可搜索加密研究进展综述

李颖，马春光
（哈尔滨工程大学计算机科学与技术学院，黑龙江 哈尔滨 150000）

摘　要：随着云计算的迅速发展，为保护用户外包数据的安全和用户隐私，越来越多的企业和用户选择将数据加密后上传。因此，对云服务器上加密数据的有效搜索成为用户关注的重点。可搜索加密技术是允许用户对密文数据进行检索的密码原语，利用云服务器的强大计算资源进行关键词检索。根据使用密码体制的不同，介绍了可搜索加密的分类，将其分为对称可搜索加密和非对称可搜索加密。基于这种分类，首先介绍了典型方案，之后从可搜索加密的语句表达能力和安全性 2 方面进行介绍，并指出了该领域当前研究中急需解决的问题及未来研究方向。

关键词：云计算；可搜索加密；对称可搜索加密；非对称可搜索加密
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.2096-109x.2018062

Overview of searchable encryption research

LI Ying，MA Chunguang
School of Computer Science and Technology, Harbin Engineering University, Harbin 150000, China

Abstract: With the development of cloud computing, there is an increasing number of companies and individuals outsourcing their data to cloud server in the encrypted form to protect data security and user privacy. As a result, efficient retrieval of encrypted data stored on cloud server has become the issue that users may pay attention to. Searchable encryption (SE) is a cryptographic primitive that supports keyword search over encrypted data, and migrates the cumbersome search operation to the cloud server to utilize its vast computational resources. Reviews previous research according to the different cryptosystems used, and divides SE into two groups, that is symmetric searchable encryption and asymmetric searchable encryption. Based on this classification, first introduces a typical program, and then introduces from the two aspects of the expression of searchable encryption and security.Finally, the need-to-be-solved problems and main research directions are discussed.

Key words: cloud computing, searchable encryption, symmetric searchable encryption, asymmetric searchable encryption

1　引言

近年来，随着网络的快速发展，大数据时代已然到来，由于人们日常产生的数据越来越多，云存储技术也随之兴起，如亚马逊简易存储服务以及国内的百度云盘等。但是，随着该技术的发展，人们发现，当把数据外包到云服务器时，用户也就无法对数据进行控制，使用户的隐私安全

收稿日期：2018-06-10；修回日期：2018-07-05
通信作者：李颖，2472796566@qq.com
基金项目：国家自然科学基金资助项目（No.61472097）
Foundation Item: The National Natural Science Foundation of China(No.61472097)

面临巨大的挑战。普遍的解决办法是数据加密后上传，但是又会遇到如何在密文上进行查询的难题，最简单的方法是将文件下载解密后查询。这种操作由于下载了不需要的文件而浪费了大量网络开销，且进行解密和查询也浪费了大量计算开销，这种方法并不适用。由于云服务器具有强大的计算能力，人们希望由服务器进行检索功能，可以把密钥发送给云服务器，之后由服务器解密并查询，但云服务器通常是“诚实且半可信”的，用户的隐私暴露在云服务器面前，仍然有泄露的风险。

为了解决这类问题，可搜索加密（SE，searchable encryption）技术应运而生。本文对可搜索加密的基本概念进行研究[1]，关注近年来可搜索加密的研究进展，针对现有方法进行分类并对可搜索加密的未来发展进行展望。

2 基本概念

2000 年，Song 等[1]首次提出了可搜索加密的概念。作为一种新型的密码原语，可搜索加密技术使用户具有在密文域上进行关键词搜索的能力。数据以密文方式存储在云服务器上时，利用云服务器的强大计算能力进行关键词的检索，而不会向服务器泄露任何用户的隐私。这不仅仅使用户的隐私得到了有效保护，而且检索效率也在服务器的帮助下得到了大幅度提升。

可搜索加密技术的一般过程如图 1 所示，主要分为 4 步。

1) 文件加密：数据拥有者在本地使用加密密钥对将要上传的文件进行加密，并将密文上传服务器。

2) 陷门生成：经过数据拥有者授权的数据使用者使用密钥对待查询的关键词生成陷门，发送给云服务器。

3) 查询检索：云服务器对数据使用者提交的陷门和每个上传文件的索引表进行检索，返回包含陷门关键词的密文文件。

4) 文件解密：数据使用者使用解密密钥对云服务器返回的密文文件进行解密。

可搜索加密主要包含对称可搜索加密（SSE，symmetric searchable encryption）和非对称可搜索加密（ASE，asymmetric searchable encryption）2 种类型，这 2 种类型来源于不同的现实问题，之后用来解决不同的需求问题。下面对这 2 类可搜索加密进行详细讲解。

3 对称可搜索加密

3.1 定义

对于可搜索加密技术的来源，要追溯到不可信赖的服务器存储问题[2]，即假设用户 Alice 希望将文件上传至云服务器，但是面临着数据泄露的风险，为了保护用户的个人隐私，可以选择将文件加密后上传。采用传统的加密算法，当 Alice 需要查询云服务器上的某个文件时，需要将所有文件全部下载，解密后检索，因为只有用户 Alice 自己拥有解密的能力，而在密文上是无法进行检索的。此类问题就需要新型的加密方案：加密后的文件可以执行检索功能，并在这个过程中不会泄露有关数据的任何明文信息。

定义 1 （对称可搜索加密）[3]定义在字典 $\Delta=\{W_1,W_2,\cdots,W_d\}$ 上的对称可搜索加密算法可描述为五元组。

$SSE=(KeyGen,Encrypt,Trapdoor,Search,Decrypt)$

其中

1) $K=KeyGen(\lambda)$：λ 是安全参数，该算法根据安全参数生成加密密钥 K。

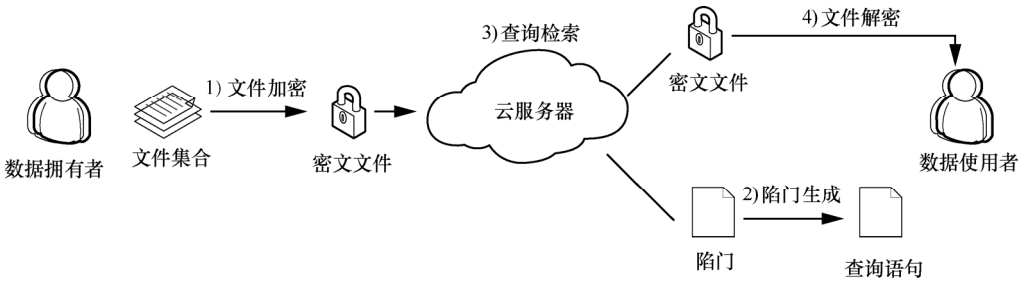

图 1 可搜索加密过程

2) $(I,C)=Encrypt(K,D)$：D 是明文文件集合，$D=(D_1,D_2,\cdots,D_n)$, $D_i\in 2^{\Delta}$，该算法生成文件索引 I 密文文件集 $C=(C_1,C_2,\cdots,C_n)$，部分方案不需要生成索引。

3) $T_W=Trapdoor(K,W)$：其中，W 是用户输入需要查询的关键词，该算法生成关键词 W 对应的陷门 T_W。

4) $D(W)=Search(I,T_W)$：该算法根据用户输入生成的陷门 T_W 以及文件的索引 I 进行查找，输出与输入关键词匹配的文件集合 $D(W)$。

5) $D_i=Decrypt(K,C_i)$：用生成的密钥 K 解密返回的密文文件 C_i，生成明文文件 D_i。

如果对称可搜索加密方案 SSE 是正确的，那么对于 $\forall\lambda\in N$，$n\in Z$，$W\in\Delta$，$D=(D_1,D_2,\cdots,D_n)$ 以及 $KeyGen(\lambda)$和 $Encrypt(K,D)$输出的 K 和(I,C)，都有 $Search(I,Trapdoor(K,W))=D(W)$和 $Decrypt(K,C_i)=D_i$ 成立。

对称可搜索加密通常对关键词首先进行处理，大多数采用伪随机函数或者散列算法等方法，模糊关键词语义进行随机化的处理。当用户进行关键词检索时，将查询关键词进行相同处理，与文件的关键词进行相似度匹配，结果满足某种格式，则说明匹配成功，返回相应的文件。

3.2　SWP 方案

2000 年，Song 等[2]第一次提出了在密文上进行搜索的方案 SWP，具体方法如图 2 所示。

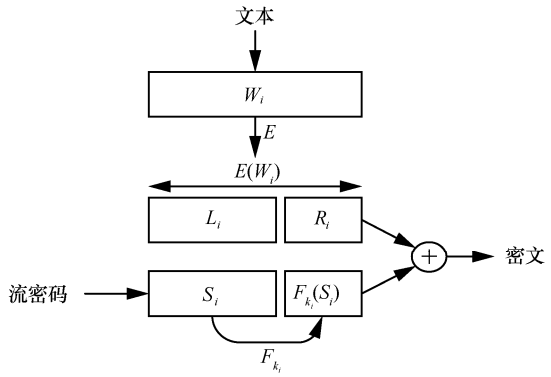

图 2　SWP 可搜索加密机制

具体构造如下。

1) $KeyGen()$：数据拥有者生成加密密钥 k'和 k''以及伪随机流 $S_1,S_2,\cdots,S_n$（n 为文件中的单词块数目）。

2) $Encrypt()$：将文件分为长度固定的单词块 W_i，计算 $X_i=E_{k''}(W_i)=(L_i,R_i)$，$k_i=f_{k'}(L_i)$，$T_i=(S_i,F_{k_i}(S_i))$和 $C_i=X_i\oplus T_i$，其中，E 是分组加密算法，F 和 f 是伪随机函数。

3) $Trapdoor()$：对于用户输入的关键词 W，计算 $X=E_{k''}(W)=(L,R)$和 $k=f_{k'}(L)$，将（X，k）发送服务器。

4) $Search()$：服务器进行如下计算

$$T_p=C_p\oplus X=(S_p,S_p')=$$

$$\{(S_p,S_p')=\begin{cases}(S_p,F_k(S_p))\\ \text{null}\end{cases}$$

如果$(S_p'=F_k(S_p))$，返回（p, C_p）。

5) $Decrypt()$：用户收到 C_p 后，根据自己的密钥解密，具体计算如下：$C_p=(C_{p,l},C_{p,r})$，$X_{p,l}=C_{p,l}\oplus S_p$，$K_p=f_{k'}(X_{p,l})$，$T_p=(S_p,F_k(S_p))$以及 $X_p=C_p\oplus T_p$ 和 $W_p=D_{k''}(X_p)$。其中，D 是分组密码解密算法。

虽然该算法可以使服务器不能获得任何明文信息，但是由于需要扫描全文，使算法效率较低，并且该算法容易收到统计攻击的威胁。

3.3　对称可搜索加密语句的表达能力

对于可搜索加密，用户希望在查询时可以快速而准确地找到所需的文件，而且能够清晰准确地描述用户的搜索条件，这就需要可搜索加密在语句表达能力方面进行深入研究。近几年，搜索语句表达能力方面的研究主要分为单关键词搜索、多关键词搜索、连接关键词搜索和模糊关键词搜索。

在可搜索加密提出时，单关键词检索也随之提出。2000 年，Song 等[2]提出了 SWP 方案，但是他们并没有进行安全性的定义，2006 年，Curtmola 等[4]则给出了安全性的定义，并给出了 2 个 SSE 方案（SSE-1 和 SSE-2）。2010 年，Wang 等[5]提出了一个排序对称可搜索加密的定义，并给出了一个基于现有密码原语对称密钥保序加密技术的有效设计。2012 年，Premasathian[6]提出了使用乘法和同时同余的快速搜索加密方案。在这些方案中，任何用户都可以确定加密文档中是否存在特定关键字。该消息可以通过任何技术加密。在某些方案中可以确定关键字

的出现次数。

单关键词检索虽然可以快速检索，但是准确度不高，不能精确定位文件，多关键词检索随之提出。2013 年，Premasathian[7]首次提出了多关键词检索方案，该方案利用连接与门将关键词进行连接，并且该方案对用户数据和搜索令牌进行隐藏，保证了安全性。2014 年，Fu 等[8]提出了一种智能语义搜索方案，该方案不仅返回基于关键字的精确匹配的结果，而且还返回基于关键字的语义匹配的结果。同时，该方案支持搜索结果的可验证性。2014 年，Fu 等[9]又提出了一种有效的解决加密云数据支持同义词查询的多关键词排序搜索问题。2016 年，Xia 等[10]提出了一个可以动态进行文件的增删改查的多关键词检索方案。2017 年，杨旸等[11]首次在可搜索加密技术中引入加权平均分的概念，对文件中不同区域的关键词设置不同的权重表示重要程度，针对 MRSE（multi-keyword ranked search over encrypted cloud data）方案的不足，提出了更加高效的多关键词排序检索方案。

起初对于可搜索加密技术的研究，并未考虑关键词之间布尔组合的情况，这也成为之后阻碍可搜索加密技术发展的一大难题。2013 年，Cash 等[12]介绍了第一个可搜索的对称加密（SSE）协议的设计和分析，该协议支持外包对称加密数据的联合搜索和一般布尔查询，并可扩展到超大型数据库和任意结构化数据，包括自由文本搜索。2016 年，Li 等[13-18]实现了“AND、OR、NOT”等布尔运算的关键字可搜索加密方案。

以上对于关键词检索的研究全部是基于精确查询的条件，但当用户输入的关键词与文件的关键词存在误差时，便不能准确查找，降低了搜索准确度。模糊关键词检索则有效地解决了这个问题。2009 年，Bringer 等[19]描述了一个用于容错可搜索加密的新原语及其安全模型。这种通用的方案只允许使用某个关键字的近似值对加密数据进行搜索。它能够有效地查询安全数据库，以便通过对其进行精确估计来获取确切的数据。2010 年，Li 等[20]利用编辑距离来量化关键字相似度并开发构建模糊关键字集的高级技术，这大大减少了存储和表示的开销。2011 年，Chuah 等[21]提出了一种基于隐私感知的基于树的方法来支持模糊多关键字特征。2017 年，杨旸等[22]提出了基于双因子排序算法的关键词模糊搜索方案，以汉明距离和相似度分数为依据。2017 年，王恺璇等[23]采用敏感散列函数对关键词建立索引，并采用布隆过滤器，实现了多关键词的模糊检索。

3.4 对称可搜索加密的安全性

在进行可搜索加密方案的研究时，除了要考虑方案的准确性和效率，还要考虑方案是否安全，为了证明方案的安全性，通常是采用与攻击模型结合的方法证明。

2000 年 Song 等[2]首次提出可搜索加密时只是要求检索时不会泄露明文信息，但是文章给出的定义不能抵抗攻击者的简单攻击。2003 年，Goh 等[24]正式定义了一个安全索引并为针对自适应选择关键字攻击（IND-CKA, semantic security against adaptive chose keyword attack）的称为语义安全性的索引制定了安全模型。但是由于方案中使用了布隆过滤器，使查询结果并不准确。2004 年，Chang 等[25]描述了可搜索加密技术的基于模拟的安全性定义，考虑了攻击者可以多次试探服务器的情况，限制了服务器无法获得除查询结果之外的任何信息。2006 年，Curtmola 等[4]提出了“适应性安全性”（adaptive security）和“非适应性安全性”（non-adaptive security）2 个新的安全模型，之后的大部分关于安全性的研究大多基于此展开，并提出了目前唯一一个符合 adaptive security 模型的对称可搜索加密方案。2012 年，Chai 等[26]采用可验证的 SSE（VSSE）方案，以提供除数据隐私之外的可验证的可搜索性，给出了满足安全性的可搜索加密方案。2015 年，柳祚鹏[27]首次提出了同义词搜索问题，采用同义词集合，给出了一个可以进行同义词检索的方案，满足 non-adaptive 安全。2017 年，陆海宁[28]提出了一种可以对搜索模式进行隐藏的方案，将关键词进行分组，组内关键词具有相同的搜索陷门，使服务器和敌手无法区分。

对于对称可搜索加密的安全性的研究，之前一直集中在适应性安全与非适应性安全 2 方面，利用可信硬件降低安全假设也是未来的研究方向之一。

3.5 小结

根据上文的介绍，可以发现，至今为止对于对称可搜索加密的研究主要在搜索语句的表达能力和安全性 2 方面，表 1 对一些对称可搜索加密机制的安全性进行了总结。

其中，“外”表示方案抵抗外部攻击，“内”表示抵抗服务器的内部攻击。从表 1 中可以看出，现有的对称可搜索加密方案虽然搜索语句的表达能力和效率方面存在差异，但基本满足日常所需的安全要求，对于特定环境下的加密方案，还需要人们针对不同的应用场景进行研究。

4 非对称可搜索加密

4.1 定义

非对称可搜索加密（即基于公钥的可搜索加密）技术的来源可以追溯到不可信赖的服务器路由问题[3]，即 Bob 希望向 Alice 发送邮件，需经由邮件服务器，为了保证邮件的隐私性，需要在邮件服务器不知道邮件内容的前提下，可以正确地按照邮件的内容将邮件发送给 Alice。

Boneh 等[29]首次将可搜索加密技术应用到非对称密码学中，提出 PEKS（public key encryption with keyword search）概念，算法描述如下。

定义 2 （PEKS）[3]非对称密码体制下可搜索加密算法可描述为

$PEKS=(KeyGen,Encrypt,Trapdoor,Test)$

1) $(pk,sk)=KeyGen(\lambda)$：λ 是安全参数，该算法根据安全参数生成公钥 pk 和私钥 sk。

2) $C_W=Encrypt(pk,W)$：利用生成的公钥 pk 和加密文件的关键词 W，生成关键词密文 C_W。

3) $T_W=Trapdoor(sk,W)$：利用生成的私钥 sk 和用户输入的关键词 W，生成关键词 W 的陷门 T_W。

4) $b=Test(pk,C_W,T_W)$：根据生成的公钥 pk、关键词 W 的陷门 T_W 和关键词密文 C_W，计算匹配相似度，输出判定值 $b\in\{0,1\}$。

对于现有的非对称可搜索加密技术，构建方法大多基于不同的困难假设，其中大部分基于双线性对（bilinear pairing），下面进行详细介绍。

定义 3 （双线性对）[29]对于双线性映射 $e:G_1\times G_1\rightarrow G_2$，需要满足以下条件。

1) 双线性（bilinear）：$\forall a,b\in Z_q$，$\forall g,h\in G_1$，$e(g^a,h^b)=e(g,h)^{ab}$。

2) 非退化性（non-degenerate）：$\exists g\in G_1$，使 $e(g,g)\neq 1$。

3) 可计算性（computable）：群 G_1，G_2 中的运算以及双线性映射 e 运算在多项式时间内可解。

定义 4 离散 Diffie-Hellman 问题（DDH）[30]：假设 G 是一个素数阶 p 的群，其中，g 是 G 的生成元，随机地从 $\{0,\cdots,p-1\}$ 中选择元素 a,b,c，给定元组 (g,g^a,g^b,g^c)，判断 g^c 是否等于 g^{ab}。

定义 5 双线性 Diffie-Hellman 问题（BDH）[31]：对于群 G 及其生成元 g，给定 g^a,g^b,g^c，计算 $e(g,g)^{abc}$。

由于双线性对涉及群元素的运算，使非对称可搜索加密技术的开销变大，但也正是由于这个特性，使非对称可搜索加密可以实现复杂的加密技术。而且，在一些相对不安全的网络中，非对称可搜索加密技术因为不需要协商密钥而更加适用，因为数据拥有者可以使用公钥对文件进行加密，而数据使用者可以使用私钥进行搜索和解密。

4.2 BDOP-PEKS 方案

2004 年，Boneh 等[29]最早提出 PEKS 概念，并基于 BF-IBE 构造了第一个 PEKS 方案 BDOP-PEKS，安全性可归结为 BDH 数学假设。具体构造如下。

1) $KeyGen(s)$：s 是安全参数，选取 $\alpha\in Z_p^*$ 和群 G_1、生成元 g，生成公钥 $A_{\text{pub}}=[g,h=g^{\alpha}]$ 和私

表 1　SSE 机制总结

方案	语句表达能力	特点	选择关键词攻击安全	选择明文攻击安全	字典攻击安全
Song[2]	单关键词	流密码	内/外	内/外	内/外
Goh[24]	单关键词	布隆过滤器	内/外	内/外	内/外
Li[20]	模糊关键词	编辑距离	内/外	内/外	内/外
王恺璇[23]	模糊多关键词	敏感散列	内/外	内/外	内/外

钥 $A_{\text{priv}}=\alpha$。

2) *PEKS*(A_{pub}, w)：选取 $r\in Z_p^*$，计算 $t=\hat{e}(H_1(w),h^r)\in G_2$，生成关键词密文 $C_w=[g^r,H_2(t)]$。

3) *Trapdoor*(A_{priv}, w')：计算陷门 $T_{w'}=H_1(w')^{\alpha}\in G_1$。

4) *Test*(A_{pub}, C_w, $T_{w'}$)：令 C_w=[A, B]，判断 $H_2(\hat{e}(T_{w'},A))=B$ 是否相等，相等为 1，否则为 0。

该方案基于 BDH 困难假设，使方案的效率极低，并且不能抵抗关键词猜测攻击。

4.3 非对称可搜索加密语句的表达能力

对于非对称可搜索加密语句表达能力的研究，起初只支持精确关键词检索，之后进行了扩展研究，包括多关键词搜索和模糊关键词搜索。

2004 年，Boneh 等[29]最早提出 PEKS 概念，并基于 BF-IBE 构造了第一个 PEKS 方案 BDOP-PEKS，安全性可归结为 BDH 数学假设。2005 年，Abdalla 等[32]提供了一个匿名 IBE 方案到安全的 PEKS 方案的变换，给出了一个统计一致的方案。

关于布尔关键词检索，公钥可搜索加密也进行了研究。2004 年，Golle 等[30]提出了一个连接关键词的方案，该方案在文档数量上是线性的，并且依赖于安全性的决策性 Diffie-Hellman（DDH）假设，并且通信成本与关键字数量级相关。2005 年，Park 等[33]给出了一种连接关键词的 PECK 方案，并提出了基于 DBDH 假设的方案 Park-1 和基于 DBDHI 假设的 Park-2 方案。2007 年，Boneh 等[31]提出了允许用户进行连接关键词检索、区间检索以及子集检索的可搜索加密方案。

针对非对称可搜索加密单关键词检索的不足，2005 年，Dong 等[34]给出了一种可以实现连接关键词搜索的公钥加密问题的解决方案。2007 年，Yong 等[35]构造了一个高效的 PECK 方案，其安全性在随机预言模型中经过决策线性 Diffie-Hellman 假设证明。引入了一种称为多用户 PECK 方案的新概念，它可以实现高效的计算和通信开销，并有效管理服务器中多个用户的存储。在 2013 年，Hu 等[36]提出了 PEKS 扩展的定义，称为公钥加密排序多关键字搜索（PERMKS），这意味着接收者可以查询关键字的任何子集和数据中出现的查询关键字的数量来评估数据与搜索查询的相似性排名。在 2016 年，Miao 等[37]设计了一个高效的加密原语，称为可验证的多关键字搜索，通过加密的云数据获取动态数据拥有者方案，以保护数据的机密性和完整性。2017 年，张楠等[38]提出了一种多关键词公钥可搜索加密方案，并实现了密文全文检索系统 Bluce。

与对称可搜索加密技术的研究方向类似，公钥可搜索加密技术的模糊搜索也已成为研究的重点。2012 年，Bringer 等[39]利用编辑距离到海明距离的经典嵌入，在查找关键关键字他和保留查询机密性的同时，在容许的编辑距离上提供了一些灵活性。在 2013 年，Dong 等[40]提出了一种新的基于模糊关键字搜索（IPEFKS）的交互式公钥加密原语，它支持在公钥设置中对加密数据进行高效的模糊关键字搜索。

4.4 非对称可搜索加密的安全性

对于早期提出的公钥可搜索加密技术，之后的研究发现很多存在不同的漏洞，这也使对非对称可搜索加密安全性的研究成为重点。

文献[41]首次提出 Boneh 等[29]的 PEKS 方案存在严重的安全漏洞，这是因为关键字的选择范围比密码小得多，用户通常使用知名关键字搜索文档，这个事实足以引起离线的关键字猜测攻击。通过进一步的研究，Jeong 等[42]展示了一个关于构建安全 PEKS 方案以防止关键字猜测攻击公开问题的负面结果。结果表明，一致性意味着 PEKS 中的关键字猜测攻击不安全。这意味着，当可能的关键字的数量受到某个多项式的限制时，构建安全且一致的 PEKS 方案来防范关键字猜测攻击是不可能的。

2010 年，Tang 等[43]提出了一个新的概念，即使用注册关键字搜索（PERKS）的公钥加密，它需要发件人在发件人为该关键字生成标签之前向接收方注册关键字。证明提出的 PERKS 语义安全定义不受离线关键词猜测攻击的影响。2011 年，方黎明[44]给出了一个可以抵抗关键词猜测攻击的公钥可搜索加密的安全模型。2013 年，Xu 等[45]使用 PEKS 的关键字隐私增强变体（称为使用模糊关键字搜索（PEFKS）的公钥加密）来解

决关键字猜测攻击问题。在 PEFKS 中，每个关键字对应一个确切的关键字搜索陷门和一个模糊关键字搜索陷门。2016 年，Chen 等[46]提出了一个名为双服务器 PEKS（DS-PEKS）的新 PEKS 框架，又提供了一个基于决策 Diffie-Hellman 的 LH-SPHF 一般框架的高效实例，并表明它可以实现对 KGA 内部的强大安全性。

根据以上的研究发现，关于公钥可搜索加密机制安全性的研究主要集中在对关键词猜测攻击的各种抵御方案，之后的研究将主要集中在研究高效的可抵御关键词猜测攻击的加密方案。

4.5　小结

根据上文的介绍，非对称可搜索加密方案的区别大多体现在基于的困难假设不同，达到的安全性也不同。对一些基本的公钥可搜索加密机制的安全性等方面进行总结，具体如表 2 所示。

其中，IND-CKA 表示自适应性选择关键词攻击，ROM 表示随机预言机模型，DBDH 代表决策双线性 Diffie-Hellman 问题，DBDHI 代表决策双线性 Diffie-Hellman 反演假设。对于非对称可搜索加密技术，虽然使用的困难假设不同，但其对于安全性的研究主演集中在是否能够抵抗关键词猜测攻击和是否需要安全通道两方面。可验证的公钥可搜索加密方案仍是待解决的问题，需要人们的深入研究。

5　结束语

本文针对可搜索加密技术的研究现状进行了介绍，首先对可搜索加密的研究机制进行了介绍，其次从对称可搜索加密和非对称可搜索加密 2 个方面对研究进展进行分析。从上文的讨论中可以看出，可搜索加密技术的研究已经逐渐成熟，并在未来的一段时间内，依然被认为是解决云计算安全的研究热点之一。笔者认为，可搜索加密机制中仍然存在值得深入研究的问题，主要包括如下内容。

1) 灵活高效的查询语句是可搜索加密技术的未来研究方向之一。现有的可搜索加密方案中，当用户进行关键词检索时，仍然需要用户进行二次检索，使搜索效率大大降低。现阶段的研究侧重多有不同，或侧重模糊检索，或侧重条件检索，不够完善，包括模糊关键词检索、关键词排序检索、多关键词检索、关键词检索结果的可验证性等。

2) 保留语义的可搜索加密技术是未来的研究难点。采用加密技术可以保护用户的数据安全，但同时也失去了词语的语义关系，无法在密文上进行关键词检索。未来需要研究的加密方案是使关键词在加密后仍然具有服务器无法获得的语义关系，不仅可以实现精确查询，还可以准确找到用户所需的文件。

3) 可搜索加密技术的安全性是研究的重点之一。如今，基本的可搜索加密技术已经初具规模，具有广阔的应用空间，其安全性问题是阻碍可搜索加密技术应用的重要原因，至今仍然有许多可搜索加密技术受到猜测关键词攻击的潜在威胁。因此，设计一种安全、高效的可搜索加密技术，也是未来的研究方向之一。

参考文献:

[1] 项菲, 刘川意, 方滨兴,等. 云计算环境下密文搜索算法的研究[J]. 通信学报, 2013(7):143-153.
XIANG F, LIU C Y, FANG B X, et al. Research on ciphertext search for the cloud environment[J]. Journal on Communications, 2013, 34(7):143-153.

[2] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]// IEEE Computer Society. 2000: 44.

[3] 李经纬, 贾春福, 刘哲理, 等. 可搜索加密技术研究综述[J]. 软件学报, 2015, 26(1): 109-128.
LI J W, JIA C F, LIU Z L, et al. Survey on the searchable encryption[J]. Journal of Software, 2015,26(1):109-128.

[4] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable sym-

表 2　　**PEKS 机制总结**

方案	安全性	抵御关键词猜测攻击	安全模型	困难假设	安全信道
Boneh[29]	IND-CKA	否	ROM	BDH	需要
Park-1[33]	IND-CKA	否	ROM	DBDH	需要
Park-2[33]	IND-CKA	否	ROM	DBDHI	需要
Tang[43]	IND-CKA	是	ROM	DBDH	需要

metric encryption: improved definitions and efficient constructions[C]//ACM Conference on Computer and Communications Security. ACM, 2006:79-88.

[5] WANG C, CAO N, LI J, et al. Secure ranked keyword search over encrypted cloud data[C]//IEEE International Conference on Distributed Computing Systems. 2010:253-262.

[6] PREMASATHIAN N, CHOTO S. Searchable encryption schemes: with multiplication and simultaneous congruences[C]//IEEE International ISC Conference on Information Security and Cryptology. 2013:147-150.

[7] PREMASATHIAN N, CHOTO S. Searchable encryption schemes: with multiplication and simultaneous congruences[C]//International ISC Conference on Information Security and Cryptology. 2013: 147-150.

[8] FU Z, SHU J, SUN X, et al. Smart cloud search services: verifiable keyword-based semantic search over encrypted cloud data[J]. IEEE Transactions on Consumer Electronics, 2014, 60(4):762-770.

[9] FU Z, SUN X, LINGE N, et al. Achieving effective cloud search services: multi-keyword ranked search over encrypted cloud data supporting synonym query[J]. IEEE Transactions on Consumer Electronics, 2014, 60(1):164-172.

[10] XIA Z, WANG X, SUN X, et al. A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data[J]. IEEE Transactions on Parallel & Distributed Systems, 2016, 27(2): 340-352.

[11] 杨旸, 杨书略, 蔡圣暐, 等. 排序可验证的语义模糊可搜索加密方案[J]. 四川大学学报(工程科学版), 2017, 49(4):119-128.
YANG Y, YANG S L, CAI S. Semantically searchable encryption scheme supporting ranking verification[J].Journal of Sichuan University(Engineering Science Edition),2017, 49(4):119-128.

[12] CASH D, JARECKI S, JUTLA C, et al. Highly-scalable searchable symmetric encryption with support for boolean queries[M]// Advances in Cryptology–CRYPTO 2013. Berlin: Springer. 2013: 353-373.

[13] LI H, YANG Y, LUAN T, et al. Enabling fine-grained multi-keyword search supporting classified sub-dictionaries over encrypted cloud data[J]. IEEE Transactions on Dependable & Secure Computing, 2016, 13(3):312-325.

[14] 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. Attribute-based encryption supporting arbitrary conjunctive key word search[J]. Journal on Communications, 2016, 37(8):77-85.

[15] 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 & Security, 2017, 11(4): 789-798.

[16] CHEN R, MU Y, YANG G, et al. Server-aided public key encryption with keyword search[J]. IEEE Transactions on Information Forensics & Security, 2016, 11(12):2833-2842.

[17] FU Z, REN K, SHU J, et al. Enabling personalized search over encrypted outsourced data with efficiency improvement[J]. IEEE Transactions on Parallel & Distributed Systems, 2016, 27(9): 2546-2559.

[18] FU Z, SUN X, JI S, et al. Towards efficient content-aware search over encrypted outsourced data in cloud[C]//IEEE International Conference on Computer Communications, 2016:1-9.

[19] BRINGER J, CHABANNE H, KINDARJI B. Error-tolerant searchable encryption[C]//IEEE International Conference on Communications. 2009:1-6.

[20] LI J, WANG Q, WANG C, et al. Fuzzy keyword search over encrypted data in cloud computing[C]//INFOCOM. 2010. 1-5.

[21] CHUAH M, HU W. Privacy-aware bedtree based solution for fuzzy multi-keyword search over encrypted data[C]// International Conference on Distributed Computing Systems Workshops. IEEE, 2011. 273-281.

[22] 杨旸, 杨书略, 柯闽. 加密云数据下基于 Simhash 的模糊排序搜索方案[J]. 计算机学报, 2017, 40(2):431-444.
YANG Y,YANG S L,KE M. Ranked fuzzy keyword search based on simhash over encrypted cloud data[J]. Chinese Journal of Computers, 2017, 40(2):431-444.

[23] 王恺璇, 李宇溪, 周福才,等. 面向多关键字的模糊密文搜索方法[J]. 计算机研究与发展, 2017, 54(2):348-360.
WANG K X, LI Y X, ZHOU F C, et al. Multi-keyword fuzzy search over encrypted data[J]. Journal of Computer Research and Development, 2017, 54(2): 348-360.

[24] GOH E J. Secure Indexes[J]. Submission, 2003.

[25] CHANG Y C, MITZENMACHER M. Privacy preserving keyword searches on remote encrypted data[C]//International Conference on Applied Cryptography and Network Security. 2005:442-455.

[26] CHAI Q, GONG G. Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers[C]//IEEE International Conference on Communications. 2012. 917-922.

[27] 柳祚鹏. 支持同义词搜索和抗信息泄漏的对称可搜索加密技术研究[D]. 上海: 上海交通大学,2015.
LIU Z P. Research on symmetric searchable encryption technology supporting synonym search and anti-information leak-age[D]. Shanghai: Shanghai Jiaotong University.2015.

[28] 陆海宁. 可隐藏搜索模式的对称可搜索加密方案[J].信息网络安全, 2017(01): 38-42.
LU H N. Searchable symmetric encryption with hidden search pattern[J]. Netinfo Security,2017(1):38-42.

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

[30] GOLLE P, STADDON J, WATERS B. Secure conjunctive keyword search over encrypted data[J]. Lecture Notes in Computer Science, 2004, 3089:31-45.

[31] BONEH D, WATERS B. Conjunctive, subset, and range queries on encrypted data[J]. TCC 2007, 2007, 4392:535--554.

[32] ABDALLA M, BELLARE M, CATALANO D, et al. Searchable encryption revisited: consistency properties, relation to anonymous ibe, and extensions[M]//Advances in Cryptology–CRYPTO 2005. 2005. 205-222.

[33] PARK D, KIM K, LEE P. Public key encryption with conjunctive field keyword search in information security applications[C]//The 5th International Workshop (WISA'04). 2004. 23-25.

[34] DONG J P, KIM K, LEE P J. Public key encryption with conjunctive field keyword search[M]//Information Security Applications. Berlin: Springer. 2004. 73-86.

[35] YONG H H, LEE P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system[C]// International Conference on Pairing-Based Cryptography. 2007. 2-22.

[36] HU C, LIU P. Public key encryption with ranked multi-keyword search[C]//International Conference on Intelligent Networking and Collaborative Systems. 2013. 109-113.

[37] MIAO Y, MA J, LIU X, et al. VMKDO: verifiable multi-keyword search over encrypted cloud data for dynamic data-owner[J]. Peer-to-Peer Networking and Applications, 2016(1):1-11.

[38] 张楠, 陈兰香. 一种高效的支持排序的关键词可搜索加密系统研究[J]. 信息网络安全, 2017(2):43-50.
ZHANG N, CHEN L X. Research on an efficient ranked keywords searchable encryption system[J].Netinfo Security,2017(2):43-50.

[39] BRINGER J, CHABANNE H. Embedding edit distance to enable private keyword search[J]. Human-centric Computing and Information Sciences, 2012, 2(1):1-12.

[40] DONG Q, GUAN Z, WU L, et al. Fuzzy keyword search over encrypted data in the public key setting[C]// International Conference on Web-Age Information Management. Springer Berlin Heidelberg, 2013, 729-740.

[41] JIN W B, RHEE H S, PARK H A, et al. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data[C]// The Workshop on Secure Data Management. Springer Berlin Heidelberg, 2006:75-83.

[42] JEONG I R, KWON J O, HONG D, et al. Constructing PEKS schemes secure against keyword guessing attacks is possible?[J]. Computer Communications, 2009, 32(2):394-396.

[43] TANG Q, CHEN L. Public-key encryption with registered keyword search[C]//European Conference on Public Key Infrastructures, Services and Applications. Springer-Verlag, 2009. 163-178.

[44] 方黎明. 带关键字搜索公钥加密的研究[D]. 南京航空航天大学, 2012.
FANG L M. Research on keyword encryption with keyword search[D]. Naijing: Nanjing Aerospace University,2012.

[45] XU P, JIN H, WU Q, et al. Public-key encryption with fuzzy keyword search: a provably secure scheme under keyword guessing attack[J]. IEEE Transactions on Computers, 2013, 62(11): 2266-2277.

[46] 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 & Security, 2017, 11(4):789-798.

[作者简介]

李颖（1993-），女，黑龙江黑河人，哈尔滨工程大学硕士生，主要研究方向为密码学可搜索加密技术。

马春光（1974-），男，黑龙江双城人，哈尔滨工程大学教授、博士生导师，主要研究方向为分布式密码算法与协议、云计算安全与隐私、格密码。