

可搜索加密的研究进展

徐鹏^{1,2,3}, 金海^{1,2,3}

- (1. 华中科技大学计算机科学与技术学院服务计算技术与系统教育部重点实验室, 湖北 武汉 430074;
2. 华中科技大学计算机科学与技术学院集群与网格计算湖北省重点实验室, 湖北 武汉 430074;
3. 华中科技大学计算机科学与技术学院湖北省大数据技术与系统工程实验室, 湖北 武汉 430074)

摘要: 可搜索加密是解决云端不可信条件下加密数据安全云检索的重要方法。针对可搜索公钥加密、可搜索对称加密这2种可搜索加密类型, 分别介绍了近几年来学术界的主要成果及其存在的问题、解决方法。在可搜索公钥加密领域, 主要介绍了高安全条件下降低检索复杂度的方法; 在可搜索对称加密领域, 主要介绍了高安全条件下支持物理删除的方法。

关键词: 可搜索加密; 云安全; 可搜索公钥加密; 可搜索对称加密

中图分类号: TP309.2

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00101

Research on the searchable encryption

XU Peng^{1,2,3}, JIN Hai^{1,2,3}

- (1. Services Computing Technology and System Lab, School of Computer Science and Technology,
Huazhong University of Science and Technology, Wuhan 430074, China;
2. Cluster and Grid Computing Lab, School of Computer Science and Technology,
Huazhong University of Science and Technology, Wuhan 430074, China;
3. Big Data Technology and System Lab, School of Computer Science and Technology,
Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: Searchable encryption has been recognized as a promising method to achieve the secure cloud search. According to the types of encryption keys, searchable encryption can be divided into searchable public-key and symmetric-key encryptions. The existing and well-known schemes of those two kinds of encryptions, their limitations, and the corresponding solutions were introduced. Specifically, two works under the condition of high security were introduced: one was to reduce the search complexity of searchable public-key encryption; the other one was to achieve the physical deletion of searchable symmetric-key ciphertexts.

Key words: searchable encryption, cloud security, searchable public-key encryption, searchable symmetric-key encryption

1 引言

近年来, 云计算和网络的快速发展使用户可

以将自身的数据存放在云端, 以节省自身的开销、实现便捷的多点访问。同时, 为了保证数据安全和用户隐私, 用户敏感数据通常需要加密后以密

收稿日期: 2016-08-12; 修回日期: 2016-09-27。通信作者: 徐鹏, xupeng@mail.hust.edu.cn

基金项目: 国家重点基础研究发展计划 (“973”项目) 基金资助项目 (No.2014CB340600); 国家自然科学基金面上基金资助项目 (No.61472156)

Foundation Items: The National Basic Research Program of China (973 Program)(No.2014CB340600), The National Natural Science Foundation of China (No.61472156)

文存储在云端服务器中。例如,采用代理重加密和基于属性加密实现云数据的加密存储与共享等。这些加密方法可以在云端不可信的条件下,实现用户数据的保密性。但是,加密云存储的方法也使用户无法便捷地从云端提取出满足某查询条件的云密文。

在传统的密文存储和查询服务中,由于云端没有检索功能,不能根据用户需求查找数据,只能将全部密文都返回给用户,用户解密后自行检索才能得到想要的结果。显然,这种处理方法在实际应用中是不能被接受的。因此,如何在用户提交检索请求时,云端能实现高效率检索并返回指定的密文是云数据安全存储的重要问题和需求。

2 可搜索加密

为了在保证用户数据机密性的同时实现安全和高效的密文数据访问,可搜索加密(SE, searchable encryption)被提出。SE是近年来快速发展的一种支持用户在密文上进行关键字查找的密码学原语,它能实现云端在不解密密文的情况下,完成对密文的检索工作。SE一般分为如下4个阶段。

1) 数据加密阶段:数据拥有者在本地使用密钥对明文数据进行加密,然后将加密后的数据上传至服务器。

2) 生成检索陷门阶段:用户使用密钥和关键字生成对应的检索陷门,并将该陷门发送给云端,其中检索陷门能保密其包含的关键字内容。

3) 密文检索阶段:根据收到的关键字检索陷门,云端对密文进行检索,并将满足检索条件的密文发送给用户,执行过程中云端不能获得除检索结果之外的更多信息。

4) 密文解密阶段:用户从云端获得返回的密文后,使用密钥解密出相关数据。

目前,根据密钥类型的不同,SE可以分为可搜索对称加密(SSE, searchable symmetric encryption)和可搜索公钥加密(PEKS, public-key encryption with keyword search)。

3 可搜索对称加密

绝大多数情况下,SSE也可称为关键字可搜

索对称密钥加密(SEKS, symmetric-key encryption with keyword search)。其核心是以对称加密形式生成关键字的可搜索密文和检索陷门。

3.1 SSE的定义

SSE的实例化方案通常基于伪随机函数构造,具有计算量小、算法简单、计算速度快等优点。安全的SSE方案能确保关键字的保密性,能抵御外部攻击和抵御来自云端的内部信息泄露。

SSE的定义^[1]。给定关键字空间 $\Delta=(W_1, W_2, \dots, W_n)$, SSE方案由5个算法组成,即 $SSE=(Keygen, Enc, Trapdoor, Search, Dec)$,各算法含义如下。

1) $K=KeyGen(k)$: 输入安全参数 k , 输出随机产生的密钥 K 。

2) $(I, C)=Enc(K, D)$: 输入密钥 K 和明文文件集 $D=(D_1, D_2, \dots, D_n)$, 输出索引和密文文件集(对于无需构造索引SSE的方案,如SWP方案^[2],索引为空)。

3) $T_w=Trapdoor(K, W)$: 输入密钥 K 和关键词 W , 输出关键字对应的陷门。

4) $D(W)=Search(I, T_w)$: 输入索引 I 和待搜索关键字的陷门 T_w , 输出包含关键字 W 的文件的标识符集合。

5) $D_i=Dec(K, C_i)$: 输入密钥 K 和密文文件 C_i , 输出解密后对应的明文文件 D_i 。

3.2 SSE的相关研究

2000年, Song等^[2]提出了第一个基于对称加密的密文检索方案,但无法实现可证明的安全性,而且检索性能与数据库规模线性相关。随后,很多工作^[3-6]遵循这一研究路线并且不断改善Song等的初始方案。Goh等^[3]提出了用布隆过滤器为每个文件构造一个索引的方法。该方法将文件包含的关键词映射到码字存储的索引中,通过布隆过滤器的运算,就能判定密文文件是否包含某个特定关键词,从而将搜索请求的计算代价减少到和密文文件数量成正比。Chang等^[4]提出了一个和Goh类似的方案,不同的是他们没有采用布隆过滤器。这些后续工作虽然提高了搜索效率,但依然无法实现主动攻击下的可证明的语义安全性。在强可证明安全的条件下,2006年, Curtmola等^[1]提出了目前性能最优的可检索对称加密,但该方案的检索陷门长度和文档的最大数量线性相

关, 因此增加了通信开销。除了致力于可证明安全性或者更好的检索性能, 实现检索的多样化逐渐受到人们的重视。Waters 等^[7]的工作展示了 SEKS 的实际运用, 并且利用它实现了安全和可搜索的审计日志系统。文献[8~11]将 SSE 应用到加密数据库。文献[12]指出早期的这类工作在安全性上存在无法衡量的问题。文献[13,14]将 SSE 方案拓展到多发送者。文献[15,16]对这些多样化查询方案进行了有效的改进。文献[17~19]实现了关键字的模糊搜索。文献[20~23]实现了多关键字排列查询和多维范围查询。Lu 等^[24]通过构建索引结构提高了范围检索的搜索效率。Boldyreva 等^[25]首次研究了对称加密原语并提出了可证明安全的保序方案。Chase 等^[26]首次研究了结构化数据的可搜索对称加密。

近几年来, 动态的 SSE 研究受到了广泛关注。2012 年, Kamara 等^[27]首次提出了支持动态更新的可搜索对称加密 (DSSE, dynamic searchable symmetric encryption) 方案, 并且形式化定义了 DSSE 的安全性。DSSE 不仅支持密文检索, 还支持可搜索密文的动态更新操作, 如密文添加、密文删除、关键字添加删除。然而, 文献[27]的方案在添加和删除操作中存在较多隐私信息泄露。针对这个问题, Kamara 等在文献[28]中提出基于红黑二叉树的 DSSE 方案, 该方案通过构造树型索引解决了文献[27]存在的问题, 但该方案增加了可搜索密文长度并且降低了检索效率。Cash 等在文献[29]中采用累加器的思想构造了一个新的方案, 保证了检索效率和可搜索密文在动态更新时的安全性。由于累加器自增不自减的天然特性, 可搜索密文的数量会只增不减。2014 年, Hahn 等^[30]提出了新的 DSSE 方案来解决已有方案存在的问题, 该方案在初始化时不构建可搜索密文结构, 而是在检索和更新过程中不断更新可搜索密文索引结构。

4 本文提出的 SSE 方案

本文调研了当前 SSE 领域的研究现状, 详细分析了近年来提出的方案和知名的 SSE 方案的优缺点, 提出了支持低泄露和物理删除的 DSSE 方案。本文的 SSE 方案在检索效率、动态更新的粒

度、可搜索密文的删除能力和安全性方面均达到了同类方案的最优。

4.1 核心理想

在标准的 DSSE 方案应用案例中, 每个文件都有一个标识符和几个对应的关键字。通常使用一个文件标识符—关键字对 (id, W) , 表示标识符为 id 的文件包含关键字 W 。假设数据库 DB 就是由所有的标识符—关键字对组成的。在本文的方案中, 对于每一个数据库中的标识符—关键字对, 都会为其生成 3 种可搜索密文, 分别是 K_1 、 K_2 、 K_3 。这 3 个可搜索密文分别对应搜索、删除文件和删除关键字这 3 个功能的实现。包含相同关键字的可搜索密文和相同文件的可搜索密文会各形成一条隐藏链结构。图 1 展示了如何生成 3 种密文的过程, 包括它们之间的隐藏关系链。图 2 展示了同一个关键字的所有 K_1 密文构成一条隐藏的关系链, 和同一个文件的标识符的所有 K_2 密文也构成一条隐藏关系链。 K_3 密文之间不存在任何隐藏关系。

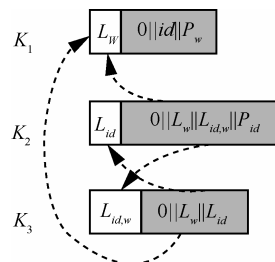


图 1 关键字—标识符对 (id, W) 生成的密文

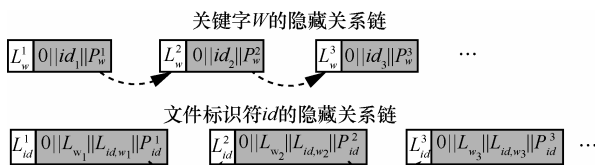


图 2 密文之间隐藏关系链

当进行关键字搜索时, 输入待搜索关键字陷门后, 寻找到对应的关键字的隐藏关系链; 在隐藏关系链的引导下, 能快速查找到该关键字匹配的剩余 K_1 密文; 通过解密 K_1 密文, 获得包含查询关键字的文件标识符。本文生成的 K_1 密文不同于 KPR'12 中提到的隐藏关系链, 因为初始化隐藏关系链时, 并不需要生成确定性的关系链头部。在本文的 DSSE 方案中, 当某关键字第一次出现时, 其对应的隐藏关系链的头部才生成。换言之,

在本文的方案中，每一条隐藏关系链的头部就是一个密文，因此，节约了关系链头部的存储空间。

当给已经存在的文件 id 添加一个新的关键字 W' 时，将会生成关键字—标识符对 (id, W') 3 个对应的密文；并将生成的 K_1 密文添加到链的末尾；同样地，生成的 K_2 密文将会被添加到 W' 链的末尾。总的来说，本文的方案在添加密文时，采取的都是将生成的密文添加到隐藏链的尾部，而不是在中部添加。因此，不同于 KPR'12 采取的在中部添加密文的方案，本文的方案泄露信息较少。

与 KPR'12 相比较，本文工作面临的最大的挑战就是实现文件和其某个关键字的物理删除，并且确保低泄露和隐私安全。简单来说，这 2 种删除功能都是用于将密文从隐藏关系链中删除。如果直接实现物理删除，那么在删除后必须修复由于删除而破坏的隐藏关系链。例如，图 2 展示的关键字隐藏链中的第 2 个密文被删除后，为了修复破坏的隐藏关系链，就必须知道 L_w^1 和 L_w^3 的具体值，然后设置 $L_w^1 = L_w^3$ 。这些操作将会泄露一些信息，如标签 L_w^1 、 L_w^3 和待删除的标签 L_w^2 处于同一个隐藏密文链中。最坏的情况下，隐藏链中所有密文都会被泄露。为了克服这个问题，本文采用逻辑删除和物理删除相配合的方法避免泄露较多的信息。

当需要删除一个标识符—关键字对 (id, W) 的所有可搜索密文时，服务器快速发现关键字对应的 K_3 密文，通过解密后得到指向 K_1 密文和 K_2 密文的索引；再通过将对应密文标志位置“1”的方式实现对这 2 个 K_1 和 K_2 密文的逻辑删除；最后，物理删除上述 K_3 密文。

当需要删除指定文件的所有可搜索密文时，服务器快速查找到文件 id 的隐藏链；根据这个隐藏关系链，所有的 K_2 密文将被快速查找到。从图 1 可看出，每个 K_2 密文可解密出 2 个索引，分别指向 K_1 和 K_3 密文；最后， K_2 密文指向的 K_1 密文

都会被逻辑删除， K_2 密文和 K_3 密文都将被物理删除。

本文目的是实现 K_1 密文的物理删除。在检索阶段，若检测到某 K_1 密文的逻辑删除标签位为“1”，则将 K_1 进行物理删除，并修复隐藏关系链。这样的方法不会泄露额外信息，因为搜索过程本身的泄露信息足以用来修复由于物理删除所破坏的隐藏关系链。简而言之，在本文提出的方案中，可搜索密文的完整删除过程包含有 2 个队伍：在删除阶段仅实现密文的逻辑删除；在检索阶段实现密文的物理删除。逻辑删除和物理删除相配合使用，保证删除操作的高安全性。

4.2 方案对比

本文提出的支持低泄露和物理删除的 DSSE 方案实现了更细致的功能。表 1 对比了已有的 DSSE 方案和本文提出的方案。本文提出方案在检索效率和存储开销方面均达到了目前最优的指标；在功能性方面，实现了文件添加、关键字添加、文件和关键字的物理删除。

5 可搜索公钥加密

在 SSE 中，由于对称密码体制自身的限制，通常在多用户场景下，用户之间具有事前构建某种安全信道来传递秘密信息，进而实现数据的加密上传与检索。相比之下，基于公钥密码体制的可搜索加密则无需事先建立安全信道就可以实现用户在公共网络中的保密通信和安全检索。

5.1 PEKS 的提出

2004 年，Boneh^[31]以加密邮件系统的检索问题为出发点，首次提出了 PEKS 的概念和实例化方案，从而初步实现了在不泄露邮件内容和关键字的条件下，邮件服务器对加密邮件的关键字检索。图 3 所示为 PEKS 在邮件加密系统中的一个应用场景。

表 1 DSSE 方案功能对比

方案	检索开销	存储开销	文件添加	关键字添加	文件删除	关键字删除	信息泄露
文献[12]方案	低	中	√	×	物理删除	×	大
文献[13]方案	中	高	√	×	物理删除	×	中
文献[14]方案	低	低	√	√	×	逻辑删除	小
文献[30]方案	高	中	√	×	物理删除	×	小
本文方案	低	低	√	√	物理删除	物理删除	小

在实际应用中, PEKS 的典型应用场景由多个发送方、一个服务器和一个接收方组成。任意发送方可以采用接收方的公钥生成关键字可搜索密文, 并发送给服务器; 接收方可以为指定关键字生成检索陷门并发送给服务器; 服务器检索出含有指定关键字的密文并返还给接收者。可以看出, 由于 PEKS 的公钥特点, 发送方不需要和接收方有任何的交互就可以生成关键字可搜索密文。但是, 在 SSE 中, 发送方必须事先和接收方建立安全信道, 协商某种共享秘密, 才能生成关键字可搜索密文。因此, 在 SSE 的应用中, 发送方和接收方必须同时在线。相反地, PEKS 适用于发送方和接收方不能保证同时在线的场景。例如, 在邮件系统中发送方和接收方不需要同时在线。

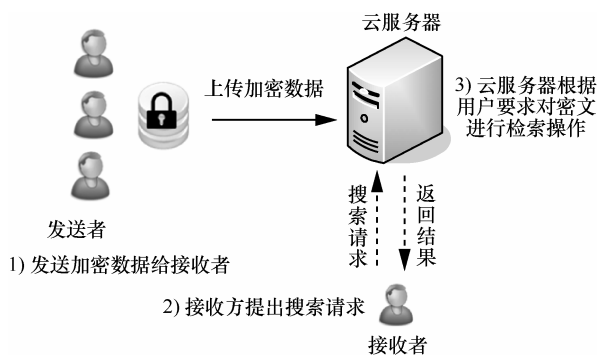


图3 PEKS 应用场景

5.2 PEKS 的概念

以图3所示的应用场景为例, PEKS 由以下4个多项式时间算法组成。

1) 系统初始化算法: 输入一个安全参数, 系统生成接收方的一组公私密钥对, 私钥由接收方秘密保存, 公钥公开。

2) 可搜索密文生成算法: 输入公钥和关键字, 发送方生成关键字可搜索密文。

3) 检索陷门生成算法: 接收方输入私钥和待检索的关键字, 生成关键字陷门。

4) 密文检索算法: 输入公钥, 一条可搜索密文和接收方检索陷门, 服务器进行匹配操作, 判断密文是否包含查询关键字。

PEKS 允许任何知道接收方公钥的人都可以将关键字可搜索密文提交至服务器, 包含加密后的文件以及提取出来的关键字。当接收者需要检索包含

某个关键字的密文时, 向服务器提交一个检索陷门; 然后服务器在不知道文件和关键字原始明文的情况下, 检索到包含该关键字的所有密文, 并将文件的密文发送给接收者; 最后接收者将该密文解密后得到自己需要的检索结果。通用地说, PEKS 允许在不泄露关键字信息的条件下, 公钥生成的密文可以被判定是否含有指定的关键字。

5.3 PEKS 的部分相关研究

PEKS 的概念提出之后, 受到了学者的广泛关注, 很多出色的相关研究工作相继发表。遵循 PEKS 的开创性工作, Abdella 等^[32]完善了 PEKS 的一致性定义, 提出了将一个匿名 IBE 方案转换为一个安全的 PEKS 方案的通用模型, 扩展了 PEKS 的基本方案, 进而提出了匿名 HIBE 方案、临时关键字的可搜索公钥加密方案和基于身份的关键字可搜索加密方案。

在实现 PKES 的检索多样化方面, 典型的工作有联合检索^[33-38]、范围检索^[39-41]、子集检索^[41]、时间范围检索^[32,42]、相似度检索^[43,44]以及授权检索^[45]。此外, Yang 等^[46]还提出了一种能够测试2条异构密文是否包含相同明文的方案。Arriaga 等^[47]提出了一个保护关键字检索陷门隐私性的 PEKS 方案。Camenisch 等^[48]构造了“不经意”的关键字检索自陷门生成器, 以此针对不可信的陷门生成器来保护关键字的隐私。

在以上 PKES 方案中, 检索复杂度与所有密文的数目线性相关。为了实现关键字的高效检索, Camenisch 等在文献[48]中非正式地描述了一种方法, 使具有相同关键字的密文形成一条隐式链。如果服务器正确查找到第一条匹配的密文, 他们的方法将会提高检索的效率。然而, 他们并没有解决如何找到第一段匹配密文的问题。同时, 他们的加密方案不具备语义安全性。在每一条链中, 第一条密文和后边的密文是平凡可区分的。这种平凡可区分性使在这个方案中很难正确定义语义安全。实际上, 他们并没有提供任何正式的安全性定义。

Boneh 等^[31]在公钥加密开山作中给出了明确的安全性定义, 即选择关键字攻击下的语义安全性 (SS-CKA)。此安全性定义意味着如果服务器没有得到关键字检索的检索陷门, 那么服务器就

不会获取含有对应关键字的密文段中的任何信息。但是，选择关键字攻击下的语义安全性并没有论述当关键字检索陷门被知晓的情况下是否依旧能保障关键字的机密性。2006 年，Byun 等^[49]首次提出了针对 PEKS 的关键字猜测攻击(KGA, keyword guessing attack)。Jeong 等^[50]证明了任何至少满足计算不可区分的一致性的 PKES 方案都易遭受 KGA 攻击。为了抵抗外部攻击者发起的 KGA 攻击，文献[51,52]分别提出 2 种方法：一种是为关键字检索陷门建立安全性的传输信道；另一种是 PEKS 的发送方和接收方通过协商关键字的别名实现关键字的匿名性。但是，由于 PEKS 的主要优点在于发送方和接收方不需要同时在线即可以完成可搜索密文的生成，因此，文献[52]提出的方案在实际应用中失去了 PEKS 的优势。解决这个问题一个直接的思路是允许发送者自定义关键字，从而增大关键字空间，使 KGA 攻击无法在有效时间内完成。然而，正如文献[53]所言，这种方法使接收者很难去生成对应的关键字检索陷门，并且如果不同的发送方使用不同的关键字来表达同一个意思，那么接收方就必须生成多个关键字检索陷门来检索密文，大幅度增加了检索开销。因此，很有必要拓展传统的 PEKS 模型，使得尽管关键字空间很小，依旧能够实现在 KGA 攻击模式下关键字的机密性^[54]。

6 确定的可搜索公钥加密

已有的具有语义安全的关键字可搜索公钥加密方案的检索时间是与所有密文的数量成线性相关的，这在海量数据库中肯定会存在性能问题。在公钥加密体制中，如果密文的生成算法为确定性算法，则该方案为确定公钥加密，且确定性加密具有更快的检索效率。因此，在引入了确定性公钥加密(DPKE, deterministic public-key encryption)后，Bellare 等^[55]首次提出确定的可搜索公钥加密(DPEKS, deterministic PEKS)，使关键字检索十分高效。

Bellare 等^[55]在提出了 DPEKS 后，形式化定义了一个安全性概念，即“尽可能强”(比单向性强，但是比语义安全性弱)，进而提出了在随机预

言机模型下的满足该安全性定义的 DPEKS 方案。经过对该工作的深入研究，2008 年 Bellare 等^[56]公开了一个 DPKE 方案和一个在随机预言机模型下将随机性 PKE 方案转化成 DPKE 的通用方法。紧接着，Bellare 等^[56]和 Boldyreva 等^[57]分别在标准模型下提出了 DPKE 的构造方案。前者使用了常用的复杂性假设且构造方案是通用的，后者使用了特殊的复杂性假设且构造方案具备更好的效率。Brakerski 等^[58]提出的 DPKE 方案具备更好的安全性。到目前为止，DPEKS 方案只能在关键字空间先验高熵条件下具有语义安全性，否则，攻击者容易发起猜测攻击，从而破解出加密的关键字。因此，DPEKS 只有在关键字空间具有先验高熵的应用场景下才适用。

7 本文提出的 PEKS 方案

直观来看，PEKS 具有的语义安全性，使得即使含有相同关键字的 2 个密文之间也相互独立，因此，PEKS 的检索复杂度似乎必须是线性级(即与密文的总量线性相关)。而且，现有的语义安全的 PEKS 实例化方案也都是这种线性级的检索复杂度。针对这个问题，本文在文献[59]中设计和实现了一种带隐藏结构的可搜索公钥加密方案(SPCHS, searchable public-key ciphertexts with hidden structures)，首次在保证语义安全性的条件下实现了亚线性级的检索效率，降低了 PEKS 方案的检索开销；在保证 PEKS 高安全性的同时提高其检索效率，在一定程度上解决了 PEKS 的低检索效率问题。

7.1 研究思路与技巧

传统 PEKS 方案中，由于服务器需要遍历完所有的密文才能找到所有的包含检索关键字的文件，因此服务器的检索效率很低。经过研究发现，如果密文之间存在如图 4 所示的隐藏的星型结构^[37]，那么在检索包含某个关键字的密文时，速度就会加快。

在图 4 的结构中，包含相同关键字的可搜索密文形成一条隐藏链结构，所有的链都有一个公共的头部。服务器在获得了关键字检索陷门后，先通过与公共头部计算，从而找到第一条符合检索条件的密文；通过该密文可以解密出一个指针，

进而找到下一条符合检索条件的密文。按照同样的方法, 就可以找到所有符合检索条件的密文。可以看出, 上述方法的检索复杂度与包含被检索关键字的密文数量成线性相关的, 而不是与所有密文的数量线性相关。

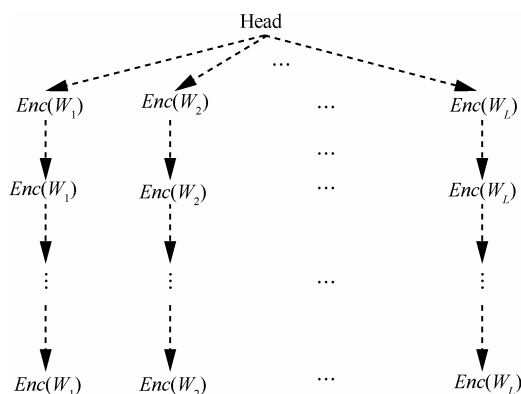


图 4 可搜索关键字密文的星型结构

在提高效率的同时, 应当保证适当的安全性, 关键字之间隐藏的星型结构是需要保证语义安全性的, 即仅仅在知道对应的关键字检索陷门时泄露部分关系。语义安全性表现在以下两点: 1) 在不知道关键字检索陷门的条件下, 所有密文都是不可区分的, 且结构的任何信息都不泄露; 2) 已知某关键字的检索陷门, 仅有相关的隐藏关系会被泄露, 而且符合检索条件的密文并没有泄露其他密文的任何信息 (除了这些密文不满足检索条件之外)。

7.2 具体贡献

本文提出了 SPCHS 及其语义安全性的定义, 然后根据这个定义在随机预言机模型下构造了一个简单的 SPCHS 方案。此方案会生成带隐藏星型结构的可搜索关键字密文。它的搜索性能取决于包含检索关键字的密文数量。它的安全性基于判定双线性映射假设, 在随机预言机模型下是语义安全的。随后, 本文基于身份加密 (IBE, identity-based encryption)^[60]和无碰撞全身份可扩展的身份密钥封装机制 (IBKEM, identity-based key encapsulation mechanism)^[61]构造了一个通用的 SPCHS 方案, 使如果存在具有语义安全性和匿名性的 IBE 和 IBKEM 方案, 那么由此构造的 SPCHS 方案也是语义安全的。最后, 本文构造了标准模型下可证明安全的 SPCHS 方案。

8 结束语

目前, SSE 的研究是密码学领域的热点研究方向之一。现有的研究成果离实际应用还存在明显的差距, 如多样化检索模式下的检索效率问题、检索完备性的可证明问题和多 SSE 方案的融合问题等。本文的已有工作为这些问题的解决部分指明了方向, 但依然存在难点和挑战。

参考文献:

- [1] CURTMOLA R, GARAY J, KAMARA S, et al. Searchable sym-metric encryption: improved definitions and efficient constructions[J]. Journal of Computer Security, 2011, 19(5):79-88.
- [2] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]//IEEE Symposium on Security & Privacy. 2000:44-55.
- [3] GOH E J. Secure indexes. Cryptography ePrint archive[R]. 2003.
- [4] CHANG Y C, MITZENMACHER M. Privacy preserving keyword searches on remote encrypted data[M]//Applied Cryptography and Network Security. Berlin Heidelberg: Springer, 2015:442-455.
- [5] BELLOVIN S M, CHESWICK W R. Privacy-enhanced searches using encrypted bloom filters[J]. Department of Computer Science Columbia University, 2004.
- [6] AGRAWAL R, KIERMAN J, SRIKANT R, et al. Order preserving encryption for numeric data[C]//ACM Sigmod. 2004: 563-574.
- [7] WATERS B R, BALFANZ D, DURFEE G, et al. Building an encrypted and searchable audit log[J]. Annual Network & Distributed System Security Symposium, 2003.
- [8] BRINKMAN R, DOUMEN J, JONKER W. Using secret sharing for searching in encrypted data[J]. Lecture Notes in Computer Science, 2004, 3178:18-27.
- [9] DAMIANI E, VIMERCATI S D C, JAJODIA S, et al. Balancing confidentiality and efficiency in untrusted relational DBMSs[C]//ACM CCS. 2003:93-102.
- [10] HACIGÜMÜŞ H, IYER B R, LI C, et al. Executing SQL over encrypted data in the database-service-provider model[C]//SIGMOD. 2002:216-227.
- [11] HACIGÜMÜŞ H, IYER B, MEHROTRA S. Efficient execution of aggregation queries over encrypted relational databases[J]. Lecture Notes in Computer Science, 2004, 2973:125-136.
- [12] KANTARCIOĞLU M, CLIFTON C. Security issues in querying encrypted data[M]//Data and Applications Security XIX. Berlin Heidelberg: Springer, 2005:325-337.
- [13] BAO F, DENG R H, DING X, et al. Private query on encrypted data in multi-user settings[J]. Lecture Notes in Computer Science, 2008, 4991:71-85.
- [14] JARECKI S, JUTLA C, KRAWCZYK H, et al. Outsourced symmetric private information retrieval[C]//ACM Sigsac Conference on Computer & Communications Security. 2013:875-888.
- [15] KATZ J, SAHAI A, WATERS B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[J]. Journal of Cryptology, 2008: 191-224.

- [16] 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 Heidelberg: Springer, 2013:353-373.
- [17] LI J, WANG Q, WANG C, et al. Fuzzy keyword search over encrypted data in cloud computing[J]. *Infocom*, 2012, 3(9):1-5.
- [18] BRINGER J, CHABANNE, KINDARJI B. Error-tolerant searchable encryption[C]//*IEEE International Conference on Communications*. 2009:1-6.
- [19] LIU Z, MA H, LI J, et al. Secure storage and fuzzy query over encrypted databases[C]//*International Conference on Network and System Security*. 2013:439-450.
- [20] NEPOLEAN D, KARTHIK I, PREETHI MU, et al. Privacy pre-serving ranked keyword search over encrypted cloud data[M]// *Recent Trends in Computer Networks and Distributed Systems Security*. Berlin Heidelberg: Springer, 2014:396-403.
- [21] WANG C, CAO N, LI J, et al. Secure ranked keyword search over encrypted cloud data[C]// *IEEE International Conference on Distributed Computing Systems*, IEEE Computer Society. 2010: 253-262.
- [22] WANG C, CAO N, REN K, et al. Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. *IEEE Transactions on Parallel & Distributed Systems*, 2012, 23(8):1467-1479.
- [23] CAO N, WANG C, LI M, et al. Privacy-preserving multi-keyword ranked search over encrypted cloud data[J]. *IEEE Transactions on Parallel & Distributed Systems*, 2014, 25(1):222-233.
- [24] LU Y. Privacy-preserving logarithmic-time search on encrypted data in cloud[C]// *NDSS*. 2012.
- [25] BOLDYREVA A, CHENETTE N, LEE Y, et al. Order-preserving symmetric encryption[C]//*The International Conference on the Theory and Applications of Cryptographic Techniques*. 2009: 224-241.
- [26] CHASE M, KAMARA S. Structured encryption and controlled disclosure[M]//*Advances in Cryptology-ASIACRYPT 2010*. Berlin Heidelberg: Springer, 2010:577-594.
- [27] KAMARA S, PAPAMANTHOU C, ROEDER T. Dynamic searchable symmetric encryption[C]//*ACM Conference on Computer & Communications Security*. 2015:965-976.
- [28] KAMARA S, PAPAMANTHOU C. Parallel and dynamic searchable symmetric encryption[M]//*Financial Cryptography and Data Security*. Berlin Heidelberg: Springer, 2013:258-274.
- [29] CASH D, JAEGER J, JARECKI S, et al. Dynamic searchable encryption in very-large databases: data structures and implementation[C]//*Network and Distributed System Security Symposium*. 2014.
- [30] HAHN F, KERSCHBAUM F. Searchable encryption with secure and efficient updates[C]//*ACM CCS*. 2014:310-320.
- [31] DAN B, CRESCENZO G D, OSTROVSKY R, et al. Public key encryption with keyword search[M]//*Advances in Cryptology - Eurocrypt*. Berlin Heidelberg: Springer, 2003:506-522.
- [32] ABDALLA M, BELLARE M, CATALANO D, et al. Searchable encryption revisited: consistency properties, relation to anonymous IBE, and extensions[J]. *Journal of Cryptology*, 2008, 21(3): 350-391.
- [33] BALLARD L, KAMARA S, MONROSE F. Achieving efficient conjunctive keyword searches over encrypted data[C]// *International Conference on Information and Communications Security*. 2005:414-426.
- [34] BAEK J, SAFAVINAINI R, SUSILO W. Public key encryption with keyword search revisited[M]//*Computational Science and Its Applications - ICCSA*. 2008:1249-1259.
- [35] GOLLE P, STADDON J, WATERS B R. Secure conjunctive keyword search over encrypted data[J]. *Lecture Notes in Computer Science*, 2004, 3089:31-45.
- [36] HWANG Y H, LEE P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system[M]// *Pairing-Based Cryptography - Pairing 2007*. Berlin Heidelberg: Springer, 2007:2-22.
- [37] DONG J P, KIM K, LEE P J. Public key encryption with conjunctive field keyword search[J]. *Lecture Notes in Computer Science*, 2004, 3325:73-86.
- [38] RYU E K, TAKAGI T. Efficient conjunctive keyword-searchable encryption[C]//*The International Conference on Advanced Information Networking and Applications Workshops*, IEEE Computer Society. 2007:409-414.
- [39] BETHENCOURT J, CHAN H, PERRIG A, et al. Anonymous multi-attribute encryption with range query and conditional decryption[C]. *IEEE Symposium on Security & Privacy*. 2006.
- [40] SHI E, BETHENCOURT J, CHAN T H, et al. Multi-dimensional range query over encrypted data[J]. *IEEE Computer Society*, 2007:350-364.
- [41] DAN B, WATERS B. Conjunctive, subset, and range queries on encrypted data[C]//*The Theory of Cryptography Conference*. 2006: 535--554.
- [42] DAVIS D, MONROSE F, REITER M K. Time-scoped searching of encrypted audit logs[C]//*The International Conference on Information and Communications Security(ICICS)*. 2004:532-545.
- [43] CHEUNG D W, MAMOULIS N, WONG W K, et al. Anonymous fuzzy identity-based encryption for similarity search[C]// *International Symposium on Algorithms and Computation*. 2010:61-72.
- [44] SEDGHI S, LIESDONK P V, NIKOVA S, et al. Searching keywords with wildcards on encrypted data[C]//*The International Conference on Security and Cryptography for Networks*. 2010: 138-153.
- [45] LUAN I, NIKOVA S, HARTEL P, et al. Public-key encryption with delegated search[M]//*Applied Cryptography and Network Security*. Berlin Heidelberg: Springer, 2011:532-549.
- [46] YANG G, TAN C H, HUANG Q, et al. Probabilistic public key encryption with equality test[C]//*The International Conference on Topics in Cryptology*. 2010:119-131.
- [47] ARRIAGA A, TANG Q, RYAN P. Trapdoor privacy in asymmetric searchable encryption schemes[M]//*Progress in Cryptology - AFRICACRYPT 2014*. Springer International Publishing, 2014:31-50.
- [48] CAMENISCH J, KOHLWEISS M, RIAL A, et al. Blind and anonymous identity-based encryption and authorised private searches on public key encrypted data[C]//*The International Conference on Practice and Theory in Public Key Cryptography*. 2009:196-214.
- [49] BYUN J W, LEE D H, LIM J. Efficient conjunctive keyword search on encrypted data storage system[C]//*European Conference on Public Key Infrastructure: Theory and Practice*. 2006:184-196.
- [50] 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.
- [51] FANG L, SUSILO W, GE C, et al. A secure channel free public key encryption with keyword search scheme without random oracle[C]//The International Conference on Cryptology and Network Security. 2009:248-258.
- [52] TANG Q, CHEN L. Public-key encryption with registered keyword search[C]// European Workshop on Public Key Infrastructures, Services and Applications. 2009:163-178.
- [53] HARROWER W. Searching encrypted data[R]. 2009.
- [54] 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.
- [55] BELLARE M, BOLDYREVA A, O'NEILL A. Deterministic and efficiently searchable encryption[M]//Advances in Cryptology - CRYPTO 2007. Berlin Heidelberg :Springer, 2007:535-552.
- [56] BELLARE M, BOLDYREVA A, O'NEILL A. Deterministic and efficiently searchable encryption[C]//The International Cryptology Conference on Advances in Cryptology. 2006:535-552.
- [57] BOLDYREVA A, FEHR S, O'NEILL A. On notions of security for deterministic encryption, and efficient constructions without random oracles[C]// Conference on Cryptology: Advances in Cryptology. 2008:335-359.
- [58] BRAKERSKI Z, SEGEV G. Better security for deterministic public-key encryption: the auxiliary-input setting[M]//Advances in Cryptology-CRYPTO 2011. Berlin Heidelberg: Springer, 2011: 543-560.
- [59] XU P, WU Q, WANG W, et al. Generating searchable public-key ciphertexts with hidden structures for fast keyword search[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(9):1.
- [60] BOYEN X, WATERS B. Anonymous hierarchical identity-based encryption (without random oracles)[C]//The International Conference on Advances in Cryptology. 2006:290-307.
- [61] ABDALLA M, CATALANO D, FIORE D. Verifiable random functions: relations to identity-based key encapsulation and new constructions[J]. Journal of Cryptology, 2014, 27(3):544-593.

作者简介:



徐鹏(1981-), 男, 湖北武汉人, 博士, 华中科技大学副教授, 主要研究方向为公钥密码学、基于身份密码学、可搜索加密、格密码、云安全。



金海(1966-), 男, 上海人, 博士, 华中科技大学教授, 主要研究方向为高性能计算、分布式计算、云计算、大数据、云安全。