研究与开发

基于 BDH 问题的支持多服务器连接关键词可搜索加密方案

卢艳华[1,2,4]，田有亮[2,3,4]，刘成[2,3,4]

（1. 贵州大学数学与统计学院，贵州 贵阳 550025;
2. 贵州省公共大数据重点实验室，贵州 贵阳 550025;
3. 贵州大学计算机科学与技术学院，贵州 贵阳 550025;
4. 贵州大学密码学与数据安全研究所，贵州 贵阳 550025)

摘　要：可搜索加密是一种支持用户在密文上进行关键字查找的密码学原语，鉴于传统单服务器可搜索加密方案数据检索效率不高的问题，基于身份在证书管理方面的优势，提出了在多服务器环境下利用双线性映射构造一种支持连接关键词搜索的加密方案。在该方案中，加密数据的存储与查询分配给不同的服务器，通过协作共同提高用户存储和关键词的检索效率；再利用多服务器与用户的身份实现连接关键词的加密与搜索；同时结合连接关键词的可搜索加密方法，基于双线性映射构造新的安全模型。且在双线性 Diffie-Hellman 问题下，该方案满足选择消息攻击下的密文不可区分性。

关键词：多服务器；连接关键词；基于身份加密；双线性 Diffie-Hellman；密文不可区分性

中图分类号：TP309.7

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2020049

Multi-server conjunctive keyword searchable encryption scheme based on BDH problem

LU Yanhua[1,2,4], TIAN Youliang[2,3,4], LIU Cheng[2,3,4]

1. College of Mathematics & Statistics, Guizhou University, Guiyang 550025, China
2. Guizhou Province Key Laboratory of Public Big Data, Guiyang 550025, China
3. College of Computer Science & Technology, Guizhou University, Guiyang 550025, China
4. Institute of Cryptography & Data Security, Guizhou University, Guiyang 550025, China

Abstract: Searchable encryption is a cryptographic primitive that supports users to search for keywords on ciphertext. In

收稿日期：2019−09−23；**修回日期**：2019−12−22

基金项目：国家自然科学基金资助项目（No.61662009，No.61772008）；贵州省教育厅科技拔尖人才支持项目（No.[2016] 060）；贵州省科技重大专项计划项目（No.20183001）；贵州省科技计划项目（No.[2017]5788）；教育部—中国移动科研基金研发项目（No.MCM20170401）；贵州大学培育项目（No.[2017]5788）；国家自然科学基金联合基金重点支持项目（No.U1836205）；贵州省科技计划项目（No.[2019]1098）

Foundation Items: The National Natural Science Foundation of China (No.61662009, No.61772008), Guizhou Provincial Department of Education Science and Technology Top Talent Support Project (No.[2016]060), Science and Technology Major Support Program of Guizhou Province of China (No.20183001), Science and Technology Program of Guizhou Province of China (No.[2017]5788), Ministry of Education-China Mobile Research Fund Project (No.MCM20170401), Guizhou University Cultivation Project of China (No.[2017]5788), Key Project Supported by the Joint Fund of the National Natural Science Foundation of China (No.U1836205), Science and Technology Program of Guizhou Province of China (No.[2019]1098)

view of the low efficiency of traditional single-server searchable encryption schemes, it was based on the advantages of identity management in certificate management. In the multi-serve environment, a bilinear mapping was used to construct an identity-based encryption scheme that supports conjunctive keyword search. In this scheme, the storage and query of the encrypted data were allocated to different servers, and the retrieval efficiency of the user storage and keyword was improved by cooperation. Re-use the encryption and search ability of the connection keywords by using the identity of multi-server and user. At the same time, combine with the searchable encryption method of conjunctive keyword, a new security model was constructed based on bilinear pairing. And under the bilinear Diffie-Hellman problem, the scheme satisfies the ciphertext indistinguishability under selected message attack.

Key words: multi-server, conjunctive keyword, ID-based encryption, bilinear Diffie-Hellman, ciphertext indistinguishability

1 引言

云计算为租户提供存储、计算和网络服务，数据安全保护和租户间的数据共享与访问控制是其必不可少的能力[1]。可搜索加密方案允许第三方客户端在不需要恢复明文的情况下搜索加密数据，它在实现密文检索功能的同时，也起到保护用户隐私的作用。首次提出可搜索加密方法的是著名密码学家 Song和Wagner[2]基于密文扫描思想和对称密钥机制提出的第一个 SSE（symmetric searchable encryption）方案。紧接着，Boneh等[3]又提出了公钥可搜索加密（PEKS）的概念，用以解决在使用公钥加密系统加密的数据上进行搜索的问题。自此之后，PEKS便引起了研究界的极大关注，许多研究人员对它进行了改进。

在实际应用场景中，单关键词检索使得云服务器返回很多不相关的密文，占用大量计算和带宽资源，鉴于搜索连接关键词是常见的检索模式，Parkd 等[4]、Hwang 等[5]、Dan 等[6]各提出了一种支持连接关键词搜索的公钥加密方案，其目的是基于PEKS检索使用“逻辑与”连接的多个关键词。2016 年，宋衍等[7]又提出了支持关键词任意连接搜索的属性加密方案，该方案基于多项式方程，实现对关键词的任意连接搜索，显著提高了连接搜索的灵活性。2017 年，Fairouz 等[8]提出了一种新的对称密钥加密方案，它支持一个关键字字段自在加密文件上的自由搜索，不需要指定关键字的位置，且关键字可以以任何顺序出现。之后，Lu 等[9]提出了高效的指定服务器的基于身份加密连接关键字搜索方案。

2004 年，Byun[10]针对Parkd 等[3]与Kim等[4]提出的两种方案，指出它们都不能抵抗离线关键字猜测攻击，也就是说，给定一个陷门，攻击者能通过穷举等方法生成陷门关键字。在PEKS中，需要满足的安全目标应包括两点，即针对没有陷门的服务器而言，除文件长度外，无法获取任何文件信息；而拥有陷门的服务器能够检索到所有包含对应关键字的密文文件。基于此，Boneh等[3]定义了 PEKS 在选择关键词攻击下的不可区分性：IND-CKA。在此安全模型中，必须在接收者和服务器之间建立一个安全信道来传送陷门，这在一定程度上增加了通信成本。鉴于此，2008 年，Baek 等[11]定义了一个新的指定服务器公钥可搜索加密方案（dPEKS方案）的安全模型，消除 Boneh 提出的利用安全信道传送陷门的要求。

在传统的公钥系统中，建立用户公钥与身份之间的映射关系需要使用证书。为了消除证书管理问题，1984 年，Shamir[12]提出了一种基于身份的加密方案（IBE），IBE 方案由于无需在线的可信第三方，因此在根本上解决了传统 PEKS 方案中可信第三方的性能瓶颈问题，从而实现公钥基础设施的简化。2001年，Boneh 等[13]紧随其后，提出了一个实用的基于身份的加密方案（IBES），该方案引入双线性对实现构造，之后双线性映射

被广泛应用到密码学各个研究领域。针对证书管理与安全信道问题，Wu 等[14]便提出了基于身份密码系统下的 dPEKS 方案，称之为 dIBEKS 方案，该方案有效解决了安全信道与证书管理的问题。但 Wu 等所提方案不能满足 dIBEKS 密文不可区分性与有效抵御离线关键词猜测攻击。鉴于此，王少辉等[15]提出了满足密文不可区分性的高效 dIBEKS 方案。

大数据拥有者出于对安全与效率的考虑，更加愿意将海量数据分布到多个服务器中进行存储与查询。在多服务器环境下，2017 年，Mohamad 等[16]在论基于块的多服务器可搜索对称加密的安全优势中，基于多服务器块的 SSE 的安全性，将文档以加密文档块集的形式存储于多个存储服务器中。紧接着，Huang 等[17]提出一种基于云存储的多服务器多关键词可搜索加密方案，较单服务器而言，极大提高了海量数据的存储与搜索效率。之后，Zhang 等[18]提出一种在云环境下基于无证书的多服务器可搜索加密方案，该方案将存储和搜索功能分配给不同的服务器，与单服务器相比，不仅能够提升数据检索效率，还能减轻服务器的负担，使方案具有更好的实用性。基于此想法，本文在多服务器环境下，通过服务器相互协作共同为用户提供存储和连接关键词的检索服务，主要贡献可阐述如下：

- 提出一种基于身份高效的支持连接关键词搜索的多服务器加密方案，此方案在完全基于身份的加密体制下，实现了对连接关键字的检索。相较于单关键词检索模型，能快速、精确地定位所需文档，一次搜索多个关键词能够缩小搜索范围，改进搜索性能；
- 加密数据的存储与查询分配给不同的服务器，将用于查询的数据分散到多个子服务器，通过协作共同为用户提供存储和连接关键词的检索服务；
- 在 RO（random oracles，随机预言机）模型下[19]，引用王少辉等[15]所提方案的安全性定义进行安全性分析，证明在 BDH 困难问题假设下，MS-CK-SE（multi-server conjunctive keyword searchable encryption，多服务器连接关键词可搜索加密）方案满足适应性选择消息攻击下的密文不可区分性。

2　基础知识

定义 2.1　双线性映射[2]：设加法循环群 G_1 和乘法循环群 G_2，具有相同的大素数阶 p，且 $G_1=\langle g\rangle$。称映射 $e:G_1\times G_1\to G_2$ 为双线性映射，当且仅当映射 e 满足下列 3 条性质：

（1）双线性：对于任意的两个点 Q，$R\in G_1$ 和任意的两个随机数 $a,b\in Z_p^*$，存在 $e(a\cdot Q,b\cdot R)=e(Q,R)^{ab}$；

（2）非退化性：对于任意的生成元 $g\in G_1$，$e(g,g)\neq 1_{G_2}$；

（3）可计算性：对于任意的两个点 $Q,R\in G_1$，$e(Q,R)$ 是容易计算的。

定义 2.2　BDH（双线性 Diffe-Hellman）假设：给出四元组 $(g,ag,bg,cg)\in G_1$，g 为 G_1 的生成元，且 $a,b,c\in Z_p^*$ 为未知，那么得到 $e(g,g)^{abc}\in G_2$ 的概率是可忽略的。

3　MS-CK-SE 方案

本节将详细描述 MS-CK-SE 方案的系统模型、形式化定义以及安全模型。

3.1　系统模型

方案架构如图 1 所示，系统模型包括 5 个部分：数据拥有者负责对数据文件进行加密，并为数据构造搜索密文，同时将加密后的数据以及搜索密文上传至云端服务器 S；云端服务器 S 用来存储数据发送者上传的密文文件，规定此服务器不直接提供数据检索功能；子服务器 S_i：为提高检索效率与抵御关键词猜测攻击，存储服务器分

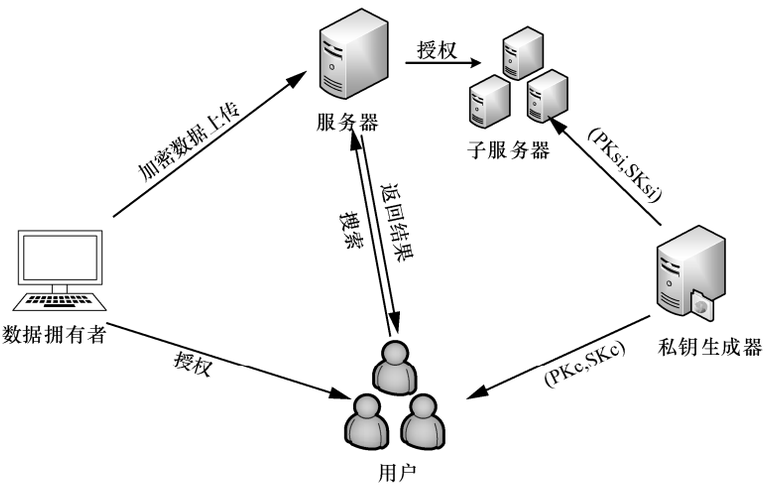

图 1　方案架构

发的加密文件，并提供针对用户的检索服务；PKG（私钥生成器）：根据用户与子服务器提供的身份信息，生成各自的公私钥对并返回部分私钥。

假设云服务器是诚实且好奇的，即云服务器会诚实地执行用户提交的搜索请求，并返回相应的搜索结果，但也想获取隐私信息。本文只考虑密钥生成、搜索密文、陷门生成以及匹配测试等问题。用户的身份信息对应记为 ID_C，云端子服务器对应的身份信息记为 ID_{Si}，云端服务器 S 对子服务器授权。数据拥有者需要加密上传至云端服务器 S 的文档为 $D=\{D_1,\cdots,D_n\}$，定义每个文档包含的连接关键字集合为 $D_n=\{w_{n,1},w_{n,2},\cdots,w_{n,k}\}$，$w_{j,h}$ 代表第 j 个文档的第 h 个关键字段。如定义文档包含有 3 个关键字段，分别为“From”“To”、“Subject”。再假设：

（1）每个文档都有 i 个关键字段；

（2）同一关键字不会出现在同一文档的两个不同关键字段中，如“From：Bob”“Bob”属于“From”字段，而不属于“To”字段；

（3）对每个文档定义每个关键字段，如空格关键字定义为“Null”[4]。

再将 n 个加密文档按 Hilbert 填充曲线的数据划分方式分配到 i 个子服务器中，由于 Hilbert 填充曲线是针对点对象而设计的，而要为空间对象赋予 Hilbert 值，首先需要对数据集进行预处理。其方法是：计算获得每个空间数据文件的中心点 O_i，以 O_i 表示第 i 个文件；根据 O_i 的横纵坐标值，计算每个多边形对象的 Hilbert 值。通过该方法，可以将空间数据集转换为点数据集，从而构造 Hilbert 曲线。本文利用 Hilbert 空间填充曲线对大型数据进行空间划分，将其分于多个服务器中，其方法描述为：对加密上传至云端服务器 S 的文件 $D=\{f_1,f_2,\cdots,f_n\}$，均匀分发至 N 个子服务器 $S_1,S_2,\cdots,S_N$。其中，V_i 表示第 i 个空间对象文件实体的大小，其中 $i\in[1,n]$；V_{other} 表示每个控件对象中所有非空间类型字段值的大小，因为除空间对象实体字段外，其他字段的大小是可以估计的，所以可以近似地用该变量统一表示；V_{avg} 每个子服务器上存储的所有空间实体的平均容量，其等式关系可以表示为：

$$V_{\mathrm{avg}}=\frac{nV_{\mathrm{other}}+\sum_{i=1}^{n}V_i}{N} \tag{1}$$

规定每个子服务器所分配到的文件个数为整数，且数据拥有者知道所属子文件分布在哪些对应的子服务器之中。当用户向服务器 S 提出搜索时，S 就将搜索请求分发至子服务器 S_i，这多个子服务器协同合作，同时进行关键字的搜索，然后子服务器将搜索匹配的结果返回给服务器 S，

S 整理后将匹配对应的密文文档反馈给用户。本文方案应同时实现对自适应选择连接关键字攻击下的密文不可区分性。

3.2　形式化定义

基于 BDH 问题的支持多服务器连接关键词可搜索加密方案通常包括以下 5 个算法。

（1）Setup：输入系统安全参数 ξ，输出主密钥 Mak 和系统的公共参数 Params，保留 Mak 并公开 Params。

（2）KeyGen：此算法由 PKG 运行，输入 Mak 和 Params 以及具有访问权限用户和子服务器的身份信息，分别输出其公私钥对。

（3）Encrypt：此算法由数据拥有者执行，首先将加密的文档分发至子服务器 S_i 中，再在其中选择对应的关键词 $D_n=\{w_{n,1},w_{n,2},\cdots,w_{n,i}\}$，利用子服务器和其身份信息对 $D_n=\{w_{n,1},w_{n,2},\cdots,w_{n,i}\}$ 进行加密。

（4）Trapdoor：此算法由数据接收者执行，输入相应的关键词查询格式 $Q=\langle I_1,\cdots,I_m,w_{I_1}',\cdots,w_{I_m}'\rangle$，$(m\leqslant i)$。接收者利用自己的私钥以及子服务器的身份信息，生成相应的关键词陷门 T。数据接收者将 T 发送给子服务器进行搜索服务请求。

（5）Test：此算法由子服务器 S_i 执行，它选择以其私钥及用户的身份信息、密文 C 与陷门 T 为输入。若密文 C 与陷门 T 对应关键词密文匹配，即 $\{(w_{I_1}=w_{I_1}'),\cdots,(w_{I_m}=w_{I_m}')\}$，则输出“True”，再将对应加密文件发送给授权用户，否则输出“False”。

3.3　安全模型

通过游戏来定义以上安全模型。

可形式化地给出 MS-CK-SE 方案要达到的安全性需求，即该方案能够满足选择消息攻击下的密文不可区分性。其证明是基于 BDH 困难性问题进行的，假设存在两类敌手，分别为任意恶意子服务器 A_0 和外部敌手 A_1。为了描述密文不可区分性的要求，定义了两个游戏，即 Game_0 和 Game_1，在两个概率多项式时间的敌手之间，分别定义为敌手 A_0、A_1 和挑战者 C。

挑战者 C 和具有多项式时间的敌手 A_0、A_1 之间的安全游戏（Game_0, Game_1）如下。

（1）Setup：C 输入安全参数，产生系统公开参数和保密的主密钥。

（2）Phase1：A_0、A_1 以一种自适应的方式对 C 进行以下查询：

1）对子服务器 S_j 的密钥产生询问：A_0、A_1 向 C 发送子服务器 S_j 的身份信息 ID_{S_j}，C 运行服务器密钥产生算法，产生对应的私钥 $\text{SK}_{\text{ID}_{S_j}}$，并把它发送给敌手。

2）对数据接收者的密钥产生询问：A_0、A_1 向 C 对用户的身份信息 ID_C 进行询问，C 运行用户的密钥产生算法，产生对应的密钥 SK_{ID_C}，并把它发送给敌手。

3）对陷门产生询问：A_0、A_1 向 C 对任何的查询格式 Q 产生询问，C 调用陷门生成算法，产生对应的陷门 T_Q，并把它发送给敌手。

（3）Challenge：A_0、A_1 输入两个包含连接关键词的文档 D_0、D_1 以及用户的身份信息 $\text{ID}_{C'}$，要求没有就用户的身份信息 $\text{ID}_{C'}$ 进行过密钥查询。C 随机选择一个比特值 $b\in\{0,1\}$，计算相应的密文 C^*，并将其发送给敌手。

（4）Phase2：A_0、A_1 适应性地执行更多从事于 Phase1 的询问，敌手对任意用户的身份信息 ID_{Ci} $(\text{ID}_C'\neq\text{ID}_{Ci})$ 进行过密钥查询，并对任何的查询格式 Q' 进行陷门询问。

（5）Guess：最后，A_0、A_1 输出对 b 的猜测 b'，其中 $b'\in\{0,1\}$，如果 $b=b'$，则敌手攻击成功。

定义　如果对于任意的多项式时间敌手 A_0、A_1，能够攻破 MS-CK-SE 方案密文不可区分性的概率优势为：

$$\text{Adv}_{A_0,A_1}^{\text{Game}_{0,1}}(\xi)=|\Pr(b=b')-1/2| \tag{2}$$

综上，若 $\text{Adv}_{A_0,A_1}^{\text{Game}_0}(\xi)$ 是安全参数 ξ 的一个可忽略函数，则 MS-CK-SE 方案满足适应性选择消息攻击下的密文不可区分性。

4 MS-CK-SE 方案设计

MS-CK-SE 方案的具体设计如下。

（1）Setup：给定安全参数 ξ，首先由 PKG 生成双线性映射 $e:G_1\times G_1\to G_2$，群 G_1、G_2 具有相同的大素数阶 p。再随机选取主密钥 $s\in Z_p^*$，并计算系统公钥 $P_{\text{pub}}=sg$，其中 $G_1=<g>$。另外 PKG 选择杂凑函数：$H_1:\{0,1\}^*\to G_1$，$H_2:\{0,1\}^*\to G_1$，$H_3:\{0,1\}^k\times\{0,1\}^*\to G_1$，$H_4:G_2\to Z_p^*$。

发布系统参数：$\text{params}=\{e,G_1,G_2,p,g,P_{\text{pub}},H_1,H_2,H_3,H_4\}$。

（2）KeyGen：给定子服务器的身份信息 $\text{ID}_{Si}\in\{0,1\}^*$ 与文件接收者的身份信息 $\text{ID}_C\in\{0,1\}^*$，PKG 首先计算 $g_{\text{ID}_{Si}}=H_1(\text{ID}_{Si})$，子服务器随机选择私钥 $x_i\in Z_p^*$，生成并返回子服务器 S_i 的公私钥对，$\text{PK}_{\text{ID}_{Si}}=x_ig$，$\text{SK}_{\text{ID}_S}=(\text{SK}_{\text{ID}_{Si_1}},\text{SK}_{\text{ID}_{Si_2}})=(sH_1(\text{ID}_{Si}),x_i)$。同理，对于有访问权限的用户，私钥生成器再计算 $g_{\text{ID}_C}=H_2(\text{ID}_C)$，生成并返回用户的私钥 $\text{SK}_{\text{ID}_C}=sg_{\text{ID}_C}$。

（3）Encrypt：利用子服务器与用户的身份信息，选择子服务器所包含文档的关键词 $D=\{w_1,w_2,\cdots,w_i\}$，数据发送者选择随机数 $r_1,r_2\in Z_p*$，计算关键词密文 $C=(A,B,C,D,E_1,E_2,\cdots,E_j,F)$，对应的密文为：

$$C=(r_1g,r_2g,r_2H_1(\text{ID}_{Si}),r_2\text{PK}_{Si},H_3(w_1,\text{ID}_{Si}),\cdots,H_3(w_j,\text{ID}_{Si}),H_4(e(r_1H_1(\text{ID}_{Si})+r_2H_2(\text{ID}_C),P_{\text{pub}}))) \tag{3}$$

（4）Trapdoor：利用子服务器的身份信息，用户选择相应的关键词查询格式 $Q=\langle I_1,\cdots,I_m,w_{I_1}',\cdots,w_{I_m}'\rangle$，$(m\leqslant i)$，$I_j$ 是 w_{I_j}' 位置上的索引。用户利用其私钥 SK_{ID_C}，选择随机数 $t\in Z_p^*$，计算 $T=(T_1,T_2,T_3,I_1,\cdots,I_m)$，对应的关键词陷门为：

$$T=(t\text{PK}_{Si},H_4(e(tH_1(\text{ID}_{Si}),P_{\text{pub}})),\text{SK}_{\text{ID}_C}+\sum_{l=1}^{m}H_3(w_l,\text{ID}_{Si})+tT_2H_1(\text{ID}_{Si}),I_1,\cdots,I_m) \tag{4}$$

用户将 $(T_1,T_3,I_1,\cdots,I_m)$ 发送至云端服务器 S，T_2 保留。

（5）Test：根据发送者发送的密文 $C=(A,B,C,D,E_1,E_2,\cdots,E_j,F)$ 以及输入的 $(T_1,T_3,I_1,\cdots,I_m)$，云端服务器将搜索任务同步发送至授权子服务器中，给出等式：

$$f=H_4(e(\text{SK}_{\text{ID}_{Si}},A)e(T_3,B)(\prod_{l=1}^{m}e(E_l,x_i^{-1}D))^{-1}e(C,x_i^{-1}T_1)^{-T_2}) \tag{5}$$

子服务器再判断等式 $f=F$ 是否成立：若等式成立，则关键词密文中包含陷门搜索关键字集合信息，即 $\{w_{I_1}',\cdots,w_{I_m}'\}\in W=\{w_1,w_2,\cdots,w_i\}$，子服务器就将搜索到的密文文档返回给服务器，服务器进行综合处理后将最终结果返回给用户。

5 方案分析

5.1 正确性分析

本节进行方案的正确性分析，利用双线性映射的性质对 Test 等式分析，易得：

$$\begin{aligned}
&f=H_4(e(\text{SK}_{\text{ID}_{Si}},A)e(T_3,B)(\prod_{l=1}^{m}e(E_l,x_i^{-1}D))^{-1}\\
&e(C,x_i^{-1}T_1)^{-T_2})=H_4(e(sH_1(\text{ID}_{Si}),r_1g)e(sH_2(\text{ID}_C)+\\
&\sum_{l=1}^{m}H_3(w_l,\text{ID}_{Si})+tT_2H_1(\text{ID}_{Si}),r_2g)e(\sum_{l=1}^{m}H_3(w_l,\text{ID}_{Si}),\\
&x_i^{-1}r_2x_ig)^{-1}e(r_2H_1(\text{ID}_{Si}),x_i^{-1}tx_ig)^{-T_2})=H_4(e(r_1H_1(\text{ID}_{Si})+\\
&r_2H_2(\text{ID}_C),P_{\text{pub}})e(\sum_{l=1}^{m}H_3(w_l,\text{ID}_{Si}),r_2g)e(tT_2H_1(\text{ID}_{Si}),r_2g)\\
&e(\sum_{l=1}^{m}H_3(w_l,\text{ID}_{Si}),r_2g)^{-1}e(r_2H_1(\text{ID}_{Si}),tg)^{-T_2})=\\
&H_4(e(r_1H_1(\text{ID}_{Si})+r_2H_2(\text{ID}_C),P_{\text{pub}})e(\sum_{l=1}^{m}H_3(w_l,\text{ID}_{Si}),r_2g)\\
&e(\sum_{l=1}^{m}H_3(w_l,\text{ID}_{Si}),r_2g)^{-1}e(tT_2H_1(\text{ID}_{Si}),r_2g)\\
&e(r_2H_1(\text{ID}_{Si}),tg)^{-T_2})=H_4(e(r_1H_1(\text{ID}_{Si})+r_2H_2(\text{ID}_C),P_{\text{pub}}))
\end{aligned} \tag{6}$$

可见等式 $f=F=H_4(e(\text{SK}_{\text{ID}_{Si}},A)e(T_3,B)(\prod_{l=1}^{m}e(E_l,x_i^{-1}D))^{-1}e(C,x_i^{-1}T_1)^{-T_2})$，所以等式 $f=F$ 成立。

5.2　安全性分析

定理 1　假设 BDH 问题是困难的，在 RO 模型下 MS-CK-SE 方案满足选择消息攻击下密文的不可区分性。在 RO 模型下证明了两个引理。在引理 1 中，假设对手 A_0 是任意恶意子服务器。在引理 2 中，对手 A_1 被视为用户。

引理 1　假设 BDH 问题是困难的，对于敌手 A_0，在 RO 模型下本文提出的方案满足密文的不可区分性。

证明　假设 $\mathrm{Adv}_{A_0}^{\mathrm{Game}_0}(\xi)$ 是不可忽略的，这时挑战者 C_0 获得 BDH 四元组 (g, ag, bg, cg)，其中 $a,b,c \in Z_p^*$。C_0 与敌手 A_0 按照 Game_0 所定义的方式进行，然后输出 $e(g,g)^{abc}$。

（1）Setup：C_0 运行初始化算法生成系统公共参数 params，令 $P_{\mathrm{pub}} = ag$，选择随机数 $v \in Z_p^*$，生成私钥 $\mathrm{SK}_{A_0} = vP_{\mathrm{pub}}$，再随机选择随机数 $z \in Z_p^*$ 作为 A_0 的私钥，生成对应子服务器公钥 $\mathrm{PK}_{A_0} = zP_{\mathrm{pub}}$，挑战者 C_0 发送 SK_{A_0}、PK_{A_0} 给 A_0。

在 RO 模型下，挑战者 C_0 按照下列方式控制敌手 A_0 对 $\{H_1, H_2, H_3, H_4\}$ 这 4 个杂凑函数进行询问，且此时 $\{H_1, H_2, H_3, H_4\}$ 为预言机。

1）H_1-query：在任何时候，A_0 可以随机查询预言机 H_1。为了响应查询，此预言机维护一个初始为空的列表 L_{H_1} 和三元组 $(\mathrm{ID}_{Sj}, g_{\mathrm{ID}_{Sj}}, u_j)$，当敌手 A_0 为云服务器进行 H_1 询问时，挑战者 C_0 的回应如下：

当 ID_{Sj} 存在 L_{H_1} 中时，C_0 回应 $H_1(\mathrm{ID}_{Sj}) = g_{\mathrm{ID}_{Sj}}$；

当 ID_{Sj} 不存在 L_{H_1} 中时，C_0 选择随机数 $u_j \in Z_p^*$ 并计算 $g_{ID_{Sj}} = H_1(\mathrm{ID}_{Sj}) = u_j g$，$C_0$ 将三元组 $(\mathrm{ID}_{Sj}, g_{\mathrm{ID}_{Sj}}, u_j)$ 存于 L_{H_1} 中同时返回 $g_{\mathrm{ID}_{Sj}}$ 给敌手。

2）H_2-query：在任何时候，A_0 可以随机查询预言机 H_2。为了响应查询，此预言机维护一个初始为空的列表 L_{H_2} 和四元组 $(\mathrm{ID}_{Cj}, g_{\mathrm{ID}_{Cj}}, v_j, \mathrm{coin})$，当 A_0 为用户进行 H_2 询问时，挑战者 C_0 的回应如下：

当 ID_{Cj} 存在 L_{H_2} 中时，C_0 回应 $g_{\mathrm{ID}_{Cj}} = H_1(\mathrm{ID}_{Cj})$；

当 ID_{Cj} 不存在 L_{H_2} 中时，如果 C_0 满足对任意的 $\delta > 0$，有依概率分布 $\Pr(\mathrm{coin} = 0) = \delta$ 产生 $\mathrm{coin} \in \{0,1\}$。当 $\mathrm{coin} = 0$，挑战者选择随机数 $v_j \in Z_p^*$ 并计算 $g_{\mathrm{ID}_{Cj}} = H_2(\mathrm{ID}_{Cj}) = v_j g$；当 $\mathrm{coin} = 1$，$g_{\mathrm{ID}_{Cj}} = H_2(\mathrm{ID}_{Cj}) = bg$，最终 C_0 将四元组 $(\mathrm{ID}_{Cj}, g_{\mathrm{ID}_{Cj}}, v_j, \mathrm{coin})$ 存于 L_{H_2} 中同时返回 $g_{\mathrm{ID}_{Cj}}$ 给敌手。

3）H_3-query：在任何时候，A_0 可以随机查询预言机 H_3。为了响应查询，此预言机维护一个初始为空的列表 L_{H_3} 和四元组 $(\mathrm{ID}_{Sj}, D_j, C_{D_j}, x_{j_m})$，当敌手 A_0 对 $(\mathrm{ID}_{Sj}, D_j), D_j = \{w_{j_1}, \cdots, w_{j_i}\}$ 进行 H_3 询问时，挑战者 C_0 的回应如下：

当 (ID_{Sj}, D_j) 存在 L_{H_3} 中时，挑战者回应 $C_{Dj} = \{H_3(w_{j_1}, \mathrm{ID}_{Sj}), \cdots, H_3(w_{j_m}, \mathrm{ID}_{Sj})\}$；

当 (ID_{Sj}, D_j) 不存在 L_{H_3} 中时，挑战者选择随机数 $x_{j_m} \in Z_p^*$ 并计算 $C_{Dj} = \{x_{j_1} g, \cdots, x_{j_m} g\}$，最终 C_0 将四元组 $(\mathrm{ID}_{Sj}, D_j, C_{D_j}, x_{j_m})$ 存于 L_{H_3} 中同时返回 $(4j+1)(h+x) + qj$ 给敌手。

4）$3h + 3x$-query：在任何时候，A_0 可以随机查询预言机 H_4。为了响应查询，此预言机维护一个初始为空的列表 L_{H_4} 和二元组 (m_j, n_j)，当 A_0 对 $m_j \in G_2$ 进行 H_4 询问时，挑战者 C_0 的回应如下：

当 m_j 存在 L_{H_4} 中时，挑战者回应 $H_4(m_j) = n_j$；

当 m_j 不存在 L_{H_4} 中时，挑战者选择随机数 $n_j \in Z_p^*$ 并令 $H_4(m_j) = n_j$，最终 C_0 将二元组 (m_j, n_j) 存于 L_{H_4} 中同时返回 n_j 给敌手。

（2）Phase1：敌手 A_0 可以以一种自适应的方式对挑战者 C_0 进行以下查询：

1）对数据接收者的密钥产生询问：A_0 向 C_0 对授权用户的身份信息 ID_{Cj} 进行询问，C_0 对存于 L_{H_2} 的四元组 $(\mathrm{ID}_{Cj}, g_{\mathrm{ID}_{Cj}}, v_j, \mathrm{coin})$ 进行查询，如果 $\mathrm{coin} = 1$，挑战者输出失败并终止游戏；如果 $\mathrm{coin} = 0$，挑战者计算 $\mathrm{SK}_{Cj} = v_j P_{\mathrm{pub}}$，同时返回 SK_{Cj} 给敌手。

2）对陷门产生询问：当 A_0 向 C_0 请求

$(\mathrm{ID}_{Sj},\mathrm{ID}_{Cj},D_j)$ 的陷门询问时，C_0 选择随机数 $y_j \in Z_p^*$，并分别在列表 L_{H_2}、L_{H_3}、L_{H_4} 中找回 $(\mathrm{ID}_{Cj},g_{\mathrm{ID}_{Cj}},v_j,\mathrm{coin})$、$(\mathrm{ID}_{Sj},D_j,C_{D_j},x_j)$ 与 (m_j,n_j)，其中 $m_j = e(H_1(\mathrm{ID}_{Sj},D_j),y_jP_{\mathrm{pub}})$。挑战者 C_0 计算：

$$T_1 = y_j g$$
$$T_2 = n_j$$

$$T_3 = \mathrm{SK}_{\mathrm{ID}_{Cj}} + \sum_{i=1}^{m} H_3(w_{j_i},\mathrm{ID}_{Sj}) + y_j T_2 H_1(\mathrm{ID}_{Sj}) = v_j P_{\mathrm{pub}} + \sum_{i=1}^{m} x_{j_i} g + y_j n_j u_j g \quad (7)$$

挑战者 C_0 将 $(T_1,T_3,I_{w_{i_1}},\cdots,I_{w_{i_m}})$ 发送给敌手 A_0。

（3）Challenge：敌手 A_0 向挑战者 C_0 发送四元组 $(\mathrm{ID}_{A_0},\mathrm{ID}_{Ci}^*,D_0,D_1)$。 C_0 随机选择值 $b \in \{0,1\}$，要求是 A_0 没有对 ID_{Ci}^* 进行过密钥查询。C_0 随机选择 $c_1,R \in Z_p^*$，在 L_{H_4} 中生成密文：

$$C^* = (A^*,B^*,C,D_1^*,\cdots,D_m^*,E_4^*) = (c_1 g, cg, cH_1(\mathrm{ID}_{Sj}), cH_3(w_{j_1},\mathrm{ID}_{Sj}),\cdots,cH_3(w_{j_m},\mathrm{ID}_{Sj}),R) \quad (8)$$

（4）Phase2：服务器 A_0 可以向挑战者 C_0 自适应对身份 ID_{Ci} 进行密钥查询，并且对任意查询格式 Q_i 进行陷门查询，要求 $\mathrm{ID}_{Ci} \neq \mathrm{ID}_{Ci}^*$ 且 Q_i 不包括 D_0、D_1 的任意查询格式。

（5）Guess：敌手 A_0 输出对 b 的猜测 b'，其中 $b' \in \{0,1\}$。

假设存在敌手 A_0 能以不可忽略的概率优势对本方案的密文 C^* 进行区分，挑战者 C_0 在列表 L_{H_3} 中找回相应的四元组（$\mathrm{ID}_{A_0}, D_b^*, C_{Db}^*, x^*$），同时在列表 L_{H_4} 中挑选出 (m^*,n^*)，可以计算出：

$$\begin{aligned} & m^* / (uP_{\mathrm{pub}}, c_1 g) = e(\mathrm{SK}_{\mathrm{ID}_{A_0}}, A^*) e(T_3^*, B^*) \\ & (\prod_{l=1}^{m} e(E_l{}^*, z_i^{-1} D^*))^{-1} e(C^*, x_i^{-1} T_1^*)^{-n^*} / (uP_{\mathrm{pub}}, c_1 g) \\ & = e(\mathrm{SK}_{\mathrm{ID}_{A_0}}, cg) e(\mathrm{SK}_{\mathrm{ID}_C}{}^*, c_1 g) / (uP_{\mathrm{pub}}, c_1 g) \\ & = e(\mathrm{SK}_{\mathrm{ID}_C}{}^*, cg) = e(bP_{\mathrm{pub}}, cg) \\ & = e(bag, cg) = e(g,g)^{abc} \end{aligned} \quad (9)$$

所以挑战者 C_0 输出的 $m^* / (uP_{\mathrm{pub}}, c_1 g)$ 是作为 BDH 问题假设的解，这与之矛盾。

引理 2 假设 BDH 问题是困难的，对于敌手 A_1，在 RO 模型下本文提出的方案满足了密文的不可区分性。

证明 假设 $\mathrm{Adv}_{A_1}^{\mathrm{Game}_1}(\xi)$ 是不可忽略的，这时挑战者 C_1 获得 (g,ag,bg,cg)，其中 $a,b,c \in Z_p{}^*$。挑战者 C_1 与敌手 A_1 按照 Game_1 所定义的方式进行，然后输出 $e(g,g)^{abc}$。

（1）Setup：按照引理 2 的初始化，选择随机数 $v \in Z_p{}^*, z_j \in Z_p{}^*$，生成 A_1 的私钥 $\mathrm{SK}_{A_1} = vP_{\mathrm{pub}}$ 以及服务器的公钥 $\mathrm{PK}_{Sj} = z_j g$，这里 $P_{\mathrm{pub}} = ag$。

在 RO 模型下，C_1 按照下列方式控制 A_1，并对 $\{H_1,H_2,H_3,H_4\}$ 这 4 个杂凑函数进行询问。

1）H_1-query：在任何时候，A_1 可以随机查询预言机 H_1。为了响应查询，此预言机维护一个初始为空的列表 L_{H_1}，当 A_1 为云服务器进行 H_1 询问时，C_1 的回应如下：

当 ID_{Sj} 存在 L_{H_1} 中时，挑战者回应 $H_1(\mathrm{ID}_{Sj}) = g_{\mathrm{ID}_{Sj}}$；

当 ID_{Sj} 不存在 L_{H_1} 中时，如果 C_1 满足对任意的 $\delta > 0$，有依概率分布 $\Pr(\mathrm{coin}=0) = \delta$ 产生 $\mathrm{coin} \in \{0,1\}$。当 $\mathrm{coin}=0$ 时，挑战者随机选择 $u_j \in Z_p^*$ 并计算 $g_{\mathrm{ID}_{Sj}} = H_1(\mathrm{ID}_{Sj}) = u_j g$；当 $\mathrm{coin}=1$ 时，$g_{\mathrm{ID}_{Sj}} = bg$，最终 C_1 将四元组 $(\mathrm{ID}_{Sj}, g_{\mathrm{ID}_{Sj}}, u_j, \mathrm{coin})$ 存于 L_{H_1} 中同时返回 $g_{\mathrm{ID}_{Sj}}$ 给 A_1。

2）H_2-query：在任何时候，服务器 A_1 可以随机查询预言机 H_2。为了响应查询，此预言机维护一个初始为空的列表 L_{H_2}，当敌手 A_1 为用户进行 H_2 询问时，C_1 选择随机数 $v_j \in Z_p^*$ 并计算 $\mathrm{SK}_{\mathrm{ID}_{Cj}} = v_j g$，$C_1$ 将三元组 $(\mathrm{ID}_{Cj}, \mathrm{SK}_{\mathrm{ID}_{Cj}}, v_j)$ 存于 L_{H_2} 中同时返回 $\mathrm{SK}_{\mathrm{ID}_{Cj}}$ 给敌手。

3）H_3-query：在任何时候，A_1 可以随机查询预言机 H_3。为了响应查询，此预言机维护一个初始为空的列表 L_{H_3} 和四元组 $(\mathrm{ID}_{Sj},D_j,C_{D_j},x_{j_m})$，当敌手 A_1 对 $(\mathrm{ID}_{Sj},D_j), D_j = \{w_{j_1},\cdots,w_{j_i}\}$ 进行 H_3 询问

时，挑战者C_1的回应如下：

当(ID_{Sj},D_j)存在L_{H_3}中时，挑战者回应$C_{Dj}=\{H_3(\mathrm{ID}_{Sj},w_{j_1}),\cdots,H_3(\mathrm{ID}_{Sj},w_{j_m})\}$；

当(ID_{Sj},D_j)不存在L_{H_3}中时，挑战者选择随机数$x_{j_m}\in Z_p^*$并计算$C_{Dj}=\{x_{j_1}g,\cdots,x_{j_m}g\}$，最终$C_1$将四元组$(\mathrm{ID}_{Sj},D_j,C_{D_j},x_{j_m})$存于$L_{H_3}$中同时返回$C_{D_j}$给敌手。

4）H_4-query：在任何时候，A_1可以随机查询预言机H_4。为了响应查询，此预言机维护一个初始为空的列表L_{H_4}和二元组(m_j,n_j)，当A_0对$m_j\in G_2$进行H_4询问时，挑战者C_1的回应如下：

当m_j存在L_{H_4}中时，挑战者回应$H_4(m_j)=n_j$；

当m_j不存在L_{H_4}中时，挑战者选择随机数$n_j\in Z_p^*$并令$H_4(m_j)=n_j$，最终C_1将二元组(m_j,n_j)存于L_{H_4}中同时返回n_j给敌手。

（2）Phase1：敌手A_1可以以一种自适应的方式对挑战者C_1进行以下的查询：

1）对服务器的密钥产生询问：敌手A_1向挑战者C_1对服务器的身份信息ID_{S_j}进行询问，C_1对存于L_{H_1}的四元组$(\mathrm{ID}_{Sj},g_{\mathrm{ID}_{Sj}},u_j,\mathrm{coin})$进行查询，如果$\mathrm{coin}=1$，挑战者输出失败并终止游戏；如果$\mathrm{coin}=0$，挑战者计算$\mathrm{SK}_{\mathrm{ID}_{Sj}}=u_jP_{\mathrm{pub}}$同时返回$\mathrm{SK}_{\mathrm{ID}_{Sj}}$给$A_1$。

2）对数据接收者的密钥产生询问：敌手A_1向挑战者C_1对授权用户的身份信息ID_{Cj}进行询问，C_1对存于L_{H_2}的三元组$(\mathrm{ID}_{Cj},\mathrm{SK}_{\mathrm{ID}_{Cj}},v_j)$进行查询，同时返回$\mathrm{SK}_{\mathrm{ID}_{Cj}}=v_jP_{\mathrm{pub}}$给敌手。

3）对陷门产生询问：A_1可以自主随意地生成任何查询格式对应的陷门，挑战者C_1选择随机数$y_j\in Z_p^*$，然后挑战者C_1计算：

$$T_1=y_jg$$

$$T_2=n_j$$

$$T_3=\mathrm{SK}_{\mathrm{ID}_{Cj}}+\sum_{i=1}^{m}H_3(w_{j_i},\mathrm{ID}_{Sj})+y_jT_2H_1(\mathrm{ID}_{Sj})=\quad(10)$$

$$v_jP_{\mathrm{pub}}+\sum_{i=1}^{m}x_{j_i}g+y_jn_ju_jg$$

4）对测试产生询问：这时敌手A_1向挑战者C_1发送四元组$(\mathrm{ID}_{Sj},\mathrm{ID}_{Cj},C,T)$，其中$C$为关键词加密的密文。挑战者$C_1$分别查看列表$L_{H_1}$、$L_{H_2}$、$L_{H_3}$、$L_{H_4}$。

（3）Challenge：敌手A_1向挑战者C_1发送四元组$(\mathrm{ID}_{A_1},\mathrm{ID}_S{}^*,D_0,D_1)$。挑战者$C_1$随机选择值$b\in\{0,1\}$，要求是$A_1$没有就服务器的身份信息$\mathrm{ID}_S{}^*$进行过秘钥查询。挑战者$C_1$随机选择$c_2,R\in Z_p{}^*$，在$L_{H_4}$中生成密文：

$$C^*=(A^*,B^*,C,D_1^*,\cdots,D_m^*,E^*)=(cg,c_2g,c_2H_1(\mathrm{ID}_{Sj}),c_2H_3(\mathrm{ID}_{Sj},w_{j_1}),\cdots,c_2H_3(\mathrm{ID}_{Sj},w_{j_m}),R)\quad(11)$$

（4）Phase1：A_1可以向C_1自适应对身份ID_S进行密钥查询，并且对任意Q_i进行陷门查询，要求$\mathrm{ID}_S\neq\mathrm{ID}_S{}^*$且$Q_i$不包括任意$D_0,D_1$的查询格式。

（5）Guess：敌手A_1输出对b的猜测b'，其中$b'\in\{0,1\}$。

假设存在敌手A_1能以不可忽略的概率优势对本文方案的密文C^*进行区分，挑战者C_1在L_{H_3}中找回相应的四元组$(\mathrm{ID}_{A_0},D_b{}^*,C_{D_b}{}^*,x^*)$，同时在列表$L_{H_4}$中挑选出$(m^*,n^*)$，可以计算出：

$$m^*/(vP_{\mathrm{pub}},c_2g)=e(\mathrm{SK}_{\mathrm{ID}_A}{}^*,A^*)e(T_3^*,B^*)$$

$$(\prod_{l=1}^{m}e(E_l^*,z_i^{-1}D^*))^{-1}e(C^*,x_i^{-1}T_1^*)^{-n^*}/(vP_{\mathrm{pub}},c_2g)=$$

$$e(\mathrm{SK}_{\mathrm{ID}_A}{}^*,cg)e(\mathrm{SK}_C{}^*,c_2g)/(vP_{\mathrm{pub}},c_2g)=\quad(12)$$

$$e(\mathrm{SK}_{\mathrm{ID}_A}{}^*,cg)=e(bP_{\mathrm{pub}},cg)=$$

$$e(\mathrm{bag},cg)=e(g,g)^{abc}$$

所以C_1输出的$m^*/(vP_{\mathrm{pub}},c_2g)$是作为BDH问题假设的解，这与之矛盾。

结合引理1与引理2可得定理1。

5.3　性能分析

本节将密钥生成代价、加密代价与测试代价进行效率比较，主要选取参考文献[14]、参考文献[17]为代表进行效率分析，分析结果见表1；然后从是否支持连接关键字加密和搜索与选择关键词攻击下的密文不可区分性，以及是否支持基于身份

表 1 效率分析

对比项	密钥生成代价	密文生成代价	测试代价
WANG [14]	$2h+2x$	$q+(2j+2)(h+x)$	$(3+2m)(h+x)+(2+m)q$
ZHANG[17]	$3h+3x$	$3j(h+x)+2qj$	$(m+3)(h+x)+mq$
本文方案	$(i+1)(h+x)$	$(4j+1)(h+x)+qj$	$(6m+1)(h+x)+3mq$

加密方案与多服务器环境，选取参考文献[14-17]为代表进行性能分析，分析结果见表 2。

表 2 性能分析

对比项	连接关键词	IND-CPA	IBE	多服务器
WANG[14]	No	Yes	Yes	No
MOESFA [15]	No	No	No	Yes
HUANG [16]	No	No	No	Yes
ZHANG[17]	No	Yes	Yes	Yes
本文方案	Yes	Yes	Yes	Yes

在表 1 中 q 表示双线性映射操作指数，x 表示群的指数操作，h 表示 Hash 操作指数，d 表示对称加密操作指数，k 表示伪随机函数操作指数。j 表示用于加密的关键词个数，m 表示需要搜索的关键词个数。

在同时对 j 个关键词加密与对 m 个连接关键词搜索的情况下，虽然成本有所消耗，但利用多服务器，在多个服务器同时协作检索运行下，能够提高对一次性检索多个连接关键词的搜索效率。且与参考文献[14-17]所提方案相比，本文所提方案在性能上具有一定的优势，首先较参考文献[14]、参考文献[17]而言，利用多服务器解决对连接关键词的搜索问题。与参考文献[15]、参考文献[16]相比，本方案在基于身份的条件下消除了对证书的管理需求，同时实现对多关键词的加密与连接关键词的检索，且在双线性 Diffie-Hellman 困难问题假设下满足 IND-CPA 安全。

6 结束语

本文利用基于身份在证书管理方面的优势，结合多服务器搜索，实现了在云计算上对连接关键词的搜索。在性能比对阶段，该搜索具有较大优势。目前提出的方案仅支持连接关键字的搜索功能，下一阶段准备将方案扩展到支持“与”“或”“非”搜索的富于表达的关键字搜索功能。此外，一个不诚实的私钥生成中心会导致许多安全隐患，导致所构造的方案可能达不到 IND-CPA 安全的目的。在未来的研究工作中，将尝试改进这些问题，从而构造更具安全性与高效性的可搜索加密方案。

参考文献：

[1] 吴国威, 樊宁, 汪来富. 云环境下基于属性加密体制算法加速方案[J]. 电信科学, 2019, 35(11): 101-107.
WU G W, FAN N, WANG L F. Algorithm acceleration scheme based on attribute encryption system in cloud environment[J]. Telecommunication Science, 2019, 35(11):101-107.

[2] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]// 2000 IEEE Symposium on Security and Privacy, May 14-17, 2000, Berkeley, CA, USA. Piscataway: IEEE Press, 2000: 44-55.

[3] BONEH D , CRESCENZO G D , OSTROVSKY R , et al. Public key encryption with keyword search[C]// Advances in Cryptology - EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, May 2-6, 2004, Switzerland. Berlin: Springer-Verlag, 2004: 506-522.

[4] PARKD, KIM K, LEE P. Public key encryption with conjunctive field keyword search[C]// International Conference on Information Security Applications, Sep 27-29, Palo Alto, CA, USA. Berlin: Springer-Verlag, 2004: 73-86.

[5] HWANG Y H, LEE P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system[C]// Pairing-Based Cryptography - Pairing 2007, First International Conference, July 2-4, 2007, Tokyo, Japan. Berlin: Springer-Verlag, 2007: 2-22.

[6] DAN B, WWTERS B. Conjunctive, subset, and range queries on encrypted data[J]. Tcc, 2007, 4392: 535--554.

[7] 宋衍, 韩臻, 陈栋, 等. 支持关键词任意连接搜索的属性加密方案[J]. 通信学报, 2016, 37(8): 77-85.
SONG Y, HAN Z, CHEN D, et al. Attribute-based encryption supporting arbitrary conjunctive key word search[J]. Journal on Communications, 2016, 37(8):77-85.

[8] FAIROUZ S A, LU S F. Searchable encryption with conjunctive field free keyword search scheme[C]//2016 International Conference on Network and Information Systems for Computers (ICNISC), April 15-17, 2016. Wuhan, China. Piscataway: IEEE Press, 2016: 260-264.

[9] LU Y, WANG G, LI J G, et al. Efficient designated server identity-based encryption with conjunctive keyword search[J]. Annals of Telecommunications, 2017, 72(5-6): 359-370.

[10] BYUN J W, RHEE H S, PARK H A, et al. Off-Line keyword guessing attacks on recent keyword search schemes over encrypted data[C]// Secure Data Management, Third VLDB Workshop, SDM 2006, September 10-11, 2006, Seoul, Korea. [S.l.: s.n.], 2006: 75-83.

[11] BAEK J, SAFAVI-NAINI R, SUSILO W. Public key encryption with keyword search revisited[C]// Computational Science and Its Applications-ICCSA 2008, International Conference, June 30-July 3, 2008, Perugia, Italy. Berlin: Springer-Verlag, 2008: 1249-1259.

[12] SHAMIR A. Identity-based cryptosystems and signature schemes[C]// Workshop on the Theory and Application of Cryptographic Techniques, April 9-11, 1984, Paris. France. Heidelberg Springer, 1984: 47-53.

[13] BONEH D, FRANKLIN M. Identity-based encryption from the weil pairing[C]// The 21st Annual International Cryptology Conference on Advances in Cryptology, Aug 19-23, 2001, Santa Barbara, California, USA. Heidelberg Springer, 2001: 213-229.

[14] WU T Y , TSAI T T, TSENG Y M. Efficient searchable ID-based encryption with a designated server[J]. Annals of Telecommunications-Annales Des Télécommunications, 2013, 69(7-8): 391-402.

[15] 王少辉, 韩志杰, 肖甫, 等. 指定测试者的基于身份可搜索加密方案[J]. 通信学报, 2014, 35(7): 22-32.
WANG S H, HAN Z J, XIAO P, et al. Identity-based searchable encryption scheme with a designated tester[J]. Journal on Communications, 2014, 35(7):22-32.

[16] MOHAMAD M S, CHIN J J, POH G S . On the security advantages of block-based multiserver searchable symmetric encryption[C]//2016 14th Annual Conference on Privacy, Security and Trust (PST), Dec 12-14, 2016, Auckland, New Zealand. Piscataway: IEEE Press, 2016: 349-352.

[17] HUANG H P, DU J P , DAI H, et al. Multi-sever multi-keyword searchable encryption scheme based on cloud storage[J]. Journal of Electronics & Information Technology, 2017, 39(2): 389-396.

[18] 张玉磊, 刘祥震, 郎晓丽, 等. 云环境下基于无证书的多服务器可搜索加密方案[J]. 信息网络安全, 2019, 219(3): 78-86.
ZHANG Y L, LIU X Z, LANG X L, et al. Certificateless multi-server searchable encryption scheme in cloud environment[J]. Information Network Security, 2019, 219(3):78-86.

[19] GUO F C, SUSILO W, MU Y. Introduction to security reduction ‖ Identity-based encryption with random oracles[J]. 2018. doi: 10.1007/978-3-319-93049-7(Chapter 9): 215-227.

[作者简介]

卢艳华（1994− ），女，贵州大学数学与统计学院硕士生，主要研究方向为可搜索加密。

田有亮（1985− ），男，博士，贵州大学计算机科学与技术学院教授、博士生导师，主要研究方向为算法博弈论、密码与安全协议、大数据安全和隐私保护、区块链和电子货币等。

刘成（1994− ），女，贵州大学计算机科学与技术学院硕士生，主要研究方向为隐私保护。