肖心雨, 李高燕, 孙文涛,等. 一种陷门随机生成的公钥认证可搜索加密方案[J]. 智能计算机与应用,2024,14(7):136-139.
DOI:10.20169/j.issn.2095-2163.240720

一种陷门随机生成的公钥认证可搜索加密方案

肖心雨[1], 李高燕[1], 孙文涛[1], 杜浩瑞[2]
(1 西藏大学 理学院, 拉萨 850000; 2 武汉大学 数学与统计学院, 武汉 430061)

摘 要: 本文针对于无配对公钥认证可搜索加密方案,相同关键字不满足陷门的不可区分性,提出一种满足陷门不可区分性的公钥认证可搜索加密方案。该方案抵抗恶意服务器关键字猜测攻击,防止在信息检索中生成的陷门的泄露,降低了检索过程中信息泄露的可能性,更好的维护了用户信息的安全性。仿真实验表明,本方案生成 2 000 个关键字密文、陷门和测试分别需要 340.005 ms、472.684 ms 和 208.056 ms,提高了检索信息的效率。

关键词: 无配对公钥认证; 可搜索加密; 陷门不可区分性; 恶意服务器
中图分类号: TN918.4 **文献标志码**: A **文章编号**: 2095-2163(2024)07-0136-04

A searchable encryption scheme for public key authentication randomly generated by trapdoor

XIAO Xinyu[1], LI Gaoyan[1], SUN Wentao[1], DU Haorui[2]
(1 College of Science, Tibet University, Lhasa 850000, China;
2 School of Mathematics and Statistics, Wuhan University, Wuhan 430061, China)

Abstract: In this paper, a searchable encryption scheme for unpaired public key authentication is proposed to satisfy the trap indistinguishability for the same keyword. The scheme resists the malicious server keyword guessing attack, prevents the leakage of trap gate generated in information retrieval, reduces the possibility of information leakage in the retrieval process, and better maintains the security of user information. Simulation results show that it takes 340.005 ms, 472.684 ms and 208.056 ms to generate 2 000 keyword ciphertext, trap gate and test respectively, which improves the efficiency of information retrieval.

Key words: unpaired public key authentication; searchable encryption; trapdoor indistinguishability; malicious server

0 引 言

云计算的发展促进了个人和组织将数据外包储存,减少了本地存储开销并简化了本地数据管理[1]。然而,数据的隐私性和安全性是首要解决的问题。数据的隐私性可以通过十分成熟的加密手段来解决,例如对称加密(国密 SM3 等)、公钥加密(国密 SM2 等)[2]。但数据加密导致数据的可用性降低,因为用户无法从一堆乱码的数据中检索到目标文件,除非用户用密钥解密之后再进行搜索。密钥直接关系到数据的安全和隐私,因此在不泄露密钥的前提下找到目标数据文件是一个棘手的问题。

可搜索加密是一种加密原语,对数据进行加密,以支持对加密数据进行关键字搜索,在保证数据机密性的同时保证了数据的可用性,现在主流的方案是从数据文件中提取对应的关键字,将关键字加密[3]。在检索的过程中,只对关键字密文做检索,因为默认加密的关键字可以直接代表加密数据,使得检索效率大幅度提高。根据使用密钥的不同,可搜索加密一般分为对称可搜索加密(SSE)和公钥可搜索加密(PEKS)[4]。

云环境下可搜索加密的场景如图 1 所示。云服务器上的数据存储和检索主要涉及 3 个参与实体,分别为数据所有者(DO)、数据用户(DU)和云服务

基金项目: 国家级大学生创新训练项目(202120694008)。

作者简介: 肖心雨(2001-),女,本科生,主要研究方向:信息安全-数据保护(密码学)-可搜索加密; 李高燕(2000-),女,本科生,主要研究方向:信息安全-数据保护(密码学)-可搜索加密; 杜浩瑞 (1994-),男,博士研究生,主要研究方向: 可搜索加密,属性加密。
通讯作者: 孙文涛 (1979-),男,硕士,副教授,主要研究方向:数论。Email:792434269@qq.com

收稿日期: 2023-08-11

器(CS)或云服务提供商。数据所有者通常是拥有合法控制权和数据所有权的数据生产者;数据用户是可以访问数据的授权实体;云服务器托管数据,用于存储和共享。Boneh 等[5]首次提出公钥可搜索加密方案,该方案中数据所有者先提取与明文相关的关键字 w,输入数据用户的公钥 PK,运行加密算法将 w 加密成密文 C,并将 C 上传至云服务器。当用户需要搜索某个 w 时,只需用自己的私钥 SK 运行陷门生成算法产生一个搜索陷门 T,发送到云服务器去查找相匹配的关键字密文,从而完成查询工作。

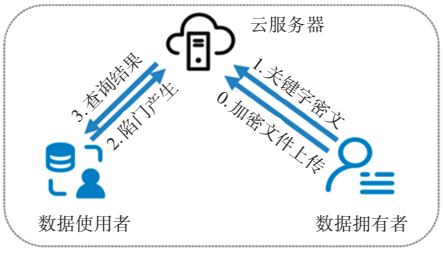

图 1　面向云环境的公钥可搜索加密模型

Fig. 1　Public key searchable encryption model for cloud environment

Byun 等[6]指出 Boneh 方案[5]的一个严重漏洞,关键字具有低熵特性,即关键字的选择空间比密码小得多,用户通常使用已知的关键字进行文档搜索,攻击者可以发起离线关键字猜测攻击。关键字猜字攻击成功的原因在于陷门生成仅仅靠关键字和私钥简单的运算生成,即任何内部/外部攻击者都可以通过配对操作将陷门与公钥关联起来,并执行无限次的测试,使得关键字猜测攻击成功。通过保护陷门不被泄露来防止对手发起外部攻击,例如,通过在接收者和服务器之间建立安全通信通道,只有服务器可以访问陷门,从而保证安全性。但是,在通信双方建立安全通道需要消耗昂贵的代价;另一个解决方案是限制对手的测试能力,即通过指定测试器获得陷门,这两种方法都不能对付恶意服务器的攻击。如何抵御恶意服务器的攻击是公钥可搜索加密(PEKS)解决的另一个问题。

为了抵抗恶意服务器关键字猜测攻击,Huang 等[7]引入了关键字搜索公钥认证加密(PAEKS)的概念。在公钥认证加密(PAEKS)中,数据所有者(DO)不仅要对关键字进行加密,还要对关键字进行身份验证,这样验证方就会相信加密后的关键字只能由数据所有者生成,但不足以抽象现实威胁,即不能多密文选择攻击;Qin 等[8]提供了一个新的公钥认证加密(PAEKS)模型,可以捕获多密文选择攻击和内部关键字猜测攻击。在不使用随机预言机模型下,杨宁滨等[9]提出无配对公钥认证可搜索加密方案,通过 Game-Hopping 方法证明该方案满足适应性选择关键词攻击下多关键词密文不可区分性以及适应性选择关键词攻击的陷门不可区分性,但该方案陷门生成算法是确定性算法,针对相同关键字不满足陷门不可区分性。

为此,本文提出了一种满足陷门不可区分性的公钥认证可搜索加密方案,该方案能降低计算成本、有效防止搜索模式泄露。具体解决的问题如下:

(1)抵抗关键字猜测攻击:关键字加密密钥由数据发送者和数据所有者基于 Diffie-Hellman 密钥协商生成,对于第三方和服务器都是保密的,因此不能产生合法的密文;

(2)搜索模式泄露:陷门是基于 ElGamaL 签名算法生成的,该算法是一种基于离散对数的加密体系,既能用于数据加密,也能用于数字签名,利用因数分解的数学方法,即使对于相同的私钥、明文进行加密,可得到的签名也各不相同,有效地防止了网络中可能出现的恶意攻击[10]。

Xu 等[11]提出用于模糊关键字搜索的公钥加密(PEFKS),其中每个关键字对应一个精确关键字搜索陷门和一个模糊关键字搜索陷门。模糊关键字搜索的公钥加密(PEFKS)的关键字空间很小,但恶意方也无法学习到准确的关键字;Chen 等[12]分析了关键字猜测攻击的另一个主要原因,只要知道基本关键字属于哪个小集合,就不能很好地保护关键字的隐私。任何了解外部接收者公钥的人都可以生成任何关键字的公钥可搜索加密密文,恶意服务器可能会在出现陷门时选择一个猜测关键字,用其来使用公钥可搜索加密生成密文,服务器可以猜测隐藏在陷门下的关键字是否是正确的关键字,直到找到正确的关键字。

Chen 等[12]提出在两台服务器不碰撞的情况下,利用关键字搜索的双服务器公钥加密来防止攻击的方法;Sun 等[13]考虑到服务器是恶意的,探索了针对关键字内部猜测攻击的公钥可搜索加密(PEKS)方案是否可以基于不同的公钥密码系统构建,例如公开密钥基础设施(PKI)的、基于身份的或无证书的密码系统。为了提高方案的效率,Hwang 等[14]提出了一种基于单词无关的平滑投影哈希函数(SPHFs)和公钥可搜索加密方案的 PAEKS 结构;在检索功能性方面,Park 等[15]首次提出支持多关键字检索的可搜索公钥加密方案,进一步满足了用户

的检索需求;Chen 等[12]构造了支持连接关键字检索的可搜索公钥加密方案,该方案的密文扩展和私钥扩展相对较小;Zhang 等[16]基于密文策略的属性加密技术提出一种多关键字的检索方案,支持检索结果可验证。

1 基础知识

定义 1 离散对数(Discrete Logarithm, DL)困难问题[17]:假设给定素数阶为 q 的循环群 G,g 为 G 的一个生成元,随机选取 $a \in Z_p^*$,DL 困难问题是给定 g^a,对于每个敌手 A 在概率多项式时间算法,能够以可忽略的概率 ε 正确计算出 a,即:

$$| [A(g,g^a) = a] | < \varepsilon$$

定义 2 密钥交换算法(Decisional Diffie-Hellman, DDH)困难问题[18]:假设给定素数阶为 q 的循环群 G,g 为 G 的一个生成元,DDH 问题随机选取 $a,b,c \in Z_q^*$,对于每个敌手在概率多项式时间算法可以忽略概率 ε 正确区分 g^c 与 g^{ab},即:

$$Pr[A(G,g,q,g^a,g^b,g^c) = 1] - Pr[A(G,g,q,g^a,g^b,g^{ab}) = 1] \leqslant \varepsilon$$

2 本文方案

本文提出一个能够抵抗在线外部攻击者关键词猜测攻击以及离线内部攻击者关键词猜测攻击的安全性的方案,即非双线性对运算下公共通道带关键词搜索的公钥认证加密方案的定义,并且给出方案的安全模型。

2.1 基础方案

由杨宁滨等[9]提出的方案,满足适应性选择关键词、多攻击下关键词密文不可区分性等条件[19]。但是,该方案陷门生成算法是确定性算法,针对相同关键字不满足陷门不可区分性,因此本文在此基础上提出了一种满足陷门不可区分性的公钥认证可搜索加密方案。其中 5 个多项式时间算法具体描述如下:

(1)初始化 GlobalSetup(λ):输入安全参数 λ,输出素数阶为 q 的循环群 G,g 是 G 的一个生成元,$Hash^{\ell}$ 函数 $H_1: G \rightarrow \{0,1\}^{\ell}$ 和 $H: \{0,1\}^* \times \{0,1\}^{\ell} \rightarrow Z_q^*$,$\ell$ 表示二进制长度。因此,输出全局参数为 $GP = (G,q,g,H,H_1,KS_{\omega})$,其中 KS_{ω} 为关键词集。

(2)密钥生成 KeyGen(GP):数据所有者随机选取私钥 $sk_s = (sk_{s_1}, sk_{s_2})$ 且 $sk_{s_1}, sk_{s_2} \in Z_q^*$,计算出公钥,数据用户随机选取私钥 $sk_R = (sk_{R_1}, sk_{R_2})$ 且 $sk_{R_1}, sk_{R_2} \in Z_q^*$,计算出公钥。

(3)加密 Encrypt(GP, sk_s, pk_R, w):数据所有者随机选取 $r \in Z_q^*$ 且 $r > H(w \| ss)$,计算关键词密文 C_w,并将 C_w 与加密的文件上传至云服务器(CSP);

(4)陷门生成 Trapdoor(GP, sk_R, pk_s, w'):数据用户选定需要搜索的关键词 w',计算搜索陷门 $T_{w'}$,并将其上传至云服务器检索;

(5)测试 Test($GP, C_{\omega}, T_{\omega'}$):云服务器(CSP)收到数据用户(DU)的搜索陷门 $T_{w'}$ 后,判断 $H_1(C_1 \times T_{\omega'}) = C_2$ 是否成立,若成立则输出 1 并返回文件密文数据,否则返回 0[20]。

可见,若关键字 $w = w^*$,可以推出陷门相等,难以避免敌手猜测,所以本文提出陷门随机生成的公钥认证可搜索加密方案。

2.2 本文方案

(1) GlobalSetup(λ):与基础方案相同。

(2)密钥生成 KeyGen(GP):数据所有者(DO)选择随机数 $y \in Z_p$,并计算公钥,公式(1):

$$pk_S = g^y \bmod p \tag{1}$$

数据用户选择随机数 $x \in Z_p$,并计算其公钥,公式(2):

$$pk_R = g^x \bmod p \tag{2}$$

其中,g 为循环群 G 的生成元,p 是大素数。

(3)加密 Encrypt(GP, sk_S, pk_R, w):GP 为全局参数,sk_s 为私钥,pk_R 为公钥,w 为关键字。数据所有者(DO)选择随机数 r,对循环群求模 A,公式(3),对哈希函数数值求模 B,公式(4),关键字 w 的密文,公式(5):

$$A = g^r \bmod p \tag{3}$$

$$B = H_2(g^r \cdot g^t \bmod p) \tag{4}$$

$$C_w = (A,B) \tag{5}$$

(4)陷门生成 Trapdoor(GP, sk_R, pk_s, w):利用公钥以及关键字计算出陷门对应参数,公式(6)和公式(7):

$$l = pk_s^x = g^{yx} \tag{6}$$

$$t = H_1(w \| l) \tag{7}$$

数据拥有者(DU)选择随机数 $k(1 < k < p-1)$,对随机数 k 进行处理、加密得到 u,公式(8),再检索关键词得出 v,公式(9),最后利用 v 和随机数 k 等进行加密,形成陷门 T_w,公式(10)。

$$u = g^k \bmod p \tag{8}$$

$$v = t - xuk^{-1} \bmod p - 1 \tag{9}$$

$$T_w = (u,v) \tag{10}$$

(5)测试 Test(GP, pk_R, pk_S, C_w, T_w)：云服务器验证值式(11)是否成立，若成立，则满足陷门可区分。

$$B = H_2(pk_R^u u^v \cdot A \bmod p) \tag{11}$$

3　性能分析

为了更加直观验证本方案的加密性能，进行仿真实验。本实验使用的平台包括 Ubuntu 18.04.5 LTS 与 Intel(R) Xeon(R) CPU E5-2620 v4@2.10 GHz和 16.00 GB RAM。伪随机排列计算使用 AES 算法(CBC 模型，128 位密钥)。使用 SHA256 算法计算哈希函数。选择了真正的安然数据集(版本 20150307，约 423 MB)，以演示本文提出的方案的实际性能，其中包含约 150 个用户的数据。本文选择了大约2 000个长度不小于 5 个字符且总出现次数大于 20 的关键字，实验结果中去掉了通信和网络效应，该实验模拟中不存在中止现象，因此模拟成功的概率为 1，满足其安全性。为了评估本方案算法的效率，在方案中生成2 000个关键字密文，陷门和测试分别需要 340.005 ms、472.684 ms 和 208.056 ms。

4　结束语

本文对公钥认证可搜索加密进行了进一步的研究，设计出了无双性对的陷门随机生成的公钥认证可搜索加密方案，该方案不仅可抵抗内外关键字猜测攻击而且提高了信息检索的效率。除此之外，由于陷门是随机产生的，可以减少用户搜索模式泄露的可能性。

参考文献

[1] 黄卫，吴誉兰. 基于云计算平台的信息公钥可搜索加密仿真[J]. 计算机仿真，2023，40(11)：143-146，383.

[2] 郭丽峰，穆念强，徐晓璇，等. 基于双服务器的公钥可搜索加密方案[J]. 山西大学学报(自然科学版)，2023，46(4)：792-801.

[3] 邓志辉. 基于合数阶双线性对的公钥可搜索加密方案的研究与实现[D]. 南京：南京邮电大学，2021.

[4] 陈振伟. 面向云存储安全的公钥可搜索加密技术研究[D]. 西安：西安邮电大学，2021.

[5] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search [C]// Proceedings of Advances in Cryptology - EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques. Interlaken, Switzerland: IEEE, 2004: 506-522.

[6] 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]//Proceedings of Secure Data Management: Third VLDB Workshop. Seoul, Republic of Korea: IEEE, 2006: 75-83.

[7] HUANG Q, LI H. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks [J]. Information Sciences, 2017, 403: 1-14.

[8] QIN B, CHEN Y, HUANG Q, et al. Public-key authenticated encryption with keyword search revisited: Security model and constructions[J]. Information Sciences, 2020, 516: 515-528.

[9] 杨宁滨，周权，许舒美. 无配对公钥认证可搜索加密方案[J]. 计算机研究与发展，2020，57(10)：2125-2135.

[10] ELGAMAL T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[11] 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, 2012, 62(11): 2266-2277.

[12] 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 and Security, 2015, 11(4): 789-798.

[13] SUN L, XU C, ZHANG M, et al. Secure searchable public key encryption against insider keyword guessing attacks from indistinguishability obfuscation [J]. Science China Information Sciences, 2018, 61(3): 038106.

[14] HWANG M S, LEE C C, HSU S T. An ElGamal-like secure channel free public key encryption with keyword search scheme [J]. International Journal of Foundations of Computer Science, 2019, 30(2): 255-273.

[15] PARK D J, KIM K, LEE P J. Public key encryption with conjunctive field keyword search[C]// Proceedings of Information Security Applications: 5th International Workshop. Cham: Springer, 2005: 73-86.

[16] ZHANG Y, ZHU T, GUO R, et al. Multi-keyword searchable and verifiable attribute-based encryption over cloud data[J]. IEEE Transactions on Cloud Computing, 2021, 11(1): 971-983.

[17] CHEN Y C, XIE X, WANG P S, et al. Witness-based searchable encryption with optimal overhead for cloud-edge computing[J]. Future Generation Computer Systems, 2019, 100: 715-723.

[18] XIE X, CHEN Y C, WANG J R, et al. Witness-based searchable encryption with aggregative trapdoor [C]// Proceedings of International Conference on Security with Intelligent Computing and Big-data Services. Cham: Springer, 2018: 561-573.

[19] HWANG Y H, LEE P J. Public key encryption with conjunctive keyword search and its extension to a multi-user system[C]// Proceedings of Pairing-Based Cryptography-Pairing 2007: First International Conference. Cham: Springer, 2007: 2-22.

[20] 纪里城，张亦辰，李继国. 可搜索加密的安全性研究进展[J]. 福建师范大学学报(自然科学版)，2024，40(1)：116-130.