计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2020.20200318
57(10): 2125-2135, 2020

无配对公钥认证可搜索加密方案

杨宁滨 周 权 许舒美
(广州大学数学与信息科学学院 广州 510006)
(yorknb@126.com)

Public-Key Authenticated Encryption with Keyword Search Without Pairings

Yang Ningbin, Zhou Quan, and Xu Shumei
(*School of Mathematics and Information Science, Guangzhou University, Guangzhou* 510006)

Abstract With the rapid development and wide application of cloud computing and 5G communication, the number of cloud mobile users has increased rapidly. The privacy protection of cloud data is getting more and more attention. Public key encryption scheme with keyword search (PEKS) and secure channel free public key encryption with keyword search (SCF-PEKS) allow any user in the system to send encrypted files to the server for retrieval by the receiver, which plays a certain role of privacy protection. However, Rhee et al. found that the scheme may result in loss of privacy security of keywords in their work. Meanwhile, many of public-key searchable encryption schemes are calculated based on bilinear pairings, and their computational efficiency is limited on battery-limited devices. To address these issue, we propose a non bilinear pairs secure channel free public key authentication encryption with keyword search scheme (NBP-SCF-PAEKS). The scheme has higher computational efficiency than the bilinear pair scheme, and has access control function in keyword retrieval process. Without random oracle model, we prove that the scheme can resist the online keyword guessing attack and the offline keyword guessing attack, by ensuring the multi-keyword ciphertext indistinguishability under adaptive chosen keyword attack and the keyword trapdoor indistinguishability under adaptive chosen keyword attack through game-hopping method. Compared with other schemes, the simulation results show that the scheme is efficient and secure.

Key words public key; keyword guessing attacks; searchable encryption; multi-keyword ciphertext security; authentication; non bilinear pairs

摘 要 随着云计算与5G通信的快速发展与广泛应用,云移动用户数迅速增长.云数据的隐私性保护越来越受大众关注.早期提出的带关键字搜索的公钥加密方案(public key encryption scheme with keyword search, PEKS)和公共通道带关键字搜索的公钥加密方案(secure channel free PEKS, SCF-PEKS)允许系统中的任何用户向服务器发送加密文件供接收者检索,起到一定的隐私保护作用.但之后Rhee等人的工作中发现方案仍存在关键词隐私性安全不足.同时,多数的公钥可搜索加密方案是基于双线性对下计算的.在运算能力有限的设备上应用,其计算效率会有所限制.针对以上问题,提出一种非双线性对运算的公共通道的公钥认证可搜索加密方案(non bilinear pairs secure channel free public key authentication

收稿日期:2020-05-01;**修回日期**:2020-07-24
基金项目:广东省重点领域研发计划项目(2019B020215004);国家自然科学基金项目(61772147);国家重点研发计划项目(2018YFB0803600)
This work was supported by the Key-Area Research and Development Plan of Guangdong Province (2019B020215004), the National Natural Science Foundation of China (61772147), and the National Key Research and Development Program of China (2018YFB0803600).
通信作者:周权(zhouqq@gzhu.edu.cn)

encryption with keyword search scheme, NBP-SCF-PAEKS),该方案的计算效率相对于双线性对方案高,并且在关键词检索过程具有访问控制功能.在不使用随机预言机模型下,通过 Game-Hopping 方法证明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,使得方案模型抵抗在线模式下外部攻击者关键词猜测攻击和离线模式下内部攻击者关键词猜测攻击.根据方案设计进行仿真实验,结果表明:该方案相对于其他方案是高效安全的.

关键词 公钥;关键词猜测攻击;可搜索加密;多关键词密文安全;认证 ;非双线性对

中图法分类号 TP309

云计算高速发展以及 5G 通信应用的推广下,云存储服务受到了人们的广泛关注.人们可以将自己的电子邮件、个人健康记录和财务信息等数据上传到云端,与他人共享或在任何地方使用.显然,云计算给人们带来了很多方便.但是,这存在着数据隐私性的安全问题.用户在上传数据到云端后,数据的所有权则由云端的服务器所管理,这可能存在云端服务器不完全可信的状态下导致数据泄露.用户不能完全地控制自己上传的数据安全性,这远远不能满足数据云端安全的实用性.

在过去的研究中,人们为了满足数据隐私性可以通过传统的数据加密来保证数据存储的安全性.然而,这仅适合数据存储并不适用于数据检索.针对这种存在的现象,不少学者提出可检索保护云端数据隐私性安全的方案.Song 等人[1]是第 1 个提出一种有效解决云存储的隐私问题的可搜索加密办法,而公钥可搜索加密(PEKS)是可搜索加密方案提出后由 Boneh 等人[2]首先提出的一种方法.在 Boneh 等人提出的公钥可搜索加密方案中,有 3 个行为主体:数据发送者(或称为数据拥有者、Bob)、数据接收者(或称数据使用者、Alice)以及云服务提供者.Bob 首先整理想要分享的一份文件以及对应的关键词 $w=urgent$,并对文件和关键词通过加密算法生成文件密文 C_f 及关键词密文 C_w 上传至云服务提供者,关键词密文可供云服务提供者检索找到对应的文件.当 Alice 想要检索带关键词 $w'=urgent$ 的文件时,只需针对关键词生成陷门 $T_{w'}$,发送至云服务提供者.然后由云服务提供者检索并匹配关键词是否相等,即 $w\stackrel{?}{=}w'$.最后把匹配结果返回给 Alice,若匹配成功,则会返回文件密文 C_f,否则返回空值.因此,Alice 可以借助密钥解密文件密文获取明文文件 $file$.在整个检索过程,云服务提供者不知道 Bob 上传文件与关键词的内容.

Boneh 等人所提出的方案是需要在秘密通道下才可以安全传输数据到云服务器.但是,一旦攻击者截获秘密通道传输的数据,用户的隐私数据则会被窃取.Baek 等人[3]对此研究并提出了公共通道的 PEKS 方案,解决了 Boneh 等人的方案中存在的隐私性问题.之后,Huang 等人[4]提出的 PAEKS 方案满足了陷门不可区分性,但是该方案在文献[5]中被指出不满足密文不可区分性.攻击者可以公开地对关键词密文进行对等测试.因此,方案抵抗外部攻击者与内部攻击者的关键词猜测攻击,是实现方案的关键词安全性的充要条件.

目前多数的公钥可搜索加密方案是基于双线性对运算所设计的.这在资源能力有限的设备上执行会降低其运算效率,从而影响用户双方的交互体验.为了提高用户与云端服务器交互的效率以及满足关键词隐私安全性,提出一个非双线性对运算的带关键词的公钥认证加密方案.

本文主要贡献包括 3 个方面:

1) 提出一个基于非双线性对运算下的公共通道的公钥认证可搜索加密方案(NBP-SCF-PAEKS),相对于双线性对运算的方案效率大大提高.该方案是基于用户双方密钥协商构造的,从而具备访问控制的功能,即具备一定的认证功能.

2) 通过无随机预言机模型下使用 Game-Hopping 方案证明该方案满足适应性选择关键词攻击下多关键词密文的不可区分性以及适应性选择关键词攻击下的陷门不可区分性,从而使该方案达到抵抗离线内部攻击者的关键词猜测攻击以及在线外部攻击者的关键词猜测攻击的安全性.

3) NBP-SCF-PAEKS 方案与 SCF-PEKS[3],PAEKS[4],SCF-PEPCKS[6],Hwang 等人方案[7]以及 PAEKSR[8]方案的计算效率和存储大小进行仿真比较,实验结果是方案的计算效率相对于其他比较的方案要高,并且所需存储内存较小.

1 相关工作

文献[1]中 Song 等人是最先提出可搜索加密

的方案,但是该方案需要遍历所有文件才可以返回搜索结果,因此需要花费较大计算代价;文献[2]中Boneh等人介绍了带关键词的公钥可搜索加密方案(PEKS),但不久之后,研究者发现了PEKS方案明显的缺陷,关键字陷门需要秘密传输到云服务器;文献[3]中Baek等人针对PEKS方案提出了一个在公共通道下实现的公钥可搜索加密方案(SCF-PEKS),解决PEKS[2]中存在的缺陷;Yau等人[9]研究离线关键词猜测攻击,并且表明容易遭受内部敌手攻击;文献[10]中Fang等人提出了在不使用随机预言机模型下证明SCF-PEKS方案的关键词安全性.但是PEKS和SCF-PEKS方案都存在着关键词的隐私性问题.当攻击者为指定服务器时,易遭受关键词猜测攻击.因此,公钥可搜索加密中关键词的隐私性成为研究者所需要解决的问题.文献[11]中Emura等人提出了自适应安全的无安全通道的公钥可搜索加密的通用构造方案;Rhee等人在文献[12]中引入了"陷门不可区分性"概念,并证明了这是抵抗关键词猜测攻击的一个充分条件.根据攻击模式可以分为关键词在线猜测攻击与关键词离线猜测攻击;文献[13]中Noroozi等人提出了新的PEKS方案来抵抗外部攻击者的离线与在线关键词攻击.

根据攻击者的类型可分为外部攻击者和内部攻击者.内部攻击者一般指的是半可信云服务器,外部攻击者一般指的是除数据提供及使用的双方用户与服务器外的攻击者.由于半可信服务器被允许对关键词密文及关键词陷门做匹配测试,所以半可信的服务器比外部攻击者的权限更大.文献[4]中Huang等人介绍其方案(PAEKS)满足抵抗内部攻击者的关键词猜测攻击.其主要工作是对关键词加密时引入发送者的私钥,实现公钥认证加密功能,但是这个方案的陷门是固定的,且被指出不满足密文不可区分性[5].文献[7]中Hwang等人提出对ElGamal改进下的非双线性对下的公钥可搜索加密,能够抵御外部攻击者的关键词猜测攻击.文献[4,14-15]中徐海琳等人及陆阳等人采用借助双方的公私钥产生密钥协商的关键词密文与陷门,只有认证的用户才能实现密文与陷门的产生,并且能够抵御已知的3种关键词猜测攻击.文献[8]中Qin等人指出了Huang等人的PAEKS方案的关键词隐私性不足,在选择明文攻击不允许敌手公开质询消息密文,并且不能满足多关键词密文猜测攻击.在此基础上改进后提出可认证的带关键词的公钥加密方案(PAEKSR),同时满足多关键词密文不可区分性安全.

文献[16]中Chen等人介绍了一种新型的抵抗内部攻击者离线关键词猜测攻击的公钥可搜索加密,即辅助服务器的公钥可搜索加密.该方案是借助服务器提供关键词的盲签名,并返回给用户再进行PEKS加密,服务器的盲签名的密钥具备密钥更新的功能,使得方案更具灵活性,并且引入限速机制来抵抗在线关键词猜测攻击.Zhang等人[17]在此工作基础上推广到区块链的公链上应用,并且能够抵抗已知的关键词猜测攻击.文献[18]中Dent提出的Game-Hopping方法是一种验证密码方案安全性的方法,攻击者在特定的攻击环境中运行一个未知的成功概率,随着调整攻击环境不断计算,直到计算出攻击者成功的概率,利用这个临界值来判断方案的安全性.

之后,研究者针对公钥可搜索加密方案设计具有不同功能的方案,其中有可验证的关键词可搜索加密[19-21]、模糊关键词的可搜索加密[22]、基于属性加密的带关键字搜索方案[23-24]以及基于代理重加密的带关键字搜索方案[25]等.

2 预备知识

本节主要介绍困难性假设,并对关键词猜测攻击类型进行分析.

2.1 困难性假设

定义1. DL困难问题假设[26].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$a\in Z_q^*$.离散对数困难问题是给定g^a,对于每个敌手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:

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

定义2. HDH困难问题假设[27].给定素数阶为q的循环群G,g为G的一个生成元,并且给定Hash函数$H:G\rightarrow\{0,1\}^l$.Hash Diffie-Hellman困难问题是随机选取$a,b\in Z_q^*$,给定Hash函数和$(g,g^a,g^b,Z)\in G_3\times\{0,1\}^l$,判断$Z$与$H(g^{ab})$是否相等.对于每个敌手在概率多项式时间算法以可忽略概率ε正确区分Z与$H(g^{ab})$,即:

$$|Pr[A(G,q,g,g^a,g^b,Z)=1]-Pr[A(G,q,g,g^a,g^b,H(g^{ab}))=1]|<\varepsilon.$$

2.2 关键词猜测攻击类型分析

本节主要对Baek等人提出的SCF-PEKS方案中存在在线模式下外部攻击者关键词猜测攻击和离线模式下内部攻击者关键词猜测攻击进行描述.

在线模式下外部攻击者关键字猜测攻击[6]是由外部攻击者执行攻击,攻击步骤为:

1) 在在线模式下,外部攻击者首先确定攻击对象(目标接收方).

2) 外部攻击者准备想要执行攻击的关键词集$\{w_1,w_2,\cdots,w_n\}$,借助被攻击对象的公钥执行 SCF-PEKS 的加密算法生成所有可能与文件密文对应的关键词密文,即$\langle C_f,C_w\rangle_i$,并且维护列表$\{w_i,C_{w_i},C_f\}$.

3) 外部攻击者将密文集合传输到云服务器.攻击者监视云服务器和目标接收方之间的通信.当目标接收方生成关键词陷门 T_w 发送至云服务器检索时,由于在公共信道传输,外部攻击者可以截获关键词陷门.一旦发现返回的搜索结果与之前注入的密文集合相关,对照维护的列表,外部攻击者就可以获取目标接收方正在搜索的关键字信息,从而获取用户搜索的关键词信息.

离线模式下内部攻击者关键词猜测攻击[6]是由内部攻击者(一般为恶意服务器)执行的.攻击步骤为:

1) 在离线模式下,内部攻击者首先确定攻击对象(目标接收方).

2) 内部攻击者接收到目标接收方的关键词陷门 T_w 后,准备想要执行猜测攻击的关键词 w,借助目标接收方的公钥信息以及服务器公钥信息执行 SCF-PEKS 加密算法产生关键词密文 C_w.

3) 内部攻击者拥有了关键词陷门 T_w 以及关键词密文 C_w 后,执行测试实验,直到攻击者猜测成功,否则返回步骤 2)重新执行.

3 方案定义与安全模型

本节给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定义,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(Non Bilinear Pairs SCF-PAEKS, NBP-SCF-PAEKS),并且给出方案的安全模型.

3.1 方案定义

图 1 所示为 NBP-SCF-PAEKS 方案的系统框架.系统框架包括 4 个主体:授权中心(authorization center, AC)、数据拥有者(data owner, DO)、数据使用者(data user, DU)以及云服务提供者(cloud service provider, CSP).

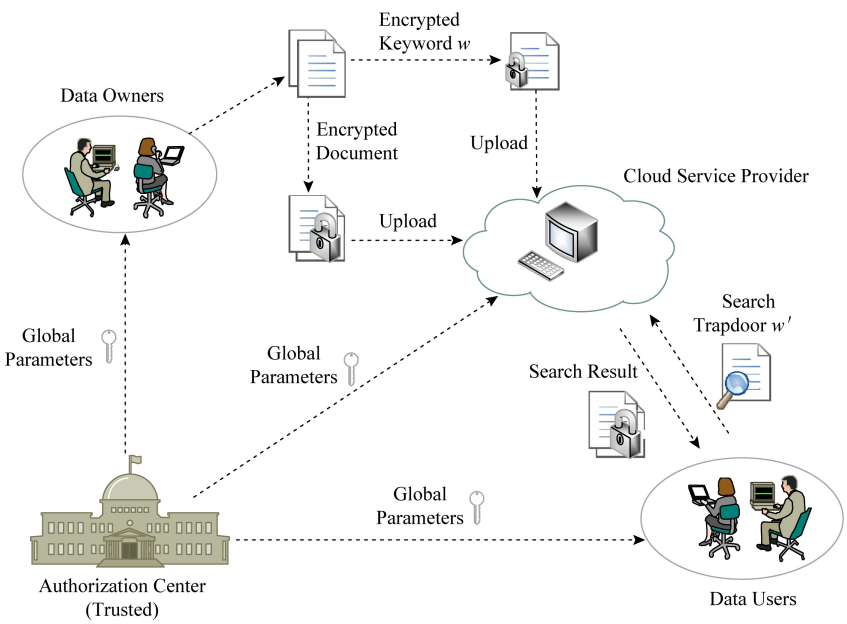


Fig. 1 The scheme system framework

图 1 方案系统框架

授权中心 AC 主要职能是分发全局参数给系统框架内的其他主体.由于 DO 的本地存储能力有限,只能将带有关键词 w 索引的文件加密进行存储于 CSP,即 DO 通过 Encrypt 算法加密产生关键词密文,与加密的文件一起存储于 CSP 中.当 DU 想要检索带关键词 w 的文件时,通过 Trapdoor 算法产生搜索陷门传至 CSP,由 CSP 检索并通过 Test 算法验证是否存在匹配的关键词的文件.最后把搜索结果返回给 DU.若匹配成功,则返回加密的文件给 DU.DU 解密即可获取明文文件.

NBP-SCF-PAEKS 方案由 5 个多项式时间算法组成:

1) $GlobalSetup(\lambda)$.该算法由授权中心 AC 执行,输入安全参数 λ,输出全局公共参数 GP.

2) $KeyGen(GP)$.该算法由 DO 与 DU 分别执行完成,输入全局公共参数 GP,DO 输出公私钥对 sk_S 与 pk_S,而 DU 输出公私钥对 sk_R 与 pk_R.

3) $Encrypt(GP, sk_S, pk_R, w)$.该算法由 DO 执行,输入全局参数 GP、关键词 w、DO 私钥 sk_S、DU 公钥 pk_R,输出关键词密文 C_w,DO 将关键词密文 C_w 与加密的文件 C_f 传至 CSP 中存储.

4) $Trapdoor(GP, sk_R, pk_S, w')$.该算法由 DU 执行,输入全局参数 GP、检索的关键词 w'、DU 私钥 sk_R 以及 DO 的公钥 pk_S,输出搜索陷门 $T_{w'}$.

5) $Test(GP, C_w, T_{w'})$.CSP 收到 DU 的搜索陷门 $T_{w'}$,对关键词密文 C_w 与搜索陷门 $T_{w'}$ 测试.若匹配成功,则输出 1,并返回文件密文数据;否则输出 0.

3.2 安全模型

Boneh 等人首先引入了密文不可区分性的概念,它旨在防止外部攻击者在不知道关键字测试陷门的情况下获取加密文件中包含的任何关键字信息.而 Qin 等人[8]在此基础上延展提出多密文不可区分性.而陷门不可区分性保证了给定一个未知关键字的测试陷门,内部攻击者无法获得关于关键字的任何有用信息.

在 2.2 节所讨论的在线模式下外部攻击者关键词猜测攻击与离线模式下内部攻击者的关键词猜测攻击是目前公钥可搜索加密中需要解决的安全性问题.而本文所提出的公钥认证可搜索加密方案则可以抵抗这 2 类攻击,值得注意的是,由于方案的正确性,避免了外部攻击者的存在.假设 NBP-SCF-PAEKS 方案中存在一个外部攻击者,由该方案正确性定义可知,攻击者若生成了可被关键词陷门匹配的可搜索密文,则该攻击者是数据使用者(DU)所认可的数据拥有者(DO),与它是外部攻击者相矛盾.这限制了外部攻击者攻击的可能,使得方案更具安全性.

因此,提出 NBP-SCF-PAEKS 方案需要同时满足 2 点:1)适应性选择关键词攻击下的多关键词密文不可区分性(multi-keyword ciphertext indistinguishability under the adaptive chosen keyword attack, MKC-IND-CKA);2)适应性选择关键词攻击下的关键词陷门不可区分性(keyword trapdoor indistinguishability under the adaptive chosen keyword attack, KT-IND-CKA).MKC-IND-CKA 保证敌手不能区分其挑战的 2 个关键词集的密文,而 KT-IND-CKA 则保证敌手不能区分其挑战的 2 个关键词陷门.针对公钥认证可搜索加密方案,敌手可分为 2 类:外部攻击者与内部攻击者.这里定义外部攻击者为除 DO,DU 以及 CSP 之外的攻击者,内部攻击者为恶意的 CSP.

结合这 2 类敌手,MKC-IND-CKA 与 KT-IND-CKA 的安全性可以由挑战者 $\mathcal{B}$ 和敌手 $\mathcal{A}$(外部攻击者或者内部攻击者)之间的游戏模型 Game MKC-IND-CKA 和 Game KT-IND-CKA 来定义,游戏模型内容所述.

Game MKC-IND-CKA:

1) 系统初始化.$\mathcal{B}$ 首先运行 $GlobalSetup(\lambda)$ 和 $KeyGen(GP)$ 算法,产生全局参数 GP、DO 的公私钥 (sk_S, pk_S) 以及 DU 的公私钥 (sk_R, pk_R).并发送 GP, pk_S, pk_R 给 $\mathcal{A}$.

2) 询问阶段 1.$\mathcal{A}$ 对 $\mathcal{B}$ 发出以下一系列的适应性预言询问.

$O^{\text{Ciphertext}}$.给定任意关键词 $w \in KS_w$,$\mathcal{B}$ 运行 $Encrypt(GP, sk_S, pk_R, w)$ 算法并返回产生的关键词密文 C_w 给 $\mathcal{A}$.

O^{Trapdoor}.给定任意关键词 $w' \in KS_w$,$\mathcal{B}$ 运行 $Trapdoor(GP, sk_R, pk_S, w')$ 算法并返回产生的关键词陷门 $T_{w'}$ 给 $\mathcal{A}$.

O^{Test}.$\mathcal{A}$ 提交关键词密文 C_w 与关键词陷门 $T_{w'}$,$\mathcal{B}$ 运行 $\text{Test}(GP, C_w, T_{w'})$ 算法并返回结果给 $\mathcal{A}$.测试询问模拟敌手通过关键词测试询问作为预言机来验证单个关键词密文和单个关键词陷门是否匹配的攻击行为.

3) 挑战阶段.$\mathcal{A}$ 提交 2 个不同的关键词集 $w_0 = \{w_{0,1}, w_{0,2}, \cdots, w_{0,n}\}$ 和 $w_1 = \{w_{1,1}, w_{1,2}, \cdots, w_{1,n}\}$ 进行挑战,并且限制未在第一阶段询问过的关键词 $w_{0,i} w_{1,i}$ $(i \in [1,n])$ 的密文和陷门.$\mathcal{B}$ 对于 $i \in [1,n]$ 随机选取 $b \in \{0,1\}$,运行 $Encrypt(GP, sk_S, pk_R, w_{b,i})$ 并返回产生的关键词 $w_{b,i}$ 的挑战密文 $C^* = \{C_1^*, C_2^*, \cdots, C_n^*\}$ 给 $\mathcal{A}$.

4) 询问阶段 2.与询问阶段 1 一样,并且限制 $\mathcal{A}$ 不能询问关键词 $w = \{w_{0,1}, w_{0,2}, \cdots, w_{0,n}, w_{1,1}, w_{1,2}, \cdots, w_{1,n}\}$ 的密文、陷门.

5) 猜测.$\mathcal{A}$ 输出猜测结果 $b' \in \{0,1\}$.如果 $b = b'$,则 $\mathcal{A}$ 赢得游戏.所以,敌手 $\mathcal{A}$ 赢得游戏的优势为

$$Adv(\lambda)^{\text{MKC-IND}} = |Pr[b = b'] - 1/2|.$$

定义 3. 若不存在多项式时间敌手能够以不可忽略的优势赢得上述 Game MKC-IND-CKA,则可认为本方案满足适应性选择关键词攻击下的多关键词密文不可区分性安全.

Game KT-IND-CKA:

1) 系统初始化.与 Game MKC-IND-CKA 的初始化阶段一致.

2) 询问阶段 1.与 Game MKC-IND-CKA 的第一阶段询问一致.

3) 挑战阶段.$\mathcal{A}$ 提交 2 个不同的关键词 w_0, w_1 进行挑战,并且限制未在第一阶段询问过的关键词 w_0, w_1 的密文和陷门.$\mathcal{B}$ 随机选取 $b \in \{0,1\}$,运行 $Trapdoor(GP, sk_R, pk_S, w')$ 并返回产生的关键词 w_b 的挑战陷门 T_{w_b} 给 $\mathcal{A}$.

4) 询问阶段 2.与询问阶段 1 一样,并且限制 $\mathcal{A}$ 不能询问关键词 w_0, w_1 的密文、陷门.

5) 猜测.$\mathcal{A}$ 输出猜测结果 $b' \in \{0,1\}$.如果 $b = b'$,则 $\mathcal{A}$ 赢得游戏.所以,敌手 $\mathcal{A}$ 赢得游戏的优势为

$$Adv(\lambda)^{\text{KT-IND-CKA}} = |Pr[b = b'] - 1/2|$$

定义 4. 若不存在多项式时间敌手能够以不可忽略的优势赢得上述 Game KT-IND-CKA,则可认为本方案满足适应性选择关键词攻击陷门不可区分性.

4 方案描述

在 3.1 节给出了 NBP-SCF-PAEKS 方案的定义,其 5 个时间算法具体描述为:

1) $GlobalSetup(\lambda)$.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 函数 $H_1: G \rightarrow \{0,1\}^l$ 和 $H: \{0,1\}^* \times \{0,1\}^l \rightarrow Z_q^*$,$l$ 表示二进制长度.因此,输出全局参数为 $GP = (G, q, g, H, H_1, KS_w)$,其中 KS_w 为关键词集.

2) $KeyGen(GP)$.DO 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 $pk_S = (pk_{S_1}, pk_{S_2}) = (g^{sk_{S_1}}, g^{sk_{S_2}})$,DU 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 $pk_R = (pk_{R_1}, pk_{R_2}) = (g^{sk_{R_1}}, g^{sk_{R_2}})$.

3) $Encrypt(GP, sk_S, pk_R, w)$.DO 随机选取 $r \in Z_q^*$ 且 $r > H(w \| ss)$,计算关键词密文 $C_w = (C_1, C_2) = (pk_{R_2}^r, H_1(pk_{R_2}^{r-H(w\|ss)}))$,其中 $ss = H_1((pk_{R_1})^{sk_{S_1}})$.并将 C_w 与加密的文件上传至 CSP.

4) $Trapdoor(GP, sk_R, pk_S, w')$.DU 选定需要搜索的关键词 w',计算搜索陷门 $T_{w'} = g^{-sk_{R_2} \times H(w' \| ss_1)}$,其中 $ss_1 = H_1((pk_{S_1})^{sk_{R_1}})$.并将其上传至 CSP 检索.

5) $Test(GP, C_w, T_{w'})$.CSP 收到 DU 的搜索陷门 $T_{w'}$ 后,计算 $H_1(C_1 \times T_{w'}) = C_2$ 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.

方案正确性:

$$ss = H_1((pk_{R_1})^{sk_{S_1}}) = H_1((pk_{S_1})^{sk_{R_1}}) = ss_1;$$

$$H_1(C_1 \times T_{w'}) = H_1(pk_{R_2}^r \times g^{-sk_{R_2} \times H(w' \| ss_1)}) = H_1(g^{r \times sk_{R_2}} \times g^{-sk_{R_2} \times H(w' \| ss_1)}) = H_1(g^{sk_{R_2}(r - H(w' \| ss_1))}) = H_1(pk_{R_2}^{r - H(w' \| ss_1)});$$

若 $w' = w$,则等式 $H_1(C_1 \times T_{w'}) = C_2$ 成立,故方案正确有效.

5 安全性证明

本节参考文献[6]以及 Game-Hopping[18] 方法给出 NBP-SCF-PAEKS 方案在无随机预言机模型下的安全性证明.下面需要使用差别引理[18]:

引理 1[18]. 定义 S_1, S_2, E 为 3 个不同的事件且 E 为错误事件,使得事件 $S_1 | \neg E$ 发生当且仅当在事件 $S_2 | \neg E$ 发生时,有:

$$|Pr[S_1] - Pr[S_2]| \leqslant Pr[E].$$

定理 1. 若 Hash 函数 H 满足抗碰撞性、群 G 上 DL 假设是困难以及多项式时间内有限的 n 个关键词查询,则所提出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的安全.

证明. 假设 $\mathcal{A}$ 是针对本方案的适应性选择关键词攻击下多关键词密文不可区分性的安全的敌手,下面证明 $Adv^{\text{MKC-IND-CKA}}$ 是的优势是可忽略的.假设由 5 个子程序游戏 $Game_j$ ($j = 0,1,2,3,4$) 组成.假设 $\mathcal{A}$ 在子程序游戏中关键词猜测攻击正确(即 $b = b'$)事件为 X_j.

Game-Hopping 方法的证明过程如下:

1) 游戏 $Game_0$.该游戏为原始敌手游戏 Game MKC-IND-CKA.因此,$\mathcal{A}$ 赢得游戏的优势为

$$Adv^{\text{MKC-IND-CKA}} = |Pr[X_0] - 1/2|.$$

2) 游戏 $Game_1$.该游戏与 $Game_0$ 相同,区别在于 $\mathcal{B}$ 随机选取 $a, sk_{R_1}, sk_{R_2} \in Z_q^*$,计算 $pk_R = (pk_{R_1}, pk_{R_2}) = (g^{sk_{R_1}}, (g^a)^{sk_{R_2}})$,其中 g 为 G 的生成元,其他参数与 $Game_0$ 等同.显然,$Game_1$ 的参数与 $Game_0$ 的分布相同,即对 $\mathcal{A}$ 仍然是不可区分的.因此,$\mathcal{A}$ 在这 2 个游戏中猜测的概率相同,即:

$$Pr[X_1] = Pr[X_0].$$

3) 游戏 $Game_2$.该游戏与 $Game_1$ 相同,区别在 $\mathcal{B}$ 改变对 $\mathcal{A}$ 对密文与陷门的询问的应答方式以及挑战密文的产生方式.

在2次询问阶段中,$\mathcal{B}$ 应答 $\mathcal{A}$ 的有限次数内密文询问与陷门询问方式为:

O^{Encrypt}.$\mathcal{A}$ 提交关键词 $w_i \in KS_w$,$\mathcal{B}$ 运行 $Encrypt(GP, sk_S, pk_R, w)$ 算法并返回产生的关键词密文 $C_w=(C_1, C_2)=(pk_{R_2}^{r}, pk_{R_2}^{r-H(w\|ss)})$ 给 $\mathcal{A}$,其中:

$$ss=H_1((pk_{R_1})^{sk_{S_1}}).$$

O^{Trapdoor}.$\mathcal{A}$ 提交一个关键词 $w'\in KS_w$,$\mathcal{B}$ 运行 $Trapdoor(GP, sk_R, pk_S, w')$ 算法并返回产生的关键词陷门 $T_{w'}=g^{-sk_{R_2}\times H(w'\|ss_1)}$ 给 $\mathcal{A}$,其中:

$$ss_1=H_1((pk_{S_1})^{sk_{R_1}}).$$

O^{Test}.$\mathcal{A}$ 提交关键词密文 C_w 与关键词陷门 $T_{w'}$,$\mathcal{B}$ 运行 $Test(GP, C_w, T_{w'})$ 算法判断 $H_1(C_1\times T_{w'})=C_2$ 是否成立,若成立返回1给 $\mathcal{A}$,否则返回0.

在挑战阶段中,$\mathcal{A}$ 提交2个不同的关键词元组 $w_0=\{w_{0,1}, w_{0,2}, \cdots, w_{0,n}\}$ 和 $w_1=\{w_{1,1}, w_{1,2}, \cdots, w_{1,n}\}$ 进行挑战,$\mathcal{B}$ 随机选择 $r\in Z_q^*$ 和 $b\in\{0,1\}$,计算出:

$$C_{w_{b,i}}=(C_{1,i}^*, C_{2,i}^*)=(pk_{R_2}^{r^*}, H_1(pk_{R_2}^{r^*-H(w_{b,i}\|ss_1)}))$$

返回给 $\mathcal{A}$,其中:

$$ss_1=H_1((pk_{R_1})^{sk_{S_1}}).$$

若令 $r^*=r'/a$,$r-H^*(w_i\|ss)=r-H'(w_i\|ss)/a$ 则有:

$$C_1^*=pk_{R_2}^{r^*}=(g^{a\times sk_{R_2}})^{r'/a}=(g^{sk_{R_2}})^{r'}=pk_{R_2}^{r'},$$

$$C_2^*=pk_{R_2}^{r^*-H^*(w_i\|ss)}=$$

$$(g^{a\times sk_{R_2}})^{(r'-H'(w_i\|ss))/a}=pk_{R_2}^{r'-H'(w_i\|ss)}$$

因此,挑战密文 $C_{w_{b,i}}=(C_{1,i}^*, C_{2,i}^*)$ 是关键词 $w_{b,i}$ 的有效密文.

在游戏 $Game_2$ 中,$\mathcal{B}$ 能够正确应答各种预言询问及产生挑战密文.显然,$Game_1$ 与 $Game_2$ 是不可区分的.因此,$\mathcal{A}$ 在2个游戏中猜测正确的概率相同,即:

$$Pr[X_2]=Pr[X_1].$$

4) 游戏 $Game_3$.该游戏与 $Game_2$ 相同,区别在于若发生下列事件之一,$\mathcal{B}$ 终止游戏.

事件 E_1.$\mathcal{A}$ 向 $\mathcal{B}$ 作关键词密文询问,其输入关键词 w 满足 $w\neq w_{b,i}$,但 $C_2=C_{2,i}^*$;

事件 E_2.$\mathcal{A}$ 向 $\mathcal{B}$ 作关键词陷门询问,其输入关键词 w 满足 $w\neq w_{b,i}$,但 $H(w\|ss_1)=H(w_{b,i}\|ss_1)$.

显然,若 $E_1\vee E_2$ 不发生,$\mathcal{A}$ 在 $Game_2$ 和 $Game_3$ 中是不可区分的.由差别引理可得,$Pr[E_1\vee E_2]=|Pr[X_2]-Pr[X_3]|$.此外,若事件 E_1 发生,则必然存在针对 Hash 函数 H 的抗碰撞的敌手 $\mathcal{A}_1$,其优势为 $n\times Adv^H\geqslant Pr[E_1]$.同理,若事件 E_2 发生,也必然存在针对 Hash 函数 H 的抗碰撞的敌手 $\mathcal{A}_1$,其优势为 $n\times Adv^H\geqslant Pr[E_2]$.因此:

$$|Pr[X_2]-Pr[X_3]|\leqslant 2n\times Adv^H.$$

5) 游戏 $Game_4$.该游戏与 $Game_3$ 相同,区别在于 $\mathcal{B}$ 使用群 G 的随机元素 Z 计算挑战密文 $C_{w_{b,i}}=(C_{1,i}^*, C_{2,i}^*)$ 中的 $C_{2,i}^*=Z^{r^*-H(w_{b,i}\|ss)}$.显然,$\mathcal{B}$ 无需知道 a 以及 sk_{R_2} 的值,仅通过 $(g, g^{sk_{R_2}}, (g^a)^{sk_{R_2}})$ 元组中 $(g^a)^{sk_{R_2}}$ 值即可应答 $\mathcal{A}$ 的所有询问以及挑战密文.显然,$Game_4$ 和 $Game_3$ 是一致的,除非敌手可以通过不可忽略的概率优势区分 Z 和 $(g^a)^{sk_{R_2}}$(即解决 DL 困难假设).假设敌手 $\mathcal{A}_2$ 成功的优势为 Adv^{DL},由差别引理可得,$|Pr[X_3]-Pr[X_4]|\leqslant n\times Adv^{\text{DL}}$.并且 Z 为群 G 的一个随机元素,因此 $\mathcal{A}$ 猜中正确的概率为

$$Adv^{\text{MKC-IND-CKA}}=|Pr[X_4]-1/2|.$$

结束 Game-Hopping 游戏并分析 $\mathcal{A}$ 的优势.

$$Adv^{\text{MKC-IND-CKA}}=|Pr[X_0]-1/2|\leqslant$$
$$|Pr[X_0]-Pr[X_1]|+|Pr[X_1]-Pr[X_2]|+$$
$$|Pr[X_2]-Pr[X_3]|+|Pr[X_3]-Pr[X_4]|+$$
$$|Pr[X_4]-1/2|.$$

因此,综合上述的游戏方程,可以得出如下结论:

$$Adv^{\text{MKC-IND-CKA}}=n\times Adv^{\text{DL}}+2n\times Adv^H.$$

本文在多项式时间内 n 个(多)关键挑战密文查询且基于 Hash 函数 H 是抗碰撞的并且基于离散对数 DL 的困难假设下,$Adv^{\text{MKC-IND-CKA}}$ 是可忽略的,即本方案满足适应性选择关键词攻击下的多关键词密文不可区分性. 证毕.

定理2. 若 Hash 函数 H 满足抗碰撞性且群 G 上 HDH 假设是困难的,则所提出方案满足适应性选择关键词攻击的陷门不可区分性的安全性.

证明. 假设 $\mathcal{A}$ 是针对本方案的适应性选择关键词攻击的陷门不可区分性的安全性的敌手,下面证明 $Adv^{\text{KT-IND-CKA}}$ 是的优势是可忽略的.假设由5个子程序游戏 $Game_j$($j=0,1,2,3,4$)组成.假设 $\mathcal{A}$ 在子程序游戏中关键词猜测攻击正确(即 $b=b'$)事件为 X_j.

Game-Hopping 方法的证明过程为:

1) 游戏 $Game_0$.该游戏为原始敌手游戏 Game KT-IND-CKA.因此,$\mathcal{A}$ 赢得游戏的优势为

$$Adv^{\text{KT-IND-CKA}}=|Pr[X_0]-1/2|.$$

2) 游戏 $Game_1$.该游戏与 $Game_0$ 相同,区别在于 $\mathcal{B}$ 随机选取 $a, b, sk_{R_2}\in Z_q^*$,计算 $pk_{S_1}=g^b$,$pk_R=(pk_{R_1}, pk_{R_2})=(g^a, g^{sk_{R_2}})$,其中 g 为 G 的生成元,其他参数与 $Game_0$ 等同.显然,$Game_1$ 的新参数与

$Game_0$ 的分布相同,即对 $\mathcal{A}$ 仍然是不可区分的.因此,$\mathcal{A}$ 在这 2 个游戏中猜测的概率相同,即:

$$Pr[X_1]=Pr[X_0].$$

3) 游戏 $Game_2$.该游戏与 $Game_1$ 相同,区别在 $\mathcal{B}$ 改变对 $\mathcal{A}$ 对关键词密文询问以及关键词陷门询问的应答方式以及挑战陷门的产生方式.

在 2 次询问阶段中,$\mathcal{B}$ 应答 $\mathcal{A}$ 的密文询问、陷门方式为:

O^{Enerypt}.$\mathcal{A}$ 提交一个关键词 $w\in KS_w$,$\mathcal{B}$ 运行 $Encrypt(GP,sk_S,pk_R,w)$ 算法并返回产生的关键词密文 $C_w=(C_1,C_2)=(pk_{R_2}^r,pk_{R_2}^{r-H(w_i\|ss)})$ 给 $\mathcal{A}$,其中,

$$ss_1=H_1(g^{ab}).$$

O^{Trapdoor}.$\mathcal{A}$ 提交一个关键词 $w'\in KS_w$,$\mathcal{B}$ 运行 $Trapdoor(GP,sk_R,pk_S,w')$ 算法并返回产生的关键词陷门 $T_{w'}=g^{-sk_{R_2}\times H(w'\|ss_1)}$ 给 $\mathcal{A}$,其中,

$$ss_1=H_1(g^{ab}).$$

O^{Test}.$\mathcal{A}$ 提交关键词密文 C_w 与关键词陷门 $T_{w'}$,$\mathcal{B}$ 运行 $Test(GP,C_w,T_{w'})$ 算法判断 $H_1(C_1\times T_{w'})=C_2$ 是否成立,若成立返回 1 给 $\mathcal{A}$,否则返回 0.

在挑战阶段中,$\mathcal{A}$ 提交 2 个不同的关键词 w_0 和 w_1 进行挑战,$\mathcal{B}$ 随机选择 $b\in\{0,1\}$,计算出 $T_{w_b}=g^{-sk_{R_2}\times H(w_b\|ss_1)}$ 返回给 $\mathcal{A}$,其中:

$$ss_1=H_1(g^{ab}).$$

因此,挑战陷门 T_{w_b} 为有效陷门.

在游戏 $Game_2$ 中,$\mathcal{B}$ 能够正确应答各种预言询问及产生挑战陷门.显然,$Game_1$ 与 $Game_2$ 是不可区分的.因此,$\mathcal{A}$ 在 2 个游戏中猜测正确的概率相同,即:

$$Pr[X_2]=Pr[X_1].$$

4) 游戏 $Game_3$.该游戏定义与定理 1 证明中 $Game_3$ 相同.

因此,存在抗碰撞的敌手 $\mathcal{A}_1$ 的优势为

$$|Pr[X_2]-Pr[X_3]|\leqslant 2Adv^H.$$

5) 游戏 $Game_4$.该游戏与 $Game_3$ 相同,区别在于 $\mathcal{B}$ 使用群 G 的随机元素 Z 代替 $H_1(g^{ab})$ 来计算挑战陷门 T_{w_b}.显然,$\mathcal{B}$ 无需知道 a 和 b 的值,仅通过 HDH 元组下的 (H_1,g,g^a,g^b,Z) 即可应答 $\mathcal{A}$ 的所有询问以及挑战陷门.显然,$Game_4$ 和 $Game_3$ 是一致的,除非敌手可以通过不可忽略的概率优势区分 Z 和 $H_1(g^{ab})$(即解决 HDH 困难假设).假设敌手 $\mathcal{A}_3$ 成功的优势为 $Adv^{\text{KT-IND-CKA}}$,由差别引理可得:

$$|Pr[X_3]-Pr[X_4]|\leqslant Adv^{\text{HDH}}.$$

并且 Z 为群 G 的一个随机元素,因此 $\mathcal{A}$ 猜中正确的概率为

$$Adv^{\text{KT-IND-CKA}}=|Pr[X_4]-1/2|.$$

结束 Game-Hopping 游戏并分析 $\mathcal{A}$ 的优势,有:

$$Adv^{\text{KT-IND-CKA}}=|Pr[X_0]-1/2|\leqslant$$
$$|Pr[X_0]-Pr[X_1]|+|Pr[X_1]-Pr[X_2]|+$$
$$|Pr[X_2]-Pr[X_3]|+|Pr[X_3]-Pr[X_4]|+$$
$$|Pr[X_4]-1/2|.$$

综合上述的游戏方程,可以得出结论:

$$Adv^{\text{KT-IND-CKA}}=Adv^{\text{HDH}}+2Adv^H.$$

由于 Hash 函数 H 是抗碰撞的并且基于 HDH 的困难假设下,$Adv^{\text{KT-IND-CKA}}$ 是可忽略的,即本方案满足适应性选择关键词攻击陷门不可区分性. 证毕.

6 性能分析

本文的 NBP-SCF-PAEKS 方案是设计非双线性对下且在公共通道能够抵抗在线外部攻击者关键词猜测攻击和离线内部攻击者关键词猜测攻击的公钥认证可搜索加密方案,该方案高效安全可行.

表 1 给出本文方案与其他方案的功能比较.其中 MKC-IND-CKA 表示适应性选择关键词攻击的多关键词密文不可区分性安全,Out-online-KGA 表示在线模式下外部攻击者关键词猜测攻击 In-offline-KGA 表示离线模式下内部攻击者的关键词猜测攻击.

Table 1 Security Properties Comparison

表 1 安全性能比较

Scheme	SCF-PEKS[3]	SCF-PEPCKS[6]	PAEKS[4]	Hwang, et al.[7]	PAEKSR[8]	Ours
Secure Channel	○	○	○	○	○	○
MKC-IND-CKA Security	○	○	×	×	○	○
AgainstOut-online-KGA	×	○	○	○	○	○
Against In-offline-KGA	×	○	○	×	○	○

Note: "○" means the requirement is met; "×" means the requirement is not met.

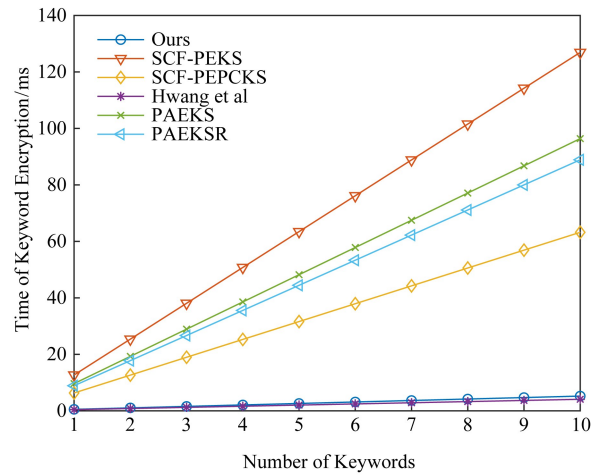
表 2 给出了本文方案与其他方案的的效率比较.其中符号 p,e 和 h 分别表示双线性对运算、群 G 中的模幂运算以及 Hash 运算,其系数表示运算次数.符号 $|G|$,$|G_T|$,$|Z_q^*|$ 和 λ 分别表示群 G 中元素的长度、群 G^{T}(双线性表示 $G\times G\rightarrow G_T$)中元素的长度、群 Z_q^* 元素的长度以及 Hash 值的长度.

Table 2 Efficiency Comparison of Different Schemes

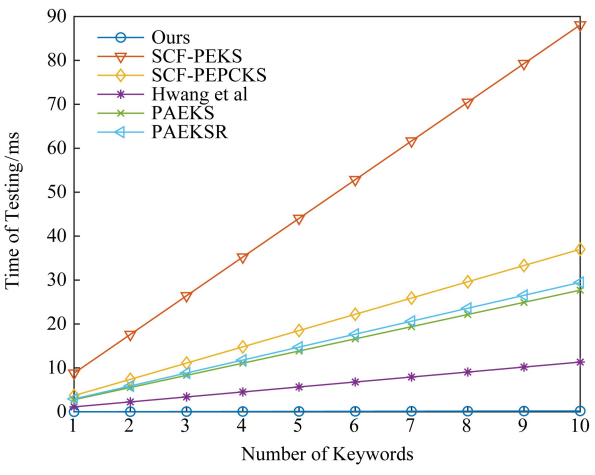
表 2 不同方案的效率比较

Scheme	SCF-PEKS[3]	SCF-PEPCKS[6]	PAEKS[4]	Hwang, et al[7]	PAEKSR[8]	Ours
Encrypt	$2p+2e+h$	$p+4e+3h$	$3e+h$	$2e+h$	$p+3e+2h$	$3e+2h$
Trapdoor	$e+h$	$2e+2h$	$p+e+h$	$3e+h$	$2e+h$	$2e+2h$
Test	$p+e+h$	$p+e+h$	$2p$	$5e+h$	$p+h$	$2e$
Ciphertext Size	$\|G\|+\lambda$	$\|G\|+\lambda$	$2\|G\|$	$3\|G\|$	$\|G\|+\lambda$	$\|G\|+\lambda$
Trapdoor Size	$\|G\|$	$\|G\|$	$\|G_T\|$	$4\|G\|$	$\|G\|$	$\|G\|$

为了直观展示 NBP-SCF-PAEKS 方案与其他方案关键词的运算时间消耗对比,进行了仿真实验.实验环境是在操作系统为 Ubuntu 16.04 LTS,处理器为 Intel® Core™ i5-4210U CPU @2.40 GHz,运行内存为 12 GB 以及 GMP 库[28]、PBC 库[29]下进行的.我们采用与文献[6]相同的实验条件下的 512 b 循环群以及 SHA-256 的 Hash 函数进行仿真.借助文献[6]与文献[8]仿真的 SCF-PEKS,SCF-PEPCKS,PAEKS 以及 PAEKSR 方案的关键词加密与测试的数据结果进行对比.仿真对比结果如图 2 所示.对于单个关键词下,NBP-SCF-PAEKS 方案关键词加密所需的时间消耗为 0.522 ms,陷门产生所需的时间消耗为 0.4 ms,测试所需的时间消耗为 0.02 ms.因此,该方案的 3 个多项式时间算法的运行时耗均在 0.1 毫秒级上,相对于包含双线性运算下的 SCF-PEKS[3],PAEKS[4],SCF-PEPCKS[6],PAEKSR[8] 以及 Hwang 等人[7]方案的计算效率要高.此外,该方案在关键词密文与关键词陷门的存储所需容量与 SCF-PEKS[3],SCF-PEPCKS[6] 以及 PAEKSR[8] 相等,相对于 PAEKS[4] 以及 Hwang 等人[7]方案要低,如图 3 所示:



(a) Computation cost of keyword encryption



(b) Computation cost of keyword testing

Fig. 2 Computation cost of keyword encryption and testing

图 2 关键词加密与验证的计算消耗比较

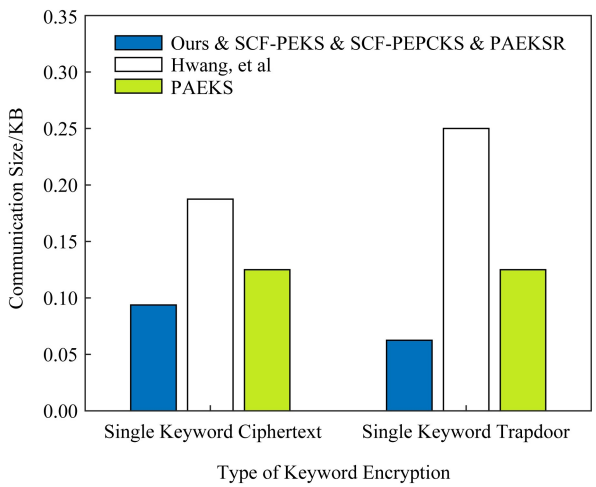


Fig. 3 Communication size of keyword ciphertext and trapdoor

图 3 关键词密文与关键词陷门通信存储大小比较

7 总结与展望

本文提出一个基于非双线性对运算、公共通道的带关键词搜索的公钥认证可搜索加密方案.与过去的其他方案进行功能与效率的比较,NBP-SCF-PAEKS方案具有非双线性对的高效运算,能够满足抵抗离线模式下内部攻击者的关键词猜测攻击和在线模式下外部攻击者的关键词猜测攻击的安全性并且具有认证的功能,使得本文方案更具有应用意义,更适合于计算能力有限的设备上使用.

随着设备的更新换代以及量子计算机的研发促使计算机的计算能力提高,导致离散对数的密码体制下的云数据存在潜在的泄露风险.因此,构造可行性高的抗量子计算的公钥可搜索加密是下一步工作重心.

参 考 文 献

[1] Song D X, Wagner D, Perrig A. Practical techniques for searches on encrypted data [C] //Proc of 2000 IEEE Symp on Security and Privacy (S&P 2000). Piscataway, NJ: IEEE, 2000: 44-55

[2] Boneh D, Di C G, Ostrovsky R, et al. Public key encryption with keyword search [C] //Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2004: 506-522

[3] Baek J, Safavi-Naini R, Susilo W. Public key encryption with keyword search revisited [C] //Proc of Int Conf on Computational Science and Its Applications. Berlin: Springer, 2008: 1249-1259

[4] Huang Qiong, Li Hongbo. An efficient public-key searchable encryption scheme secure against inside keyword guessing attacks [J]. Information Sciences, 2017, 403: 1-14

[5] Wu T Y, Chen C M, Wang K H, et al. Security analysis of a public key authenticated encryption with keyword search scheme [C] //Proc of Int Conf on Intelligent Information Hiding and Multimedia Signal Processing. Berlin: Springer, 2018: 178-183

[6] Lu Yang, Li Jiguo, Zhang Yichen. SCF-PEPCKS: Secure channel free public key encryption with privacy-conserving keyword search [J]. IEEE Access, 2019, 7: 40878-40892

[7] 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

[8] Qin Baodong, Chen Yu, Huang Qiong, et al. Public-key authenticated encryption with keyword search revisited: Security model and constructions [J]. Information Sciences, 2020, 516: 515-528

[9] Yau W C, Heng S H, Goi B M. Off-line keyword guessing attacks on recent public key encryption with keyword search schemes [C] //Proc of Int Conf on Autonomic and Trusted Computing. Berlin: Springer, 2008: 100-105

[10] Fang L, Susilo W, Ge C, et al. A secure channel free public key encryption with keyword search scheme without random oracle [C] //Proc of Int Conf on Cryptology and Network Security. Berlin: Springer, 2009: 248-258

[11] Emura K, Miyaji A, Rahman M S, et al. Generic constructions of secure-channel free searchable encryption with adaptive security [J]. Security and Communication Networks, 2015, 8(8): 1547-1560

[12] Rhee H S, Park J H, Susilo W, et al. Trapdoor security in a searchable public-key encryption scheme with a designated tester [J]. Journal of Systems and Software, 2010, 83(5): 763-771

[13] Noroozi M, Eslami Z. Public-key encryption with keyword search: A generic construction secure against online and offline keyword guessing attacks [J]. Journal of Ambient Intelligence and Humanized Computing, 2020, 11(2): 879-890

[14] Lu Yang, Wang Gang, Li Jiguo. Keyword guessing attacks on a public key encryption with keyword search scheme without random oracle and its improvement [J]. Information Sciences, 2019, 479: 270-276

[15] Xu Hailin, Lu Yang, Searchable public key encryption secure against keyword guessing attacks [J] Computer Engineering and Applications, 2018, 54(24): 108-115 (in Chinese)
(徐海琳, 陆阳. 抗关键词猜测攻击的可搜索公钥加密方案[J]. 计算机工程与应用, 2018,54 (24): 108-115)

[16] Chen Rongmao, Mu Yi, Yang Guomin, et al. Server-Aided public key encryption with keyword search [J]. IEEE Transactions on Information Forensics and Security, 2016, 11(12): 2833-2842

[17] Zhang Yuan, Xu Chunxiang, Ni Jianbing, et al. Blockchain-assisted public-key encryption with keyword search against keyword guessing attacks for cloud storage [J]. IEEE Transactions on Cloud Computing, 2019 [2020-05-01]. https://ieeexplore.ieee.org/abstract/document/8737775

[18] Dent A W. A note on game-hopping proofs [EB/OL]. Nevada, USA: International Association for Cryptologic Research, 2006 [2019-12-01]. https://eprint.iacr.org/2006/260.pdf

[19] Miao Yinbin, Weng Jian, Liu Ximeng, et al. Enabling verifiable multiple keywords search over encrypted cloud data [J]. Information Sciences, 2018, 465: 21-37

[20] Zhou Quan, Yang Ningbin, Xu Shumei. Fault-tolerant and verifiable public key searchable encryption scheme based on FBDH algorithm [J]. Netinfo Security, 2020, 20(3): 29-35 (in Chinese)
(周权, 杨宁滨, 许舒美. 基于FBDH算法的容错可验证公钥可搜索加密方案[J]. 信息网络安全, 2020, 20(3): 29-35)

[21] Guo Lifeng, Li Zhihao, Hu Lei. Efficient public encryption scheme with keyword search for cloud storage [J]. Journal of Computer Research and Development, 2020, 57(7): 1404-1414 (in Chinese)
(郭丽峰, 李智豪, 胡磊. 面向云存储的带关键词搜索的公钥加密方案[J]. 计算机研究与发展, 2020, 57(7): 1404-1414)

[22] Xu Peng, Jin Hai, Wu Qianhong, 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

[23] Li Jiguo, Lin Xiaonan, Zhang Yichen, et al. KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage [J]. IEEE Transactions on Services Computing, 2016, 10(5): 715-725

[24] Gao Jiaxin, Sun Jiameng, Qin Jing. Traceable outsourcing attribute-based encryption with attribute revocation [J]. Journal of Computer Research and Development, 2019, 56(10): 2160-2169 (in Chinese)
(高嘉昕, 孙加萌, 秦静. 支持属性撤销的可追踪外包属性加密方案[J]. 计算机研究与发展, 2019, 56(10): 2160-2169)

[25] Dong C, Russello G, Dulay N. Shared and searchable encrypted data for untrusted servers [J]. Journal of Computer Security, 2011, 19(3): 367-397

[26] Sadeghi A R, Steiner M. Assumptions related to discrete logarithms: Why subtleties make a real difference [C] //Proc of Int Conf on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2001: 244-261

[27] Abdalla M, Bellare M, Rogaway P. The oracle Diffie-Hellman assumptions and an analysis of DHIES [C] //Proc of Cryptographers' Track at the RSA Conf. Berlin: Springer, 2001: 143-158

[28] The GNU Multiple Precision Arithmetic Library [EB/OL]. [2020-02-15]. https://gmplib.org/

[29] Lynn B. PBC Library: The pairing-based cryptography library [EB/OL]. [2020-06-01]. https://crypto.stanford.edu/pbc/

Yang Ningbin, born in 1996. Master candidate. His main research interests include cryptography and cloud security.

Zhou Quan, born in 1971. PhD, associate professor. His main research interests include information security and cloud computing.

Xu Shumei, born in 1995. Master. Her main research interests include authentication agreement, privacy protection and smart grid.