# 多用户环境下无证书认证可搜索加密方案

张玉磊[①] 文 龙[*①] 王浩浩[①] 张永洁[②] 王彩芬[③]

[①](西北师范大学计算机科学与工程学院 兰州 730070)

[②](甘肃卫生职业学院 兰州 730070)

[③](深圳技术大学 深圳 518118)

**摘 要**：可搜索加密技术的提出使用户能够将数据加密后存储在云端，而且可以直接对密文数据进行检索。但现有的大部分可搜索加密方案都是单用户对单用户的模式，部分多用户环境下的可搜索加密方案是基于传统公钥密码或基于身份公钥密码系统，因此这类方案存在证书管理和密钥托管问题，且容易遭受内部关键词猜测攻击。该文结合公钥认证加密和代理重加密技术，提出一个高效的多用户环境下无证书认证可搜索加密方案。方案使用代理重加密技术对部分密文进行重加密处理，使得授权用户可以利用关键字生成陷门查询对应密文。在随机预言模型下，证明方案具有抵抗无证书公钥密码环境下两类攻击者的内部关键词猜测攻击的能力，且该方案的计算和通信效率优于同类方案。

**关键词**：可搜索加密；无证书；多用户环境；代理重加密；内部关键词猜测攻击

**中图分类号**：TP309 **文献标识码**：A **文章编号**：1009-5896(2020)05-1094-08

**DOI**: 10.11999/JEIT190437

# Certificateless Authentication Searchable Encryption Scheme for Multi-user

ZHANG Yulei[①] WEN Long[①] WANG Haohao[①]

ZHANG Yongjie[②] WANG Caifen[③]

[①](*College of Computer Science and Engineering*, *Northwest Normal University*, *Lanzhou* 730070, *China*)

[②](*Gansu Health Vocational College*, *Lanzhou* 730070, *China*)

[③](*Shenzhen Technology University*, *Shenzhen* 518118, *China*)

**Abstract**: The searchable encryption technology enables users to encrypt data and store it in the cloud, and can directly retrieve ciphertext data. Most existing searchable encryption schemes are single-to-single mode, and the searchable encryption scheme in some multi-user environments is based on public key cryptography or identity-based public key cryptosystem. Such schemes have certificate management and key escrow issues and scheme are vulnerable to suffer internal keyword guessing attacks. Public key authentication encryption and proxy re-encryption technology are combined, and an efficient certificateless authentication searchable encryption scheme is proposed for multi-user environment. The scheme uses proxy re-encryption technology to re-encrypt portion of ciphertexts, so that authorized users can generate trapdoor with the keywords to query ciphertext. In the random oracle model, the scheme is proved that it has the ability to resist the internal keyword guessing of two type attackers in the certificateless public key cryptosystem, and the calculation and communication efficiency of the scheme is better than the similar scheme.

**Key words**: Searchable-encryption; Certificateless; Multi-user; Proxy-re-encryption; Internal-keyword-guessing-attack

收稿日期：2019-06-13；改回日期：2019-12-24；网络出版：2020-01-07

*通信作者： 文龙 770293027@qq.com

基金项目：国家自然科学基金(61662069)，甘肃省高等学校科研项目(2017A-003, 2018A-207)

Foundation Items: The National Natural Science Foundation of China(61662069), The Higher Educational Scientific Research Foundation of Gansu Province (2017A-003, 2018A-207)

## 1　引言

在基于云智能医疗数据分析的机器学习应用中，利用关键词搜索特定文档作为其重要构建模块可应用于医疗物联网设备收集的临床数据智能分析中。然而云端存储的用户临床数据可能由于不完全可信的云服务器提供商的访问，导致用户隐私数据泄露。因此，数据拥有者在上传或分享有关隐私文件前需要对敏感数据先进行本地加密然后再发送到云服务器端。但是密文形式的文件使得一些文件操作变得较为困难，搜索需要的文件时，只能先将密文下载到本地解密后再查看是否是需要的内容。

为了解决云服务器对密文实现搜索操作的问题，Boneh等人[1]提出了公钥可搜索加密方案(Public key Encryption with Keyword Search, PEKS)，但此方案的搜索效率较低且安全性不高。之后文献[2–4]相继对PEKS方案进行改进，提出了更为安全高效PEKS方案。2010年，Shao等人[5]首次将公钥可搜索加密和代理重加密结合，提出带关键字搜索的代理重加密的概念，随后文献[6,7]对文献[5]中方案进行改进，但改进方案的计算效率仍然不理想。并且现有的大部分PEKS方案都可能遭受内部关键字猜测攻击(Inside Keyword Guessing Attack, IKGA)。在IKGA中恶意攻击者可以逐一测试候选关键字是否与给定的关键字密文匹配。由于现实生活中关键词空间较小，所以该攻击可行。2017年，Huang等人[8]引入了公钥认证PEKS方案，提出在加密关键词的同时对其进行认证实现抵御IKGA。但是由于这些方案大多是基于传统公钥密码或基于身份公钥密码，因此这类方案存在证书管理以及密钥托管问题。2014年Peng等人[9]在无证书加密环境下提出了带有关键字搜索的无证书公钥加密的概念(CertificateLess Public key authenticated Encryption with Keyword Search, CLPEKS)解决了之前PEKS中的密钥托管和证书管理问题。之后，2016年Wu等人[10]指出Peng的方案容易受到内部关键字猜测攻击(IKGA)。2017年Ma等人[11,12]提出了适用于工业物联网和移动健康网络环境的CLPEKS方案，但是这些方案[10–12]也容易受到恶意系统内部人员发起的IKGA。

单用户环境下的PEKS方案无法支持加密文件的分享。为了解决该问题，Curtmola等人[13]提出通过直接扩展单用户方案，在多个用户之间共享文件搜索的安全密钥来解决该问题。随后研究人员提出了一些新的多用户环境PEKS方案[14–17]。在这些方案中，用户管理者管理多个用户的搜索能力使他们能够搜索彼此的文件，但是云环境下通常不存在完全可信的管理员。为了解决这些问题，2014年，Tang等人[18]提出了一种安全可扩展多方可搜索加密方案。然而此方案仅支持对用户检索授权，但不明确支持用户检索授权的撤销，并且此方案同样容易遭受内部关键词猜测攻击。

如何在多用户环境下实现授权用户使用关键字对密文进行检索，抵抗内部关键词猜测攻击是本文工作的出发点。针对这些关键性问题，本文提出了一个多用户环境下无证书认证可搜索加密方案。方案具有如下特点：

(1) 在无证书公钥密码环境下不仅解决了之前PEKS中复杂的证书管理和密钥托管问题，而且通过结合代理重加密技术对部分密文进行重加密，使多个授权用户可以利用关键字生成的陷门查询对应关键字密文。提高了方案的实用性；

(2) 在随机预言模型下，证明方案具有抵御两类攻击者的内部关键词猜测攻击能力，并且与同类无证书可搜索加密方案相比性能表现更好；

(3) 数据拥有者在加密关键字时，在关键词加密算法中加入数据拥有者的私钥实现对关键词的认证。因此，第三方(例如，恶意服务器)不能在没有数据所有者的私钥的情况下加密关键字来进行IKGA。且只对部分密文进行1次标量乘法运算的重加密处理，运算效率较高；

(4) 通过对授权用户生成授权密钥，当特定用户被撤销授权时，对应的授权密钥也被删除。在没有授权密钥帮助下，用户无法获得对称密钥从而无法解密密文得到明文数据，实现了用户授权撤销操作。

## 2　基础知识

### 2.1　双线性对

定义 设$G_1$和$G_2$分别为$q$阶加法循环群和$q$阶乘法循环群($q$为素数)，$e: G_1 \times G_1 \to G_2$为一个双线性对，它满足以下3个特性：

(1)双线性：对于任意$a,b \in Z_q^*$，$P,Q \in G_1$，$e(aP,bQ)=e(P,Q)^{ab}$；

(2)非退化性：存在$P \in G_1$使$e(P,P) \neq 1$(1为$G_2$的单位元)；

(3)可计算性：对于任意$P,Q \in G_1$都存在一个有效的算法来计算$e(P,Q)$。

### 2.2　计算双线性Diffie-Hellman (Computational Bilinear Diffie-Hellman, CBDH)问题

给定：$e: G_1 \times G_1 \to G_2$为一个双线性对，$P, aP, bP, cP \in G_1$，其中$a,b,c \in Z_q^*$为未知数，计算$e(P,P)^{abc}$。

## 3　多用户环境下无证书认证可搜索加密方案

### 3.1　方案系统模型

多用户环境下无证书认证可搜索加密方案包括

以下4个实体：密钥生成中心(KGC)、数据拥有者Do、数据用户Du和云服务器CS。如图1所示。

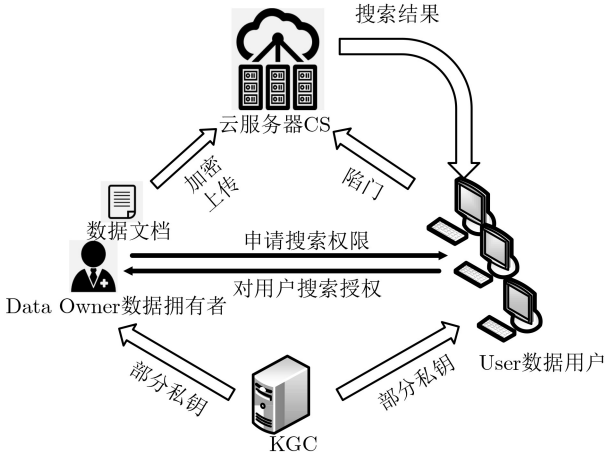


图 1 方案系统模型

(1) KGC: KGC可以生成系统参数、系统主密钥和数据拥有者/数据用户的部分私钥；

(2)数据拥有者Do：数据拥有者将数据加密后上传至云服务器端，并且可以对授权数据用户进行密文检索；

(3)数据用户Du：得到检索权限的数据用户可以根据相应关键词在云端搜索对应密文；

(4)云服务器CS：云服务器CS是诚实而好奇的，它可以存储数据拥有者上传的加密数据，执行复杂的密文匹配操作。在数据用户提出搜索申请时检验用户搜索权限，确认搜索用户权限后对密文进行重加密处理。再对接收到陷门进行密文匹配，返回对应密文。

### 3.2 方案算法构成

多用户环境下无证书认证可搜索加密方案包括以下多项式时间算法。

(1) setup：输入安全参数$k$，返回公开参数prms和主密钥$s$；

(2) Extract − partial − private − key：输入公开参数prms、主密钥$s$、数据拥有者身份$\mathrm{ID_{Do}}$和数据用户身份$\mathrm{ID_{Du_i}}$(其中$1 \le i \le t$, $t$为获得搜索授权人数)，KGC返回部分私钥$D_{\mathrm{Do}}$, $D_{\mathrm{Du}_i}$；

(3) Set − user − key：输入公开参数prms，数据拥有者身份$\mathrm{ID_{Do}}$和数据用户身份$\mathrm{ID_{Du_i}}$，返回对应的秘密值$x_{\mathrm{Do}}$和$x_{\mathrm{Du}_i}$；

(4) Set − private − key：输入公开参数prms，数据拥有者与数据用户的秘密值$x_{\mathrm{Do}}$, $x_{\mathrm{Du}_i}$，部分私钥$D_{\mathrm{Do}}$和$D_{\mathrm{Du}_i}$，返回对应私钥$\mathrm{SK_{Do}}$和$\mathrm{SK_{Du_i}}$；

(5) Set − public − key：输入公开参数prms，数据拥有者与数据用户的秘密值$x_{\mathrm{Do}}$, $x_{\mathrm{Du}_i}$，返回对应公钥$\mathrm{PK_{Do}}, \mathrm{PK_{Du_i}}$；

(6) MCLPEnc：输入公开参数prms，数据拥有者私钥$\mathrm{SK_{Do}}$，明文信息$M$以及关键词$w$，数据拥有者返回对应密文集CT；

(7) Adduser：输入公开参数prms，数据用户$\mathrm{Du}_i$的公钥$\mathrm{PK_{Du_i}}$和对称密钥$K$，数据拥有者对数据用户进行搜索授权，生成授权密钥$\mathrm{AK}_i$和$V_i$。将对称密钥$K$和随机值$V_i$加密后，将元组$< K', V'_i >$返回给数据用户；

(8) Verify：输入公开参数prms和数据用户私钥$\mathrm{SK_{Du_i}}$，服务器CS对用户搜索权限进行验证，若验证通过则继续执行ReEnc算法，否则返回“$\perp$”；

(9) ReEnc：若数据用户搜索权限验证通过，则输入密文集CT和重加密密钥rk，云服务器CS返回重加密处理后的密文集$\mathrm{CT}_r$；

(10) Trapdoor：输入公开参数prms，关键词$w_t$，数据用户私钥$\mathrm{SK_{Du_i}}$与数据拥有者的公钥$\mathrm{PK_{Do}}$，数据用户生成对应陷门$T_{w_t}$；

(11) Test：输入陷门$T_{w_t}$和密文集$\mathrm{CT}_r$，若$\mathrm{CT}_r$和$T_{w_t}$包含相同关键词，云服务器CS返回对应密文CT′，否则输出“$\perp$”；

(12) Dec：输入数据用户的私钥$\mathrm{SK_{Du_i}}$和密文$\mathrm{CT}_r$，用户解密$\mathrm{CT}_r$后得到明文$M$；

(13) Deleteuser：输入待撤销授权的数据用户身份，撤销的搜索授权。

### 3.3 方案安全模型

在无证书公钥密码体制中有两种类型攻击者：类型I攻击者$A_{\mathrm{I}}$和类型II攻击者$A_{\mathrm{II}}$：$A_{\mathrm{I}}$可以替换用户公钥但无法访问主密钥。$A_{\mathrm{II}}$无法对用户公钥进行替换操作但可以访问主密钥。

本文通过挑战者$C$和攻击者$A \in \{A_{\mathrm{I}}, A_{\mathrm{II}}\}$之间的安全游戏来定义方案的安全模型：

Game：给定安全参数$k$, $C$返回公开参数prms和主密钥$s$。如果$A = A_{\mathrm{I}}$, $C$将系统参数prms返回给$A$，否则$C$将prms和$s$发送给$A$。攻击者$A$开始进行如下查询。

Hash查询：$A$询问方案中的Hash预言获得相应Hash值；部分私钥提取查询：$A$向$C$提交查询身份$\mathrm{ID}_i$, $C$计算对应部分私钥$D_{\mathrm{Du}_i}$返回给$A$；秘密值提取查询：$A$向$C$提交查询身份$\mathrm{ID}_i$, $C$返回对应秘密值给$A$；公钥查询：$A$向$C$提交查询身份$\mathrm{ID}_i$进行公钥查询，$C$计算对应公钥$\mathrm{PK_{Du_i}}$返回给$A$；替换公钥查询：如果$A = A_{\mathrm{I}}$，则$A_{\mathrm{I}}$可以替换任意用户的公钥；陷门查询：$A$向$C$提交查询关键词$w$进行陷门查询，$C$计算对应关键字的陷门$T_w$返回给$A$。

挑战：$A$输出两个没有经过陷门查询的关键词$(w_0, w_1)$, $C$随机选择$b \in \{0, 1\}$，输出$w_b$的相应密文。

更多陷门查询：$A$可以继续对$w_i$进行陷门查询，但$w_i \notin \{w_0, w_1\}$。猜测：最后$A$输出其猜测的$b'$，如果$b'=b$则$A$赢得游戏。如果$A$赢得游戏的概率$\mathrm{Adv}=|\Pr[b'=b]-1/2|$是可以忽略的，那么方案在语义上对于IKGA是安全的。

## 4　具体方案

### 4.1 算法描述

多用户模型下无证书认证可搜索加密方案包括以下算法。

(1) setup($k$)：输入安全参数$k$, KGC选择两个相同素数阶($q>2^k$)的循环群$G_1$, $G_2$($g$为$G_1$生成元)和双线性对$e: G_1 \times G_1 \to G_2$，选择随机数$s \in Z_q^*$为主密钥，$s' \in Z_q^*$, $\mu \in Z_q^*$。选取抗碰撞Hash函数：$H_1: \{0,1\}^* \to Z_q^*$, $H_2: \{0,1\}^* \to G_1$和$h_3: G_2 \to Z_q^*$。设定主公钥$P=sg$, $\lambda=s'g$和重加密密钥$\mathrm{rk}=s/s' \pmod q$。输出公开参数$\mathrm{prms}=(\mathrm{e}, g, G_1, G_2, P, \lambda, \mu, \mathrm{rk}, H_1, H_2, h_3)$，保留$s$。

(2) Extract$-$partial$-$private$-$key($\mathrm{prms}, s, \mathrm{ID_{Do}}, \mathrm{ID_{Du_i}}$)KGC执行如下步骤：

步骤 1　输入数据拥有者的身份$\mathrm{ID_{Do}} \in \{0,1\}^*$, KGC选择随机数$r_{\mathrm{Do}} \in Z_q^*$，计算$R_{\mathrm{Do}}=r_{\mathrm{Do}}g$, $a_{\mathrm{Do}}=H_1(\mathrm{ID_{Do}})$, $D_{\mathrm{Do}}=r_{\mathrm{Do}}+s \cdot a_{\mathrm{Do}} \pmod q$。然后KGC将$R_{\mathrm{Do}}$, $D_{\mathrm{Do}}$返回给数据拥有者Do。

步骤2　对于数据用户$\mathrm{Du}_i$ $(1 \le i \le t)$，其中$t$为授权的数据用户人数。输入其身份$\mathrm{ID_{Du_i}} \in \{0,1\}^*$, KGC选择随机数$r_{\mathrm{Du_i}} \in Z_q^*$，计算$R_{\mathrm{Du_i}}=r_{\mathrm{Du_i}}g$, $a_{\mathrm{Du_i}}=H_1(\mathrm{ID_{Du_i}})$, $D_{\mathrm{Du_i}}=r_{\mathrm{Du_i}}+s \cdot a_{\mathrm{Du_i}} \pmod q$。然后KGC将$R_{\mathrm{Du_i}}$, $D_{\mathrm{Du_i}}$返回给数据用户$\mathrm{Du}_i$。

(3) Set–user–key($\mathrm{prms}, \mathrm{ID_{Do}}, \mathrm{ID_{Du_i}}$)：输入$\mathrm{ID_{Do}} \in \{0,1\}^*$和$\mathrm{ID_{Du_i}} \in \{0,1\}^*$，参数prms。

(a) 数据拥有者Do选择随机数$x_{\mathrm{Do}} \in Z_q^*$作为其自己的秘密值；

(b) 数据用户$\mathrm{Du}_i$选择随机数$x_{\mathrm{Du_i}} \in Z_q^*$作为其自己的秘密值。

(4) Set$-$private$-$key($\mathrm{prms}, D_{\mathrm{Do}}, D_{\mathrm{Du_i}}, x_{\mathrm{Do}}, x_{\mathrm{Du_i}}$)：输入参数prms，数据拥有者Do与数据用户$\mathrm{Du}_i$的秘密值$x_{\mathrm{Do}}$, $x_{\mathrm{Du_i}}$和部分私钥$D_{\mathrm{Do}}, D_{\mathrm{Du_i}}$，

(a) 设置数据拥有者Do私钥$\mathrm{SK_{Do}}=(x_{\mathrm{Do}}, D_{\mathrm{Do}})$；

(b) 设置数据用户$\mathrm{Du}_i$私钥$\mathrm{SK_{Du_i}}=(x_{\mathrm{Du_i}}, D_{\mathrm{Du_i}})$。

(5) Set $-$ public $-$ key($\mathrm{prms}, x_{\mathrm{Do}}, x_{\mathrm{Du_i}}$)：输入参数prms，数据拥有者Do的秘密值$x_{\mathrm{Do}}$和数据用户$\mathrm{Du}_i$的秘密值$x_{\mathrm{Du_i}}$。设置数据拥有者Do的公钥$\mathrm{PK_{Do}}=(X_{\mathrm{Do}}, Y_{\mathrm{Do}})$其中$X_{\mathrm{Do}}=x_{\mathrm{Do}}g$, $Y_{\mathrm{Do}}=R_{\mathrm{Do}}=r_{\mathrm{Do}}g$。数据用户$\mathrm{Du}_i$的公钥$\mathrm{PK_{Du_i}}=(X_{\mathrm{Du_i}}, Y_{\mathrm{Du_i}})$其中$X_{\mathrm{Du_i}}=x_{\mathrm{Du_i}}g$, $Y_{\mathrm{Du_i}}=R_{\mathrm{Du_i}}=r_{\mathrm{Du_i}}g$。

(6) MCLPEnc($\mathrm{prms}, \mathrm{SK_{Do}}, m, w$)：输入参数prms, Do的私钥$\mathrm{SK_{Do}}$，文档$m$，文档对应关键词$w$。数据拥有者Do随机选择数$r \in Z_q^*$，对称密钥$K \in Z_q^*$。数据拥有者Do使用$K$加密明文$m \in \{0,1\}^l$。对文档$m$提取对应关键词$w$, Do使用自身私钥$\mathrm{SK_{Do}}$加密关键词$w$，将$C=(c_1, c_2, c_3)$发送至服务器CS，其中$c_1=(x_{\mathrm{Do}}+D_{\mathrm{Do}})H_2(w)+rP$, $c_2=r\lambda$, $c_3=\mathrm{Enc}(K, m)$。

(7) Adduser($\mathrm{prms}, \mathrm{PK_{Du_i}}, K$)：数据用户$\mathrm{Du}_i$将其公钥作为申请信息，提交给数据拥有者Do。数据拥有者Do执行以下步骤：

步骤 1　对$\mathrm{Du}_i$生成对应随机值$V_i \in Z_q^*$，并使用$V_i$生成$\mathrm{AK}_i=\mu+h_3(V_i \cdot g)$，并将元组$<\mathrm{Du}_i, \mathrm{AK}_i>$上传至云服务器CS的访问控制表中；

步骤 2　输入$\mathrm{Du}_i$的公钥$\mathrm{PK_{Du_i}}$加密随机值$V_i$生成授权密钥$V'_i=\mathrm{Enc_{PK_{Du_i}}}(V_i)$；

步骤 3　输入对称密钥$K$和随机值$V_i$生成$K'=K \cdot h_3(e(P, V_i \cdot g))$；

步骤 4　数据拥有者Do将元组$<K', V'_i>$返回给数据用户$\mathrm{Du}_i$。

(8) Verify($\mathrm{prms}, \mathrm{SK_{Du_i}}$)：云服务器CS对提出检索请求的数据用户进行授权验证，检验用户检索权限：

步骤 1　数据用户$\mathrm{Du}_i$使用私钥$\mathrm{SK_{Du_i}}$对$V'_i$解密$\mathrm{Dec_{SK_{Du_i}}}(V'_i)$得到随机值$V_i$；

步骤 2　$\mathrm{Du}_i$计算$\mu+h_3(V_i \cdot g)$，并将元组$\langle \mathrm{Du}_i, \mu+h_3(V_i \cdot g) \rangle$上传至服务器CS；

步骤 3　服务器CS收到元组$\langle \mathrm{Du}_i, \mu+h_3(V_i \cdot g) \rangle$后，检查访问控制表中是否存在匹配项，当$\mu+h_3(V_i \cdot g)=\mathrm{AK}_i$时验证通过，若验证不通过则返回“$\perp$”。

(9) ReEnc($C, \mathrm{rk}$)：若Verify算法中用户授权信息验证通过，云服务器CS对存储的密文进行重加密处理$c'_2=c_2 \cdot \mathrm{rk}$返回$C'=(c_1, c'_2, c_3)$。

(10) Trapdoor($\mathrm{prms}, w_t, \mathrm{SK_{Du_i}}, \mathrm{PK_{Do}}$)：输入参数prms、数据用户$\mathrm{Du}_i$私钥$\mathrm{SK_{Du_i}}$、数据拥有者Do公钥$\mathrm{PK_{Do}}$和查询关键词$w_t$, $\mathrm{Du}_i$生成关键词$w_t$对应陷门$T_{w_t}=e((x_{\mathrm{Du_i}}+D_{\mathrm{Du_i}})H_2(w_t), X_{\mathrm{Do}}+Y_{\mathrm{Do}}+a_{\mathrm{Do}}P)$并将$T_{w_t}$上传至服务器CS。

(11) Test($T_w, C'$)：服务器CS收到$\mathrm{Du}_i$发送的陷门$T_{w_t}$后，判断$T_{w_t}e(c'_2, X_{\mathrm{Du_i}}+Y_{\mathrm{Du_i}}+a_{\mathrm{Du_i}}P)=e(c_1, X_{\mathrm{Du_i}}+Y_{\mathrm{Du_i}}+a_{\mathrm{Du_i}}P)$是否成立。若成立则返回对应密文$C'=(c_1, c'_2, c_3)$，否则输出“$\perp$”。

(12) Dec($\mathrm{SK_{Du_i}}, C'$)：数据用户$\mathrm{Du}_i$在接收到CS返回的密文$C'=(c_1, c'_2, c_3)$后，使用$V_i$计算对称密钥$K=K'/h_3(e(P, g)^{V_i})$，并通过$K$解密$c_3$得到文档$m$。

(13) Deleteuser($\mathrm{Du}_i$)：输入用户身份标识符$\mathrm{Du}_i$，数据拥有者Do通知云服务器删除数据用户

$\mathrm{Du}_i$的访问控制表中的数据检索权限。即从访问控制表中删除元组$<\mathrm{Du}_i, \mathrm{AK}_i>$。

### 4.2 正确性

多用户模型下无证书公钥认证可搜索加密方案满足以下正确性。

$$\begin{aligned} & e(c_1, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P) \\ &= e((x_{\mathrm{Do}}+D_{\mathrm{Do}})H_2(w)+rP, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P) \\ &= e((x_{\mathrm{Do}}+D_{\mathrm{Do}})H_2(w), X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i} \\ &\quad + a_{\mathrm{Du}_i}P)+e(rP, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P) \end{aligned} \tag{1}$$

$$\begin{aligned} & T_{w_t}e(c'_2, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P) \\ &= e((x_{\mathrm{Du}_i}+D_{\mathrm{Du}_i})H_2(w_t), X_{\mathrm{Do}}+Y_{\mathrm{Do}} \\ &\quad + a_{\mathrm{Do}}P)e(c'_2, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P) \\ &= e((x_{\mathrm{Du}_i}+D_{\mathrm{Du}_i})H_2(w_t), (x_{\mathrm{Do}}+r_{\mathrm{Do}} \\ &\quad + s\cdot a_{\mathrm{Do}})g)e(rP, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P) \\ &= e((x_{\mathrm{Do}}+D_{\mathrm{Do}})H_2(w_t), X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i} \\ &\quad + a_{\mathrm{Du}_i}P)e(rP, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P) \end{aligned} \tag{2}$$

当且仅当$w=w_t$时，

$$T_{w_t}e(c'_2, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P)=e(c_1, X_{\mathrm{Du}_i}+Y_{\mathrm{Du}_i}+a_{\mathrm{Du}_i}P),$$

由于$K'=K\cdot h_3(e(P, V_i g))$，所以$K=\dfrac{K'}{h_3\left(e(P,g)^{V_i}\right)}$。

## 5 安全性分析

**定理1** 在随机预言模型中，如果CBDH问题困难，那么本文方案是语义抗IKGA安全。

如果$A_{\mathrm{I}}$可以用概率$\varepsilon$攻破方案，则在随机预言模型下，可以构造一个算法$C$解决CBDH问题，其解决问题的概率为$\varepsilon' \geq \left(\dfrac{2\varepsilon}{\mathrm{e}q_T q_{H_1}}\right)\left(1-\dfrac{1}{q_{H_1}}\right)^{q_s}$。其中$q_{H_1}$, $q_T$和$q_s$分别表示$H_1$查询，Trapdoor查询和提取秘密值查询的最大次数，e为自然对数。

**证明：** 给定一个CBDH问题的实例$(g, ag, bg, cg)$，然后构造一个算法$C$计算$e(g,g)^{abc}$。$C$执行setup算法生成公共参数prms，设$P=ag$。$C$选择身份$\mathrm{ID}_d(1\leq d\leq q_{H_1})$作为挑战身份，$C$返回参数$\mathrm{prms}=(\mathrm{e}, g, G_1, G_2, P, \lambda, \mu, \mathrm{rk}, H_1, H_2, h_3)$给攻击者$A_{\mathrm{I}}$。

$H_1$询问：$C$维护$L_{H_1}$列表，其中包含元组$<\mathrm{ID}_i, R_{\mathrm{ID}_i}, a_i>$，攻击者$A_{\mathrm{I}}$提出关于$<\mathrm{ID}_i, R_{\mathrm{ID}_i}>$的询问时，如果元组$<\mathrm{ID}_i, R_{\mathrm{ID}_i}, a_i>$已经存在于$L_{H_1}$表中，$C$输出$a_i$，否则$C$选择一个随机数$a_i\in Z_q^*$，并将$<\mathrm{ID}_i, R_{\mathrm{ID}_i}, a_i>$加入$L_{H_1}$表中，返回$a_i$。

$H_2$询问：$C$维护包含元组$<w_i, u_i, c_i, H_{2i}>$的$L_{H_2}$列表，接收到攻击者$A_{\mathrm{I}}$关于$w_i$的询问后，如果$<w_i, u_i, c_i, H_{2i}>$已经存在于表$L_{H_2}$中，返回$H_{2i}$。否则，$C$选择一个随机数$u_i\in Z_q^*$并掷硬币$c_i\in\{0,1\}$，其中$\Pr[c_i=0]=\delta$。$C$设置$H_{2i}=(1-c_i)bg+u_i g$，并将元组$<w_i, u_i, c_i, H_{2i}>$加入到$L_{H_2}$中并返回$H_{2i}$。

提取部分私钥询问：$C$维护包含元组$<\mathrm{ID}_i, R_{\mathrm{ID}_i}, D_{\mathrm{ID}_i}>$的表$L_{E_1}$。接收到攻击者$A_{\mathrm{I}}$关于$\mathrm{ID}_i$的部分私钥询问后，$C$选择两个随机数$a_i, D_{\mathrm{ID}_i}\in Z_q^*$，输出$R_{\mathrm{ID}_i}=D_{\mathrm{ID}_i}g-a_i P$，并将$<\mathrm{ID}_i, R_{\mathrm{ID}_i}, A_{\mathrm{ID}_i}>$添加到表$L_{H_1}$，$<\mathrm{ID}_i, R_{\mathrm{ID}_i}, D_{\mathrm{ID}_i}>$添加到表$L_{E_1}$并返回$R_{\mathrm{ID}_i}$和$D_{\mathrm{ID}_i}$给攻击者$A_{\mathrm{I}}$。

秘密值提取询问：$C$维护表$L_{E_2}$, $A_{\mathrm{I}}$对$\mathrm{ID}_i$进行询问。如果$\mathrm{ID}_i=\mathrm{ID}_d$，$C$设$P_{\mathrm{ID}_i}=cg$并将$<\mathrm{ID}_i, \perp, P_{\mathrm{ID}_i}>$添加到$L_{E_2}$($E_1$表示此事件发生)。否则，$C$随机选择$x_{\mathrm{ID}_i}\in Z_q^*$。计算$P_{\mathrm{ID}_i}=x_{\mathrm{ID}_i}g$将$<\mathrm{ID}_i, x_{\mathrm{ID}_i}, P_{\mathrm{ID}_i}>$加入$L_{E_2}$，并输出$x_{\mathrm{ID}_i}$。

公钥询问：当$A_{\mathrm{I}}$对$\mathrm{ID}_i$进行公钥问时，$C$分别在表$L_{E_1}$和$L_{E_2}$中搜索$<\mathrm{ID}_i, R_{\mathrm{ID}_i}, D_{\mathrm{ID}_i}>$和$<\mathrm{ID}_i, x_{\mathrm{ID}_i}, P_{\mathrm{ID}_i}>$，然后输出$\mathrm{PK}_{\mathrm{ID}_i}=(P_{\mathrm{ID}_i}, R_{\mathrm{ID}_i})$。

公钥替换询问：$C$使用$<\mathrm{ID}'_i, P'_{\mathrm{ID}_i}, R'_{\mathrm{ID}_i}>$替换$<\mathrm{ID}_i, P_{\mathrm{ID}_i}, R_{\mathrm{ID}_i}>$，在替换公钥之后设置$R_{\mathrm{ID}_i}=R'_{\mathrm{ID}_i}$，$P_{\mathrm{ID}_i}=P'_{\mathrm{ID}_i}$, $D_i=\perp$, $x_{\mathrm{ID}_i}=\perp$。

陷门询问：接收到$A_{\mathrm{I}}$对关于$\mathrm{ID}_i$的关键字$w_i$陷门询问后，$C$在表$L_{H_2}$中得到元组$<w_i, u_i, c_i, H_{2\mathrm{i}}>$。如果$c_i=0$, $C$终止模拟($E_2$表示此事件发生)。否则，$C$通过公钥询问得到$\mathrm{PK}_{\mathrm{ID}_i}=(P_{\mathrm{ID}_i}, R_{\mathrm{ID}_i})$, $C$从表$L_{H_1}$里得到$a_i$，计算$T_w=e(u_i(R_{\mathrm{ID}_i}+a_i P+P_{\mathrm{ID}_i}), P_{\mathrm{Do}}+R_{\mathrm{Do}}+a_{\mathrm{Do}}P)$并将$T_{w_i}$返回给$A_{\mathrm{I}}$。

挑战阶段：$A_{\mathrm{I}}$输出$(w_0, w_1)$作为对$\mathrm{ID}^*$的挑战关键词。如果$\mathrm{ID}^*\neq\mathrm{ID}_d$, $C$终止模拟。($E_3$表示此事件发生)。如果$\mathrm{ID}^*=\mathrm{ID}_l$, $C$从表$L_{H_2}$中得到$<w_0, u_0, c_0, H_{20}>$和$<w_1, u_1, c_1, H_{21}>$。如果$c_0=c_1=1$, $C$终止模拟。($E_4$表示此事件发生)否则，$C$选择随机选择$b\in\{0,1\}$使$c_b=0$。$C$随机选择数$r\in Z_q^*$和点$Q\in G_1$，将$C_1=Q, C_2=rg$作为密文返回给$A_{\mathrm{I}}$。

更多陷门询问：除了挑战的关键词外，$A_{\mathrm{I}}$可对继续对关键字$w_i$进行陷门询问($E_5$表示事件$A_{\mathrm{I}}$在更多陷门询问中不对挑战关键字进行询问)。

猜测：最后，$A_{\mathrm{I}}$输出$b'\in\{0,1\}$。这时可以通过如下步骤计算$e(g,g)^{abc}$。

$$\begin{aligned} & \frac{e(D_{\mathrm{Du}_i}g+cg, P_{\mathrm{Do}}+R_{\mathrm{Do}}+a_{\mathrm{Do}}ag)^{b+u_i}}{e(D_{\mathrm{Du}_i}g+cg, P_{\mathrm{Do}}+R_{\mathrm{Do}}+a_{\mathrm{Do}}ag)^{u_i}} \\ &= e(D_{\mathrm{Du}_i}g+cg, P_{\mathrm{Do}}+R_{\mathrm{Do}}+a_{\mathrm{Do}}ag)^b \end{aligned} \tag{3}$$

$$\begin{aligned} & \frac{e(D_{\mathrm{Du}_i}g+cg, P_{\mathrm{Do}}+R_{\mathrm{Do}}+a_{\mathrm{Do}}ag)^b}{e(D_{\mathrm{Du}_i}bg, P_{\mathrm{Do}}+R_{\mathrm{Do}}+a_{\mathrm{Do}}ag)} \\ &= e(cg, P_{\mathrm{Do}}+R_{\mathrm{Do}}+a_{\mathrm{Do}}ag)^b \end{aligned} \tag{4}$$

$$\begin{aligned} & \left(\frac{e(cg, P_{\mathrm{Do}}+R_{\mathrm{Do}}+a_{\mathrm{Do}}ag)^b}{e(cg, x_{\mathrm{Do}}bg+r_{\mathrm{Do}}bg)}\right)^{\frac{1}{a_{\mathrm{Do}}}}=\left(e(cg, a_{\mathrm{Do}}ag)^b\right)^{\frac{1}{a_{\mathrm{Do}}}} \\ &= (e(g,g)^{a_{\mathrm{Do}}\cdot abc\cdot\frac{1}{a_{\mathrm{Do}}}})=e(g,g)^{abc} \end{aligned} \tag{5}$$

如果$C$在上述游戏中没有停止，则$C$可以优势$\varepsilon'$解决CBDH困难问题。其中$\Pr[\neg E_1\wedge\neg E_2\wedge\neg E_3\wedge\neg E_4]=\left(1-\frac{1}{q_{H_1}}\right)^{q_s}\left(\frac{1}{q_{H_1}}\right)(1-(1-\delta)^2)$，可得

$$\varepsilon'\geq\frac{1}{2}\cdot 2\varepsilon\cdot\left(1-\frac{1}{q_{H_1}}\right)^{q_s}\left(\frac{1}{q_{H_1}}\right)\frac{2}{\mathrm{e}q_T}=\left(\frac{2\varepsilon}{\mathrm{e}q_Tq_{H_1}}\right)\left(1-\frac{1}{q_{H_1}}\right)^{q_s} \tag{6}$$

证毕

**定理2**　在随机预言模型下，如果$A_{\mathrm{II}}$以概率$\varepsilon$攻破方案。可以构建算法$C$以概率$\varepsilon'\geq\frac{2\varepsilon}{\mathrm{e}q_Tq_{H_1}}$解决CBDH困难问题，$q_{H_1}$和$q_T$分别代表$H_1$询问和陷门询问的最大次数，e为自然对数。

**证明**：$C$构造与定理1中证明过程相似，除了$C$返回给$A_{\mathrm{II}}$的$\mathrm{prms}=(\mathrm{e},g,G_1,G_2,P,\lambda,\mu,\mathrm{rk})$中$P=sg$，$P_{\mathrm{Du}}=aP,P_{\mathrm{Do}}=bP$。

$H_1$询问：与定理1中证明过程相同；

$H_2$询问：与定理1中证明过程相同。

提取部分私钥询问：与定理1中证明过程相似，除了$C$在接收到$A_{\mathrm{II}}$关于$\mathrm{ID}_i$部分私钥询问时，随机选择数$r_{\mathrm{ID}_i}\in Z_q^*$。计算$R_{\mathrm{ID}_i}=r_{\mathrm{ID}_i}g$，再从表$L_{H_1}$中得到$<\mathrm{ID}_i,R_{\mathrm{ID}_i},D_{\mathrm{ID}_i}>$，将其添加到表$L_{E_1}$并返回$R_{\mathrm{ID}_i}$和$D_{\mathrm{ID}_i}$给$A_{\mathrm{II}}$。

陷门询问：与定理2中证明过程相似，除了当$c_i\neq 0$时，$C$可以从表$L_{E_1}$中得到$<\mathrm{ID}_i,R_{\mathrm{ID}_i},D_{\mathrm{ID}_i}>$。并计算$T_w=e(d_{\mathrm{ID}_i}g+ag,bg+R_{\mathrm{Do}}+a_{\mathrm{Do}}P)^{u_i}$，将其返回给$A_{\mathrm{II}}$。

挑战阶段：与定理2中挑战阶段相同。

更多陷门询问：与定理2中相同。

猜测：最后，$A_{\mathrm{II}}$输出$b'\in\{0,1\}$，这时$C$可以通过如下步骤计算$e(g,g)^{abc}$。

$$\frac{e(D_{\mathrm{ID}_i}g+ag,bg+R_{\mathrm{Do}}+a_{\mathrm{Do}}P)^{c+u_i}}{e(D_{\mathrm{ID}_i}g+ag,bg+R_{\mathrm{Do}}+a_{\mathrm{Do}}P)^{u_i}}=e(D_{\mathrm{ID}_i}g+ag,bg+R_{\mathrm{Do}}+a_{\mathrm{Do}}P)^{c} \tag{7}$$

$$\frac{e(D_{\mathrm{ID}_i}g+ag,bg+R_{Do}+a_{Do}P)^{c}}{e(D_{\mathrm{ID}_i}cg,bg+R_{Do}+a_{Do}P)}=e(ag,bg+R_{\mathrm{Do}}+a_{\mathrm{Do}}P)^{c} \tag{8}$$

$$\frac{e(ag,bg+R_{\mathrm{Do}}+a_{\mathrm{Do}}P)^{c}}{e(ag,r_{\mathrm{Do}}cg+a_{\mathrm{Do}}cP)}=e(g,g)^{abc} \tag{9}$$

如果$C$在上述游戏中没有中止，则$C$可以解决CBDH问题。　　证毕

以下分析$C$解决CBDH问题的优势。

$$\Pr[\neg E_1\wedge\neg E_2\wedge\neg E_3]=(1-\delta)^{q_T}\left(1-(1-\delta)^2\left(\frac{1}{q_{H_1}}\right)\right),$$
$$\varepsilon'\geq\frac{1}{2}\cdot 2\varepsilon\cdot\left(\frac{1}{q_{H_1}}\right)\left(\frac{2}{\mathrm{e}q_T}\right)=\frac{2\varepsilon}{\mathrm{e}q_Tq_{H_1}} \tag{10}$$

本文方案具有认证性，方案中发送者在对关键词进行加密时，将其自身私钥加入到加密算法中对关键词进行数字签名使接收者在收到密文后对其验证。文中的认证性实质上就是签名的不可伪造性。由于其具体证明过程与文献[8]中证明步骤相似，限于篇幅，此处省略具体证明细节。

## 6　性能分析

### 6.1　计算性能分析

本节中，对本文方案和文献[9,11,12]中的方案进行性能对比。使用i5-2400 3.10 GHz处理器、4 GB内存和win10操作系统的计算机在Eclipse环境下，利用JPBC密码库[19]对相关的密码运算进行模拟。

首先对比方案与文献[9]方案和文献[11]方案在计算性能上的表现(其中Tsm为标量乘法运算的运行时间；Tbp为双线性配对运行时间；TH为哈希函数映射到群上点的运行时间；Th为一般哈希函数运行时间；Tpa为群上点加法运算的运行时间；Tmul为乘法运算的运行时间)。从表1和图2可知，相较于文献[9]方案，本文方案在KeyGen阶段降低了69.53%。相较文献[11,12]方案，本文方案在密文生成阶段分别降低了69.39%和26.81%。本文方案虽然在Trapdoor阶段和Test阶段的执行时间略逊于文献[9,11]的方案，但Trapdoor阶段较于文献[12]方案降低了13%。而且，本文方案的Trapdoor算法和Test算法比文献[12]方案中的KeyGen和Trapdoor算法时间消耗更少。因此，本文方案在整体方案计算

**表 1　计算性能分析**

| 方案 | KeyGen | 密文生成 | Trapdoor | Test | 抗IKGA | 支持多用户 |
|---|---|---|---|---|---|---|
| 文献[9] | 2TH+8Tsm=161.2918 | 3TH+2Th+5Tsm+3Tbp=235.8 | TH+Th+3Tsm=68.5 | Th+Tsm+2Tpa+Tbp=39.2 | × | × |
| 文献[11] | 2TH+4Tsm=112.2746 | 3TH+Th+4Tsm+3Tbp+3Tpa=224.1 | TH+Tpa+Tsm=44.1 | 2TH+Tsm+Th+2Tpa+Tbp=102.5 | × | × |
| 文献[12] | 2Th+4Tsm=49.1384 | TH+3Th+5Tsm+Tbp+3Tpa=93.7 | TH+3Th+3Tsm+Tbp+2Tpa=95.5 | 2Tsm+2Th+2Tpa+2Tbp+Tmul=78.1 | √ | × |
| 本文 | 2Th+4Tsm=49.1384 | TH+3Tsm+Tpa=68.6 | TH+Th+2Tsm+Tbp+2Tpa=83.1 | 2Tsm+2Th+4Tpa+2Tbp+Tmul=78.8 | √ | √ |

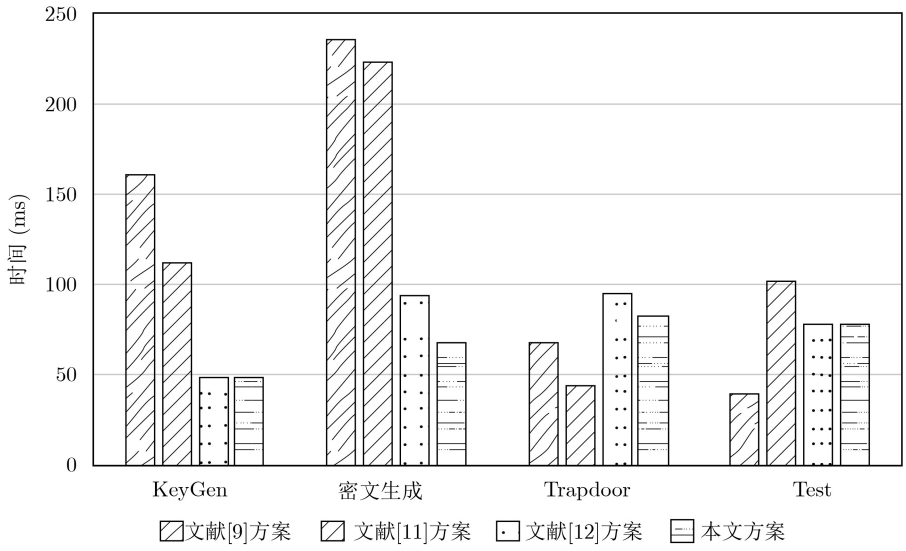


图 2 计算量对比

效率上性能表现更佳。同时与文献[12]方案相比，尽管本文方案效率并不占优势，但是本文方案在抵抗IKGA的同时，能够支持多用户功能。

### 6.2 通信性能分析

本文将对公钥(PK)，密文($C$)和陷门($T$)方面的通信成本与其他方案进行比较。设|PK|, $|C|$和$|T|$分别表示PK, $C$和$T$的大小。设$|G_1|$, $|G_2|$和$|Z_q|$表示$G_1$, $G_2$和$Z_q$中元素的大小。由表2可得，虽然本文方案与文献[11,12]方案相比通信成本几乎相同，但与文献[9]方案相比，本文方案具有更低的通信成本。

表 2 通信量分析比较

| 方案 | 公钥PK大小 | 密文大小 | 陷门T大小 |
|---|---|---|---|
| 文献[9] | $4\|G_1\|$ | $\|G_1\|+\|Z_q\|$ | $3\|G_1\|$ |
| 文献[11] | $2\|G_1\|$ | $\|G_1\|+\|Z_q\|$ | $\|G_1\|$ |
| 文献[12] | $2\|G_1\|$ | $2\|G_1\|$ | $\|G_2\|$ |
| 本文 | $2\|G_1\|$ | $2\|G_1\|$ | $\|G_2\|$ |

## 7 结束语

为了实现多个授权用户利用关键词进行密文检索，同时抵抗IKGA、解决证书管理和密钥托管问题。本文结合公钥认证加密技术和代理重加密技术，提出了一个高效的多用户模型下无证书公钥认证的可搜索加密方案。该方案对部分密文只进行1次标量乘法的重加密处理，使得多个授权用户可以利用关键字生成陷门查询对应密文，在解决密钥托管和证书管理问题同时实现了在多用户模型下的应用。在随机预言模型下，证明本文方案具有抵抗无证书公钥密码环境下两类攻击者的内部关键词猜测攻击的能力，且其计算和通信效率优于同类方案。

## 参 考 文 献

[1] BONEH D, DI CRESCENZO G, OSTROVSKY R, *et al*. Public key encryption with keyword search[C]. 2004 International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2004: 506–522.

[2] CHANG Y C and MITZENMACHER M. Privacy preserving keyword searches on remote encrypted data[C]. The 3rd International Conference on Applied Cryptography and Network Security, New York, USA, 2005: 442–455.

[3] KAMARA S, PAPAMANTHOU C, and ROEDER T. Dynamic searchable symmetric encryption[C]. 2012 ACM Conference on Computer and Communications Security, Raleigh, USA, 2012: 965–976.

[4] SAMANTHULA B K, JIANG Wei, and Bertino E. Privacy-preserving complex query evaluation over semantically secure encrypted data[C]. The 19th European Symposium on Research in Computer Security, Wroclaw, Poland, 2014: 400–418.

[5] SHAO Jun, CAO Zhenfu, LIANG Xiaohui, *et al*. Proxy re-encryption with keyword search[J]. *Information Sciences*, 2010, 180(13): 2576–2587. doi: 10.1016/j.ins.2010.03.026.

[6] LEE S H and LEE I Y. A study of practical proxy reencryption with a keyword search scheme considering cloud storage structure[J]. *The Scientific World Journal*, 2014: 615679. doi: 10.1155/2014/615679.

[7] 郭丽峰, 卢波. 有效的带关键字搜索的代理重加密方案[J]. 计算机研究与发展, 2014, 51(6): 1221–1228. doi: 10.7544/issn1000-1239.2014.20130329.

GUO Lifeng and LU Bo. Efficient proxy re-encryption with keyword search scheme[J]. *Journal of Computer Research and Development*, 2014, 51(6): 1221–1228. doi: 10.7544/issn1000-1239.2014.20130329.

[8] HUANG Qiong and LI Hongbo. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks[J]. *Information Sciences*, 2017, 403/404: 1–14. doi: 10.1016/j.ins.2017.03.038.

[9] PENG Yanguo, CUI Jiangtao, PENG Changgen, *et al*. Certificateless public key encryption with keyword search[J]. *China Communications*, 2014, 11(11): 100–113. doi: 10.1109/CC.2014.7004528.

[10] WU T, MENG Fanya, CHEN C, *et al*. On the security of a certificateless searchable public key encryption scheme[C]. The 10th International Conference on Genetic and Evolutionary Computing, Fuzhou, China, 2016: 113–119.

[11] MA Mimi, HE Debiao, KHAN M K, *et al*. Certificateless searchable public key encryption scheme for mobile healthcare system[J]. *Computers & Electrical Engineering*, 2018, 65: 413–424. doi: 10.1016/j.compeleceng.2017.05.014.

[12] MA Mimi, HE Debiao, KUMAR N, *et al*. Certificateless searchable public key encryption scheme for industrial internet of things[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(2): 759–767. doi: 10.1109/TII.2017.2703922.

[13] CURTMOLA R, GARAY J, KAMARA S, *et al*. Searchable symmetric encryption: Improved definitions and efficient constructions[J]. *Journal of Computer Security*, 2011, 19(5): 895–934. doi: 10.3233/JCS-2011-0426.

[14] RANE D D and GHORPADE V R. Multi-user multi-keyword privacy preserving ranked based search over encrypted cloud data[C]. 2015 International Conference on Pervasive Computing, Pune, India, 2015: 1–4.

[15] YANG Yanjiang, LU Haibing, and WENG Jian. Multi-user private keyword search for cloud computing[C]. The 2011 IEEE 3rd International Conference on Cloud Computing Technology and Science, Athens, Greece, 2011: 264–271.

[16] CHANG Y and WU J. Multi-user searchable encryption scheme with constant-size keys[C]. The 2017 IEEE 7th International Symposium on Cloud and Service Computing, Kanazawa, Japan, 2017: 98–103.

[17] WANG Guofeng, LIU Chuanyi, Dong Yingfei, *et al*. IDCrypt: A multi-user searchable symmetric encryption scheme for cloud applications[J]. *IEEE Access*, 2018, 6: 2908–2921. doi: 10.1109/ACCESS.2017.2786026.

[18] TANG Qiang. Nothing is for free: Security in searching shared and encrypted data[J]. *IEEE Transactions on Information Forensics and Security*, 2014, 9(11): 1943–1952. doi: 10.1109/TIFS.2014.235938.

[19] CARO A D and IOVINO V. JPBC library[EB/OL]. http://gas.dia.unisa.it/projects/jpbc/index.html#.VTDrLSOl_Cw, 2013.

张玉磊：男，1979年生，副教授，研究方向为密码学和信息网络安全.

文　龙：男，1996年生，硕士生，研究方向为网络与信息安全.

王浩浩：男，1993年生，硕士生，研究方向为网络与信息安全.

张永洁：女，1978年生，副教授，研究方向为密码学和信息网络安全.

王彩芬：女，1963年生，教授，研究方向为密码学与信息安全.