搜索时间与系统关键字数成正比。为此，Sun 等[17]的方案利用 CP-ABE 和代理重加密技术实现了文件级别的访问授权且支持数据用户的属性撤销。但该方案每次属性更新与系统中属性数量相关，造成大量的计算开销。

针对现有的可搜索加密方案不能同时支持用户撤销和文件级别的访问授权等问题，本文利用 CP-ABE 提出了支持文件级别的访问授权和用户撤销的多关键字密文查询方案。本文方案在多数据拥有者多数据用户的场景下，对某类文件采用相同的访问控制策略，该类文件可以来自不同的数据拥有者，并采用不同的密钥加密；满足访问控制策略的数据用户可以进行多关键字检索得到被授权文件。例如，对于来自不同医院的医疗记录，对安全等级相同的记录采用相同的访问控制策略，该类记录可以由不同密钥加密的。本文方案的优点如下，表 1 给出了本文方案与其他方案的功能比较。

1) 文件级别的访问授权：不同的数据拥有者用不同的密钥加密文件数据，本文方案利用 CP-ABE 加密密钥能实现文件级别的访问控制。

2) 用户撤销：当数据用户的属性集发生改变，数据用户无法利用旧的私钥解密密文。

3) 多关键字检索：多关键字避免了带宽和计算资源的浪费，且增强了数据用户的搜索体验。

4) 安全性：严格的安全分析表明文中方案在随机预言模型下是抵抗选择关键字攻击的；且合谋的数据用户不能通过授权中心的审计，本文方案能有效抵抗共谋攻击。

5) 效率：基于实际数据集的性能分析表明本文方案在实际应用场景中是可行的、高效的。

表 1 方案比较

方案	属性撤销	多关键字	文件级访问授权
Zheng 等[11]方案	不支持	不支持	不支持
Qian 等[14]方案	支持	不支持	不支持
Yang 等[15]方案	支持	支持	不支持
本文方案	支持	支持	支持

2 系统模型和安全模型

本节分别给出本文方案的系统模型和安全模型。

2.1 系统模型

本文方案的系统模型如图 1 所示，具体包括 5 个实体：数据拥有者（DO, data owner）、数据用户集（U, user）、云服务器（CS, cloud server）、证书中心（CA, certificate authority）、第三方审计（TPA, third-party auditor）。

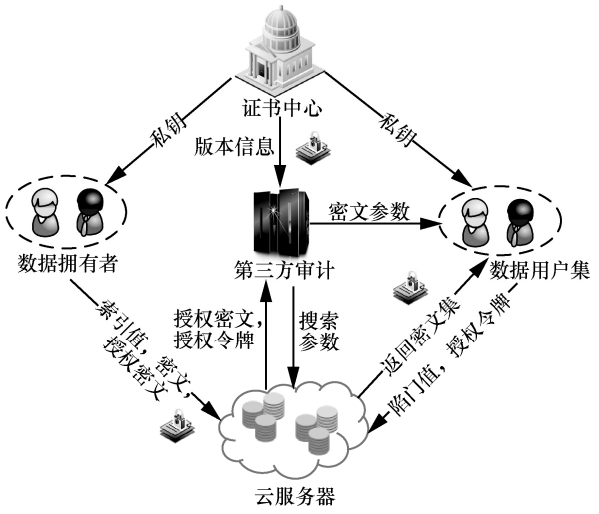


图 1　系统模型

1) 证书中心。本文假定 CA 是完全可信的，其主要负责系统初始化和生成数据用户的私钥。当数据用户 U_i 的属性集发生改变时，CA 更新数据用户的版本信息，并撤销数据用户旧的属性集。

2) 数据拥有者。DO 用传统对称加密算法加密文件，根据 CP-ABE 生成索引值和授权密文，并将密文、索引值和授权密文上传给 CS。

3) 数据用户集。数据用户 U_i 根据查询关键字集生成陷门值和授权令牌，最后将位置集、陷门值和授权令牌发送给 CS。

4) 云服务器。本文假定 CS 是诚实但好奇的，其诚实地执行既定协议，但又会好奇地获取敏感信息。CS 验证数据用户 U_i 是否满足访问控制策略，并与 TPA 交互获取搜索参数 D_r，然后匹配陷门值和索引值，得到密文，并将密文发送给数据用户，将密文对应的授权密文和搜索令牌发送给 TPA。

5) 第三方审计服务器。本文假定 TPA 是完全可信的，其主要负责接收 CS 的请求计算搜索参数 D_r，并根据密文对应的授权密文和搜索令牌，审计数据用户 U_i 是否被授权访问密文，最后发送密文参数给数据用户 U_i。

2.2　安全模型

本文通过定义选择关键字攻击游戏和关键字隐私安全游戏来构造安全模型。

2.2.1　选择关键字攻击游戏

如果不存在敌手 A 能够在概率多项式时间内推断出任何明文信息，本文考虑抗选择关键字语义安全性。本文按以下定义选择关键字攻击游戏。

1) 初始化。挑战者 C 选择安全参数 l，并且执行初始化算法 $\mathrm{Init}(1^l)$ 生成主密钥 msk 和公共参数 pm，接着执行 $\mathrm{KeyGen}(pm, msk, Atts)$，生成私钥 SK，然后把公共参数 pm 给敌手 A，主密钥 msk 和私钥 SK 由挑战者 C 持有。

2) 阶段 1。敌手 A 查询关键字集 $W_a,\cdots,W_t$，挑战者 C 执行陷门生成算法 $\mathrm{Trap}(pm, SK, W_i)$ 得到陷门值 T_{W_i}，并发送给敌手 A。

3) 挑战。敌手 A 选择 2 个挑战关键字集 (W_0, W_1) 并发送给挑战者 C，挑战者 C 随机选择 $b \in \{0,1\}$，并要求 W_0 和 W_1 在阶段 1 未被查询，然后挑战者 C 执行加密算法 $\mathrm{Enc}(pm, W_b, D, T)$ 生成索引 I_b，并将索引 I_b 返回给敌手 A。

4) 阶段 2。敌手 A 查询关键字集 $W_{t+1},\cdots,W_\tau$，挑战者 C 执行陷门生成 $\mathrm{Trap}(pm, SK, W_i)$ 算法得到陷门值 T_{W_i}，然后挑战者 C 将陷门值 T_{W_i} 返回给敌手 A，其中，$W_i \neq W_0, W_1$。

5) 猜测。敌手 A 输出猜测比特 $b' \in \{0,1\}$。如果 $b' = b$，则敌手 A 在游戏中获胜。

定义敌手 A 攻破安全游戏的优势为 $Adv_A(1^l) = |\Pr[b \neq b'] - \frac{1}{2}]|$。

2.2.2　关键字隐私安全游戏

如果不存在敌手 A 能够在概率多项式时间内从密文关键字或陷门值推断出关键字明文信息，则关键字的隐私安全可以得到保证。本文按以下定义关键字隐私安全游戏。

1) 初始化。给定安全参数 l，挑战者 C 执行初始化算法 $\mathrm{Init}(1^l)$，生成主密钥 msk 和公共参数 pm。

2) 阶段 1。敌手 A 执行以下算法多项式的次数。

私钥生成。挑战者 C 生成私钥 SK 发送给敌手 A，并把对应的属性集添加到列表 l_{KeyGen} 中。

陷门生成。给定私钥 SK 和关键字集 W，挑战者 C 得到陷门值 T_W 并返回给敌手 A。

3) 挑战。敌手 A 选取私钥 SK 发送给挑战者 C，挑战者 C 从关键字空间随机选取关键字集 W'，然后执行加密算法 $\mathrm{Enc}(pm, W', D, T)$，最后将索引值 I 发送给敌手 A。

4) 猜测。敌手 A 查询了 τ 个不同的关键字集合后，敌手 A 输出一个关键字集 W'，如果 $W = W'$，则敌手 A 在安全游戏中获胜。

本文方案是支持关键字安全隐私的，如果敌手

A 在安全游戏中获胜的概率最多是 $\frac{1}{|\Psi|-\tau}+\varepsilon$。其中，$\tau$ 表示关键字集的个数，ε 表示在安全参数 l 下可以忽略的概率，Ψ 表示关键字的空间。

3 预备知识

本节给出与相关的基础知识及定义。

3.1 双线性映射

假设 G_1, G_T 是阶为素数 p 的循环群，g 是群 G_1 的生成元，双线性映射 $e: G_1 \times G_1 \to G_T$ 满足以下性质。

1) 双线性：对任意的 $x, y \in G_1$，$a, b \in Z_p$，有 $e(x^a, y^b) = e(x^b, y^a) = e(x, y)^{ab}$。

2) 非退化性：存在 $g \in G_1$，使 $e(g, g) \neq 1$。

3) 可计算性：对所有的 $x, y \in G_1$，存在有效的算法计算 $e(x, y)$。

3.2 访问树

访问树可以用来描述访问控制策略，树中包含非叶子节点和叶子节点。其中，每个非叶子节点 v 代表一个门限，k_v 表示节点 v 的门限值，num_v 表示节点 v 的子节点个数，并对子节点从左至右依次编号 $1, \cdots, num_v$，并且 $1 \leqslant k_v \leqslant num_v$，当 $k_v = 1$ 表示节点 v 是或门，当 $k_v = num_v$ 表示节点 v 是与门，$parent(v)$ 表示节点 v 的父节点，$index(v)$ 表示节点 v 的编号。每个叶子节点 n 和属性值相关，$lvs(T)$ 表示访问树 T 的叶子节点集，T_v 表示根节点是 v 的子树，$att(n)$ 表示叶子节点 n 的属性值。

数据用户的属性集 $Atts$ 满足属性访问控制策略 T 是指：如果访问树 T 的叶子节点 n 的属性值 $att(n) \in Atts$，记 $T_n(atts) = 1$；对访问树 T 的非叶子节点 v，如果节点 v 存在 $|I|$ 个子节点 v' 满足 $T_{v'}(atts) = 1$，并且 $|I| \geqslant k_v$，记 $T_v(atts) = 1$。对访问树 T 的根节点 r，若 $T_r(atts) = 1$，则说明数据用户的属性集 $Atts$ 满足属性访问控制策略 T。

自顶向下的递归算法为每个节点构造多项式：对根节点 r，令 $q_r(0) = s$，并在其他 $k_r - 1$ 点处随机选取，构造出 $k_r - 1$ 次多项式 q_r。对非根节点 v，令 $q_v(0) = q_{parent(v)}(index(v))$，并在其他 $k_v - 1$ 点处随机选取，构造出 $k_v - 1$ 次多项式 q_v，从而由上述递归算法最终可以得到叶子节点 n 的多项式 q_n。

自底向上的递归算法恢复秘密值 s：若属性集 $\{att(u_1), \cdots, att(u_m)\}$ 满足访问控制策略 T_v，对叶子节点 n，计算 $D_n = e(g, g)^{q_{u_j}(0)}$；对非叶子节点 v，存在子节点集的子集 I 使 $|I| = k_v$，$j \in I$，则 $D_v = \prod_{j \in I} D_{v_j}^{\Delta_{v_j}} = \prod_{j \in I} (e(g, g)^{q_{v_j}(0)})^{\Delta_{v_j}} = e(g, g)^{q_v(0)}$，其中，$\Delta_{v_j} = \prod_{j \in I, l \neq j} \frac{-j}{l - j}$，最后恢复 $D_r = e(g, g)^s$。

4 方案描述

本文采用传统的对称加密算法加密文件数据，在此不做重点讨论。本文方案具体包括以下 8 种算法。

4.1 方案定义

1) $\text{Init}(1^l) \to (msk, pm)$：给定安全参数 l，完全可信的 CA 输出双线性映射参数 (G, G_T, e, p, g)，主密钥 msk 和公共参数 pm，其中，主密钥 msk 被 CA 私有。

2) $\text{KeyGen}(pm, msk, Atts) \to (SK, V)$：CA 首先为数据用户 U_i 生成版本信息 $V = (i, v_i)$，然后为数据用户 U_i 指定属性集合 $Atts$，并生成相应的私钥 SK，最后，CA 将私钥 SK 发送给数据用户 U_i，将版本信息 V 发送给 TPA。

3) $\text{Enc}(pm, k, W, D, T) \to (Cph, I, C)$：数据拥有者（DO）用密钥 k 加密文件 D 得到密文 C，定义访问结构 T，并利用密文策略的属性加密技术加密密钥 k，接着建立索引 I，生成授权密文 Cph，最后将密文 C、索引值 I 和授权密文 Cph 上传给 CS。

4) $\text{Trap}(pm, SK, W') \to (tk, L, T_{W'})$：数据用户 U_i 首先根据查询关键字集 $W' = (w_1', \cdots, w_l')$ 中每个关键字在给定关键字集 $W = \{w_1, \cdots, w_m\}$ 的相对位置得到位置集 L，然后利用私钥 SK 生成陷门值 $T_{W'}$ 和搜索令牌 tk，最后数据用户 U_i 将授权令牌 tk、陷门值 $T_{W'}$ 和位置集 L 发送给 CS。

5) $\text{Search}(pm, T_{W'}, I) \to (C')$：CS 首先验证数据用户是否满足访问控制策略，如果满足访问控制策略，CS 将授权密文 Cph 和授权令牌 tk 发送给 TPA，向 TPA 请求 D_r；TPA 根据递归算法自底向上地计算得到 D_r，返回给 CS；CS 匹配索引值 I 和陷门值 $T_{W'}$ 得到返回密文集 C'；CS 将返回密文集 C' 对应的授权密文 Cph 和授权令牌 tk 发送给 TPA，将返回密文集 C' 给数据用户。

6) $\text{Audit}(tk, Cph) \to \{0, 1\}$：TPA 验证数据用户 U_i 是否被授权访问返回密文集 C'，如果是被授权的，TPA 将返回密文集 C' 的相关参数 D_r、η_1、η 发送给数据用户 U_i。

7) $\mathrm{Dec}(SK, D_r, \eta, \eta_1) \to (k)$：数据用户 U_i 根据返回的密文参数，利用私钥 SK 解出用 CP-ABE 加密的密钥 k，从而完成对文档的解密。

8) $\mathrm{Revocation}(V)$：当数据用户 U_i 的属性集发生改变，CA 会将数据用户 U_i 新版本信息 $V' = (i, v_i')$ 发送给 TPA，数据用户 U_i 用旧版本信息 $V = (i, v_i)$ 生成的私钥 SK 不能通过审计，无法得到密钥 k，从而实现了数据用户 U_i 的撤销。只有当 CA 用新的版本信息 V' 为数据用户 U_i 生成新的私钥 SK'，此时数据用户 U_i 才能解密被授权的密文。

4.2　方案构造

在介绍本文方案的具体构造之前，表 2 给出方案用到的符号定义。

表 2　　符号定义

符号	定义
$W = \{w_1, \cdots, w_m\}$	给定的关键字集
$W' = (w'_1, \cdots, w'_l)$	查询关键字集
$D = \{d_1, \cdots, d_p\}$	文件集合
T	访问结构
$T_{W'}$	查询陷门值
I	索引值
C'	返回密文集
tk	授权令牌
Cph	授权密文
$Atts$	数据用户的属性集合
Ts	访问树叶子节点属性集合

初始化 $\mathrm{Init}(1^l) \to (msk, pm)$。给定安全参数 l，完全可信的 CA 首先输出双线性映射参数 (G, G_T, e, p, g)，其中，G 和 G_T 是阶为素数 p 的乘法循环群，g 是群 G 的生成元，双线性映射 $e: G \times G \to G_T$，然后选取随机数 $a, b, c, \beta, \mu \in Z_p$，接着定义散列函数 $H_1: \{0,1\}^* \to G$ 和散列函数 $H_2: \{0,1\}^* \to Z_p$，最后输出主密钥 msk 和公共参数 pm，其中，主密钥 msk 被 CA 私有。

$$msk = (a, b, c, \beta, \mu) \tag{1}$$

$$pm = (G, G_T, e, p, g, g^a, g^b, g^c, g^\beta, e(g,g)^\mu, H_1, H_2) \tag{2}$$

私钥生成 $\mathrm{KeyGen}(pm, msk, Atts) \to (SK, V)$：CA 首先为数据用户 U_i 选取随机版本号 $v_i \in Z_p$，得到数据用户 U_i 的版本信息 $V = (i, v_i)$，接着为数据用户 U_i 指定属性集 $Atts$，并为属性集 $Atts$ 中每个元素 a_j 选取随机数 $t_j \in Z_p$，然后再选取随机数 $r \in Z_p$，并计算 $A = g^{\frac{ac-r}{b}}$，$B = g^{\frac{\mu+r}{\beta}}$，$S_j = (g^r H_1(a_j)^{t_j})^{v_i}$，$K_j = (g^{t_j})^{v_i}$，最后 CA 将私钥 SK 发送给数据用户 U_i，将版本信息 V 发送给 TPA。其中，私钥 SK 为

$$SK = \{Atts, A, B, \{(S_j, K_j \mid a_j \in Atts)\}\} \tag{3}$$

1) 加密阶段

$\mathrm{Enc}(pm, k, W, D, T) \to (Cph, I, C)$：DO 首先利用传统对称加密算法 $Enc()$ 和密钥 k 加密文件集 D，得到密文集 $C = Enc_k(D)$；接着 DO 选取随机数 $r_1, r_2 \in Z_p$，定义访问结构 T。其中，Ts 表示访问树叶子节点的属性值集合，$att(n) \in Ts$ 表示每个叶子节点的属性值，访问树的每个节点按如下步骤自顶向下地生成多项式。对于访问树的根节点 r，令根节点多项式 $q_r(0) = r_2$，并随机选取其他 $k_r - 1$ 个不同点，则可得到根节点多项式 $q_r(x)$，其中，k_r 是节点 r 的门陷值；对于访问树的非根节点 v，令 $q_v(0) = q_{parent(v)}(index(v))$，并随机选取其他 $k_v - 1$ 个不同点，则可得到非根节点多项式 $q_v(x)$，其中，k_v 是节点 v 的门陷值；从而由上述递归算法最终可以得到叶子节点 n 的多项式 $q_n(x)$。对于给定关键字集 $W = \{w_1, \cdots, w_m\}$，$w_i \in \Psi$ 关键字空间，DO 首先为每个文件 d 提取关键字集并建立索引，计算 $\delta = g^{cr_1}$，$\delta_1 = g^{a(r_1+r_2)} g^{br_1}$，$\delta_2 = g^{br_2}$，$\delta_3 = g^{ar_2}$，$\eta = ke(g,g)^{\mu r_2}$，$\eta_1 = g^{\beta r_2}$，$\pi_n = g^{q_n(0)}$，$\vartheta_n = H_1(att(n))^{q_n(0)}$，若文件 d 含关键字 $w_i (1 \leqslant i \leqslant m)$，则令 $\varphi_i = g^{a r_1 H_2(w_i)} (1 \leqslant i \leqslant m)$，否则令 $\varphi_i = 1$；最后 DO 将密文集 C、索引值 I 和授权密文 Cph 上传给 CS。其中，索引值 I 如式(4)所示，授权密文 Cph 如式(5)所示。

$$I = \{\varphi_i (1 \leqslant i \leqslant m), \delta, \delta_2, \delta_3\} \tag{4}$$

$$Cph = \{\delta, \delta_1, \delta_2, \eta, \eta_1, \{(\pi_n, \vartheta_n \mid at(n) \in Ts)\}\} \tag{5}$$

陷门生成 $\mathrm{Trap}(pm, SK, W') \to (tk, L, T_{W'})$：数据用户 U_i 首先根据查询关键字集 $W' = (w'_1, \cdots, w'_l)$ 中每个关键字在给定关键字集 $W = \{w_1, \cdots, w_m\}$ 的相对位置得到位置集 L，数据用户 U_i 选取随机数 $s \in Z_p$，计算 $t_1 = (g^a g^b)^s$，$t_2 = g^{cs}$，$t_3 = A^s$，$t_4 = \prod_{\tau=1}^{l} g^{asH_2(w'_\tau)}$，并对每个属性值 $a_j \in Atts$ 计算

$S'_j = S_j^s$，$K'_j = K_j^s$，最后，数据用户 U_i 将授权令牌 tk、陷门值 $T_{W'}$ 和位置集 L 提交给 CS。其中，陷门值 $T_{W'}$ 如式(6)所示，授权令牌 tk 如式(7)所示。

$$T_{W'} = \{Atts, t_2, t_3, t_4\} \tag{6}$$

$$tk = \{Atts, t_1, t_2, t_3, \{(S'_j, K'_j \mid a_j \in Atts)\}\} \tag{7}$$

2) 搜索阶段

Search $(pm, T_{W'}, I) \to (C')$：按照以下步骤进行。

步骤 1 CS 验证数据用户 U_i 是否满足访问控制策略，如果不满足访问控制策略，结束；否则转步骤 2。

步骤 2 CS 将授权密文 Cph 和授权令牌 tk 发送给 TPA，向 TPA 请求 D_r，转步骤 3。

步骤 3 TPA 按以下步骤自底向上地计算 D_r。对于叶子节点 n，验证每个叶子节点 n 的属性值 $att(n)$ 是否属于数据用户 U_i 的属性集 $Atts$，如果属于，则按式(8)计算 D_n，否则令 $D_n = \perp$；对于非叶子节点 v，先计算 v 所有子节点 v' 的 $D_{v'}$，如果 v 存在 k_v 个子节点 v'，记该子节点集合为 ω_v；如果不存在，则记 $D_{v'} = \perp$，接着计算 $D_v = \prod_{v' \in \omega_v} D_{v'}^{\Delta_{i,\omega'_v}(0)} = e(g,g)^{rsq_v(0)}$；其中，$i = index(v')$，$\omega'_v = \{index(v') : v' \in \omega_v\}$。由上述递归算法最终可以得到根节点 r 的 D_r，$D_r = e(g,g)^{rsq_r(0)} = e(g,g)^{rsr_2}$；将 D_r 发送给 CS，转步骤 4。

步骤 4 CS 利用索引值 I 和陷门值 $T_{W'}$ 验证式(9)是否成立，如果等式不成立，则输出 $\perp$，如果成立，则说明匹配成功得到返回密文集 C'，转步骤 5。其中，符号 $\tau \to i$ 表示查询关键字下标在给定关键字中的映射关系。

步骤 5 CS 将匹配成功的返回密文集 C' 对应的授权密文 Cph 和授权令牌 tk 发送给 TPA，将返回密文集发送给数据用户。

$$D_n = \frac{e(S_j'^{\frac{1}{v_i}}, \pi_n)}{e(K_j'^{\frac{1}{v_i}}, \vartheta_n)} = e(g,g)^{rsq_n(0)} \tag{8}$$

$$e(\prod_{\tau=1}^{l} \varphi_{\tau \to i} \delta_3, t_2) = e(\delta, t_4) D_r e(\delta_2, t_3) \tag{9}$$

3) 审计阶段

Audit $(tk, Cph) \to \{0,1\}$：TPA 验证式(10)是否成立，如果等式不成立，则说明数据用户 U_i 没有被授权访问这个文件，输出 $\perp$；如果等式成立，TPA 将返回密文集 C' 的相关参数 D_r、η_1、η 发送给数据用户 U_i。

$$e(\delta_1, t_2) = e(\delta, t_1) D_r e(\delta_2, t_3) \tag{10}$$

4) 解密阶段

Dec $(SK, D_r, \eta, \eta_1) \to (k)$：数据用户 U_i 根据返回的密文参数，利用私钥 SK 解出用密文策略的属性加密技术加密的密钥 k，从而完成对文档的解密。

$$\frac{\eta}{\frac{e(\eta_1, B)}{(D_r)^{\frac{1}{s}}}} = \frac{ke(g,g)^{\mu r_2}}{e(g^{\beta r_2}, g^{\frac{\mu + r}{\beta}}) e(g,g)^{-r r_2}} = k \tag{11}$$

5) 撤销阶段

Revocation (V)：当数据用户 U_i 的属性集发生改变，CA 会将数据用户 U_i 新版本信息 $V' = (i, v'_i)$ 发送给 TPA，数据用户 U_i 用旧版本信息 $V = (i, v_i)$ 生成的私钥 SK 不能通过审计阶段，无法得到密文密钥 k，从而实现了数据用户 U_i 的撤销。只有当 CA 用新的版本信息 V' 为数据用户 U_i 生成新的私钥 SK'，此时数据用户 U_i 才能解密被授权的密文。

4.3 正确性分析

为了验证式(9)的正确性，当数据用户 U_i 满足属性访问控制，并且提交的关键字集合满足 $W' \subseteq W$，则

$$\begin{aligned}
&e(\delta, t_4) D_r e(\delta_2, t_3) \\
&= e(g,g)^{cr_1 as \sum_{\tau \in [1,l]} H_2(w'_i)} e(g,g)^{rsr_2} e(g,g)^{r_2 sac - r_2 sr} \\
&= e(g,g)^{csa(r_2 + r_1 \sum_{\tau \in [1,l]} H_2(w'_i))} \\
&e(\prod_{\tau=1}^{l} \varphi_{\tau \to i} \delta_3, t_2) \\
&= e(g^{ar_2 + ar_1 \sum_{\tau \in [1,l]} H_2(w'_i)}, g^{cs}) \\
&= e(g,g)^{csa(r_2 + r_1 \sum_{\tau \in [1,l]} H_2(w'_i))}
\end{aligned}$$

最终，可以验证式(9)的正确性，即

$$e(\prod_{\tau=1}^{l} \varphi_{\tau \to i} \delta_3, t_2) = e(\delta, t_4) D_r e(\delta_2, t_3)$$

为了验证式(10)的正确性，当数据用户 U_i 满足属性访问控制，CS 进行多关键字搜索得到返回密文集 C'，TPA 验证返回密文集是否对数据用户授权，则

$$\begin{aligned}
&e(\delta, t_1) D_r e(\delta_2, t_3) \\
&= e(g,g)^{cr_1 s(a+b)} e(g,g)^{rsr_2} e(g,g)^{r_2 s(ac - r)}
\end{aligned}$$

$$= e(g,g)^{car_1(a+b)+casr_2}$$

$$e(\delta_1,t_2) = e(g,g)^{csr_1(a+b)+ascr_2}$$

最终，可以验证式(10)的正确性，即

$$e(\delta_1,t_2) = e(\delta,t_1)D_r e(\delta_2,t_3)$$

5　安全分析

本文方案能够保证文件安全性，数据拥有者将明文文件外包给云服务器之前，用传统的对称密钥 k 加密文件，并用 CP-ABE 加密密钥 k。只有当文件对数据用户授权时，才能解密得到密钥 k，从而得到明文文档。此外，本文方案是抗共谋攻击的，不同的数据用户即使拥有相同的属性集合，由于版本信息的不同，他们的私钥也是完全不同的。即使数据用户之间用私钥合谋生成搜索令牌，该搜索令牌将无法通过审计，数据用户之间合谋是无法得到额外信息的。同时，本文方案能抵抗选择关键字攻击和保护关键字隐私，接下来，给出相应的定理分析和证明。

定理 1　基于一般双线性群，本文方案在随机预言模型下是抗选择关键字攻击的。其中，散列函数 H_1 是随机预言机，H_2 是单向的散列函数。

证明　在安全游戏中，敌手 A 尝试区分 $g^{ar_1H_2(w_0)}$ 和 $g^{ar_1H_2(w_1)}$。选取随机数 $q\in Z_p$，从 $g^{ar_1H_2(w_0)}$ 中区分 g^q 的概率和从 $g^{ar_1H_2(w_1)}$ 中区分 g^q 的概率是相同的。具体的安全游戏如下。

初始化。挑战者 C 选取随机数 $a,b,c,\beta,\mu\in Z_p$，计算得到公共参数 $pm=(e,g,p,g^a,g^b,g^c,g^\beta,e(g,g)^\mu)$，并发送给敌手 A。敌手 A 选择访问控制策略 T' 并返回给挑战者 C，挑战者 C 按以下方法模拟随机预言 $O_{H_1(a_j)}$：如果属性 a_j 没有被查询过，挑战者 C 选取随机数 $t_j'\in Z_p$，并把 (a_j,t_j') 添加到 O_{H_1} 中，输出 $g^{t_j'}$；否则挑战者 C 检索随机预言 $O_{H_1(a_j)}$ 得到 t_j'，输出 $g^{t_j'}$。

1) 敌手 A 按以下方式查询预言机 O_{KeyGen} 和 O_{Trap}。

$O_{\mathrm{KeyGen}}(pm,msk,Atts)$：挑战者 C 选择随机数 $r^*\in Z_p$ 并计算 $A=g^{\frac{ac-r^*}{b}}$，$B=g^{\frac{\mu+r^*}{\beta}}$，然后选择随机数 $t_j{}^*\in Z_p$ 对每个属性 $a_j\in Atts$ 计算 $S_j=(g^{r^*}H_1(a_j)^{t_j{}^*})^{v_i}$，$K_j=(g^{t_j{}^*})^{v_i}$，挑战者 C 得到私钥 $SK=\{Atts,A,B,\{(S_j,K_j\mid a_j\in Atts)\}\}$，并将 SK 返回给敌手 A。

O_{Trap}：挑战者 C 查询 O_{KeyGen} 预言，得到私钥 SK，然后挑战者 C 选择随机数 $s\in Z_p$，并计算 $t_2=g^{cs}$，$t_3=A^s$，$t_4=\prod_{\tau=1}^{l}g^{asH_2(w_\tau)}$，如果属性 $Atts$ 满足访问控制策略，挑战者 C 把 W^* 添加到关键字集列表 L_W。

挑战：给定不在关键字集列表 L_W 中的关键字集 W_0 和 W_1，挑战者 C 选取随机数 $r_1,r_2\in Z_p$，利用访问树共享秘密值 r_2，挑战者 C 输出猜测比特 $b^*\in\{0,1\}$。如果 $b^*=0$，输出 $\varphi_i=g^{qH_2(w_i)}$ $(1\leqslant i\leqslant m)$，$\delta=g^{cr_1}$，$\delta_2=g^{br_2}$，$\delta_3=g^{ar_2}$。否则，挑战者 C 输出 $\varphi_i=g^{ar_1H_2(w_i)}(1\leqslant i\leqslant m)$，$\delta=g^{cr_1}$，$\delta_2=g^{br_2}$，$\delta_3=g^{ar_2}$。

2) 该阶段和 1)类似。

假设 $\exists\xi\in Z_p$，对于 g^ξ，若敌手 A 可以由查询过的预言输出构造 $g^{\xi ar_1H_2(w_i)}$，则敌手 A 可以区分 $g^{ar_1H_2(w_i)}$ 和 g^q，因此本文只需要证明敌手 A 能以可以忽略的优势从 g^ξ 构造出 $e(g,g)^{\xi ar_1H_2(w_i)}$，即敌手 A 只能以可以忽略的优势赢得选择关键字攻击游戏。本文注意到 r_1 以 cr_1 的形式存在，所以构造 $e(g,g)^{\xi ar_1H_2(w_i)}$ 要求 ξ 包含 c。对某些 ξ'，令 $\xi=\xi'c$，敌手 A 只需构造出 $e(g,g)^{\xi' car_1}$。又因为 $\frac{br_2(ac-r^*)}{b}=r_2(ac-r^*)$，敌手 A 需要利用 r^* 和 $q_r(0)$ 消去 r_2r^*，而只有当数据用户的属性满足访问控制策略时，才能构造出 r_2r^*。

因此，本文可以得出结论，敌手只能以可以忽略的优势赢得选择关键字攻击游戏。

定理 2　给定单向的散列函数 H_2，本文方案在随机预言模型下是关键字隐私安全的。

证明　初始化。挑战者 C 选取随机数 $a,b,c,\beta,\mu\in Z_p$，$x\in G$，单向的散列函数 $H_2:\{0,1\}^*\to Z_p$，主密钥为 $msk=(a,b,c,\beta,\mu)$，公共参数 $pm=(e,p,g,g^a,g^b,g^c,g^\beta,e(g,g)^\mu,x)$。挑战者 C 按以下方法模拟随机预言 $O_{H_1(a_j)}$：如果属性 a_j 没有被查询过，挑战者 C 选取随机数 $t_j\in Z_p$，并把 (a_j,t_j) 添加到 O_{H_1} 中，输出 g^{t_j}；否则挑战者 C 检索随机预言 $O_{H_1(a_j)}$ 得到 t_j，输出 g^{t_j}。

敌手 A 按以下方式以多项式次数查询预言机 O_{KeyGen} 和 O_{Trap}。

O_{KeyGen}：挑战者 C 执行私钥生成算法得到私钥 SK 并返回给敌手 A，并把属性 $Atts$ 添加到列表 l_{KeyGen} 中。

O_{Trap}：挑战者 C 查询 O_{KeyGen} 预言，得到私钥 SK，然后执行陷门生成算法得到陷门值 T_W，并将陷门值 T_W 返回给敌手 A。

挑战：敌手 A 随机选取属性集 $Atts'$，挑战者 C 选择访问控制策略 T'，生成私钥 SK'，并发送给敌手 A，敌手 A 随机选取关键字集 W'，执行加密算法和陷门生成算法，得到密文 C' 和陷门值 $T_{W'}$，其中，属性集 $Atts'$ 满足访问控制策略 T'。

猜测：敌手 A 查询了 τ 个关键字集后，输出关键字集 $W*$，如果 $W'=W*$，则敌手 A 在安全实验中获胜。

敌手 A 查询了 τ 个关键字集后，正确猜测出关键字集 W'，则敌手 A 最多以概率 $\frac{1}{|\Psi|-\tau}+\varepsilon$ 赢得关键字隐私安全游戏。其中，关键字集的剩余空间是 $|\Psi|-\tau$，H_2 表示单向安全的散列函数，敌手 A 只能以可以忽略的优势 ε 从 $H_2(W')$ 中分离关键字 W'，所以本文方案能够保证关键字隐私安全。

6 性能分析

本文分别从理论和实际性能的角度对比分析 ABKS-UR[17] 方案和本文方案的优劣性。

6.1 理论分析

表 3 是 ABKS-UR[17] 方案和本文方案之间的理论性能比较，本文主要考虑几种比较耗时的密码运算，即群 G 中的指数运算 E、群 G_T 中的指数运算 E_T、散列运算 H_1 以及双线性对运算 P。其中，$|N|$ 表示系统属性个数；$|S|$ 表示数据用户属性个数；m 表示关键字数；l 表示数据用户查询关键字数；$|R|$ 表示返回密文文件数；–表示没有这项操作。

表 3 效率理论分析

算法	方案	
	ABKS-UR	本文方案
Init	$3\|N\|E+E_T+P$	$4E+E_T+P$
KeyGen	$(2\|N\|+1)E+2E_T$	$(2\|S\|+3)E+\|S\|H_1$
Enc	$(\|N\|+1)E+E_T$	$(2\|N\|+m+6)E+\|N\|H_1+E_T$
Trap	$(2\|N\|+1)E$	$(2\|S\|+l+4)E$
Search	$(\|N\|+1)E+E_T$	$2\|S\|E+E_T+5P$
Audit	–	$3\|R\|P$
Dec	–	$\|R\|(P+E_T)$

本文方案包括以下算法：Init、KeyGen、Enc、Trap、Search、Audit、Dec。在 Init 阶段，本文方案的初始化时间明显少于 ABKS-UR 方案。因为 ABKS-UR 方案初始化时间会随着系统属性个数 $|N|$ 增加而线性增加，而本文方案初始化时间是固定的。在 KeyGen、Trap 和 Search 阶段，本文方案的效率都是优于 ABKS-UR 方案的。因为 ABKS-UR 方案的私钥生成时间，陷门生成时间和搜索时间随着系统属性个数 $|N|$ 增加而线性增加，本文方案的私钥生成时间，陷门生成时间和搜索时间是随着数据用户属性个数 $|S|$ 增加而线性增加，而在实际应用中，数据用户的属性个数是远远小于系统属性个数的。在 Enc 阶段，本文方案尽管在效率上劣于 ABKS-UR 方案，但是数据的加密操作是一次性的，对方案的性能并没有本质的影响。此外，本文方案在 Audit 和 Dec 阶段的时间开销是多于 ABKS-UR 方案的。但从整体上看，对于大规模的系统，系统属性个数会严重影响 ABKS-UR 方案的效率，而本文方案是高效可行的。

6.2 实验分析

本文通过一系列的仿真实验，对比分析了 ABKS-UR[17] 方案和本文方案的实际性能。实验是基于实际数据集以及密码函数库（PBC, pairing-based cryptography）中的 A 类椭圆曲线。其中，A 可表示为 $E(F_q): y^2=x^3+x$，群 G 是 $E(F_q)$ 的子群，群 G 的阶为 160 bit，基域为 512 bit。实验平台是 CPU 为酷睿 i5，2.3 GHz，内存为 4 GB，操作系统为 Ubuntu 15.04 的笔记本电脑，且 $|S|$、$|N|$、$|R|$、l、m 的取值范围分别是[1,10]、[1,100]、[1,50]、[1,10]、[1,1 000]。

ABKS-UR 方案和本文方案在 Init 阶段时间开销的对比如图 2 所示，其中，系统属性个数的取值是 $|N|=\{20,40,60,80,100\}$。ABKS-UR 方案的初始化时间会随着系统中属性集个数 $|N|$ 增加而线性增加，而本文方案初始化时间是固定的，故本文方案的初始化时间是远远小于 ABKS-UR 方案的。特别地，当系统属性个数|N|=100，本文方案的初始化时间仅为 ABKS-UR 方案的 6.4%。

ABKS-UR 方案和本文方案在 KeyGen 阶段时间开销的对比如图 3 所示，其中，数据用户提交属性个数的取值是 $|S|=\{2,4,6,8,10\}$，固定系统属性个数

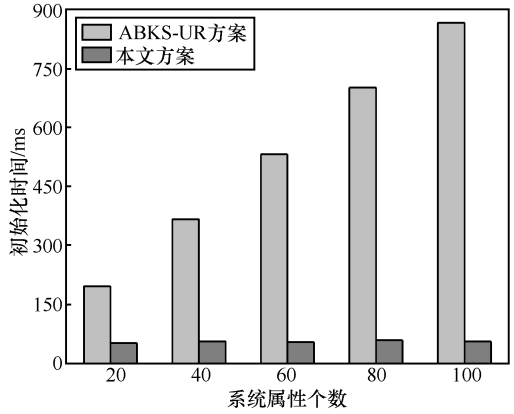


图 2　初始化开销

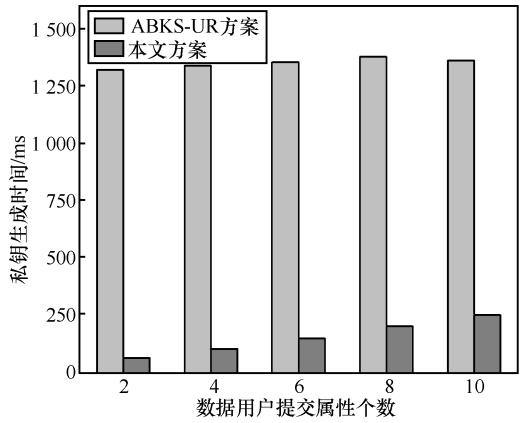


图 3　私钥生成开销

为 100。ABKS-UR 方案的私钥生成时间 $(2|N|+1)E+2E_T$ 是和系统属性个数 $|N|$ 成正比，而本文方案的私钥生成时间 $(2|S|+3)E+|S|H_1$ 是随着数据用户属性个数 $|S|$ 增加而线性增加。在实际应用中，数据用户的属性个数是远远小于系统属性个数的，所以本文方案的私钥生成效率优于 ABKS-UR 方案。特别地，当系统属性个数固定是 100，数据用户的属性个数是 10 时，本文方案的私钥生成时间仅为 ABKS-UR 方案的 18.5%。

ABKS-UR 方案和本文方案在 Enc 阶段的时间开销的对比如图 4 所示，其中，固定文件数为 10 000，关键字数是 1 000，系统属性个数的取值是 $|N|=\{20,40,60,80,100\}$。本文方案和 ABKS-UR 方案的密文生成时间都是随着系统属性个数 $|N|$ 的增加而线性增加。本文方案密文生成时间 $(2|N|+m+6)E+|N|H_1+E_T$ 比 ABKS-UR 方案 $(|N|+1)E+E_T$ 多出 $|N|$ 个群 G 上的指数操作 E 和 $|N|$ 个散列运算 H_1，尽管本文方案在效率上略劣于 ABKS-UR 方案，但是数据的加密操作是一次性的，对方案的性能并没有本质的影响。

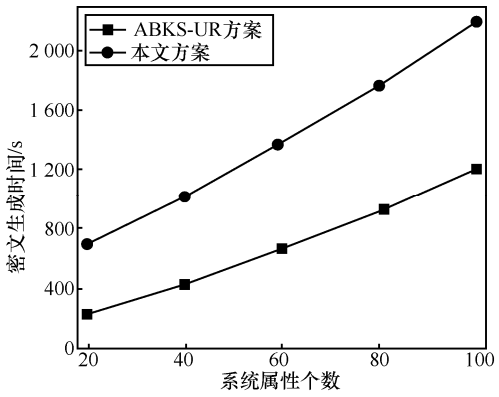


图 4　密文生成开销

ABKS-UR 方案和本文方案在 Trap 阶段时间开销的对比如图 5 所示，其中，固定系统属性个数为 100，数据用户提交的属性个数为 10，数据用户查询关键字数的取值是 $l=\{10,20,30,40,50\}$。ABKS-UR 方案的陷门生成时间 $(2|N|+1)E$ 是和系统属性个数 $|N|$ 成正比，与查询关键字数 l 无关。而本文方案的陷门生成时间 $(2|S|+l+4)E$ 是与数据用户属性个数 $|S|$ 和查询关键字数 l 成正比的。固定系统属性和用户提交的属性个数，尽管随着查询关键字数的增加，本文方案的陷门生成时间会逐渐增加，但是数据用户的属性个数是远远小于系统属性个数的，从总体上看本文方案的陷门生成效率优于 ABKS-UR 方案。特别地，当查询关键字数是 50 时，本文方案陷门生成时间开销是 ABKS-UR 方案的 43.1%。

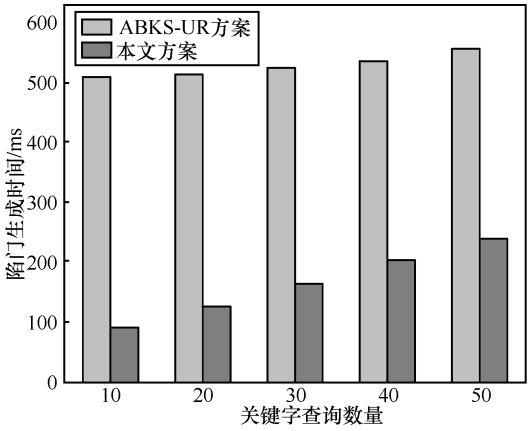


图 5　陷门生成开销

ABKS-UR 方案和本文方案在 Trap 阶段时间开销的对比如图 6 所示，其中，固定系统属性个数为 100，数据用户的查询关键字数为 50，数据用户的属性个数取值是 $|S|=\{2,4,6,8,10\}$。固定系统属性和

数据用户的查询关键字数，尽管随着数据用户的属性个数的增加，本文方案的陷门生成时间会逐渐增加，但是数据用户的属性个数是远远小于系统属性个数的，从总体上看本文方案的陷门生成效率优于 ABKS-UR 方案。特别地，当数据用户的属性个数 10 时，本文方案陷门生成时间开销是 ABKS-UR 方案的 51.9%。

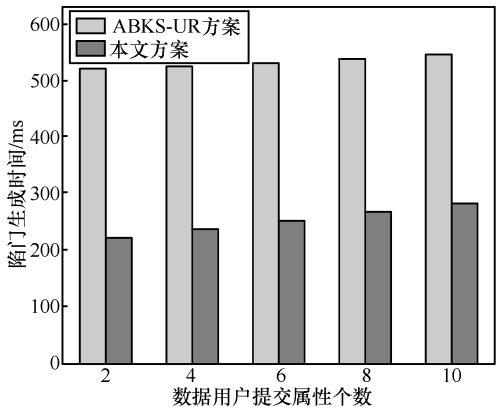


图 6　陷门生成开销

ABKS-UR 方案和本文方案在 Search 阶段时间开销的对比如图 7 所示，其中，固定系统属性个数为 100，数据用户提交属性个数的取值是 $|S|=\{2,4,6,8,10\}$。ABKS-UR 方案的密文搜索时间 $(|N|+1)E+E_T$ 是和系统中属性集个数 $|N|$ 成正比，而本文方案的密文搜索时间 $2|S|E+E_T+5P$ 是随着数据用户属性个数 $|S|$ 增加而线性增加。在实际应用中，数据用户的属性个数是远远小于系统属性个数的，所以本文方案的密文搜索效率优于 ABKS-UR 方案。特别地，当系统属性个数固定是 100，数据用户的属性个数是 10 时，本文方案的时间开销是 ABKS-UR 方案的 25.4%。

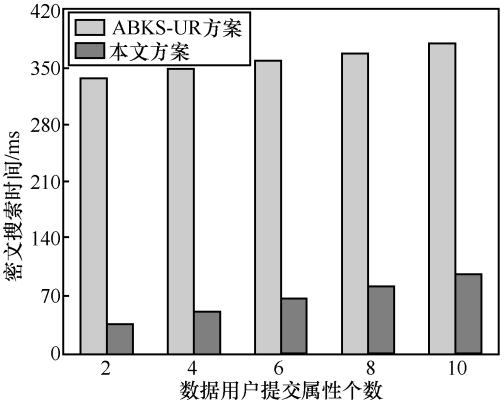


图 7　密文搜索开销

本文方案在 Audit 和 Dec 阶段的时间开销如图 8 所示，其中，返回密文数的取值范围是 $|R|=\{10,20,30,40,50\}$。Audit 阶段的审计开销 $3|R|P$ 和返回密文数 $|R|$ 成正比，Dec 阶段的解密时间开销 $|R|(P+E_T)$ 也和返回密文数 $|R|$ 成正比。

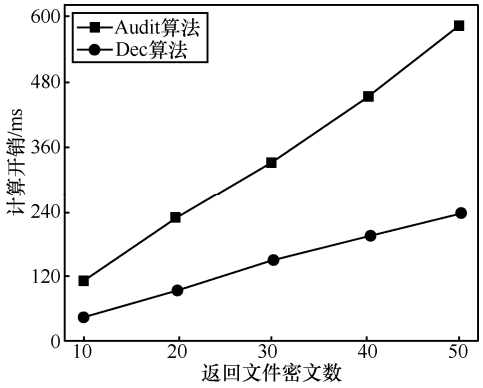


图 8　审计和解密开销

通过以上分析，本文方案理论性能分析和实际性能验证一致，因此本文方案在实际应用场景中是高效可行的。

7　结束语

本文提出了支持文件级别的访问授权和用户撤销的多关键字密文查询方案。方案结合 CP-ABE 和 SE，在多数据拥有者多数据用户场景下实现文件级别的访问控制，同时支持撤销属性集发生改变的数据用户的搜索权限。方案在随机预言模型下是抗选择关键字攻击和抗合谋攻击的，且方案在实际应用场景中是高效可行的。未来的工作将改进本文方案，使其拥有更高的搜索效率，支持动态搜索的功能。

参考文献：

[1] JIANG Q, MA J F, WEI F S. On the security of a privacy-aware authentication scheme for distributed mobile cloud computing services[J]. IEEE Systems Journal, 2017, pp(99): 1-4.

[2] JIANG Q, KHAN M K, LU X, et al. A privacy preserving three-factor authentication protocol for e-health clouds[J]. Journal of Supercomputing, 2016, 72(10): 3826-3849.

[3] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//IEEE Symposium on Security and Privacy. 2000: 44-55.

[4] BONEH D, DI C G, OSTROVSKY R, et al. Public key encryption with keyword search[C]//International Conference on the Theory and Applications of Cryptographic Techniques. 2004: 506-522.

[5] LI J, WANG Q, WANG C, et al. Fuzzy keyword search over encrypted

data in cloud computing[C]//The 29th IEEE International Conference on Computer Communications. 2010: 1-5.

[6] CHEN R, MU Y, YANG G, et al. Dual-server public-key encryption with keyword search for secure cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2016, 11(4): 789-798.

[7] MIAO Y, MA J, WEI F, et al. VCSE: verifiable conjunctive keywords search over encrypted data without secure-channel[J]. Peer-to-Peer Networking and Applications, 2016: 1-13.

[8] LI H, LIU D, JIA K, et al. Achieving authorized and ranked multi-keyword search over encrypted cloud data[C]//IEEE International Conference on Communications. 2015: 7450-7455.

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

[10] 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.

[11] ZHENG Q, XU S, ATENIESE G. VABKS: verifiable attribute-based keyword search over outsourced encrypted data[C]//IEEE Conference on Computer Communications. 2014:522-530.

[12] LIU Z, WENG J, LI J, et al. Cloud-based electronic health record system supporting fuzzy keyword search[J]. Soft Computing, 2015: 1-13.

[13] MIAO Y, LIU J, MA J. Fine-grained searchable encryption over encrypted data in multi-clouds[C]//The 10th International Conference on Wireless Algorithms, Systems, and Applications. 2015: 407-416.

[14] 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. 2014, 14(6): 1-11.

[15] YANG Y. Attribute-based data retrieval with semantic keyword search for e-health cloud[J]. Journal of Cloud Computing. 2015, 4(1):1-6.

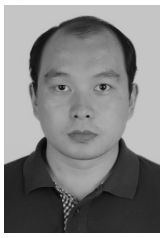
[16] LI M, YU S, CAO N, et al. Authorized private keyword search over encrypted data in cloud computing[C]//International Conference on Distributed Computing Systems. 2011:383-392.

[17] SUN W, YU S, LOU W, et al. Protecting your right: verifiable attribute-based keyword search with fine-grained owner-enforced search authorization in the Cloud[J]. IEEE Transactions on Parallel and Distributed Systems, 2016, 27(4):1187-1198.

作者简介：

伍祈应（1994-），女，湖南邵阳人，西安电子科技大学硕士生，主要研究方向为网络与信息安全。

马建峰（1963-），男，陕西西安人，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、无线和移动安全等。



李辉（1983-），男，湖北武汉人，博士，西安电子科技大学副教授，主要研究方向为社交网络的知识发现和挖掘、安全的数据管理和查询等。

张俊伟（1982-），男，陕西西安人，博士，西安电子科技大学副教授，主要研究方向为密码学、网络安全等。

姜奇（1983-），男，安徽全椒人，博士，西安电子科技大学副教授，主要研究方向为安全协议分析、无线网络安全。

苗银宾（1988-），男，河南驻马店人，博士，西安电子科技大学讲师，主要研究方向为应用密码学、无线网络安全。