# 分级管理权限匿名多用户云加密搜索方案

段阳阳 李诗旸

(暨南大学信息科学技术学院 广州 510632)

**摘 要** 针对目前云计算环境下多用户加密搜索方案存在的问题,首先提出了一个基本的多用户加密搜索方案,然后将这个基本方案延伸为匿名的分级管理权限的多用户加密搜索方案。与已有的大多数方案相比,该方案不仅实现了对关键字信息的保护,也实现了对用户身份隐私的保护;同时数据拥有者可以直接控制用户查询权限,而不是云端服务器。此外,通过采用一种特殊的查询密钥生成规则,实现了分级管理用户的查询权限。安全分析表明该方案是安全的,同时性能分析及实验数据表明该方案是实际可行的。

**关键词** 加密关键字查询,匿名查询,多用户加密搜索,分级管理权限

**中图法分类号** TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.2.035

## Anonymous Multi-user Searchable Encryption Scheme with Hierarchial Permission Management

DUAN Yang-yang LI Shi-yang

(College of Information Science and Technology, Jinan University, Guangzhou 510632, China)

**Abstract** To deal with the existing problems of multi-user searchable encryption schemes in the cloud computing, we firstly proposed a basic multi-user searchable encryption scheme, and then extended this basic scheme to a multi-user searchable encryption scheme with anonymous hierarchical permission management. Compared with existing schemes, our scheme not only achieves privacy preserving in both of the searching content and users' identities, but also allows the data owner to directly control the dynamic updating of query permission. Additionally, our scheme realizes the hierarchical users' query permission management by adopting a specific query key generation rule. The security of our scheme was illustrated by security analysis. Performance evaluation and experimental result show that our scheme is practical and feasible.

**Keywords** Encrypted keyword search, Anonymous query, Multi-user searchable encryption, Hierarchical permission management

## 1 引言

随着计算机网络技术的迅速发展以及人们对信息资源的需求不断增加,越来越多的企业和个人希望通过云存储技术来降低本地存储设备的成本。但是云存储在带来方便、易用和低成本的同时也引了许多新的安全问题,数据拥有者不能直接控制用户的访问权限,而云端服务器并不是完全可信的,因此云端数据面临着泄漏的风险。

为了保证数据的安全性,通常大多数方案使用密码学理论知识加密数据,数据以密文的形式存储在云服务器中,因此关于加密数据的搜索技术应运而生。数据加密是防止云端数据泄漏的最基本的方法,数据拥有者在把数据传送到云端服务器之前先对数据进行加密。云端服务器和攻击者即使获取了加密数据也得不到任何相关的信息,从而保证云端数据是安全的。但是,如何在云端加密数据库中搜索到用户所需要的信息? 2000年,Song、Wagner、Perrig[1]等人首次提出了可加密搜索的概念,并且构造了一个对称加密关键字搜索方案,该课题引起了学者们的广泛关注。但是这个方案只能提供查询服务,无法实现信息共享。2004年,Boneh、Crescenzo、Ostrovsky[2]等人利用基于身份的匿名加密方案构造了一个基于公钥密码体制的可搜索加密方案。该方案使用双线性映射的特性实现了加密索引和查询门限的匹配,同时初步实现了云端数据库信息共享的功能。

但是,已有的可搜索加密方案仅限于关键字密文与查询方一对一关系的单个用户查询的场景。在云计算环境中,当数据拥有者希望与其他用户共享数据时,数据与接收方之间是一对多的关系。随着多用户查询需求不断增加,显然单个用户查询不能直接有效地应用到多用户查询中。比如,单个用户查询中并没有考虑用户查询权限的变更,而这在多用户查询中是非常重要的。其中Yang、Lu、Weng[8]等人和Bao、Deng、Ding[9]等人提出多用户加密搜索方案,Yang、Lu、Weng[8]等人的方案使用双线性映射和重加密技术实现了多用户查询请求。该方案中,云端服务器存储了一张包含用户重加密密钥的列表,而且云端服务器通过执行数据拥有者的指令添加和删除用户的重加密密钥来控制用户的查询权限,但是云端服务器并不是完全可信的或者为了某种利益并没有

到稿日期:2015-04-10 返修日期:2015-08-01

段阳阳(1989—),女,硕士生,主要研究方向为密码学及信息安全,E-mail:duanyangyang0709@foxmail.com;李诗旸(1991—),男,硕士生,主要研究方向为密码学及信息安全。

按照数据拥有者的指令控制用户的查询权限。Yang、Lu、Weng[8]等人的方案仅实现了对查询内容的保护，并未实现用户匿名查询，因此用户在进行搜索的过程中云端服务器能够识别出是哪个用户发送的数据查询请求服务，从而泄露了用户的相关信息，而且该方案也没有对关键字索引随机化。Bao、Deng、Ding[9]等人在 Yang、Lu、Weng[8]等人的方案的基础上提出改进方案，并且给出了安全证明，该方案的加密机制实现了索引随机化；但是在生成关键字索引时，数据拥有者要与云端服务器进行交互，导致通讯成本增加，并且该方案与文献[8]的方案一样也未实现用户匿名查询的功能。

与 Yang、Lu、Weng[8]等人和 Bao、Deng、Ding[9]等人的方案相比，本文方案不需要使用用户身份即可生成关键字查询门限，而且云服务器通过分析查询门限也不会获得用户的相关信息，因此本方案可以实现用户匿名查询。本方案中，数据拥有者将秘密参数通过安全信道发送给每一个授权的用户，用户的查询权限直接由数据拥有者控制，而不是由云端服务器控制。Yang、Lu、Weng[8]等人和 Bao、Deng、Ding[9]等人的方案使用重加密技术实现关键字加密搜索，本文方案不用重加密技术也可以实现加密搜索，而且云端服务器不需要存储一张重加密密钥表，从而节省了云端服务器的存储空间，同时所提方案还实现了索引随机化。

## 2 相关工作

2000 年，Song、Wagner、Perrig[1]等人提出加密搜索的概念，并且给出第一个关键字加密搜索方案，即为了提高加密搜索查询效率。2006 年，R. Courtmola[10]等人给出一个对称加密搜索方案，该方案使用序列列表和链表构造特殊的查询索引，这一方法简化了加密关键字索引的结构，从而提升了加密搜索的效率和安全性。2004 年，Boneh、Cresc-enzo、Ostrovsky[2]等人首次提出基于公钥密码体制的关键字加密搜索方案，即发送者使用接收者的公钥加密数据文件，只有接收者使用自己的私钥才能产生有效的查询门限。在查询过程中，该方案使用双线性映射和安全的哈希函数防止加密数据内容泄漏。这个方案在文献[12-14]中得到进一步的完善。为满足云端服务器在现实中更多的应用需求，Yang、Lu、Weng[8]等人和 Bao、Deng、Ding[9]等人的方案实现了在多用户场景下的加密搜索。随着加密搜索技术的不断发展，为了更加贴近实际应用需求，一系列新方案相继被提出，比如文献[3,15]中的模糊关键字搜索、文献[4]中的连接词搜索和文献[6,7]中的范围搜索等。沈志荣、薛巍、舒继武[11]介绍了 SE(Searchable Encryption)机制的研究背景和目前的研究进展，通过对比阐述了基于对称密码学和基于公钥密码学构造的 SE 机制的不同特点，分析了 SE 机制在支持单词搜索、连接关键字搜索和复杂逻辑结构搜索语句的研究进展，最后阐述了其所适用的典型应用场景，并讨论了 SE 机制未来可能的发展趋势。

## 3 基础知识

### 3.1 双线性对

双线性对(Bilinear Parings)定义：

设 $G_1$，$G_2$ 都是阶为素数 $p$ 的乘法循环群，$g$ 是 $G_1$ 的生成元，称映射 $e:G_1\times G_1\rightarrow G_2$ 为双线性映射，如果映射 $e$ 满足以下 3 个性质：

(1)双线性(Bilinear)。对于任意 $a,b\in Z_p$，$g\in G_1$，都有 $e(g^a,g^b)=e(g,g)^{ab}$。对于任意的 $g_1,g_2,g\in G_1$，都有 $e(g_1g_2,g)=e(g_1,g)e(g_2,g)$。对于任意的 $g_1,g_2,g\in G_1$，都有 $e(g,g_1g_2)=e(g,g_1)e(g,g_2)$。

(2)非退化性(Non-degenerate)。$e(g,g)\neq 1$。

(3)可计算性(Computable)。对于任意的 $P,Q\in G_1$，都可以计算出 $e(P,Q)\in G_2$。

### 3.2 同态哈希(Hash)函数

同态哈希(Hash)函数是具有同态性质的哈希函数。同态哈希函数的性质如下。

(1)同态性：$H(w_1m_1+w_2m_2)=H(m_1)^{w_1}\times H(m_2)^{w_2}$。

(2)抗碰撞性：不存在 $m_3\neq w_1m_1+w_2m_2$，使得 $H(m_3)=H(m_1)^{w_1}\times H(m_2)^{w_2}$。

文献[16]给出了一个具体的同态哈希函数实例。随机选取大素数 $p$ 和 $q$ 并满足 $2q|p-1$，选取 $n$ 个乘法群 $Z_p^*$ 中阶为 $q$ 的随机元素 $g_1,g_2,\cdots,g_n$，设 $m$ 为由个 $n$ 加法群 $Z_p^*$ 中元素 $\{b_i|0\leqslant i\leqslant n-1\}$ 组成的数据块，同态哈希函数 $h_r(\cdot)$ 为：$h_r(m)=\prod_{i=1}^{n}g_i^{b_i} \bmod p$。

## 4 系统模型和算法形式化定义

### 4.1 系统模型

该系统模型中有 3 个角色：数据拥有者、授权用户以及云端服务器。数据拥有者是资源提供者，把数据文件以及文件中的关键字索引加密后外包到云端服务器与其他授权用户共享。同时，数据拥有者通过定期更新秘密参数，可以授权或者撤销用户的查询权限。因此数据拥有者直接控制了用户的查询权限，而不是云端服务器来控制。授权用户使用私钥生成查询关键字门限，并向云端服务器发送查询请求。云端服务器在接收到用户的查询请求时，将查询门限与云端服务器存储的加密关键字索引依次进行匹配，如果匹配成功，则云端服务器将查询结果返回给用户；否则，不返回任何信息。

### 4.2 算法形式化定义

设 $n$ 为授权用户个数，多用户云加密搜索方案由 6 个多项式时间算法组成，分别如下：

1. $Setup(1^k)\rightarrow\delta$：其中 $k$ 是系统参数，输出全局参数 $\delta$。

2. $KeyGen(\delta)\rightarrow(PK_{DO},\{SK_i\},ek)$：输入全局参数 $\delta$，输出数据拥有者的公钥 $PK_{DO}$ 和每一个授权用户 $U_i$ 的私钥 $SK_i$，对称密钥 $ek$ 用于加密数据文件，其中 $i=1,2,\cdots,n$。

3. $BuildIndex(\delta,w,PK_{DO})\rightarrow IND(w)$：输入数据拥有者的公钥 $PK_{DO}$、关键字 $w$、全局参数 $\delta$，输出关键字索引 $IND(w)$。

4. $Enc(\delta,ek,M)\rightarrow E_{ek}(M)$：输入全局参数 $\delta$、对称密钥 $ek$ 以及文件 $M$，输出密文 $C=E_{ek}(M)$。

5. $Trapdoor(\delta,\widetilde{w},SK_i)\rightarrow T(\widetilde{w})$：输入全局参数 $\delta$、用户私钥 $SK_i$ 和关键字 $\widetilde{w}$，输出关键字查询门限 $T(\widetilde{w})$。

6. $Test(\delta,IND(w),T(\widetilde{w}))\rightarrow 1/0$：输入全局参数 $\delta$、关键字索引 $IND(w)$和关键字查询门限 $T(\widetilde{w})$，如果 $w=\widetilde{w}$，则输出 1；否则输出 0。

## 5 分级管理多用户查询权限的加密搜索方案

### 5.1 基本方案

#### 5.1.1 生成公共参数和密钥

首先系统初始化生成全局参数，数据拥有者生成关键字索引和文件的加密密钥、秘密参数以及每一个授权用户的查询密钥。

1. $Setup(1^k)\rightarrow\delta$：$k$ 为系统参数，设 $G_1$，$G_2$ 都是阶为素数 $p$ 的乘法群，随机选取群 $G_1$ 的生成元 $g$，定义双线性映射 $e$：$G_1\times G_1\rightarrow G_2$，设 $H_1:\{0,1\}^*\rightarrow G_1$ 是安全的单向哈希函数，$H_r(\cdot)$是同态哈希函数。生成全局参数：$\delta=\{p,G_1,G_2,g,e,H_1(\cdot),H_r(\cdot)\}$。

2. $KeyGen(\delta)\rightarrow(PK_{DO},\{SK_i\},ek)$：密钥生成算法由数据拥有者执行，全局参数 $\delta$ 作为输入。数据拥有者随机均匀选取 $a,k\in Z_p^*$，$r\in G_2$，$n_i\in Z_p^*$，其中 $i=1,2,\cdots,n$，数据拥有者的私钥 $SK_{DO}=\{a,k\}$。计算数据拥有者的公钥 $PK_{DO}=(g^{ak},g^a)$用于生成关键字索引，用户 $U_i$ 的私钥 $Sk_i=(g^{m_i},g^{am_i},r)$用于生成关键字查询门限，其中 $m_i=k-n_i \bmod p$。数据拥有者随机选取对称密钥 $ek\in K$ 用于加密数据文件，其中 $K$ 是密钥空间。算法输出数据拥有者的公钥 $PK_{DO}$以及每一个授权用户 $U_i$ 的私钥集$\{SK_i\}$。数据拥有者保留自己的私钥 $SK_{DO}$，通过安全信道把授权用户私钥集$\{SK_i\}$传送给每一个授权用户 $U_i$。

5.1.2 *加密关键字索引和数据文件*

数据拥有者加密关键字索引和数据文件，并将加密后的关键字索引和数据文件外包到云端服务器与其他用户共享数据。

1. $BuidIndex(\delta,w,PK_{DO})\rightarrow IND(w)$：数据拥有者执行生成关键字索引算法，使用公钥 $PK_{DO}$为每一个关键字 $w$ 生成关键字索引 $IND(w)$。将全局参数 $\delta$、公钥 $PK_{DO}$以及关键字 $w$ 作为输入。数据拥有者随机均匀选取 $s\in Z_p^*$，计算 $c_1=H_r(e(g^{H_1(w)},g^{ak})^s+r)$，$c_2=g^s$，$c_3=g^{as}$，将生成的关键字索引 $IND(w)=(c_1,c_2,c_3)$发送给云端服务器。

2. $Enc(\delta,ek,M)\rightarrow E_{ek}(M)$：数据拥有者使用对称加密算法 $E_{ek}(\cdot)$加密与关键字 $w$ 相关的文件 $M$，全局参数 $\delta$、文件 $M$、加密密钥 $ek\in K$ 作为输入，其中 $K$ 为密钥空间，数据拥有者把 $C=E_{ek}(M)$发送给云端服务器。在接收到关键字索引 $IND(w)$以及与关键字 $w$ 相应的文件 $M$ 的密文后，云端服务器将它们存放在查询索引表中。

5.1.3 *查询过程*

查询过程包括两部分：用户生成关键字查询门限和云端服务器进行搜索。首先用户生成关键字查询门限，执行 $Trapdoor(\delta,\tilde{w},SK_i)\rightarrow T(\tilde{w})$算法，全局参数 $\delta$、要查询的关键字 $\tilde{w}$、授权用户私钥 $SK_i$ 作为输入，计算关键字 $\tilde{w}$ 的查询门限：

$$T(\tilde{w})=(g^{m_i\times H_1(\tilde{w})},g^{am_i\times H_1(\tilde{w})},H_r(r))$$

授权用户把关键字 $\tilde{w}$ 的查询门限 $T(\tilde{w})$发送给云端服务器。云端服务器在接收到用户的查询请求后，通过执行 $Test(\delta,IND(w),T(\tilde{w}))\rightarrow 1/0$ 算法完成用户的查询请求。将全局参数 $\delta$、关键字索引 $IND(w)$、查询门限 $T(\tilde{w})$作为输入，计算：

$$H_r(e(g^{H_1(\tilde{w})\times m_i},c_3)\times e(g^{H_1(\tilde{w})\times am_i},c_2))\times H_r(r)$$

通过计算：$H_r(e(g^{H_1(\tilde{w})\times m_i},g^{as})\times e(g^{H_1(\tilde{w})\times am_i},g^s)+r)\overset{?}{=}c_1$，云端服务器判断是否把与关键字 $w$ 相应的加密文件 $E_{ek}(M)$返回给用户。如果等式成立，则输出 1，将结果返回给用户；否则输出 0。

## 5.2 更新用户的查询权限

在 Yang、Lu、Weng 等人[8]和 Bao、Deng、Ding 等人[9]的方案中，云端服务器通过执行数据拥有者的撤销指令删除用户的重加密密钥，进而控制用户的查询权限。但是云端服务器并不是完全可信的，如果云端服务器为了某种利益，与用户合谋，而不执行数据拥有者的撤销指令，那么非授权的用户依然可以访问外包数据库中的数据。由于云端服务器而不是数据拥有者控制用户的查询权限，因此可能带来机密数据泄漏的风险。本文提出一种新的更新用户查询权限的方法。

为了动态更新用户查询权限，数据拥有者按照如下规则定期更新秘密参数 $r$。数据拥有者随机均匀选取 $l\in Z_p^*$，计算 $r_{i+1}=r_i+l \bmod p$。然后数据拥有者通过安全信道把秘密参数 $r_{i+1}$发送给每一个授权用户。注意：撤销的用户拿不到秘密参数 $r_{i+1}$。数据拥有者计算 $H_r(l)$，并把 $H_r(l)$发送给云端服务器。云端服务器在接收到 $H_r(l)$之后，利用同态哈希函数的同态性质，计算 $\tilde{c}_1=c_1\times H_r(l)$，并更新关键字索引 $IND(w)=(\tilde{c}_1,c_2,c_3)$，其中：

$$\begin{aligned}\tilde{c}_1&=c_1\times H_r(l)\\&=H_r(e(g^{H_1(w)},g^{ak})^s+r_i)\times H_r(l)\\&=H_r(e(g^{H_1(w)},g^{ak})^s+r_i+l)\\&=H_r(e(g^{H_1(w)},g^{ak})^s+r_{i+1})\end{aligned}$$

授权用户使用新的秘密参数 $r_{i+1}$生成新的有效的查询门限 $T(\tilde{w})=(g^{m_i\times H_1(\tilde{w})},g^{am_i\times H_1(\tilde{w})},H_r(r_{i+1}))$，但是撤销用户因为拿不到新的秘密参数 $r_{i+1}$，所以不能生成有效的查询门限。通过这一方法，数据拥有者可以有效地管理用户的查询权限，而不是云端服务器。

## 5.3 分级管理用户查询权限

为实现分级管理用户查询权限，云端加密数据库中的文件被分为不同等级，根据所访问文件的等级，用户也分为不同的组。高等级的用户可以查询和访问低等级的文件，但是低等级的用户不能查询和访问高等级的文件。为了简单起见，假设文件分为 3 个等级：level-A、level-B、level-C，相应的用户也分为 3 组：group-A、group-B、group-C。group-C 中的用户只能查询和访问 level-C 中的文件。

5.3.1 *生成用户密钥和关键字索引*

数据拥有者随机均匀选取，$k_1,k_2,k_3\in Z_p^*$ 为每组的用户计算私钥：

group-A：$SK_{Ai}=(g^{m_{Ai}},g^{am_{Ai}},k_2,k_3)$，其中 $m_{Ai}+n_{Ai}=k_1k_2k_3 \bmod p$

group-B：$SK_{Bi}=(g^{m_{Bi}},g^{am_{Bi}},k_2)$，其中 $m_{Bi}+n_{Bi}=k_1k_2 \bmod p$

group-C：$SK_{Ci}=(g^{m_{Ci}},g^{am_{Ci}})$，其中 $m_i+n_{Ci}=k_1 \bmod p$

其中 $i=1,2,\cdots,m$，数据拥有者分别将 $SK_{Ai}$，$SK_{Bi}$，$SK_{Ci}$通过安全信道传送给用户 $U_{Ai}$，$U_{Bi}$，$U_{Ci}$。为每级文件生成关键字索引：

Level-A：$IND_A(w)=(H_r(e(g^{H_1(w)},g^{ak_1k_2k_3})^s+r),g^s,g^{as})$

Level-B：$IND_B(w)=(H_r(e(g^{H_1(w)},g^{ak_1k_2})^s+r),g^s,g^{as})$

Level-C：$IND_C(w)=(H_r(e(g^{H_1(w)},g^{ak_1})^s+r),g^s,g^{as})$

5.3.2 *生成查询门限和查询数据*

以 group-A 的用户 $U_{Ai}$为例，说明用户 $U_{Ai}$在访问各级文件时如何生成门限以及怎样查询数据。

(1)查询 leve-A 的文件：用户 $U_{Ai}$用自己的私钥 $SK_{Ai}=(g^{m_{Ai}},g^{am_{Ai}},k_2,k_3,r)$中的$(g^{m_{Ai}},g^{am_{Ai}},r)$参数生成查询门限：$T_A(\tilde{w})=(g^{m_{Ai}\times H_1(\tilde{w})},g^{am_{Ai}\times H_1(\tilde{w})},H_r(r))$。

将查询门限 $T_A(\tilde{w})$发送给云端服务器。云端服务器执

行查询请求时，查询门限 $T_A(\widetilde{w})$ 与 level-A 的关键字索引：$IND_A(w)=(H_r(e(g^{H_1(w)},g^{ak_1k_2k_3})^s+r),g^s,g^{as})$ 进行匹配。

(2)查询 level-B 的文件：用户 $U_{Ai}$ 用自己的私钥 $SK_{Ai}=(g^{m_{Ai}},g^{am_{Ai}},k_2,k_3,r)$ 中的 $(g^{m_{Ai}},g^{am_{Ai}},k_3,r)$ 参数生成查询门限：$T_B(\widetilde{w})=(g^{m_{Ai}\times H_1(\widetilde{w})/k_3},g^{am_{Ai}\times H_1(\widetilde{w})/k_3},H_r(r))$。

将查询门限 $T_B(\widetilde{w})$ 发送给云端服务器。云端服务器在执行查询请求时，查询门限 $T_B(\widetilde{w})$ 与 level-B 的关键字索引：$IND_A(w)=(H_r(e(g^{H_1(w)},g^{ak_1k_2})^s+r),g^s,g^{as})$ 进行匹配。

(3)查询 level-C 的文件：用户 $U_{Ai}$ 使用自己的私钥 $SK_{Ai}=(g^{m_{Ai}},g^{am_{Ai}},k_2,k_3,r)$ 中 $(g^{m_{Ai}},g^{am_{Ai}},k_2,k_3,r)$ 参数生成查询门限：$T_C(\widetilde{w})=(g^{m_{Ai}\times H_1(\widetilde{w})/k_2k_3},g^{am_{Ai}\times H_1(\widetilde{w})/k_2k_3},H_r(r))$。

将查询门限 $T_C(\widetilde{w})$ 发送给云端服务器。云端服务器在执行查询请求时，查询门限 $T_C(\widetilde{w})$ 与 level-C 的关键字索引：$IND_C(w)=(H_r(e(g^{H_1(w)},g^{ak_1})^s+r),g^s,g^{as})$ 进行匹配。但是级别低的用户 $U_G$ 没有查询高级文件的权限。比如：group-C 的用户 $U_G$ 不能访问或者查询 level-B 或者 level-A 里面的文件。用户 $U_G$ 只能使用他自己的私钥 $SK_G=(g^{m_G},g^{am_G},r)$ 生成查询门限：$T_C(\widetilde{w})=(g^{m_G\times H_1(\widetilde{w})},g^{am_G\times H_1(\widetilde{w})},H_r(r))$。

将查询门限 $T_C(\widetilde{w})$ 发送给云端服务器。云端服务器执行查询请求时，查询门限 $T_C(\widetilde{w})$ 与 level-C 的关键字索引：$IND_C(w)=(H_r(e(g^{H_1(w)},g^{ak_1})^s+r),g^s,g^{as})$ 进行匹配。因为用户 $U_G$ 没有 $k_1,k_2$ 这两个秘密参数，所以用户 $U_G$ 无法产生与 level-A 和 level-B 的关键字索引相匹配的查询门限，所以用户 $U_G$ 不能访问 level-A 和 level-B 的文件。

## 6 安全分析与性能分析

### 6.1 安全分析

1. 实现关键字信息隐私保护。数据拥有者使用自己的公钥加密关键字生成关键字索引，然后把关键字索引发送到云端服务器。云端服务器在加密数据库上执行关键字搜索操作，授权用户用自己的私钥加密关键字生成查询门限，之后向云端服务器发送查询请求。由于云端服务器和攻击者无法获取数据拥有者和用户的私钥，因此他们也无法得到关于关键字的任何信息。

2. 实现动态管理用户查询权限。该方案中数据拥有者通过定期更新秘密参数 $r$，授权或者撤销用户的查询权限。因此数据拥有者控制用户的查询权限，而不是云端服务器。

3. 支持用户匿名查询。所提方案不需要用户的身份生成关键字查询门限，因此云服务器通过分析查询门限也不会得到用户的任何信息。所以方案实现了用户匿名查询。

4. 提供多用户查询。在用户进行加密搜索之前，数据拥有者首先对用户授权，对于用户 $U_i$，数据拥有者随机选取 $n_i\in Z_p^*$，计算用户 $U_i$ 的私钥 $SK_i=(g^{m_i},g^{am_i},r)$，其中 $m_i=k-n_i \bmod p$。每一个授权用户使用自己的私钥生成关键字查询门限，用于查询云端服务器中加密数据库中的数据。每个授权用户的查询权限是独立的，一个用户的加入和撤销不会影响到其他用户。

5. 不可伪造查询门限。有效的查询门限是用授权用户的私钥加密生成的，由于无法获取授权用户的私钥，云端服务器和攻击者无法伪造出有效的查询门限。

6. 实现分级管理用户查询权限。根据用户访问或者查询文件的级别，将用户分为不同的组。采用特殊的查询密钥生成规则，实现高级用户可以访问或者查询低级文件，而低级用户不能访问或者查询高级文件。

### 6.2 性能分析

从算法的复杂度和实际执行时间这两方面对方案进行性能分析。

算法复杂度：表 1 包括方案中各个算法的计算成本和通信成本，其中 $E$ 表示在群 $G$ 上的求幂运算操作，$E_T$ 表示在群 $G_T$ 上的求幂运算操作，$Pair$ 表示配对操作，$H_r$ 表示同态哈希函数，$[Z_p]$ 代表域 $[Z_p]$ 的数据元素个数，$[G]$ 代表群 $[G]$ 的数据元素个数，$[G_T]$ 代表群 $[G_T]$ 的元素个数。

表 1 搜索加密方案各算法复杂度

| | 算法 | 计算代价 | 通信代价 |
|---|---|---|---|
| 多用户关键字加密搜索方案 | KeyGen | 4E | $2[Z_p]$ |
| | BuildIndex | $2E+E_T+Pair+2H_r$ | $[G_T]+2[G]$ |
| | Trapdoor | $2E+2H_r$ | $2[G]$ |
| | Test | 2Pair | |

从表 1 可以观察出生成关键字索引算法的复杂度和通信代价更高。但是系统初始化时只需要执行一次密钥生成算法和关键字索引生成算法。用户生成查询门限时执行两次求幂运算和两次哈希运算。用户使用计算能力低的计算机时，这个复杂度也是可以接受的。查询算法执行两次配对操作，对于云端服务器而言是可行的。

算法执行时间：本文通过实验分析方案中各算法的性能。实验环境是 Intel Pentium Dual E2140 1.5GHz 1GB 内存，在 Windows XP 系统下，方案基于 JPBC 平台使用 Java 语言实现多用户加密搜索方案的各个算法。表 2 和图 1 示出了各算法的执行时间。

表 2 搜索加密方案各算法的执行时间(单位：s)

| 索引项个数 | 10 | 20 | 50 | 100 | 200 | 500 | 1000 |
|---|---|---|---|---|---|---|---|
| KeyGen | 0.668 | 0.719 | 0.703 | 0.672 | 0.678 | 0.703 | 0.672 |
| BuildIndex | 3.984 | 9.959 | 19.687 | 39.453 | 78.813 | 197.875 | 392.109 |
| Trapdoor | 0.17 | 0.172 | 0.188 | 0.172 | 0.187 | 0.175 | 0.185 |
| Test | 2.328 | 5.797 | 11.625 | 23.234 | 46.516 | 119.637 | 231.719 |

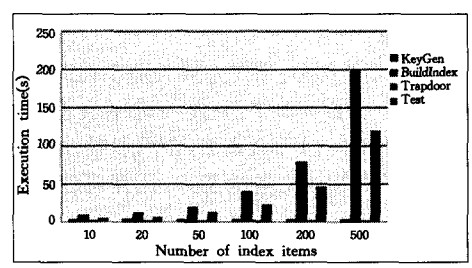


图 1 搜索加密方案各算法的执行时间

**结束语** 针对当前云计算环境下多用户关键字搜索加密方案存在的一些问题，本文首次提出一种分级管理用户查询权限的匿名的多用户关键字搜索加密方案。本方案通过定期更新秘密参数，实现数据拥有者直接控制用户查询权限这一特性。在查询过程中云端服务器通过验证关键字索引与查询门限是否相等来实现用户查询内容和身份的隐私保护。通过采用一种特殊的密钥生成规则，将该方案扩展为分级管理用户查询权限的多用户关键字加密搜索方案，使得高级用户可以访问或者查询同级或者低级文件，但是低级用户不能访问或者查询高级文件。安全分析表明本方案实现了关键字信息隐私保护，提供了多用户查询，支持用户匿名查询，提供了动态权限管理、不可伪造查询门限并实现了分级管理用户查询。

(下转第 174 页)

究[J]. 通信学报,2013,34(7):134-142

[9] Ferhat K. ITUbee: A Software Oriented Lightweight Block Cipher[C]// Proceedings of Lightweight Cryptography for Security and Privacy 2013. Heidelberg: Springer Berlin, 2013: 16-27

[10] Carlet C, Faugère J-C, Goyet C, et al. Analysis of the algebraic side channel attack[J]. Journal of Cryptographic Engineering, 2012, 2(1): 45-62

[11] Zhang Guo-ji, Xiao Huang-pei. Quadratic Equations on S-Boxes and a New S-Box Design Criterion[J]. Journal of South china University of Technology(Natural Science Edition), 2008, 36(8): 140-144(in Chinese)
张国基,肖黄培. S盒的二次方程及一个新的设计准则[J]. 华南理工大学学报,2008,36(8):140-144

[12] Fischer S, Meier W. Algebraic immunity of S-boxes and augmented functions[C]// Proceedings of Foundations of Software Engineering. Heidelberg: Springer Berlin, 2007: 366-381

[13] Armknecht F, Krause M. Constructing single and multi-output Boolean functions with maximal immunity[C]// Proceedings of International Colloquium on Automata, Languages and Programming. Heidelberg: Springer Berlin, 2006: 180-191

[14] Carlet C. On the algebraic immunities and higher order nonlinearities of vectorial Boolean functions[C]// Proceedings of NATO Science for Peace and Security Series, D: Information and Communication Security. Heidelberg: Springer Berlin, 2009: 104-116

[15] Oren Y, Kirschbaum M, Popp T, et al. Algebraic side-channel analysis in the presence of errors[C]// Proceedings of Cryptography Hardware and Embedded Systems. Heidelberg: Springer Berlin, 2010: 428-442

[16] Bogdanov A, Kizhvatov I, Pyshkin A. Algebraic Methods in Side-Channel Collision Attacks and Practical Collision Detection [C]// Proceedings of INDOCRYPT. Berlin: Springer, 2008: 251-265

[17] Moradi A, Mischke O, Eisenbarth T. Correlation-enhanced power analysis collision attack[C]// Proceedings of Cryptography Hardware and Embedded Systems. Heidelberg: Springer Berlin, 2010: 125-139

[18] Oren Y, Kirschbaum M, Popp T, et al. Algebraic side channel analysis in the presence of errors[C]// Proceedings of Cryptography Hardware and Embedded Systems. Heidelberg: Springer Berlin, 2010: 428-442

[19] Whitnall C, Oswald E, Mather L. An exploration of the kolmogorov-smirnov test as competitor to mutual information analysis [EB/OL]. [2011-03-08]. http://eprint.iacr.org/2011/380.pdf

[20] Knudsen L R, Miolance C V. Counting equations in algebraic attacks on block ciphers[J]. International Journal of Information Security, 2010, 9(2): 127-135

[21] Soos M, Nohl K, Castelluccia C. Extending SAT solvers to cryptographic problems[C]// Proceedings of Lecture Notes in Computer Science. Heidelberg: Springer Berlin, 2009: 244-257

(上接第 162 页)

## 参 考 文 献

[1] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data[C]// Proceedings IEEE Symposium on Security and Privacy. 2000: 44-55

[2] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[M]// Advances in Cryptology-Eurocrypt. Springer Berlin Heidelberg, 2004: 506-522

[3] Chen F, Liu A X. Privacy-and integrity-preserving range queries in sensor networks[J]. IEEE/ACM Transactions on Networking, 2012, 20(6): 1774-1787

[4] Shi E, Bethencourt J, Chan T H H, et al. Multi-dimensional range query over encrypted data[C]// IEEE Symposium on Security and Privacy(P'07). IEEE, 2007: 350-364

[5] Li Shuang, Xu Mao-zhi. Attribute-based public encryption with keyword search[J]. Chinese Journal of Computers, 2014, 37(5): 1017-1024(in Chinese)
李双,徐茂智. 基于属性的可搜索加密方案[J]. 计算机学报,2014,37(5):1017-1024

[6] Boneh D, Waters B. Conjunctive, subset, and range queries on encrypted data[M]// Theory of Cryptography. Springer Berlin Heidelberg, 2007: 535-554

[7] Li J, Wang Q, Wang C, et al. Fuzzy keyword search over encrypted data in cloud computing[C]// INFOCOM. IEEE, 2010: 1-5

[8] Yang Y, Lu H, Weng J. Multi-user private keyword search for cloud computing[C]// IEEE Third International Conference on Cloud Computing Technology and Science (CloudCom). IEEE, 2011: 264-271

[9] Bao F, Deng R H, Ding X, et al. Private query on encrypted data in multi-user settings[M]// Information Security Practice and Experience. Springer Berlin Heidelberg, 2008: 71-85

[10] Curtmola R, Garay J, Kamara S, et al. Searchable symmetric encryption: improved definitions and efficient constructions[C]// Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006: 79-88

[11] Shen Zhi-rong, Xue Wei, Shu Ji-wu. Survey on the research and development of searchable encryption schemes[J]. Journal of Software, 2014, 25(4): 880-895(in Chinese)
沈志荣,薛巍,舒继武. 可搜索加密机制研究与进展[J]. 软件学报,2014,25(4):880-895

[12] Gu C, Zhu Y. New Efficient Searchable Encryption Schemes from Bilinear Pairings[J]. International Journal of Network Security, 2010, 10(1): 25-31

[13] Wang C, Cao N, Li J, et al. Secure ranked keyword search over encrypted cloud data[C]// IEEE 30th International Conference on Distributed Computing Systems(ICDCS). 2010: 253-262

[14] Fang Zhong-jin, Zhou Shu, Xia Zhi-hua. Research on fuzzy search over encrypted cloud data based on keywords[J]. Computer Science, 2015, 42(3): 136-139(in Chinese)
方忠进,周舒,夏志华. 基于关键字的加密云数据模糊搜索策略研究[J]. 计算机科学,2015,42(3):136-139

[15] Zheng Q, Xu S, Ateniese G. VABKS: Verifiable Attribute-based Keyword Search over Outsourced Encrypted Data[J]. IACR Cryptology ePrint Archive, 2013: 462

[16] Zheng Yu, Gao Bao. Method based on homomorphic hash for data changes capture of LDAP directory[J]. Application Research of Computers, 2013, 30(7): 2007-2009(in Chinese)
郑煜,高宝. 基于同态哈希的目录服务数据变化捕获方法[J]. 计算机应用研究,2013,30(7):2007-2009