公钥可搜索加密体制综述

秦志光, 徐 骏, 聂旭云, 熊 虎
电子科技大学信息与软件工程学院 成都 中国 610054

摘要 伴随着云计算技术的广泛应用, 外包到云服务器存储的数据通常采用密文方式进行存储以确保数据安全和用户隐私。可搜索加密体制允许用户对密文数据通过关键词进行检索, 从而极大减少了数据共享用户的通信和计算开销。基于公钥的可搜索加密体制解决了对称可搜索加密体制中的密钥分发问题而受到广泛关注。本文侧重于阐述公钥可搜索加密体制的研究进展, 描述了它的形式化定义、安全模型; 分析和讨论了典型的公钥可搜索加密体制的设计机理、相关的扩展方案以及它们的安全性问题。最后, 本文还讨论了公钥可搜索加密体制的应用场景,并指出了未来可能的发展方向。

关键词 云安全; 可搜索加密; 公钥可搜索加密; 关键词猜测攻击
中图法分类号 TP309 DOI 号 10.19363/j.cnki.cn10-1380/tn.2017.07.001

A Survey of Public-Key Encryption with Keyword Search

QIN Zhiguang, XU Jun, NIE Xuyun, XIONG Hu
Department of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China

Abstract With the population of cloud computing technology, tremendous data is outsourced in the cloud server in the encrypted form to ensure data security and user privacy. Searchable encryption allows users to retrieve the encrypted data by keywords, thus greatly reduce the user's communication and computation overhead. Public key cryptography based searchable encryption has solved the key distribution problem in symmetric key cryptography based searchable encryption and thus received a lot of attention recently. This paper focuses on the development of public-key encryption with keyword search (PEKS) by surveying the state-of-the-art of PEKS, describing the formal definition and security model of PEKS and analyzing the design philosophy of classical PEKS schemes. Furthermore, some extensions of PEKS in terms of function and security enhancement have also been given. Finally, this paper discusses the application scenario of PEKS, and demonstrates the future research directions of PEKS.

Key words cloud security; searchable encryption; public-key encryption with keyword search; keyword guessing attacks

1 引言

近年来, 随着云计算的快速发展, 云存储服务越来越成熟, 同时也受到了学术界和工业界越来越多的关注。但是云计算在为用户带来便利的同时, 还有很多待解决的问题, 其中安全问题就是急需解决的一个问题。对于数据拥有者而言, 云服务器并不是完全可信的。为了保护数据隐私, 在把数据发送给云服务器存储之前, 必须要先对数据进行加密处理。但是这样一来, 已有的基于明文的关键词搜索技术就失效了。为了解决如何在密文上进行关键词搜索的问题, 可搜索加密的概念被提了出来, 如图 1 所示, 可搜索加密的工作流程如下: 首先数据拥有者把加密的文件数据以及相关的关键词密文上传到云服务器, 然后用户利用私钥生成搜索陷门, 并把该陷门信息发送给云服务器, 云服务器通过使用该陷门信息搜索到用户感兴趣的数据, 并把数据发回给用户。该技术实现了用户在不可信赖云服务器环境下进行快速有效的密文关键词检索, 同时不泄漏任何关于数据的信息。

可搜索加密体制分为对称可搜索加密体制和公钥可搜索加密体制。第一个对称可搜索加密方案是由 Song 等人[1]提出来的, 该方案中使用了类似流密码的方法进行加密, 通过线性扫描来查找特定的关键词, 实现了在密文上进行关键词检索的功能。根据对称加密体制的性质, 对称可搜索加密体制中的数

通讯作者: 熊虎, 博士, 电子科技大学信息与软件工程学院副教授, Email: xionghu.uestc@gmail.com。
本课题得到国家自然科学基金 (Nos.61370026, 61672135); 国家自然基金重点国际(地区)合作研究项目(No.61520106007); 四川省科技支撑项目(No.2016GZ0065); 国家高科技研究发展计划(863 计划)(No.2015AA016007)资助。
收稿日期: 2016-06-14; 修改日期: 2016-08-05; 定稿日期: 2017-03-24

据文件和要检索的关键词陷门都必须使用同一个的密钥进行加密, 因此对称可搜索加密体制更适合应用于个人的数据存储等应用场景中。

公钥可搜索加密方案是由 Boneh 等人[2]首次提出来的, 该方案主要被应用在邮件路由的应用场景, 在该应用场景中有三个参与方分别是发送方、接收方和邮件服务器。发送方使用接收方的公钥来加密邮件和关键词信息, 接收方使用自身的私钥生成搜索陷门, 最后由邮件服务器来进行数据检索, 将包含某个关键词的邮件密文发送给接收方。

与对称可搜索加密方案不同, 大部分的公钥可搜索加密方案都是基于双线性对构造的, 因此其运算效率比对称可搜索加密方案要低不少。但是由于公钥可搜索加密方案使用了数据共享者的公钥对数据进行加密, 因此在整个加密过程中, 数据加密者不需要与数据共享者进行密钥协商, 这使得该方案更适合于多用户的数据共享等领域, 其应用场景比对称可搜索加密的应用场景更为广阔。

在文献[3,4]中从构造思想、运行效率和典型应用场景等几个方面详细阐述了对称可搜索加密和公钥可搜索加密的不同特点, 并且还分析了对称可搜索加密和公钥可搜索加密在查询方式上的扩展方案。但是这两篇综述对公钥可搜索加密的讨论略有些粗糙, 尤其是PEKS的安全性问题和一些其他的扩展方案没有详细探讨。本文侧重于分析公钥可搜索加密体制, 总结了近几年来公钥可搜索加密体制的研究成果, 详细阐述了公钥可搜索加密体制的安全性问题和一些扩展方案, 最后探讨了该领域未来可能的发展方向。

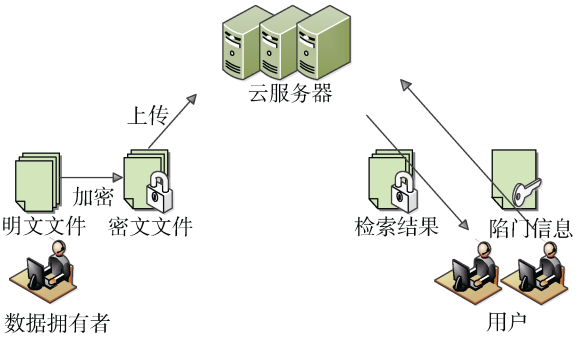

图 1　可搜索加密体制的应用模型

2　形式化定义和安全目标

公钥可搜索加密方案(Public-Key Encryption with Keyword Search, PEKS)是一类具有密文可搜索性质的加密体制, 它在保证数据保密性的基础上, 允许用户搜索包含某些特定关键词的密文数据。Boneh 等人[2]首次提出了公钥可搜索加密的概念, 利用公钥加密技术和双线性映射给出了相应的构造方案, 并把该方案应用在邮件路由的应用场景中, 方便邮件服务器进行邮件的分发。本节主要介绍公钥可搜索加密的形式化定义以及相关的安全模型。

2.1　公钥可搜索加密的形式化定义

定义 1(PEKS). 一个公钥可搜索加密体制一般由 4 个概率多项式时间算法组成:

(1) $\mathrm{KeyGen}(\lambda)$: 输入安全参数λ, 输出公钥pk和私钥sk。

(2) $\mathrm{PEKS}(pk, w)$: 输入公钥pk和关键词w, 输出关键词密文C_w。

(3) $\mathrm{Trapdoor}(sk, w')$: 输入私钥sk和关键词w', 输出陷门$T_{w'}$。

(4) $\mathrm{Test}(pk, C_w, T_{w'})$: 输入公钥pk、关键词密文C_w和陷门$T_{w'}$, 如果$w = w'$则输出 1, 否则输出 0。

根据定义 1, 公钥可搜索加密方案的工作流程如下: 邮件发送者使用邮件接收者的公钥pk来加密邮件信息和相应的关键词w, 并将加密后的密文C_w发送给邮件服务器。同时, 邮件接收者使用自己的私钥sk和要搜索的关键词w'生成陷门$T_{w'}$, 并把该陷门发送给邮件服务器。邮件服务器在接收到陷门$T_{w'}$和邮件密文 C_w之后, 执行 Test 算法进行关键词匹配检索。

2.2　公钥可搜索加密的安全目标

2.2.1　公钥可搜索加密的安全模型

公钥可搜索加密体制的 IND-CKA (indistinguishability against chosen keyword attack)安全模型可以通过挑战者$\mathcal{C}$与敌手$\mathcal{A}$之间的安全游戏进行定义, 该安全游戏的描述如下:

初始化阶段: 挑战者$\mathcal{C}$运行$\mathrm{KeyGen}(\lambda)$算法生成公钥pk和私钥sk, 将公钥pk发送给敌手$\mathcal{A}$。

问询阶段 1: 敌手$\mathcal{A}$自适应查询陷门预言机$\mathcal{O}_{Trapdoor}$, 获得关键词$w \in \{0,1\}^*$的陷门T_w。

挑战阶段: 敌手$\mathcal{A}$随机选取两个不同的关键词w_0、w_1, 发送给挑战者$\mathcal{C}$。其中限制条件为关键词w_0、w_1的陷门信息之前没有被询问过。挑战者$\mathcal{C}$随机选取一个比特$b \in \{0,1\}$生成挑战密文$C = \mathrm{PEKS}(pk, w_b)$, 将该挑战密文发送给敌手$\mathcal{A}$。

问询阶段 2: 与问询阶段 1 类似, 但是不允许询问关键词w_0、w_1的陷门信息。

猜测阶段: 敌手$\mathcal{A}$输出一个比特$b' \in \{0,1\}$,如果$b = b'$, 那么敌手$\mathcal{A}$在游戏中获胜, 否则失败。

敌手$\mathcal{A}$赢得上述游戏的攻击优势为:

$$Adv_A(\lambda) = \|Pr(b = b') - \tfrac{1}{2}\|$$

定义 2(PEKS-IND-CKA). 公钥可搜索加密体制是语义安全的, 如果对于任意的 PPT(probabilistic polynomial time)敌手$\mathcal{A}$, 其赢得上述游戏的优势是关于ε可忽略的, 即$Adv_{\mathcal{A}}(\lambda) < negl(\varepsilon)$。

以上的 PEKS-IND-CKA 安全定义是由 Boneh 等人在文献[2]中提出的, 但随后的研究表明该安全定义还存在诸多安全性问题, 比如文献[5]中指出 Boneh 的 PEKS 方案中存在安全信道问题, 接收者与服务器之间的交互必须要在一个安全信道中进行才能保证 PEKS 的安全性。在 2006 年, Byun 等人[6]指出由于关键词空间远小于密钥空间, 因此已有的 PEKS 方案不能抵御关键词猜测攻击。

除了上述定义的 PEKS-IND-CKA 安全模型外, 公钥可搜索加密体制还具有其他形式的安全模型。针对各种 PEKS 及其扩展方案, 表 1 对它们的安全模型进行了对比。

表 1 公钥可搜索加密方案的安全模型对比

方案	安全信道	预言机	攻击者类型	安全性	抵御关键词猜测攻击
Boneh[2]	需要	$\mathcal{O}_{Trapdoor}$	外部攻击者	IND-CKA	否
Baek[5]	不需要	$\mathcal{O}_{Trapdoor}$	内部攻击者、外部攻击者	IND-CKA	否
Rhee[11]	不需要	$\mathcal{O}_{Trapdoor}$、$\mathcal{O}_{dTest}$	内部攻击者、外部攻击者	IND-CKA	否
Tang[13]	需要	$\mathcal{O}_{Trapdoor}$、$\mathcal{O}_{KeywordReg}$	外部攻击者	IND-CKA	是
Park[9]	需要	$\mathcal{O}_{Trapdoor}$	外部攻击者	IND-CKA	否
Fuhr[14]	需要	$\mathcal{O}_{Trapdoor}$、$\mathcal{O}_{Dec}$	外部攻击者	IND-CCA	否
Yau[18]	不需要	$\mathcal{O}_{dTrapdoor}$、$\mathcal{O}_{ReKeyGen}$、$\mathcal{O}_{RedPEKS}$	内部攻击者、外部攻击者	IND-CKA	否

(注: $\mathcal{O}_{Trapdoor}$和$\mathcal{O}_{dTrapdoor}$表示陷门预言机; $\mathcal{O}_{dTest}$表示测试预言机; $\mathcal{O}_{KeywordReg}$表示关键词注册预言机; $\mathcal{O}_{Dec}$表示解密预言机; $\mathcal{O}_{ReKeyGen}$表示重加密密钥生成预言机; $\mathcal{O}_{RedPEKS}$表示关键词重加密预言机; IND-CKA 代表 indistinguishability against chosen keyword attack; IND-CCA 代表 indistinguishability against chosen ciphertext attack)

2.2.2 公钥可搜索加密的一致性问题

任何密码学体制都必须要符合两个性质, 第一个是安全性, 第二个是一致性。对于传统的公钥加密体制来讲, 其一致性是指解密应该是加密的逆运算。对于公钥可搜索加密体制来讲, 其一致性的定义最初由 Abdalla 等人在文献[7]中提出, 该定义要求对于任意两个关键词w_1、w_2, 生成关于关键词w_1的陷门T_{w_1}, 以及生成关于关键词w_2的关键词密文C_{w_2}, 如果$w_1 = w_2$, 则测试算法$Test(C_{w_2}, T_{w_1})$返回“1”, 否则返回“0”, 以下是具体的定义。

定义 3 (Consistency for PEKS). 假设存在一个敌手$\mathcal{A}$, 定义如下安全游戏:

$Exp_{\mathcal{A}}^{Consistency}(\lambda)$:
$(pk, sk) \leftarrow KeyGen(\lambda)$
$(w_1, w_2) \leftarrow \mathcal{A}(pk)$
$C_{w_1} \leftarrow PEKS(pk, w_1)$
$T_{w_2} \leftarrow Trapdoor(sk, w_2)$
$if\ w_1 \neq w_2\ and\ Test(C_{w_1}, T_{w_2}) = 1$
$then\ output\ 1$
$else\ output\ 0$

敌手赢得上述游戏的攻击优势为: $Adv_{\mathcal{A}}(\lambda) = Pr(Exp_{\mathcal{A}}^{Consistency}(\lambda) = 1)$

(1) 若对于任意的攻击者$\mathcal{A}$,其赢得上述游戏的攻击优势为$Adv_{\mathcal{A}}(\lambda) = 0$, 则称该 PEKS 体制是完美一致的。

(2) 若对于任意的攻击者$\mathcal{A}$,其赢得上述游戏的攻击优势$Adv_{\mathcal{A}}(\lambda)$是关于$\varepsilon$可忽略的, 则称该 PEKS 体制是统计一致的。

(3) 若对于任意的概率多项式时间攻击者$\mathcal{A}$,其赢得上述游戏的攻击优势$Adv_{\mathcal{A}}(\lambda)$是关于$\varepsilon$可忽略的, 则称该 PEKS 体制是计算一致的。

Abdalla 等人[7]在给出该定义的同时, 还指出了文献[2]中的公钥可搜索加密方案并不满足完美和统计一致性, 只满足计算一致性, 最后他们给出了一个满足统计一致性的 PEKS 方案。现有的 PEKS 方案大多数使用的是计算一致性定义。

3 典型的构造方案

3.1 Boneh 的 PEKS 方案

在 2004 年, Boneh 等人[2]首次提出了公钥可搜索加密的概念, 并给出了基于双线性对的构造方案, 其安全性是基于 BDH(Bilinear Diffie-Hellman)困难性问题。该方案以邮件系统为应用背景, 解决了加密邮件的路由分发问题。

Boneh 等人[2]的具体构造方案是基于双线性对$\hat{e} : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$构造的, 其中$\mathbb{G}_1$、$\mathbb{G}_2$的阶均为$p$。同时该方案还需要两个哈希函数$H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$以及$H_2 : \mathbb{G}_2 \rightarrow \{0,1\}^{\log p}$。该方案包括 4 个概率多项式时间算法, 具体构造如下:

(1) $\mathrm{KeyGen}(s)$：该算法以一个安全参数s作为输入, 随机选取$\alpha \in \mathbb{Z}_p^*$以及群$\mathbb{G}_1$和生成元$g$, 输出公钥$A_{pub} = [g, h = g^{\alpha}]$, 私钥$A_{priv} = \alpha$。

(2) $\mathrm{PEKS}(A_{pub}, w)$：随机选取$r \in \mathbb{Z}_p^*$, 计算$t = \hat{e}(H_1(w), h^r) \in \mathbb{G}_2$, 输出关键词密文$C_w = [g^r, H_2(t)]$。

(3) $\mathrm{Trapdoor}(A_{priv}, w')$：输出陷门信息$T_{w'} = H_1(w')^{\alpha} \in \mathbb{G}_1$。

(4) $\mathrm{Test}(A_{pub}, C_w, T_{w'})$：令$C_w = [A, B]$, 判断等式$H_2(\hat{e}(T_{w'}, A)) = B$是否成立。若成立则输出 1, 否则输出 0。

该 PEKS 方案存在以下不足之处:

(1) 检索效率低, 由于该方案是基于双线性对实现的, 因此其计算开销较大, 不适合用于海量数据的检索。

(2) 该方案的陷门要在安全信道中传递, 即接收者与服务器之间需要建立一条安全信道, 来避免攻击者截获到陷门信息。

(3) 不能抵御离线关键词猜测攻击, 由于关键词空间远小于密钥空间, 因此攻击者可以通过暴力猜测的方式轻松破解该方案。

3.2 Khader 的 KR-PEKS 方案

在 2006 年, Khader 等人[8]指出文献[2]中的 PEKS 方案有一些安全性局限, 即该方案只能在随机预言机模型下被证明是安全的, 在标准模型下可能并不安全。针对这个问题, 他们提出了一种基于 K-Resilient IBE 的公钥可搜索加密方案(KR-PEKS), 该方案被证明在标准模型下是安全的。由于该 KR-PEKS 方案不是用双线性对构造的, 因此其运行效率比较高效。

虽然该 KR-PEKS 方案相比于 Boneh 的 PEKS 方案有众多的优点, 但它仍然有一些缺陷, 如恶意用户的数量必须要被限制在某个 K 值, 即生成的陷门数量不能超过 K 个, 不过该缺陷可以通过为系统设置一个比较大的 K 值来解决。

基于 K-Resilient IBE 的 KR-PEKS 方案包括 4 个概率多项式时间算法, 具体构造如下。

(1) KeyGen:

步骤 1: 选择一个q阶的群$\mathbb{G}$和两个生成元g_1, g_2。

步骤 2: 随机选择$\mathbb{Z}_q$上的 6 个k次多项式。

$f_1(x) = a_0 + a_1 x + \cdots + a_k x^k = \sum_{t=0}^{k} a_t x^t$

$f_2(x) = a'_0 + a'_1 x + \cdots + a'_k x^k = \sum_{t=0}^{k} a'_t x^t$

$h_1(x) = b_0 + a_1 x + \cdots + b_k x^k = \sum_{t=0}^{k} b_t x^t$

$h_2(x) = b'_0 + a_1 x + \cdots + b'_k x^k = \sum_{t=0}^{k} b'_t x^t$

$p_1(x) = d_0 + a_1 x + \cdots + d_k x^k = \sum_{t=0}^{k} d_t x^t$

$p_2(x) = d'_0 + d'_1 x + \cdots + d'_k x^k = \sum_{t=0}^{k} d'_t x^t$

步骤 3: 对于 $t\,(0 \leqslant t \leqslant k)$, 计算$A_t = g_1^{a_t} g_2^{a'_t}$, $B_t = g_1^{b_t} g_2^{b'_t}$, $D_t = g_1^{d_t} g_2^{d'_t}$。

步骤 4: 选择一个随机的抗碰撞的哈希函数$H : \mathbb{G} \to \{0,1\}^{\lambda}$。

步骤 5: 选择一个随机的抗碰撞的哈希函数 TCR。

步骤 6: 输出公钥$pk_R = (g_1, g_2, A_0, \cdots, A_k, B_0, \cdots, B_k, D_0, \cdots, D_k, H, TCR)$和私钥$sk_R = (f_1, f_2, h_1, h_2, p_1, p_2)$。

(2) KR-PEKS:

步骤 1: 选择一个随机值$r \in \mathbb{Z}_q$。

步骤 2: 计算$u_1 = g_1^r$, $u_2 = g_2^r$。

步骤 3: 对于每个关键词w, 计算

$A_w \leftarrow \prod_{t=0}^{k} A_t^{w^t}$; $B_w \leftarrow \prod_{t=0}^{k} B_t^{w^t}$; $D_w \leftarrow \prod_{t=0}^{k} D_t^{w^t}$。

步骤 4: 计算$s \leftarrow D_w^{r_1}$。

步骤 5: 计算$e \leftarrow (0^{\lambda}) \oplus H(s)$。

步骤 6: 计算$\alpha \leftarrow TCR(u_1, u_2, e)$。

步骤 7: 计算$v_w \leftarrow (A_w)^r \cdot (B_w)^{r\alpha}$。

步骤 8: 输出密文$C \leftarrow < u_1, u_2, e, v_w >$。

(3) Trapdoor:

输出陷门$T_{w'} =< f_1(w'), f_2(w'), h_1(w'), h_2(w'), p_1(w'), p_2(w') >$。

(4) Test:

步骤 1: 计算$\alpha \leftarrow TCR(u_1, u_2, e)$。

步骤 2: 判断以下不等式是否成立

$v_w \neq (u_1)^{f_1(w') + h_1(w')\alpha} (u_2)^{f_2(w') + h_2(w')\alpha}$, 如果成立则终止, 否则运行步骤 3。

步骤 3: 计算$s \leftarrow (u_1)^{p_1(w')} (u_2)^{p_2(w')}$。

步骤 4: 计算$M \leftarrow e \oplus H(s)$。

步骤 5: 如果$M = 0^{\lambda}$, 则输出yes, 否则输出no。

4 研究脉络与进展

在 2004 年, Boneh 等人[2]首次提出了公钥可搜索加密的概念, 并给出了基于匿名 IBE 的 PEKS 构造方案。该方案被应用在邮件系统中, 解决了不可信赖服务器的邮件路由问题。

在 2005 年, Abdalla 等人[7]对公钥可搜索加密方案进行了深入的研究, 分析了 PEKS 体制的一致性问题, 指出文献[2]中的方案是计算一致的, 随后给出

了一个统计一致的方案, 同时他们还给出了PEKS方案与匿名的IBE方案之间的转化关系。

在2005年, Park等人[9]提出了一种支持连接关键词检索的公钥可搜索加密方案(Public Key Encryption with Conjunctive Field Keyword Search, PECK), 并给出了两种安全性分别基于DBDH假设(decision bilinear Diffie-Hellman assumption)和DBDHI假设(decision bilinear Diffie-Hellman inversion assumption)的构造方案。由于该方案并不支持关键词的子集查询以及比较查询, 为了进一步提高查询的灵活性, Boneh等人[10]提出了一种支持连接、子集和比较查询的PEKS方案, 并给出了基于HVE体制(hidden vector encryption)的具体构造方案。

在2006年, Byun等人[6]发现当前的PEKS体制存在严重的安全隐患: 由于关键词空间远小于密钥空间, 因此攻击者通过离线关键词猜测攻击(Off-Line Keyword Guessing Attacks)能很轻松破解PEKS体制。为了抵御离线关键词猜测攻击, Rhee等人[11]提出了一种陷门安全的dPEKS(searchable public key encryption with a designated tester)方案, 该方案引入了陷门不可区分概念, 加强了PEKS方案中的陷门安全, 但随后Wang等人[12]指出该方案无法抵御来自恶意服务器的离线关键词猜测攻击。之后, Tang等人[13]提出了一种基于注册关键词的公钥可搜索加密方案(public key encryption with registered keyword search, PERKS), 该方案引入了注册关键词的概念, 要求发送者在生成关键词密文之前, 要先向接收者注册该关键词, 这个方案被证明能抵御离线关键词猜测攻击。

在2007年, Fuhr等人[14]提出了一种支持对关键词密文进行解密运算的公钥可搜索加密方案(Decryptable Searchable Encryption, DSE), 并给出了一种基于KEM(Key Encapsulation Mechanisms)和IDKEMs(identity-based versions of KEMs)的通用构造方案, 然后在随机预言机模型下证明了该方案的安全性。在2008年, Hofheinz等人[15]提出了一种基于匿名IBE的DSE构造方案, 并且在标准模型下证明了该方案的安全性。

在2008年, Baek等人[5]指出文献[2]中的方案需要建立在一个安全信道之上, 因此缺乏实际应用价值。针对该问题, 他们提出了一种无需安全信道的公钥可搜索加密方案, 该方案引入了指定测试者的概念, 要求服务器拥有自己的公私钥对, 以保证在公开信道下的安全通信。之后, Fang等人[16]提出了一种更高效的并且安全性证明不依赖于随机预言机模型的SCF-PEKS方案。

在2010年, Shao等人[17]提出了可搜索代理重加密的概念(Proxy Re-encryption with Keyword Search, PRES), 并构造了一种在随机预言机模型下可证明安全的PRES方案。之后, Yau等人[18]对该概念做了一些改进, 提出了一种新的可搜索代理重加密概念, 并给出了一种基于双线性对的具体构造方案, 同时他们还提出了一种带有指定测试者的PRES方案, 该方案只允许指定的服务器来执行测试算法。

在2012年, Xu等人[19]提出了一种能抵御关键词猜测攻击的模糊关键词公钥可搜索加密方案(public key encryption with fuzzy keyword search, PEFKS), 并且给出了一种基于IBE的具体构造方案。该方案的检索分为两个阶段, 第一个阶段在服务器上进行模糊匹配检索, 然后第二个阶段在本地执行精确的匹配检索。由于攻击者不能获得精确的搜索陷门, 因此该方案能有效抵御关键词猜测攻击。

在2013年, Wang等人[20]提出了一种基于CP-ABE的属性基公钥可搜索加密方案, 该方案将ABE和PEKS相结合, 实现了带有访问控制策略的密文检索功能。同时他们还给出了基于双线性对的构造方案, 并且证明该方案能抵御内部和外部攻击者的攻击。

在2014年, Zheng等人[21]提出了一种可验证的属性基可搜索加密方案(verifiable attribute-based keyword search, VABKS), 该方案把检索操作外包给云服务器的同时, 还可以验证云服务器是否执行了正确的检索操作, 这实现了检索的机密性和完整性。

在2015年, Xu等人[22]提出了一种支持快速关键词检索的PEKS方案, 传统的PEKS方案的检索时间复杂度与总的密文数量成正比, 在该方案中检索的时间复杂度只与包含相关查询关键词的密文数量成正比。同时他们还给出了基于IBE和IBKEM(Identity-Based Key Encapsulation Mechanism)的通用构造方案, 并在随机预言机模型DBDH假设下证明该方案是语义安全的。

在2015年, Emura等人[23]提出了一种支持关键词撤销的公钥可搜索加密方案(keyword revocable public key encryption with keyword search, KR-PEKS), 并给出了基于PA-RIBE(partially-anonymous revocable IBE)的通用构造方案。该方案能抵御陷门泄漏带来的安全风险, 并且在一个关键词被撤销后还可以生成该关键词的陷门。

在2016年, Rhee等人[24]提出了一种支持关键词更新的KU-PEKS(keyword updatable PEKS)体制, 并

给出了一种基于 IBPRE(identity-based proxy re-encryption)的具体构造方案。该方案允许服务器把关键词w的密文CT_w更新为关键词w'的密文$CT_{w'}$, 并且在更新的过程中不会泄漏任何关于关键词的信息。

在 2016 年, Liang 等人[25]提出了一种支持正则语言检索的 PEKS 方案, 他们首先给出了 S-DFA-FE (Searchable Deterministic Finite Automata-based Functional Encryption) 的概念, 然后给出了具体的 S-DFA-FE 构造方案。该方案在支持正则语言检索的同时, 还提供了数据完整性的验证, 并且该方案在构建关键词索引结构时, 不需要数据拥有者提供一些特殊关键词。

在 2016 年, Zhang 等人[26]提出了一种 EPEKS(efficient public-key encryption with keyword search)方案, 并给出了基于素数群的具体构造方案。该方案通过对明文索引排序来实现对基于倒排索引的加密数据进行二分搜索。在安全性方面, 该方案具有统计的 IND-PEKS-CKA 安全和统计的搜索模式隐私性。

总的来说, 公钥可搜索加密经历了如下 3 个阶段:

2004~2005 年, 公钥可搜索加密的起步阶段, 这一阶段的研究工作主要是给出了 PEKS 的形式化定义和安全模型以及相关的应用场景。

2006~2010 年, 公钥可搜索加密的安全性完善阶段, 这个阶段主要研究并解决了 PEKS 的安全性问题, 诸如安全信道问题以及关键词猜测攻击的问题。

2011 年~现在, 公钥可搜索加密的扩展阶段, 在该阶段提出了多种新的扩展方案, 比如一些查询功能扩展的方案以及一些跟其他密码学体制相结合的扩展方案。

表 2 公钥可搜索加密方案的性能对比

方案	私钥长度	密文长度	陷门长度	加密开销	陷门生成开销	搜索开销
Boneh[2]	L_3	$L_1 + L_2$	L_1	$2e + p$	e	p
Baek[5]	L_3	$L_1 + L_2$	L_1	$2e + 2p$	e	$e + p$
Park[9]-1	$2L_3$	$2L_1 + nL_2$	$L_1 + L_3$	$(n + 2)e + np$	e	$e + p$
Park[9]-2	$(n + 2)L_3$	$(2n + 3)\ L_1$	$2L_1 + L_3$	$(3n + 2)e$	$2e$	$e + 2p$
Hwang[40]	L_3	$(n + 2)\ L_1$	$3L_1$	$(2n + 2)e$	$3e$	$3p$
Fang[31]	L_3	$2L_1 + 2L_2$	$L_1 + L_3$	$6e + 3p$	$2e$	$3e + 2p$
Rhee[11]	L_3	$L_1 + L_2$	$2L_1$	$2e + p$	$3e$	$2e + p$
Tang[13]	$L_1 + 2L_3$	$L_1 + L_2$	L_1	$2e + p$	e	p

(注: L_1 表示一个 G_1 中的元素的长度; L_2 表示一个 G_2 中的元素的长度; L_3 表示一个 Z_p^*中的元素的长度; e 表示一次模指数运算的时间开销; p 表示一次双线性对运算的时间开销; n 表示关键词的个数)

表 3 公钥可搜索加密方案的安全性对比

方案	密文不可区分	陷门不可区分	安全信道	抵御关键词猜测攻击	安全模型	困难假设
Boneh[2]	是	否	需要	否	ROM	BDH
Baek[5]	是	否	不需要	否	ROM	BDH
Park[9]-1	是	否	需要	否	ROM	DBDH
Park[9]-2	是	否	需要	否	ROM	DBDHI
Hwang[40]	是	否	需要	否	ROM	DLDH
Fang[31]	是	否	不需要	否	SM	DBDH、ABDHE
Rhee[11]	是	是	不需要	否	ROM	BDH、HDH、BDHI
Tang[13]	是	是	需要	是	ROM	DBDH

(注: ROM 表示随机预言机模型; SM 表示标准模型; BDH 代表 Bilinear Diffie-Hellman assumption; DBDH 代表 Decision Bilinear Diffie-Hellman assumption; BDHI 代表 Bilinear Diffie-Hellman Inversion assumption; DBDHI 代表 Decision Bilinear Diffie-Hellman Inversion assumption; DLDH 代表 Decision Linear Diffie-Hellman assumption; HDH 代表 Hash Diffie-Hellman assumption; ABDHE 代表 Augmented Bilinear Diffie-Hellman Exponent assumption)

5 公钥可搜索加密的安全问题

5.1 关键词猜测攻击及其防御措施

文献[6]首次提出 Boneh 等人[2]的 PEKS 方案存在严重的安全漏洞, 并利用离线关键词猜测攻击攻破了该 PEKS 方案。之后, Yau 等人[52]发现文献[5]中的 SCF-PEKS 方案以及文献[27]中的 PKE/PEKS 方案也存在同样的安全漏洞。

该安全漏洞产生的主要原因是由于关键词空间远小于密钥空间, 并且用户平常只检索一些常用的

关键词。通过进一步的研究, Jeong 等人[28]指出 PEKS 的安全漏洞是由于它的一致性要求导致的, 并指出在关键词集合是多项式大小的情况下, 要构造一个满足一致性要求并且能抵御关键词猜测攻击的 PEKS 方案是不可能的。

为了抵御离线关键词猜测攻击, Rhee 等人[11]提出了陷门不可区分的概念, 构造了一种陷门安全的 dPEKS 方案, 并且在新的安全模型下证明了该方案的安全性。但是, 随后 Wang 等人[12]指出该方案只能抵御外部攻击者的离线关键词猜测攻击, 无法抵御来自恶意服务器的离线关键词猜测攻击。

在 2010 年, Tang 等人[13]提出了 PERKS(public key encryption with registered keyword search) 方案, 该方案引入了注册关键词的概念, 要求发送者在加密关键词之前, 先向接收者注册该关键词, 注册后接收者会生成一个预标签(pre-tag), 然后通过安全信道把它传递给发送者。这个方案被证明能抵御关键词猜测攻击, 但是由于该方案在注册阶段需要使用安全信道, 因此其实用性不强。

在 2013 年, Xu 等人[19]提出了一种能抵御关键词猜测攻击的模糊关键词公钥可搜索加密方案(Public Key Encryption with Fuzzy Keyword Search), 在该方案中服务器只能进行模糊匹配搜索, 精确的匹配搜索在本地执行, 因此攻击者不能获得精确的搜索陷门, 从而确保了方案的安全性。

在 2016 年, Chen 等人[29]为了解决来自恶意服务器的关键词猜测攻击, 提出了 DS-PEKS(Dual-Server Public Key Encryption with Keyword Search)方案, 同时还给出了基于 Lin-Hom SPHF(linear and homomorphic Smooth Projective Hash Function)的通用构造方案, 该方案通过将测试算法分成两部分, 分别让两个独立的服务器来执行, 以此来抵御来自恶意服务器的关键词猜测攻击。

5.2 安全信道问题及其改进

Baek 等人[5]在 2005 年首次指出了文献[2]中的 PEKS 方案需要在邮件接收者和邮件服务器之间建立一个安全信道(secure channel), 用于传输关键词陷门信息。由于该安全信道在实际应用中会带来很大的开销, 针对这个问题, Baek 等人提出了一种不需要安全信道的公钥可搜索加密方案, 该方案引入了指定测试者的概念, 并要求服务器拥有自己的公私钥对, 发送者在加密关键词信息时不但要使用接收者的公钥还要使用服务器的公钥, 以保证在公开信道下的安全通信。

在 2009 年, Rhee 等人[30]指出文献[5]中的 SCF-PEKS 方案的安全模型仍有安全缺陷, 该安全模型假设敌手可以在公开信道上截获陷门信息, 但是没有假设敌手可以获得关键词密文与陷门之间的关系, 这在实际应用场景中是不现实的。针对这个问题, Rhee 等人[30]加强了 SCF-PEKS 方案的安全模型, 并给出了在新的安全模型下的构造方案。

但是以上的 SCF-PEKS 方案仍然有一定的局限性, 因为它们的安全性证明依赖于随机预言机模型。在 2009 年, Fang 等人[31]提出了一种不依赖于随机预言机模型的高效并且安全的 SCF-PEKS 方案, 该方案的安全性是基于 DBDH 和 q-ABDHE 困难性问题。

6 公钥可搜索加密的扩展方案

6.1 功能性扩展

6.1.1 可解密的公钥可搜索加密方案

传统的公钥可搜索加密方案不支持对关键词密文进行解密操作, 但在某些特定的应用场景下需要这些解密功能, 比如邮件接收者想要根据邮件密文的关键词对邮件进行排序, 这时需要解密被加密的关键词信息。针对这个问题, Fuhr 等人[14]提出了一种可解密的公钥可搜索加密方案(Decryptable Searchable Encryption, DSE), 给出了一种基于 KEM(Key Encapsulation Mechanisms)和 IDKEMs(identity-based versions of KEMs)的通用构造方案, 并且在随机预言机模型下证明了该方案的安全性。最后他们提出了一个开放性的问题: 能否构造一个高效的并且安全性不依赖于随机预言机模型的 DSE 方案。在 2008 年, Hofheinz 等人[15]解决了该问题, 提出了一种在标准模型下安全的 DSE 方案, 该方案是基于匿名 IBE 构造的, 并且他们证明了如果匿名 IBE 是 IND-CCA 安全的, 则该 DSE 方案也是 IND-CCA 安全的。在 2012 年, Hu 等人[32]构造了一种能抵御关键词猜测攻击的 dPEKS 方案, 并将它与 DSE 体制相结合, 提出了一种可解密的 dPEKS 方案(Decryptable Searchable Public Key Encryption with a Designated Tester), 该方案在 q-ABDHE 困难问题假设下是 IND-CKA 安全的。

6.1.2 基于属性的公钥可搜索加密方案

在 2013 年, Wang 等人[20]提出了一种基于 CP-ABE 的属性基公钥可搜索加密方案(Attribute Based Encryption with Keyword Search, ABEKS), 该方案允许数据拥有者控制他的数据访问策略, 并且只有满足该访问策略的合法用户才能检索数据。同时他们还给出了基于双线性对的构造方案, 并证明该构造方案能抵御内部攻击者和外部攻击者的攻击。同年, Han 等人[33]提出了一种弱的匿名 ABE 概

念, 并给出了 ABE 与 ABEKS 之间的通用转换关系, 同时他们还给出了一种支持多用户的 ABEKS 构造方案。

在 2014 年, Zheng 等人[21]提出了一种可验证的属性基公钥可搜索加密方案(verifiable attribute-based keyword search, VABKS), 该方案允许数据拥有者根据访问控制策略来检索外包加密数据, 同时还可以验证服务器是否执行了正确的检索操作。同年, Liu 等人[34]指出文献[21]中的方案需要在接收者和服务器之间建立一个安全信道, 这导致该方案缺乏实用性。针对这个问题, 他们提出了一种基于 KP-ABKS (key policy attribute based keyword search)的无需安全信道的 VABKS 方案, 该方案能有效抵御离线关键词猜测攻击。

在 2014 年, Khader 等人[35]提出了一种基于属性的公钥可搜索加密方案的形式化定义, 并且给出了基于 ACKA 攻击(Atrribute-Based Chosen Keyword Attacks)的语义安全模型。与文献[21]中的方案不同, 该方案是基于混合的密文、密钥策略构造的, 这使得该方案更加灵活、安全。

6.1.3 可搜索代理重加密方案

在 2010 年, Shao 等人[17]首次提出了可搜索代理重加密的概念(Proxy Re-Encryption with Keyword Search, PRES), 并构造了一种在随机预言机模型下可证明安全的双向 PRES 方案, 该方案可以被应用在如下的场景中: Bob 利用 Alice 的公钥加密包含某个关键词的邮件密文, 并把该邮件通过邮件服务器发送给 Alice。Alice 由于某些原因无法接收该邮件, 因此她把检索和解密权限代理给了她的助手 Carol, 之后 Carol 能够使用她自己的私钥来检索和解密该邮件。

在 2010 年, Yau 等人[18]在文献[17]的基础上提出了一种新的可搜索代理重加密体制的形式化定义, 给出了基于双线性对的构造方案, 并且在随机预言机模型下证明了该方案的安全性。同时他们还提出了一种带有指定测试者的可搜索代理重加密方案(searchable proxy re-encryption scheme with a designated tester, Re-dPEKS), 该方案只允许指定的服务器来执行测试算法。

在 2011 年, Wang 等人[36]提出了一种支持连接关键词的可搜索代理重加密方案, 并给出了基于双线性对的构造方案, 然后在随机预言机模型下证明了该方案的安全性。在 2012 年, Fang 等人[37]将条件代理重加密体制与公钥可搜索加密体制相结合, 提出了一种可搜索的匿名条件代理重加密方案。在 2013 年, Guo 等人[38]提出了一种不依赖于随机预言机模型的 Re-dPEKS 方案, 该方案的安全性是基于 DBDH 和 QDBDH 困难性问题。并且由于该方案具有陷门不可区分性的性质, 因此它能抵御离线的关键词猜测攻击。在 2014 年, Shi 等人[39]提出了一种基于属性的可搜索代理重加密方案(attribute-based proxy re-encryption with keyword search, ABRKS), 给出了基于密钥策略的 ABRKS 构造方案以及基于密文策略的 ABRKS 构造方案, 并且在随机预言机模型 MDDH 假设(multilinear decisional Diffie-Hellman assumption)下证明了该方案的安全性。

6.2 查询方式扩展

6.2.1 支持多关键词检索

在传统的单关键词公钥可搜索加密方案中, 用户一次只能发送包含一个关键词的陷门。如果用户要进行多关键词查询, 则必须使用不同的关键词进行多轮查询。这样不但效率低, 而且给用户带来了极差的操作体验。针对单关键词检索在实际应用中的不足, Park 等人[9]在 2004 年提出了一种支持连接关键词检索的公钥可搜索加密方案(Public Key Encryption with Conjunctive Field Keyword Search, PECK), 并给出了两种构造方案。第一种构造方案的搜索效率比较高, 其测试算法只需要一个双线性对的计算开销。第二种构造方案的测试算法需要两个双线性对的计算开销, 但其关键词加密算法比第一种构造方案更高效。这两个方案的安全性分别是基于 DBDH(decision bilinear Diffie-Hellman assumption)假设以及 DBDHI(decision bilinear Diffie-Hellman inversion assumption)假设, 并且在随机预言机模型下证明是 IND-CKA 安全的。在 2007 年, Hwang 等人[40]构造了一种高效的 PECK 方案, 并在随机预言机模型 DLDH 假设(decisional linear Diffie-Hellman assumption)下证明了该方案的安全性。与之前的方案相比较, 该方案的密文占用空间较小, 并且只需要存储一个私钥。

为了进一步提高查询的灵活性, Boneh 等人[10]在 2007 年提出了一种支持连接、子集和比较查询的公钥可搜索加密方案, 该方案通过使用 HVE 体制(hidden vector encryption)来实现对加密数据的检索, 其安全性是基于 BDH(Bilinear Diffie-Hellman)困难问题和 C3DH(Composite 3-party Diffie-Hellman)困难问题。从效率上分析, 该方案的加密算法对每个关键词需要 5k+3 个模指数运算开销, 其中 k 是关键词所包含的字符个数, 该方案的密文和陷门的长度与关键词的个数成正比。

在 2013 年, Hu 等人[41]提出了一种支持排序的多

关键词公钥可搜索加密方案(Public-Key Encryption with Ranked Multi-Keyword Search, PERMKS), 该方案能够将符合条件的结果进行排序, 只返回给用户最相关的 k 个文件, 这为用户节省了大量的计算开销, 最后他们还给出了一种基于 AHIBE(anonymous hierarchical identity-based encryption)的构造方案。

在 2015 年, Wang 等人[42]提出了一种基于倒排索引的多关键词公钥可搜索加密方案。由于该方案使用了倒排索引, 只涉及一些乘法运算和指数运算, 因此该方案比基于双线性对的多关键词公钥可搜索加密方案更高效。在安全性方面, 该方案具有索引和陷门的保密性, 并且由于该方案使用了一种高效的不经意传输协议来隐藏访问模式, 因此其安全性也更强。

在 2016 年, Miao 等人[43]提出了一种支持动态数据拥有者的可验证的多关键词公钥可搜索加密方案。该方案在实现多关键词检索和可验证功能的同时, 还允许数据拥有者将其搜索的权利代理给其他授权的数据拥有者, 最后他们在标准模型下证明该方案能抵御关键词猜测攻击。

6.2.2 支持模糊关键词检索

传统的可搜索加密方案只支持精确的关键词检索, 即用户输入的关键词中含有任何微小的错误或者形式不一致都会导致检索失败, 这降低了系统的实用性和用户的搜索体验。针对该问题, 在 2010 年, Li 等人[44]首次提出了支持模糊关键词查询的可搜索加密方案, 在方案的构造中使用了编辑距离的概念来测量关键词的相似度, 并且使用了一种新的技术来构造基于通配符的模糊关键词集合。在 2011 年, Liu 等人[45]在文献[44]的基础上提出了基于字典的模糊关键词集合, 该改进减小了索引的存储空间消耗。

但是以上的方案都是对称的可搜索加密方案, 下面是一些支持模糊关键词的公钥可搜索加密方案。

在 2012 年, Bringer 等人[46]在文献[47]的基础上, 提出了一种基于编辑距离的模糊关键词公钥可搜索加密方案, 该方案中的模糊是指能容忍一些关键词编辑距离的偏差。同年, Xu 等人[19]提出了一种支持模糊关键词搜索的公钥可搜索加密方案(PEFKS), 并且证明该方案在选择关键词攻击和关键词猜测攻击下是安全的, 同时他们还给出了 PEFKS 体制与基于身份的加密体制之间的转化关系。

在 2013 年, Dong 等人[48]也提出了一种基于同态加密的交互式模糊关键词公钥可搜索加密方案, 并证明该方案在适应性选择关键词攻击下是安全的, 最后通过效率分析对比得出该方案比文献[44,46]中的方案都要高效。

7 公钥可搜索加密的应用研究

7.1 邮件路由

这个应用场景最早由 Boneh 等人[2]提出, 在该应用场景中有三个参与方: 发送方、接收方和邮件服务器。假定接收方 Alice 希望通过使用笔记本电脑、台式电脑、手机等设备来阅读她的邮件。邮件服务器会通过邮件所包含的关键词来将邮件发送到合适的设备上。例如, 当发送方 Bob 发送一个包含“urgent”关键词的邮件时, 那么该邮件将被发送到 Alice 的手机上。当 Bob 发送一个包含“lunch”关键词的邮件时, 该邮件将被发送到 Alice 的台式电脑上。

在 Boneh 等人[2]的方案中, 发送方 Bob 使用接收者 Alice 的公钥加密一封邮件以及相应的关键词, 然后把加密后的数据发送给邮件服务器。接收者 Alice 使用自己的私钥生成关于某个关键词的陷门信息, 通过向邮件服务器发送该陷门信息来检索邮件密文, 同时保证在检索过程中不会泄漏数据的隐私信息。

文献[2]中的 PEKS 方案所考虑的应用场景是针对多发送者-单接收者的情况。在文献[40]中提出了一种新的应用场景, 即多发送者-多接收者的邮件路由场景。在该方案中, 发送方使用多个接收者的公钥对邮件进行一次加密, 然后把这份密文分别发送给多个接收者, 这避免了分别使用多个接收者的公钥单独对邮件进行加密而带来的重复计算开销。

7.2 审计日志

在 2004 年, Waters 等人[49]提出了公钥可搜索加密方案的另一个应用场景: 安全审计日志。在该应用场景中主要涉及三个参与方, 分别为不可信的云服务器、查询者以及可信的审计机构。

某一家公司将自己的审计日志信息存储在不可信的云服务器中, 并使用公钥对该审计日志和相应的关键词信息进行加密, 由可信的审计机构来管理私钥。当查询者想要查询关于某个关键词的信息时, 需要向该审计机构提出授权申请, 如果该审计机构认为可以授权, 则使用私钥生成一个陷门信息并把它发送给查询者, 查询者使用该陷门信息在存储审计日志的云服务器上搜索到所需要的信息。

这个应用场景与邮件路由应用场景的主要不同点在于, 在该应用场景中由可信第三方来生成搜索陷门, 而不是由查询者自己来生成搜索陷门。

7.3 云存储文件安全检索

云存储服务是公钥可搜索加密另一个重要的应

用场景, 在该应用场景中公钥可搜索加密提供了安全的数据存储以及数据检索功能, 其中涉及到三个参与方: 云服务器、数据拥有者和用户。

云服务器提供第三方的数据存储以及检索服务。由于云服务器往往是不可信的, 并且存放在其上的数据可能包含用户的个人敏感信息。因此, 出于安全性的考虑, 云服务器上的数据文件必须先进行加密, 以保证数据存储的机密性。当用户想要搜索包含特定关键词的数据时, 用户会经过数据拥有者的授权得到相应的搜索凭证, 然后在云服务器上进行关键词检索。云服务器对存储在本地的密文文件进行匹配检索, 如果匹配成功, 则说明该密文中包含用户要检索的关键词。

采用公钥可搜索加密方案的云存储系统节约了用户大量的通信开销和存储开销。用户可以直接检索到自己感兴趣的密文, 下载到本地并进行解密操作, 而无需把密文文件全部下到本地, 然后再一一解密。

8 总结与展望

随着互联网技术的不断发展, 越来越多的企业和个人用户已经把数据存储在第三方云服务器上, 由于云服务器一般不是完全可信任的, 因此数据一般以密文的形式存储在云服务器中。如何在密文数据上进行高效地检索成为了一个急需解决的问题, 一种普遍的解决方案就是使用公钥可搜索加密技术。本文主要介绍了公钥可搜索加密的概念和一些应用场景以及国内外的研究现状, 并且详细论述了 PEKS 方案的安全性问题及其解决方案和一些查询功能扩展等方面的研究成果。

虽然目前已经存在大量研究公钥可搜索加密体制的文献, 并且公钥可搜索加密体制也日益完善, 但仍然还有很多需要进一步研究的问题, 其中主要包括:

1) 构造高效且支持复杂查询语句的公钥可搜索加密方案。以往提出的支持复杂查询语句的公钥可搜索加密方案往往效率较低, 如文献[9, 10]中的多关键词可搜索加密方案, 其加密算法的运算复杂度和密文的长度与关键词个数成正比, 这导致这些方案难以在海量数据的应用场景中使用。

2) 构造高效且安全的公钥可搜索加密方案。虽然文献[13,19]中的方案能够抵御关键词猜测攻击, 但是这些方案在性能上并不是很高效, 缺乏一定的实用性。因此设计一种安全且高效的 PEKS 方案将是未来需要解决的问题。

3) 构造可验证的公钥可搜索加密方案, 可验证功能可以确保检索结果的正确性和完整性。在文献[50,51]中分别提出了可验证的对称可搜索加密方案和可验证的支持数据更新的对称可搜索加密方案, 但这两个方案都是采用对称加密体制设计的, 如何设计可验证的公钥可搜索加密方案仍然是未来需要研究的内容。

4) 构造支持关键词排序的公钥可搜索加密方案。在对称加密体制下, 已有较多研究成果[53-55], 但如何在公钥加密体制下设计支持关键词排序的 PEKS 方案仍然是未来需要解决的问题。

参考文献

[1] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in *Proc. IEEE Symposium on Security and Privacy (S&P 2000)*, pp. 44-55, 2000.

[2] D. Boneh, G. Di Crescenzo, R. Ostrovsky, et al, “Public key encryption with keyword search,” in *Proc. Advances in Cryptology-Eurocrypt 2004 (*Eurocrypt’04*)*, pp. 506-522, 2004.

[3] Z.R. Shen, W. Xue and J.W. Shu, “Survey on the research and development of searchable encryption schemes,” *Journal of Software*, vol. 25, no. 4, pp. 880-895(in Chinese), 2014.
(沈志荣, 薛巍, 舒继武, “可搜索加密机制研究与进展”, *软件学报*, 2014, 25(4):880-895。)

[4] J.W. Li, C.F Jia, Z.L. Liu, et al, “Survey on the Searchable Encryption,” *Journal of Software*, vol. 26, no. 01, pp. 109-128(in Chinese), 2015.
(李经纬, 贾春福, 刘哲理, 等, “可搜索加密技术研究综述”, *软件学报*, 2015, 26(01):109-128。)

[5] J. Baek, R. Safiavi-Naini, W. Susilo, “Public key encryption with keyword search revisited,” in *Proc. Computational Science and Its Applications (ICCSA’08)*, pp. 1249-1259, 2008.

[6] J.W. Byun, H.S. Rhee, H.A. Park, et al, “Off-line keyword guessing attacks on recent keyword search schemes over encrypted data,” in *Secure Data Management (SDM’06)*, pp. 75-83, 2006.

[7] M. Abdalla, M. Bellare, D. Catalano, et al, “Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions,” in *Proc. Advances in Cryptology–CRYPTO 2005*, pp. 205-222, 2005.

[8] D. Khader, “Public key encryption with keyword search based on K-resilient IBE,” in *International Conference on Computational Science and Its Applications (ICCSA 2006)*, pp. 298-308, 2006.

[9] D. Park, K. Kim, and P. Lee, “Public key encryption with conjunctive field keyword search,” in *Information Security Applications: 5th International Workshop (WISA’04)*, pp. 23-25, 2004.

[10] D. Boneh, and B. Waters, “Conjunctive, subset and range queries

on encrypted data", in *Proc. Theory of Cryptography (TCC'07)*, pp. 535-554, 2007.

[11] H. Rhee, J. Park, W. Susilo, et al, "Trapdoor security in a searchable public-key encryption scheme with a designated tester," *Journal of Systems and Software*, vol. 83, no. 5, pp. 763-771, 2010.

[12] B.J. Wang, T.H. Chen, and F.G. Jeng, "Security improvement against malicious server's attack for a dPEKS scheme," *International Journal of Information and Education Technology*, vol. 1, no. 4, pp. 350-353, 2011.

[13] Q. Tang, and L. Chen, "Public-Key encryption with registered keyword search," in *Proc. Public Key Infrastructures, Services and Applications: 6th European Workshop (EuroPKI 2009)*, pp. 163-178, 2010.

[14] T. Fuhr, and P. Paillier, "Decryptable searchable encryption," in *Proc. International Conference on Provable Security* (ProvSec 2007), pp. 228-236, 2007.

[15] D. Hofheinz, and E. Weinreb, "Searchable encryption with decryption in the standard model," *IACR Cryptology ePrint Archive*, 2008.

[16] L. Fang, J. Wang, C. Ge, et al, "Decryptable public key encryption with keyword search schemes," *Journal of Digital Content Technology and its Applications*, vol. 4, no. 9, pp. 141-150, 2010.

[17] J. Shao, Z.F. Cao, X.H. Liang, and H. Lin, "Proxy re-encryption with keyword search," *Information Sciences*, vol. 180, no. 13, pp. 2576-2587, 2010.

[18] W.C. Yau, R.C.W. Phan, S.H. Heng, and B.M. Goi, "Proxy re-encryption with keyword search: new definitions and algorithms," in *Security Technology, Disaster Recovery and Business Continuity (SecTech and DRBC 2010)*, pp. 149-160, 2010.

[19] P. Xu, H. Jin, Q. Wu, and W. Wang, "Public-key encryption with fuzzy keyword search: A provably secure scheme under keyword guessing attack," *IEEE Transactions on Computers*, vol. 62, no. 11, pp. 2266-2277, 2013.

[20] C. Wang, W. Li, Y. Li, and X. Xu, "A ciphertext-policy attribute-based encryption scheme supporting keyword search function," in *Cyberspace Safety and Security* (CSS 2013), pp. 377-386, 2013.

[21] Q. Zheng, S. Xu, and G. Ateniese, "VABKS: Verifiable attribute-based keyword search over outsourced encrypted data," in *Proc. IEEE Conference on Computer Communications(Infocom 2014)*, pp. 522-530, 2014.

[22] P. Xu, Q. Wu, W. Wang, et al, "Generating searchable public-key ciphertexts with hidden structures for fast keyword search," *IEEE Transactions on Information Forensics & Security*, vol. 10, no. 9, pp. 1-1, 2015.

[23] K. Emura, Y. Watanabe, "Keyword revocable searchable encryption with trapdoor exposure resistance and re-generateability," in *Proc. International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2015)*, pp. 736-744, 2015.

[24] H.S. Rhee, H.L. Dong, "Keyword Updatable PEKS," in *International Workshop on Information Security Applications (WISA 2015)*, pp. 96-109, 2015.

[25] K. Liang, X. Huang, F. Guo, et al, "Privacy-preserving an regular language search over encrypted cloud data," in Proc. *IEEE Transactions on Information Forensics & Security (TIFS)*, pp. 1-1, 2016.

[26] R. Zhang, R. Xue, "Efficient keyword search for public-key setting," in *Proc. Military Communications Conference (MILCOM 2015)*, pp. 1236-1241, 2015.

[27] J. Baek, R. Safavi-Naini, and W. Susilo, "On the Integration of Public Key Data Encryption and Public Key Encryption with Keyword Search," in *Proc. Information Security (ISC 2006)*, pp. 217-232, 2006.

[28] I.R. Jeong, J.O. Kwon, D. Hong, and D.H. Lee, "Constructing peks schemes secure against keyword guessing attacks is possible?," *Computer Communications*, vol. 32, no. 2, pp. 394-396, 2009.

[29] R. Chen, Y. Mu, G. Yang, et al, "Dual-server public-key encryption with keyword search for secure cloud storage," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 789-798, 2016.

[30] H.S. Rhee, J.H. Park, W. Susilo, and D.H. Lee, "Improved searchable public key encryption with designated tester," in *Proc. International Symposium on Information, Computer, and Communications Security (ASIACCS 2009)*, pp. 376-379, 2009.

[31] L. Fang, W. Susilo, C. Ge, and J. Wang, "A Secure Channel Free Public Key Encryption With Keyword Search Scheme Without Random Oracle," in *Proc. Cryptology and Network Security (CANS 2009)*, pp. 248-258, 2009.

[32] C. Hu, and P. Liu, "An enhanced searchable public key encryption scheme with a designated tester and its extensions," *Journal of Computers*, vol. 7, no. 3, pp. 716-723, 2012.

[33] H. Fei, J. Qing, H. Zhao, and J. Hu, "A general transformation from kp-abe to searchale encryption," in *Cyberspace Safety and Security (CSS 2012)*, pp. 165-178, 2012.

[34] P. Liu, J. Wang, H. Ma, and H. Nie, "Efficient veriable public key encryption with keyword search based on KP-ABE," in *Ninth International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA 2014)*, pp. 584-589, 2014.

[35] D. Khader, "Introduction to attribute based searchable encryption," in *Proceedings of 15th international conference on communications and multimedia security (CMS 2014)*, pp. 131-135, 2014.

[36] X.A. Wang, X. Huang, X. Yang, L. Liu, and X. Wu, "Further observation on proxy re-encryption with keyword search," *Journal of Systems and Software*, vol. 85, no. 3, pp. 643-654, 2012.

[37] L. Fang, W. Susilo, C. Ge, and J. Wang, "Chosen-ciphertext secure anonymous conditional proxy re-encryption with keyword search,"

Theoretical Computer Science, vol. 462, pp. 39-58, 2012.

[38] L. Guo, B. Lu, X. Li, et al, "A Verifiable proxy re-encryption with keyword search without Random Oracle," in *Proc. Computational Intelligence and Security (CIS 2013)*, pp. 474-478, 2013.

[39] Y. Shi, J. Liu, Z. Han, Q. Zheng, R. Zhang, and S. Qiu, "Attribute-based proxy re-encryption with keyword search," *PloS One*, vol. 9, no. 12, 2014.

[40] Y.H. Hwang, and P.J. Lee, "Public key encryption with conjunctive keyword search and its extension to a multi-user system," in *Proc. Pairing-Based Cryptography (Pairing 2007)*, pp. 2-22, 2007.

[41] C. Hu, and P. Liu, "Public key encryption with ranked multi-keyword search," in *Intelligent Networking and Collaborative Systems (INCoS)*, pp. 109-113, 2013.

[42] B. Wang, W. Song, W. Lou, et al, "Inverted index based multi-keyword public-key searchable encryption with strong privacy guarantee," in Proc. *IEEE Conference on Computer Communications (INFOCOM)*, pp. 2092-2100, 2015.

[43] Y. Miao, J. Ma, X. Liu, et al, "VMKDO:Verifiable multi-keyword search over encrypted cloud data for dynamic data-owner," in *Proc. Peer-to-Peer Networking and Applications (P2PNA 2016)*, pp. 1-11, 2016.

[44] J. Li, Q. Wang, C. WANG, et al, "Fuzzy keyword search over encrypted data in cloud computing," in *Proceedings of the 29th Conference on Information Communications (INFOCOM 2010)*, pp. 441-445, 2010.

[45] C. Liu, L. Zhu, L. Li, et al, "Fuzzy keyword search on encrypted cloud storage data with small index," in *Proceedings of the 2011 IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS 2011)*, pp. 269-273, 2011.

[46] J. Bringer, and H. Chabanne, "Embedding edit distance to enable private keyword search," *Human-centric Computing and Information Science*, vol. 2, no. 1, pp. 1-12, 2012.

[47] R. Ostrovsky, Y. Rabani, "Low distortion embeddings for edit distance," in *Proceedings of the Thirty-Seventh Annual ACM Symposium on Theory of Computing(STOC 2005)*, pp. 218-224, 2005.

[48] Q. Dong, Z. Guan, L. Wu, and Z. Chen, "Fuzzy keyword search over encrypted data in the public key setting," in *Web-Age Information Management (WAIM 2013)*, pp. 729-740, 2013.

[49] B. Waters, D. Balfanz, G. Durfee, and D. Smetters, "Building an encrypted and searchable audit log," in *Annual Network & Distributed System Security Symposium (NDSS'04)*, vol. 4, pp. 5-6, 2003.

[50] Q. Chai, G. Gong, "Verifiable symmetric searchable encryption for semi-honest-but-curious cloud servers," in *Proc. IEEE International Conference on Communications (ICC)*, pp. 917-922, 2012.

[51] K. Kurosawa, Y. Ohtaki, "How to Update Documents Verifiably in Searchable Symmetric Encryption," in *Proc. International Conference on Cryptology and Network Security (ICCNS 2013)*, pp. 309-328, 2013.

[52] W.C. Yau, S.H. Heng, B.M. Goi, "Off-Line Keyword Guessing Attacks on Recent Public Key Encryption with Keyword Search Schemes," in *Proc. International Conference on Autonomic and Trusted Computing (ATC 2008)*, pp. 100-105, 2008.

[53] N. Cao, C. Wang, M. Li, et al, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," *IEEE Transactions on Parallel and Distributed System*, vol. 25, no. 1, pp. 222-233, 2013.

[54] C. Wang, N. Cao, J. Li, et al, "Secure Ranked Keyword Search over Encrypted Cloud Data," in *Proc. International Conference on Distributed Computing Systems(ICDCS 2010)*, pp. 253-262, 2010.

[55] N. Zhang, L.X. Chen, "Research on An Efficient Ranked Keywords Searchable Encryption System," *Netinfo Security*, vol. 2, pp. 43-50(in Chinese), 2017.
(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", *信息网络安全*, 2017, 2:43-50。)

秦志光 于 1996 年在电子科技大学计算机应用技术专业获得博士学位。现任电子科技大学信息与软件工程学院院长。研究领域为网络安全、网络计算。研究兴趣包括: 网络与信息系统安全。Email: qinzg@uestc.edu.cn

徐骏 于 2013 年在天津理工大学数学与应用数学专业获得学士学位。现在电子科技大学软件工程专业攻读硕士学位。研究领域为信息安全、软件工程。研究兴趣包括: 可搜索加密。Email: xujun130657@163.com

聂旭云 于 2007 年在中科院研究生院信息安全国家重点实验室获得博士学位。现任电子科技大学信息与软件工程学院副教授。研究领域为信息安全、密码学。研究兴趣包括: 多变量公钥密码学、云计算安全。Email: xynie@uestc.edu.cn

熊虎 于 2009 年在电子科技大学信息与通信工程专业获得博士学位。现任电子科技大学信息与软件工程学院副教授。研究领域为信息安全、公钥密码学。研究兴趣包括: 属性基加密。Email: xionghu.uestc@gmail.com