群组内基于区块链的匿名可搜索加密方案

王泽锐[1,2], 郑 东[1,2], 郭 瑞[1,2], 朱天泽[1,2]

[1] 西安邮电大学网络空间安全学院 西安 中国 710121
[2] 西安邮电大学无线网络安全技术国家工程实验室 西安 中国 710121

摘要 公钥可搜索加密技术不仅可以保护云存储中用户的数据隐私, 还可以提供数据在不解密的条件下进行密态数据搜索的功能。针对群组内用户进行密文安全搜索的需求, 本文以群组为单位使用基于身份的广播加密进行数据的加密与密钥封装, 以基于身份的可搜索加密构造关键词密文及关键词陷门, 提出了一种群组内的公钥可搜索加密方案, 保证了只有群组内的授权用户才可以进行安全搜索并解密数据。此外, 为保护用户的身份隐私, 通过构造匿名身份, 避免了因云服务器好奇行为而造成的用户身份泄露问题。同时, 在按需付费的云环境中, 为了防止云服务器向用户返回部分或不正确的搜索结果, 文章结合区块链技术, 使用区块链作为可信第三方, 利用智能合约的可信性, 在用户验证搜索结果正确后向云服务器支付搜索费用, 解决了用户与云服务器之间的公平支付问题。并加入了违规名单机制, 防止恶意用户对系统可用性造成影响。在安全性方面, 通过基于判定性双线性 Diffie-Hellman 问题与判定性 Diffie-Hellman 问题进行安全性分析, 证明了在随机谕言机模型与标准模型下方案满足关键词密文与关键词陷门的不可区分性。最后, 通过功能对比表明本方案有较强的实用性, 利用 Charm-crypto 密码库对方案进行效率对比, 其结果表明本方案与其他相关方案相比具有较低的计算以及通信开销。

关键词 匿名可搜索加密; 群组共享; 区块链; 智能合约; 公平支付
中图法分类号 TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2022.05.09

Blockchain-Enabled Anonymous Searchable Encryption Scheme in the Group Communication

WANG Zerui[1,2], ZHENG Dong[1,2], GUO Rui[1,2], ZHU Tianze[1,2]

[1] School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
[2] National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Abstract The public-key searchable encryption technology not only protects the data privacy of users in the cloud storage, but also provides the function of searching encrypted data without decryption. To resolve the demands of ciphertext secure search for the group users, this paper uses identity-based broadcast encryption to encrypt data and encapsulate key, and used identity-based searchable encryption to construct keywords ciphertext and keywords trapdoor. A public-key searchable encryption scheme within the group is proposed to ensure that only the authorized users in the group can search and decrypt the data safely. In addition, in order to protect the privacy of users' identity, anonymous identity is constructed to avoid the problem of users' identity leakage caused by the curious behavior of cloud server. At the same time,in according to the need to pay cloud environment,in order to prevent the cloud server from returning partial or incorrect search results to the users. The paper combined with blockchain technology, using blockchain as a trusted third party, take advantage of the credibility of smart contracts, after the user authenyicated the search results is the right and then pay the searching fee to the cloud server, solved the fair payment issues between the users and the cloud server. In addition, a violation list mechanism is added to prevent malicious users from affecting system availability. In terms of security, security analysis is carried out based on the decisional bilinear Diffie-Hellman problem and the decisional Diffie-Hellman problem, and it is proved that the scheme satisfies the indiscriminability of key word ciphertext and key word trapdoor under the random oracle model and the standard model. Finally, through the function comparison shows that the scheme has strong practicability.The efficiency of the proposed scheme is compared with that of other related schemes by using the Charm-crypto cipher library, and the results show that the proposed scheme has lower computational and communication costs compared with other related schemes.

Key words anonymous searchable encryption; group sharing; blockchain; smart contracts; payment fairness

---

通讯作者: 王泽锐, 硕士, Email: wangzr0730@163.com。

国家自然科学基金(No. 62072369, No. 62072371, No. 61802303, No. 61772418),陕西省重点研发计划(No. 2020ZDLGY08-04, No. 2019KW-053),陕西省创新能力支持计划(No. 2020KJXX-052, No. 2017KJXX-47),陕西省自然科学基金(No. 2019JQ-866, No. 2018JZ6001),陕西省教育厅科研项目(No. 19JK0803),青海省基础研究计划项目(No. 2020-ZJ-701)
收稿日期: 2021-02-06; 修改日期: 2021-08-18; 定稿日期: 2022-03-15

1 引言

随着信息技术的发展, 企业和个人用户产生的数据呈爆发式增长态势, 海量数据导致本地存储压力增大。且本地存储存在极大风险, 一旦服务器出现故障, 将对用户数据造成严重损失。因此, 云存储作为一种新兴的数据管理模式, 以其使用便捷、存储空间大、节约成本、在任何时间、任何地点都可以对数据进行访问等优势受到越来越多用户的欢迎[1]。然而, 云存储服务也存在许多问题。首先, 云服务器通常是由云服务商提供的, 作为一个独立的实体, 数据存储至云服务器, 由于其自身的经济价值, 经常遭受黑客攻击, 造成数据泄露。其次, 云服务器并非完全可信的, 用户将数据存储在云服务器上, 云服务器可能在用户不知情的情况下对数据进行篡改或者删除, 对数据的完整性造成破坏。为了解决云存储环境下数据安全的问题, 用户通常将数据进行加密后上传至云服务器。然而, 在数据加密后又将面临密态数据检索困难的问题[2]。

安全搜索是指对加密数据的有效检索, 为了解决加密数据存储在云服务器上时, 云服务器半诚实且好奇的条件下如何利用云服务器进行安全的关键词检索的问题。2000 年, Song 等人[3]首次提出了一对一的对称可搜索加密方案, 数据拥有者产生加密数据和关键词密文上传至云服务器, 云服务器通过数据使用者生成的陷门对整个加密数据进行搜索, 得到包含该关键词的密文数据。Boneh 等人[4]首次提出了多对一带有关键词搜索的公钥可搜索方案(Public Key Encryption with Keyword Search, PEKS)并定义了公钥可搜索加密安全性的概念, 但该方案在密钥的传输中存在被敌手窃取的安全隐患。为了解决这个问题, Baek 等人[5]提出了在无安全信道条件下的公钥可搜索加密方案(Secure Channel Free Public Key Encryption with Keyword Search, SCF-PEKS), 在该方案中数据拥有者利用使用者和云服务器的公钥构造 PEKS 密文, 使用者利用自身私钥和云服务器公钥构造陷门, 在测试时云服务器只有使用自身的私钥才可以匹配正确, 保证了数据在无安全信道下传输。为了提高可搜索加密方案的功能性, 文献[6-7]分别提出了带有连接关键字的可搜索加密方案(Public Key Encryption with Conjunctive Field Keyword Search, PECKS)。

在公钥可搜索加密的安全性方面, Boneh 等人[4]证明了该方案是基于语义安全的, 却无法抵抗关键词猜测攻击。Tang 等人[8]提出了可以抵抗关键词猜测攻击的方案。Rhee 等人[9]指出文献[5]的方案不可以抵抗离线关键词猜测攻击, 提出了“陷门不可区分性”的概念, 指出公钥可搜索加密满足陷门不可区分性是抵抗离线关键词猜测攻击的充分条件, 并设计出一个具有陷门不可区分性的无安全信道的公钥可搜索加密方案。Xu 等人[10]提出了双陷门方案, 使该方案可以抵抗内部关键词猜测攻击。Qin 等人[11]提出了多密文不可区分性的概念, 使该方案可以同时抵抗选择多关键词攻击和关键词猜测攻击。陆海宁[12]提出了可隐藏搜索模式的对称可搜索加密方案, 该方案将搜索结果关键词进行分组, 同组单词在搜索时生成相同的陷门, 从而使敌手无法区分用户进行检索的关键词。

为了减小公钥基础设施建立以及证书维护的开销, Boneh 等人在文献[13]中提出一个实用的基于身份的加密体制(Identity Based Encryption, IBE), 以用户的身份、地址、电子邮箱等标识信息作为用户的公钥, 用户的私钥通过密钥生成中心(Private Key Generation, PKG)生成。Abdalla 等人[14]给出了 IBE 到 PEKS 的转换, 提出基于身份的可搜索加密方案(Indetity Based Ecrtyption with Keyword Search, IBEKS)且支持临时关键词搜索。Yang 等人在文献[15]提出了一个满足关键词密文和陷门不可区分性的指定服务器基于身份的可搜索加密方案, 但是在该方案中如果敌手穷举关键字集合, 则可以从陷门中获得关键词信息。王少辉等人[16]在文献[15]的基础上进行改进, 提出了一个高效的指定测试者的基于身份可搜索加密方案, 证明了该方案在随机谕言模型下满足适应性选择消息攻击的密文和陷门的不可区分性, 可以有效抵御离线关键词猜测攻击。魏晶等人[17]提出一种指定发送者的可搜索加密方案, 该方案在满足关键词密文和陷门的不可区分性的基础上还满足抵抗内部敌手的关键词猜测攻击。牛淑芬等人[18]提出了一种在加密邮件系统中基于身份的可搜索加密方案, 该方案通过在密文和陷门生成中加入身份信息来进行相互认证, 同时指定服务器进行搜索, 保证用户隐私不被泄露。Ma 等人[19]提出了一种应用于工业物联网环境下无安全信道下的基于身份无证书可搜索加密方案, 并证明了该方案在选择关键字猜测攻击下是安全的。张玉磊等人[20]将基于身份的密码体制与无证书密码相结合, 提出了一种基于无证书的多服务器可搜索加密方案, 将存储与搜索功能分配给不同的服务器, 减轻了单一服务器环境下服务器的计算开销。文献[21]将基于身份的广播加密[22]与可搜索加密相结合, 提出一种带有用户授权

的数据共享可搜索加密方案, 通过广播加密使数据使用者可以自主授权密文数据的访问权限, 通过用户身份指定用户的搜索权限。朱敏惠等人[23]提出了支持代理重加密的基于身份可搜索加密方案, 并且证明了该方案能抵抗适应性选择身份和选择明文攻击。然而, 在基于身份的可搜索加密方案中, 云服务器作为一个半诚实且好奇的实体, 会因为其好奇行为而造成用户身份泄露, 从而对用户的隐私安全造成威胁。采用匿名身份可以有效的解决这个问题。夏逸珉等人[24]提出了一种在标准模型下基于身份的匿名加密方案, 解决了接收者匿名性保护的问题, 并证明了该方案在选择明文攻击下是不可区分的。本文通过 PKG 为数据使用者生成假名, 使用假名作为该用户的唯一标识, 这种情况下即使云服务器获得了数据使用者的匿名身份, 但也无法获得其真实身份。

但是在实际应用中, 云服务器作为一个并非完全可信的实体, 可能存在一些半诚实且好奇的行为。随着区块链技术的发展与应用, 利用区块链技术可以解决传统方案中第三方服务器半诚实且好奇的问题。区块链是一个分布式的账本与数据库, 具有去中心化, 不可篡改, 公开透明等优点[25]。这些特点保证了区块链的“诚实”与“透明”, 为区块链创造信任奠定基础。利用区块链技术能够解决信息不对称问题, 实现多个主体之间的协作信任与一致行动。将区块链与可搜索加密相结合, 极大的提升了可搜索加密方案的可用性。2017 年 Li 等人[26]提出了基于区块链的对称可搜索加密方案, 杜瑞忠等人[27]在此基础上进行了修改, 使该方案既可以防止内部关键词猜测攻击, 又保证了系统的可用性。文献[28-29]基于区块链机制分别提出了应用在电子医疗病例下的可搜索加密方案。翁昕耀等人[30]提出了一种基于区块链的结果可追溯的可搜索加密方案, 通过第三方可信机构验证数据传输过程中的一致性, 并利用区块链记录验证结果以防篡改。在按需付费的云存储环境下, 云服务器作为一个不可信的第三方, 会存在欺诈行为, 即云服务器给数据使用者返回部分搜索结果或者错误的搜索结果而收取全部的搜索费。针对云服务器不可信的问题, 黑一鸣等人[31]提出了一种基于区块链的可公开验证分布式云存储系统, 使用智能合约保证数据服务交易公平, 并提升了系统判罚的时效性。闫玺玺等人[32]提出了基于区块链的且支持验证的属性基可搜索加密方案, 将对称可搜索加密与属性加密(Attribute Based Encryption, ABE)相结合实现了一对多可搜索加密, 同时解决了用户在使用可搜索加密方案时的检索公平性问题。

综合上述分析, 为了解决群组内用户的密文共享与安全搜索问题和用户与服务器之间公平支付的问题。本文提出了一种群组内基于区块链的匿名可搜索加密方案, 本文的贡献如下:

(1) 结合基于身份的可搜索加密和广播加密体制, 实现了在群组内的密文共享和安全搜索。此外, 群组内用户采用匿名方式进行搜索, 保证了云服务器不会获取用户身份信息。并结合区块链技术, 解决了云服务器与用户之间的公平支付问题。

(2) 本方案验证了匹配、解密、匿名追责算法的正确性。基于判定性双线性 Diffie-Hellman 问题和判定性 Diffie-Hellman 问题, 证明了在选择明文攻击下本方案具有关键词密文及陷门的不可区分性。

(3) 通过 Charm-crypto 密码库进行仿真模拟, 与其他方案在效率方面进行对比, 其结果表明本方案在确保安全性的前提下具有较低的计算开销与较高的实用价值。

2 预备知识

2.1 双线性映射

假设群 G,G_1 是两个阶为素数 q 的循环群, 存在双线性映射 $\hat{e}:G\times G\to G_1$ 满足如下 3 个性质:

(1) 双线性: 对于任意的两个数 $a,b\in Z_q^*$, $x,y\in G$, 存在 $\hat{e}(x^a,y^b)=\hat{e}(x,y)^{ab}$。

(2) 非退化性: 存在 $x,y\in G$, 有 $\hat{e}(x,y)\neq 1$。

(3) 可计算性: 对于所有的 $x,y\in G$, 均存在多项式时间算法计算 $\hat{e}(x,y)$。

2.2 困难问题

(1) 判定性双线性 Diffie-Hellman(DBDH)问题: 令 G_1,G_2 为两个阶为 q 的循环群, g 是 G_1 的生成元, 给定四元组 $(g,g^a,g^b,g^c)\in G_1$ 与 $e(g,g)^z\in G_2$, 其中 $a,b,c,z\in Z_q^*$, DBDH 问题就是区 $Q=e(g,g)^{abc}$ 和 $Q=e(g,g)^z$。

(2) 判定性 Diffie-Hellman(DDH)问题: 令 G_1 为一个阶为 q 的循环群, g 是 G_1 的生成元, 给定四元组 $(g,g^a,g^b,g^z)\in G_1$, 其中 $a,b,z\in Z_q^*$, DDH 问题就是区分 $Q=g^{ab}$ 和 $Q=g^z$。

2.3 区块链与智能合约

区块链是由连接在一起的区块组成, 其中区块的主要构成部分是区块头和区块体, 区块头主要存

放的是当前区块的 HASH 值、时间戳、下一个区块的 HASH 值, 区块体主要存放的是智能合约以及该区块的其他信息。

智能合约是一套控制着数字资产并包含了合约参与方约定的权利和义务、由计算机按照事先约定的规则自动执行而不需要人为参与的协议。智能合约允许在没有中央机构参与的情况下执行可信的交易和协议[33], 如图 1 所示。将智能合约写入至区块链中, 由区块链的不可篡改性以及密码学散列算法保证存储、读取、执行的整个过程透明、可跟踪、不可篡改、不可否认。智能合约提供的安全性优于传统的合同, 并且降低了与合同有关的交易成本。

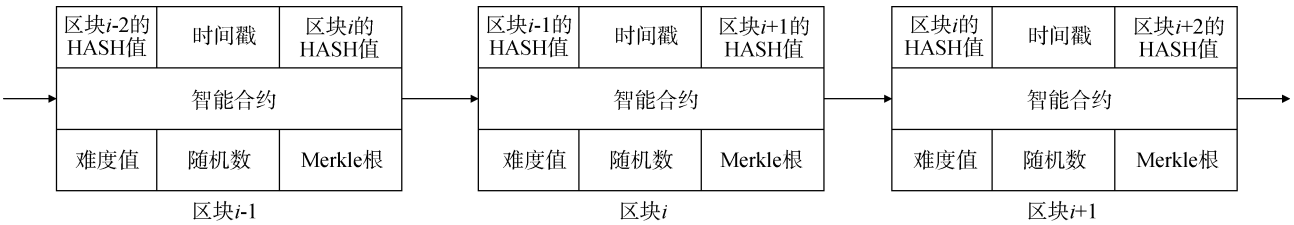

图 1　区块链与智能合约的结构

Figure 1　The structure of blockchain and smart contract

3　系统模型

表 1 中展示了群组内基于区块链的匿名可搜索加密系统中常用的符号。

表 1　系统常用符号

Table 1　Common symbols in the system

(msk, mpk)	主私钥, 主公钥
key_{Tra}	追踪密钥
$(pk_{\mathrm{CS}}, sk_{\mathrm{CS}})$	云服务器公私钥
$(\mathrm{RID}_i, \mathrm{ID}_i)$	用户真名, 用户假名
$(dsk_{\mathrm{ID}_i}, sk_{\mathrm{ID}_i})$	用户文件解密私钥, 私钥
M	明文文件
C	密文文件
CT	关键词密文
$T_{w'}$	关键词陷门

3.1　系统简介

群组内基于区块链的匿名可搜索加密系统中总共包含 6 个实体, 即密钥生成中心(Private Key Generation, PKG)、数据拥有者(Data Owner, DO)、云服务器(Cloud Server, CS)、数据使用者(Data Users, DU)、智能合约(Smart Contract, SC)、违规名单(Violator List, VL)。系统模型如图 2 所示:

(1) 密钥生成中心: PKG 是系统中唯一的可信第三方机构。主要工作是为系统生成公开参数与主私钥、追踪密钥, 为 DU 注册假名以及生成 DU 对应的密钥, 通过智能合约上传的违规名单进行追责恢复出 DU 的真实身份。

(2) 数据拥有者: 主要的工作是在收到 PKG 发送的用户集后对明文数据进行加密并生成关键词密文, 将加密后的密文数据与关键词密文上传至 CS。

(3) 云服务器: CS 在本系统中是一个半诚实且好奇的实体。主要的工作是接受 SC 的搜索请求以及对关键词陷门并进行匹配, 并将结果上传至 SC。

(4) 数据使用者: 主要的工作是计算关键词陷门, 并将陷门上传至 SC。在收到搜索结果后对密文数据进行解密。

(5) 智能合约: 主要的工作是接收 DU 上传的陷门, 再将陷门发送至 CS。CS 执行搜索操作完毕后将密文数据通过 SC 发送至 DU。

(6) 违规名单: 为了减小系统开销、提高系统可用性而增加的实体。主要的工作是记录违规用户, 由 SC 生成。

3.2　算法的形式化定义

群组内基于区块链的匿名可搜索加密方案含 11 个时间多项式算法 $\pi = \{Setup, KeyGen_{Tra}, KeyGen_{\mathrm{CS}}, Regist, KeyGen_{DU}, Enc, PEKS, Trapdoor, Test, Dec, Account\}$, 具体描述如下:

(1) 系统初始化算法 $Setup(k, N) \to (params)$: 该算法由密钥生成中心执行, 输入安全参数 k 以及群组内最大人数 N, 返回公开参数 $params$。

(2) 追踪密钥生成算法 $KeyGen_{Tra}(params) \to (key_{Tra})$: 该算法由密钥生成中心执行, 输入公开参数 $params$, 返回追踪密钥 key_{Tra}。

(3) 云服务器密钥生成算法 $KeyGen_{\mathrm{CS}}(params) \to (pk_{\mathrm{CS}}, sk_{\mathrm{CS}})$: 该算法由云服务器执行, 输入公开

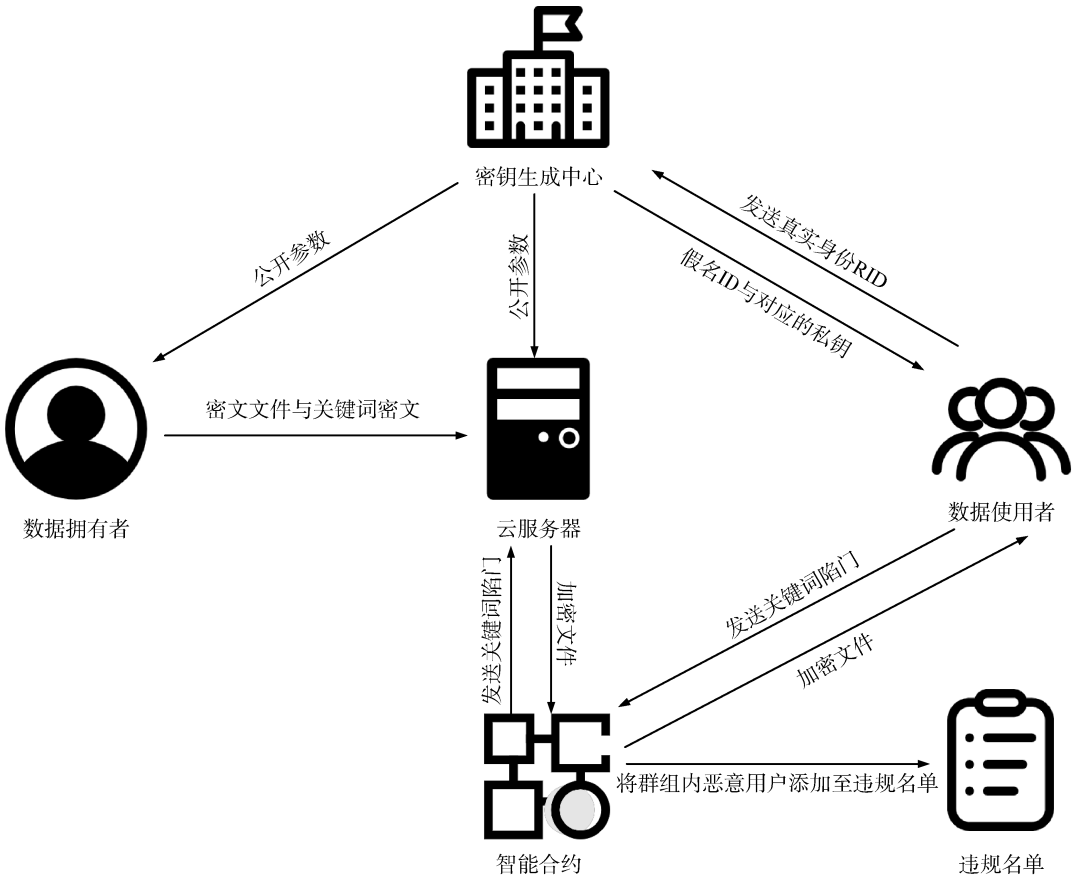

图 2　系统模型图

Figure 2　The diagram of system model

参数 $params$，返回云服务器的公私钥对 $(pk_{\mathrm{CS}}, sk_{\mathrm{CS}})$。

(4) 注册算法 $Regist(params, \mathrm{RID}_i) \to (\mathrm{ID}_i)$：该算法由密钥生成中心执行，输入公开参数 $params$，数据使用者的真实身份 RID_i，返回数据使用者假名 ID_i。

(5) 数据使用者密钥生成算法 $KeyGen_{DU}$ $(params, msk, \mathrm{ID}_i) \to (dsk_{\mathrm{ID}_i}, sk_{\mathrm{ID}_i})$：该算法由密钥生成中心执行，输入公开参数 $params$，系统主私钥 msk，数据使用者的假名 ID_i，返回数据使用者文件解密私钥 dsk_{ID_i}，数据使用者的私钥 sk_{ID_i}。

(6) 文件加密算法 $Enc(params, \mathrm{M}, S) \to C$：该算法由数据拥有者执行，输入公开参数 $params$，明文文件 M，用户集 S，返回密文文件 C。

(7) 关键词密文生成算法 $PEKS(params, pk_{\mathrm{DU}_i}, mpk, w) \to (CT)$：该算法由数据拥有者执行，输入公开参数 $params$，数据使用者的身份 ID_i，主公钥 mpk，关键词 w，返回关键词密文 CT。

(8) 关键词陷门生成算法 $Trapdoor(params, sk_{\mathrm{ID}_i}, pk_{\mathrm{CS}}, w') \to (T_{w'}^i)$：该算法由数据使用者执行，输入公开参数 $params$，数据使用者的私钥 sk_{ID_i}，云服务器的公钥 pk_{CS}，关键词 w'，返回关键词陷门 $T_{w'}^i$。

(9) 测试算法 $Test(CT, T_{w'}^i, sk_{\mathrm{CS}}) \to (1/0)$：该算法由云服务器执行，输入关键词密文 CT，关键词陷门 $T_{w'}^i$，云服务器的私钥 sk_{CS}，若验证正确则返回 1，匹配错误则返回 0。

(10) 文件解密算法 $Dec(dsk_{ID_i}, C, S) \to \mathrm{M}$：该算法由数据使用者执行，输入数据使用者的文件解密私钥 dsk_{ID_i}，密文文件 C，用户集 S，返回明文文件 M。

(11) 追责算法 $Account(\mathrm{ID}_i) \to \mathrm{RID}_i$：该算法由密钥生成中心执行，输入数据使用者的假名 ID_i，返回数据使用者真实身份 RID_i。

3.3　安全模型

Game1：下面通过敌手 $\mathcal{A}$ 与挑战者之间的安全

游戏来定义本方案中的关键词密文不可区分性。游戏定义如下:

(1) 系统建立: 挑战者运行 *Setup* 算法产生系统的公开参数 *params* 和系统主私钥 *msk* 。

(2) 询问阶段 1: 在此阶段敌手 $\mathcal{A}$ 进行多项式有界次的适应性询问。并记意欲挑战的身份为 ID^*, 否则记为 ID_i。敌手 $\mathcal{A}$ 发出对身份和密钥提取的询问。挑战者对敌手 $\mathcal{A}$ 的询问进行应答, 返回敌手 $\mathcal{A}$ 对意欲挑战的身份 ID^* 进行询问后的应答 $Q\mathrm{ID}^*$ 和对应的密钥, 否则返回 ID_i 对应的 $Q\mathrm{ID}_i$。

(3) 挑战阶段: 敌手 $\mathcal{A}$ 输出两个长度相等的关键词 (w_0, w_1) 和一个挑战身份 ID^*, 其中要求 $\mathcal{A}$ 没有对 ID^* 进行过密钥提取询问, 挑战者随机选择 $\beta \in_R \{0,1\}$, ID^* 通过 *PEKS* 算法生成 CT^* 并发送给敌手 $\mathcal{A}$。

(4) 询问阶段 2: 敌手 $\mathcal{A}$ 对另外 ID 的密钥产生询问, 要求 $\mathrm{ID} \neq \mathrm{ID}^*$, 挑战者以询问阶段 1 中的方式进行回应。

(5) 猜测: 敌手 $\mathcal{A}$ 输出猜测 $\beta' \in \{0,1\}$, 如果 $\beta=\beta'$, 则敌手 $\mathcal{A}$ 挑战成功。

定义 1: 敌手 $\mathcal{A}$ 攻破本方案的关键词密文不可区分性的概率优势为 $\mathrm{Adv}^{Game1}(\lambda) = |\Pr(\beta = \beta') - 1/2|$, 其中 $\Pr(\beta)$ 意为敌手 $\mathcal{A}$ 攻破本方案的关键词密文不可区分性的概率。如果对于任意的概率多项式敌手 $\mathcal{A}$, $\mathrm{Adv}^{Game1}(\lambda)$ 是可忽略的, 称本方案满足在选择明文攻击下的关键词密文不可区分性。

Game2: 下面通过敌手 $\mathcal{A}$ 与挑战者之间的安全游戏来定义本方案中的关键词陷门不可区分性, 游戏定义如下:

(1) 系统建立: 挑战者运行 *Setup* 算法产生系统的公开参数 *params* 和系统主私钥 *msk* 。

(2) 挑战阶段: 敌手 $\mathcal{A}$ 输出两个长度相等的关键词 (w_0, w_1), 挑战者随机选择 $\beta \in_R \{0,1\}$, 通过 *Trapdoor* 算法生成关键词陷门 $T_{w'}^*$ 并返回给敌手 $\mathcal{A}$。

(3) 猜测: 敌手 $\mathcal{A}$ 输出猜测 $\beta' \in \{0,1\}$, 如果 $\beta=\beta'$, 则敌手 $\mathcal{A}$ 挑战成功。

定义 2: 敌手 $\mathcal{A}$ 攻破本方案的关键词陷门不可区分性的概率优势为 $\mathrm{Adv}^{Game2}(\lambda) = |\Pr(\beta = \beta') - 1/2|$, 其中 $\Pr(\beta)$ 意为敌手 $\mathcal{A}$ 攻破本方案的关键词密文不可区分性的概率。如果对于任意的概率多项式敌手 $\mathcal{A}$, $\mathrm{Adv}^{Game2}(\lambda)$ 是可忽略的, 称本方案满足在选择明文攻击下的关键词陷门不可区分性。

4 方案构造

图3为群组内基于区块链的匿名可搜索加密方案的运行流程框架, 本方案具体实现的细节如下:

4.1 关键词搜索方案

(1) 系统初始化算法 $Setup(k, N) \to (params)$: 输入安全参数 k, 群组内最大人数 N。产生两个 $q \geqslant 2^k$ 的素数阶群 G, G_1, 构成双线性映射 $\hat{e}: G \times G \to G_1$, g 是 G 的生成元, $H_1: \{0,1\}^* \to Z_q^*$, $H_2: \{0,1\}^* \to G$, $H_3: G_1 \to Z_q^*$ 是 3 个稳定抗碰撞的哈希函数。

① 选取 $h \in G$, 随机选择 $\alpha \in Z_q^*$, 计算 $u = h^\alpha$, $v = \hat{e}(g, h)$。

② 返回系统的公开参数 $params = \{q, G, G_1, \hat{e}, H_1, H_2, H_3, u, v, g, g^\alpha, \cdots, g^{\alpha^N}\}$, 主私钥 $msk = (a, h)$, 主公钥 $mpk = g^\alpha$。

(2) 追踪密钥生成算法 $KeyGen_{Tra}(params) \to (key_{Tra})$: 输入公开参数 *params*, 密钥生成中心选择 $g_1, g_2 \in G$, 随机选择 $k_1, k_2 \in Z_q^*$, 计算 $\eta = g_1^{k_1} = g_2^{k_2}$, 返回追踪密钥 $key_{Tra} = \{k_1, k_2\}$。

(3) 云服务器密钥生成算法 $KeyGen_{\mathrm{CS}}(params) \to (pk_{\mathrm{CS}}, sk_{\mathrm{CS}})$: 输入公开参数 *params*, 云服务器随机选择 $z \in Z_q^*$, 计算 $pk_{\mathrm{CS}} = g^z$, 返回云服务器的私钥 $sk_{\mathrm{CS}} = z$, 公钥 $pk_{\mathrm{CS}} = g^z$。

(4) 注册算法 $Regist(params, \mathrm{RID}_i) \to (\mathrm{ID}_i)$: 输入公开参数 *params*, 数据使用者向密钥生成中心发送真实身份 RID_i, 密钥生成中心验证 RID_i 正确后随机选择 $\beta_1, \beta_2 \in Z_q^*$, 计算 $l_1 = g_1^{\beta_1}, l_2 = g_2^{\beta_2}$, 密钥生成中心为数据使用者生成假名 $\mathrm{ID}_i = \mathrm{RID}_i \cdot \eta^{\beta_1+\beta_2}$。并将 ID_i 添加到用户集 S 中, 将用户集 S 发送给数据拥有者。

(5) 数据使用者密钥生成算法 $KeyGen_{DU}$ $(params, msk, \mathrm{ID}_i) \to (dsk_{\mathrm{ID}_i}, sk_{\mathrm{ID}_i})$: 输入公开参数 *params*, 系统主私钥 *msk*, 数据使用者假名 ID_i。

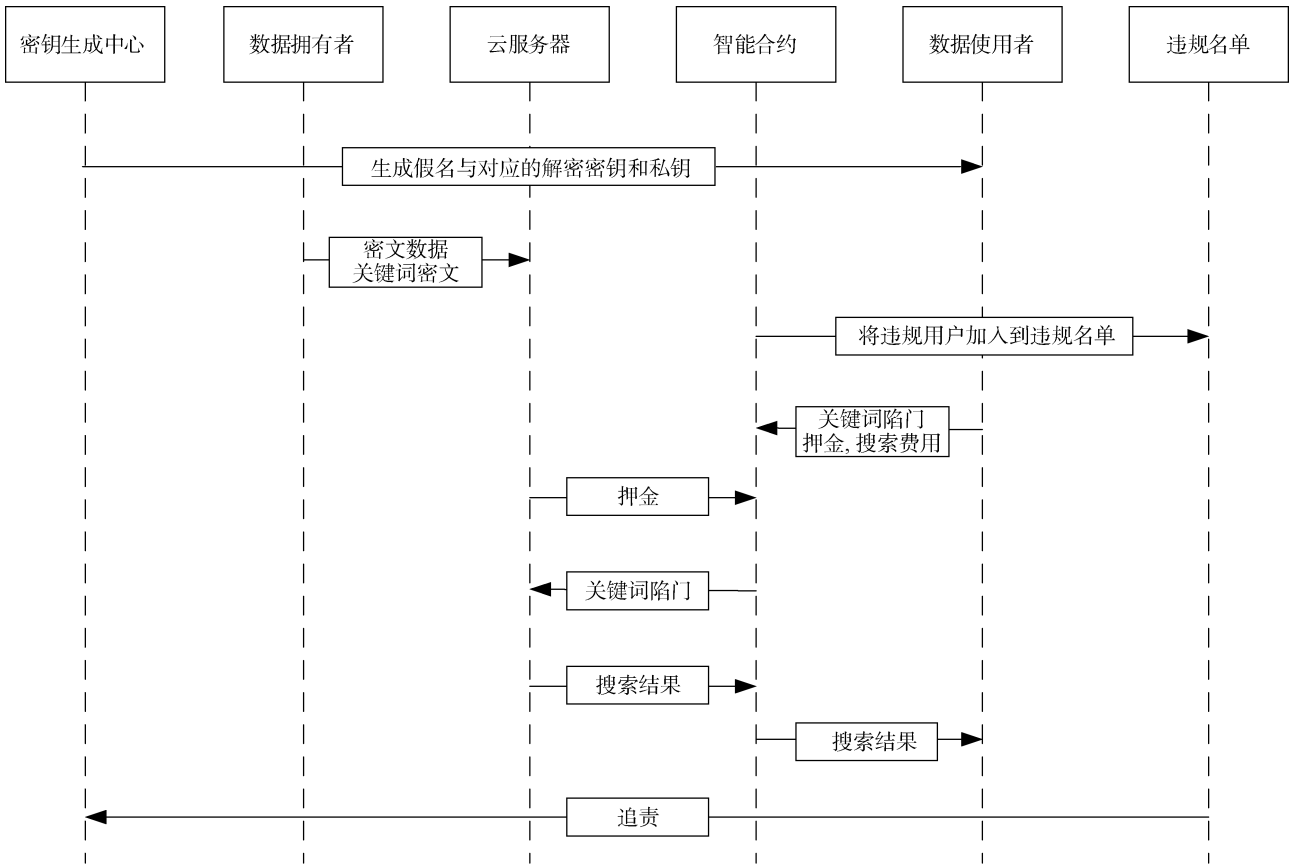

图 3　群组内基于区块链的匿名可搜索加密方案的运行流程框架图

Figure 3　The framework diagram of the operation flow of blockchain-enabled anonymous searchable encryption scheme in the group

① 生成数据使用者的文件解密私钥 $dsk_{\mathrm{ID}_i}=h^{\frac{1}{\alpha+H_1(\mathrm{ID}_i)}}$。

② 生成数据使用者的私钥 $sk_{\mathrm{ID}_i}=H_2(\mathrm{ID}_i)^{\alpha}$。

③ 密钥生成中心将 $(dsk_{\mathrm{ID}_i}, sk_{\mathrm{ID}_i})$ 发送至数据使用者。

(6) 文件加密算法 $Enc(params,\mathrm{M},S)\rightarrow C$：输入公开参数 $params$，明文文件 M，用户集 S，其中群组内人数 $s\leqslant N$。

① 随机选择 $k\in Z_q^*$，计算 $K=v^k, C_1=u^{-k}, C_2=g^{k\cdot\prod_{i=1}^{s}(\alpha+H_1(\mathrm{ID}_i))}$，令 $Hdr=(C_1,C_2), C_{\mathrm{M}}=\mathrm{AES}.Enc(K,\mathrm{M})$。

② 返回密文 $C=(Hdr,C_{\mathrm{M}})$ 并发送至云服务器。

(7) 关键词密文生成算法 $PEKS(params,\mathrm{ID}_i,mpk,w)\rightarrow(CT)$：输入公开参数 $params$，数据使用者的身份 ID_i，主公钥 mpk，关键词 w。

① 随机选择 $t\in Z_q^*$，计算 $CT_1=g^t, CT_2^i=H_3(\hat{e}(H_2(\mathrm{ID}_i)^t,mpk)\hat{e}(H_2(w),CT_1))$。

② 返回关键词密文 $CT=(CT_1,\{CT_2^i\}_{i=1}^{s})$ 并发送至云服务器。

(8) 关键词陷门生成算法 $Trapdoor(params, sk_{\mathrm{ID}_i}, pk_{\mathrm{CS}}, w')\rightarrow(T_{w'}^i)$：输入公开参数 $params$，数据使用者的的私钥 sk_{ID_i}，云服务器的公钥 pk_{CS}，关键词 w'。

① 随机选择 $v\in Z_q^*$，计算 $T_{w_1'}=g^v$，$T_{w_2'}^i=\frac{sk_{\mathrm{ID}_i}H_2(w')}{(pk_{\mathrm{CS}})^v}$。

② 返回关键词陷门 $T_{w'}^i=(T_{w_1'},T_{w_2'}^i)$。

(9) 测试算法 $Test(CT,T_{w'}^i,sk_{\mathrm{CS}})\rightarrow(1/0)$：输入关键词密文 CT，关键词陷门 $T_{w'}^i$，云服务器的私钥 sk_{CS}。

① 云服务器首先计算 $T_i=T_{w_2'}^i\cdot(T_{w_1'})^{sk_{\mathrm{CS}}}$。

② 再验证 $H_3(\hat{e}(T_i,CT_1))=CT_2^i$。

③若匹配正确则返回 1, 匹配错误则返回 0。

(10) 文件解密算法 $Dec(dsk_{\mathrm{ID}_i}, C, S) \to \mathrm{M}$: 输入数据使用者的文件解密私钥 dsk_{ID_i}, 密文文件 C, 用户集 S。

① 首先, 用 dsk_{ID_i} 获取封装在 *Hdr* 中的对称密钥 K, 计算:

$$p_{i,S}(\alpha)=\frac{1}{\alpha}\Big(\prod_{j=1,j\neq i}^{s}(\alpha+H_1(\mathrm{ID}_j))-\prod_{j=1,j\neq i}^{s}(H_1(\mathrm{ID}_j))\Big),$$

获得对称密钥:

$$K=(\hat{e}(g^{p_{i,S}(\alpha)},C_1)\cdot\hat{e}(C_2,dsk_{\mathrm{ID}_i}))^{\frac{1}{\prod_{j=1,j\neq i}^{s}H_1(\mathrm{ID}_j)}}。$$

② 解密明文 $\mathrm{M}=\mathrm{AES}.Dec(K, C_{\mathrm{M}})$。

(11) 追责算法 $Account(\mathrm{ID}_i)\to\mathrm{RID}_i$: 输入数据使用者的假名 ID_i, 计算数据使用者真实身份 $\mathrm{RID}_i=\dfrac{\mathrm{ID}_i}{l_1^{k_1}\cdot l_2^{k_2}}$。

4.2 公平支付机制

为了防止云服务器给数据使用者返回部分搜索结果或者错误的搜索结果等不可信行为而收取全部的搜索费。本文在系统中加入区块链以及违规名单机制, 具体流程如下:

(1) 在系统初始化阶段智能合约同时进行初始化, 设置数据使用者最大重复提交检索次数 *countMax*, 数据使用者提交检索次数 *count* (初始值为 0), 押金 \$*deposit*。云服务器设置检索单价 \$*searchPay*。数据使用者向账户存款 \$*DUSum*。

Algorithm 1	系统初始化
1.	SC **SET:** *countMax*, \$*deposit*
2.	CS **SET:** \$*searchPay*
3.	DU **SET:** \$*DUSum*, *count*

(2) 在搜索阶段, 为了减小系统开销, 智能合约建立违规名单, 若数据使用者存款小于检索单价且重复发起检索请求次数超过 *countMax*, 智能合约将其移至违规名单。

Algorithm 2	违规名单执行
1.	**WHILE** *count* < *countMax*
2.	**IF** \$*DOSum* < \$*searchPay*
3.	*count* ++
4.	**ELSE BREAK**
5.	**END WHILE**
6.	**IF** *count* > *countMax* **ADD TO** VL

(3) 数据使用者向智能合约发送检索请求, 向智能合约支付检索单价 \$*searchPay* 与押金 \$*deposit*, 并将陷门发送至智能合约。云服务器收到检索请求后, 向智能合约支付押金 \$*deposit* 并获得陷门。

Algorithm 3	支付检索费用及押金
1.	DU **SEND TO** SC: \$*searchPay*, \$*deposit*, $T_{w'}^{i}$
2.	CS **SEND TO** SC: \$*deposit*
3.	SC **SEND TO** CS: $T_{w'}^{i}$

(4) 云服务器执行 *Test* 算法, 并将搜索结果通过智能合约发送给数据使用者, 数据使用者收到后执行 *Enc* 算法获取明文数据。流程如图 4 所示。

Algorithm 4	执行测试算法及解密密文
1.	CS **RUN** *Test* **AND GET** *C*
2.	CS **SEND TO** SC: *C*
3.	SC **SEND TO** DU: *C*
4.	DU **GET:** *C* **AND RUN** *Dec*

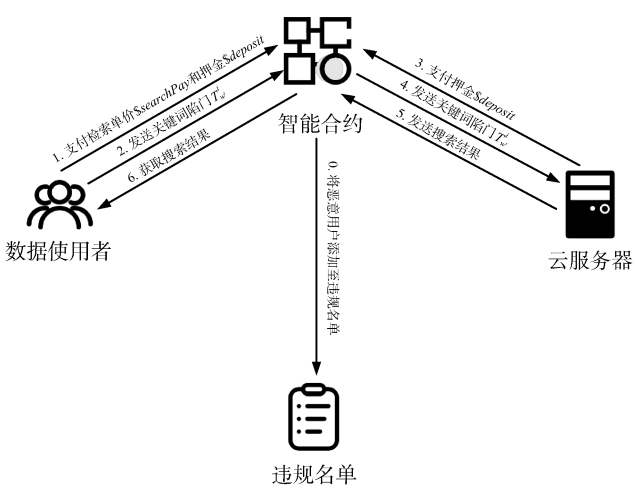

图 4 公平支付流程图

Figure 4 The flow chart of payment fairness

(5) 数据使用者验证搜索结果并向智能合约发送验证结果, 如果验证结果正确智能合约则将检索单价 \$*searchPay* 与云服务器押金 \$*deposit* 转移到云服务器, 数据使用者押金 \$*deposit* 进行返还; 如果结果错误则将检索单价 \$*searchPay* 与数据使用者的押金 \$*deposit* 转移到数据使用者账户, 云服务器押金 \$*deposit* 进行返还。费用转移如图 5 所示。

Algorithm 5	验证以及费用转移
1.	DU **VERIFY** M
2.	**IF TRUE**
3.	**PAY** $\$searchPay + \$deposit$ **TO** CS
4.	**RETURN** $\$deposit$ **TO** DU
5.	**IF FALSE**
6.	**RETURN** $\$searchPay + \$deposit$ **TO** DU
7.	**RETURN** $\$deposit$ **TO** CS
8.	**END IF**

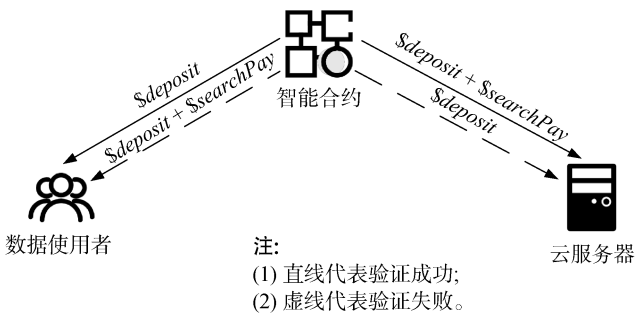

图 5 费用转移流程图

Figure 5 The flow chart of costs passing

(6) 智能合约将违规名单发送至密钥生成中心, 密钥生成中心将该数据使用者移除出用户集 S, 再运行 *Account* 算法恢复出数据使用者真实身份并禁止该其再次注册。

Algorithm 6	追责
1.	SC **SEND** VL **TO** PKG
2.	PKG **DELETE** ID_i
3.	PKG **RUN** *Account*
4.	**GET** RID_i

4.3 正确性验证

4.3.1 匹配正确性

如果关键词密文 w 等于关键词陷门中的 w', 则有:

① 首先计算 $T_i = T_{w_2'}^{i} \cdot (T_{w_1'})^{sk_{\mathrm{CS}}} = \dfrac{H_2(\mathrm{ID}_i)^{\alpha} H_2(w)}{(g^z)^v} \cdot (g^v)^z = H_2(\mathrm{ID}_i)^{\alpha} H_2(w)$。

② 验证

$$
\begin{aligned}
&H_3(\hat{e}(T_i, CT_1)) \\
&= H_3(\hat{e}(H_2(\mathrm{ID}_i)^{\alpha} H_2(w), g^t)) \\
&= H_3(\hat{e}(H_2(\mathrm{ID}_i)^{\alpha}, g^t)\hat{e}(H_2(w), g^t)) \\
&= H_3(\hat{e}(H_2(\mathrm{ID}_i)^{t}, mpk)\hat{e}(H_2(w), CT_1)) \\
&= CT_2^i
\end{aligned}
$$

4.3.2 解密正确性

数据使用者收到密文数据后, 通过其自身的文件解密私钥恢复出 K, 使用 K 对密文数据进行解密。

$$
\begin{aligned}
K' &= (\hat{e}(g^{P_{i,S(\alpha)}}, C_1) \cdot \hat{e}(C_2, dsk_{\mathrm{ID}_i})) \\
&= \hat{e}(g^{P_{i,S}(\alpha)}, h^{-k\cdot\alpha}) \cdot \hat{e}(g^{k\cdot\prod_{i=1}^{s}(\alpha+H_1(\mathrm{ID}_i))}, h^{\frac{1}{\alpha+H_1(\mathrm{ID}_i)}}) \\
&= \hat{e}(g,h)^{-k\cdot\left(\prod_{j=1,j\neq i}^{s}(\alpha+H_1(\mathrm{ID}_j))-\prod_{j=1,j\neq i}^{s}(H_1(\mathrm{ID}_j))\right)} \cdot \\
&\quad \hat{e}(g,h)^{k\cdot\left(\prod_{j=1,j\neq i}^{s}(\alpha+H_1(\mathrm{ID}_j))\right)} \\
&= \hat{e}(g,h)^{k\prod_{j=1,j\neq i}^{s}(H_1(\mathrm{ID}_j))} \\
&= K^{\prod_{j=1,j\neq i}^{s}(H_1(\mathrm{ID}_j))}
\end{aligned}
$$

所以 $K=K'^{\frac{1}{\prod_{j=1,j\neq i}^{s}(H_1(\mathrm{ID}_j))}}$。

4.3.3 匿名追责正确性

密钥生成中心收到违规名单后, 利用追踪密钥与数据使用者假名恢复出用户真实身份, 并追责禁止其再次在系统中注册。

$$
\mathrm{RID}_i = \frac{\mathrm{ID}_i}{l_1^{k_1} \cdot l_2^{k_2}} = \frac{\mathrm{ID}_i}{g_1^{\beta_1 k_1} \cdot g_2^{\beta_2 k_2}} = \frac{\mathrm{ID}_i}{\eta^{\beta_1+\beta_2}}
$$

5 安全性分析

5.1 关键词密文的不可区分性

定理 1: 假设 DBDH 问题是困难的, 本方案在随机谕言机模型下能够满足关键词密文的不可区分性。

证明: 假设敌手 $\mathcal{A}$ 是一个试图攻破关键词密文不可区分性的多项式时间攻击者, 挑战者建立 DBDH 困难问题, 设敌手 $\mathcal{B}$ 是攻击 DBDH 问题的多项式时间敌手, $\mathcal{B}$ 获得五元组 (g, g^a, g^b, g^c, Q), 其中 $Q = \hat{e}\ (g,g)^{abc}$ 或者 $Q = \hat{e}(g,g)^z$, $a,b,c,z \in Z_q^*$, 目的是区分 $Q = \hat{e}(g,g)^{abc}$ 或者 $Q = \hat{e}(g,g)^z$。游戏过程如下:

(1) 系统建立: 敌手 $\mathcal{B}$ 首先运行 *Setup* 算法产生系统的公开参数 $params=\{q,G,G_1,\hat{e},g,mpk,H_2\}$, 其中 H_2 是随机谕言机。设置系统主公钥 $mpk=g^a$。

(2) 询问阶段 1: 在此阶段敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发起询问, $\mathcal{B}$ 对 $\mathcal{A}$ 发起的询问进行应答。

① H_2 询问: 设敌手 $\mathcal{A}$ 询问 ID_i 的 H_2 值, 敌手 $\mathcal{B}$ 首先创建列表 L_{H_2} (初始化为空), 并做如下应答:

- 如果 L_{H_2} 中存在 ID_i, 敌手 $\mathcal{B}$ 以 $H_2(\mathrm{ID}_i)=Q\mathrm{ID}_i$ 作为回应。

- 如果 L_{H_2} 中不存在 ID_i, 敌手 $\mathcal{B}$ 生成一个 $coin$, 并随机选择 $coin\in\{0,1\}$ 并设 $\Pr[coin=0]=\delta$。记 $coin$=0 时身份为 ID_i, 否则为 ID^*。如果 $coin=0$, $\mathcal{B}$ 随机选择 $r_i\in Z_q^*$, 计算 $H_2(\mathrm{ID}_i)=Q\mathrm{ID}_i=g^{r_i}$。否则计算 $H_2(\mathrm{ID}^*)=Q\mathrm{ID}^*=g^b$。

敌手 $\mathcal{B}$ 将三元组 $(\mathrm{ID}^*,Q\mathrm{ID}^*,coin)$ 加入至 L_{H_2}, 并将 $H_2(\mathrm{ID}^*)=Q\mathrm{ID}^*$ 回应给 $\mathcal{A}$。

敌手 $\mathcal{B}$ 将四元组 $(\mathrm{ID}_i,Q\mathrm{ID}_i,r_i,coin)$ 加入至 L_{H_2}, 并将 $H_2(\mathrm{ID}_i)=Q\mathrm{ID}_i$ 回应给敌手 $\mathcal{A}$。

② 密钥提取询问(最多进行 q_E 次): 此时 ID_i 是敌手 $\mathcal{A}$ 向敌手 $\mathcal{B}$ 发出的密钥提取询问, $\mathcal{B}$ 查询 L_{H_2} 中存储的四元组 $(\mathrm{ID}_i,Q\mathrm{ID}_i,r_i,coin)$。

- 如果 $coin=1$, $\mathcal{B}$ 报错并退出。

- 否则 $\mathcal{B}$ 从 L_{H_2} 中取出 $(\mathrm{ID}_i,Q\mathrm{ID}_i,r_i,coin)$, 并将 mpk^{r_i} 作为 ID_i 对应的密钥发送给敌手 $\mathcal{A}$。

(3) 挑战阶段: 敌手 $\mathcal{A}$ 选择两个长度相等的关键字 (w_0,w_1), 计算 $H_2(w_0)$ 和 $H_2(w_1)$, 并将 $H_2(w_0)$, $H_2(w_1)$ 发送给敌手 $\mathcal{B}$, 其中要求 $\mathcal{A}$ 没有对 ID^* 进行过密钥提取询问, $\mathcal{B}$ 收到三元组后, 随机选择 $\beta\in_R\{0,1\}$, 计算 $CT_1^*=g^c,CT_2^{i*}=H_3(Q\cdot\hat{e}(H_2(w_\beta),CT_1^*))$, 并返回 $CT^*=(CT_1^*,CT_2^{i*})$。

(4) 询问阶段 2: 与询问阶段 1 一致。

(5) 猜测: 敌手 $\mathcal{A}$ 输出猜测 $\beta'\in\{0,1\}$, 若 $\beta'=\beta$, 则 $\mathcal{A}$ 挑战成功并输出 1, 否则输出 0。

记五元组 (g,g^a,g^b,g^c,Q) 为 T。当 $Q=\hat{e}(g,g)^z$ 时, T 为随机五元组 T_R。因为 Q 在 G_1 中是均匀分布的, 所以 CT_2^{i*} 在 G_1 中也是均匀分布的, $\mathcal{A}$ 最多以 1/2 的概率输出 1。而 $\mathcal{B}$ 输出 1 当且仅当 $\mathcal{A}$ 成功, 所以 $\Pr[B(T)=1|T_R]=1/2$。

当 $Q=\hat{e}(g,g)^{abc}$ 时, T 为 DBDH 五元组 T_D, 因为 $mpk=g^a$, $Q\mathrm{ID}_i=g^b$, $CT_1^*=g^c$, $CT_2^{i*}=H_3(\hat{e}(g,g)^{abc}\cdot\hat{e}(H_2(w_\beta),CT_1^*))$。由此可得, $\mathcal{B}$ 拥有 g^a,g^b,g^c 攻破 DBDH 困难问题等同于 $\mathcal{A}$ 拥有 $mpk,Q\mathrm{ID}_i,CT_1^*$ 区分 β, 所以 $\mathcal{B}$ 输出 1 当且仅当 $\mathcal{A}$ 成功, 所以 $\Pr[B(T)=1|T_D]=\Pr[\mathrm{succ}]$。此外, succ 意味着 $\mathcal{A}$ 攻击成功。由此:

$$\begin{aligned}\Pr[B(T)=1]&=\Pr[T_D]\Pr[B(T)=1|T_D]+\\&\quad\Pr[T_R]\Pr[B(T)=1|T_R]\\&=1/2\Pr[\mathrm{succ}]+1/2\times1/2\\\Pr[B(T)=0]&=\Pr[T_D]\Pr[B(T)=0|T_D]+\\&\quad\Pr[T_R]\Pr[B(T)=0|T_R]\\&=1/2[1-\Pr[\mathrm{succ}]]+1/2\times1/2\end{aligned}$$

$$|\Pr[B(T)=1]-\Pr[B(T)=0]|=|\Pr[\mathrm{succ}]-1/2|,$$

$$|\Pr[B(T_R)=1]-\Pr[B(T_D)=1]|=|\Pr[\mathrm{succ}]-1/2|。$$

等式左边为敌手 $\mathcal{B}$ 攻破 DBDH 困难问题的优势, 等式右边为敌手 $\mathcal{A}$ 区分 CT_2^{i*} 的优势, 由于 DBDH 问题是困难的, 所以敌手 $\mathcal{B}$ 区分 $Q=\hat{e}(g,g)^{abc}$ 或者 $Q=\hat{e}(g,g)^z$ 的优势是可忽略的, 故敌手 $\mathcal{A}$ 攻破本方案的优势是可以忽略的。所以本方案的关键词密文在选择明文攻击下是不可区分的。 证毕

5.2 关键词陷门的不可区分性

定理 2: 假设 DDH 问题是困难的, 本方案在标准模型下能够满足关键词陷门的不可区分性。

证明: 假设敌手 $\mathcal{A}$ 是一个试图攻破关键词陷门不可区分性的多项式时间攻击者, 挑战者建立 DDH 困难问题, 设敌手 $\mathcal{B}$ 是攻击 DDH 问题的多项式时间敌手, $\mathcal{B}$ 获得四元组 (g,g^a,g^b,Q), 其中 $Q=g^z$ 或者 $Q=g^{ab}$, $a,b,z\in Z_q^*$, 目的是区分 $Q=g^z$ 还是 $Q=g^{ab}$。游戏过程如下:

(1) 系统建立: 敌手 $\mathcal{B}$ 首先运行 *Setup* 算法产生系统公开参数 *params*, 设置云服务器公钥 $pk_{\mathrm{CS}}=g^a$。

(2) 挑战阶段: 敌手 $\mathcal{A}$ 选择两个等长的明文关键词 (w_0',w_1'), 计算 $H_2(w_0')$ 和 $H_2(w_1')$, 在选择 $g_1\in G$, 计算 $M_0=g_1\cdot H_2(w_0')$ 和 $M_1=g_1\cdot H_2(w_1')$ 并将 (M_0,M_1) 发送给敌手 $\mathcal{B}$, $\mathcal{B}$ 收到 (M_0,M_1) 后, 随机选择 $\beta\in_R\{0,1\}$, 计算 $T_{w_1'}^*=g^b,T_{w_2'}^*=\dfrac{M_\beta}{Q}$, 将

$T^*_{w'}=(T^*_{w'_1}, T^*_{w'_2})$ 返回给敌手 $\mathcal{A}$。

(3) 猜测阶段: 敌手 $\mathcal{A}$ 输出猜测 $\beta'\in\{0,1\}$, 若 $\beta'=\beta$, 则 $\mathcal{A}$ 挑战成功并输出 1, 否则输出 0。

记四元组 (g,g^a,g^b,Q) 为 T。当 $Q=g^z$ 时, T 为随机四元组 T_R。因为 Q 在 G_1 中是均匀分布的, 所以 $T^*_{w'_2}$ 在 G_1 中也是均匀分布的, $\mathcal{A}$ 最多以 $1/2$ 的概率输出 1。而 $\mathcal{B}$ 输出 1 当且仅当 $\mathcal{A}$ 成功, 所以 $\Pr[B(T)=1|T_R]=1/2$。

当 $Q=g^{ab}$ 时, T 为 DDH 四元组 T_D, 因为 $pk_{\mathrm{CS}}=g^a$, $T^*_{w'_1}=g^b$, $T^*_{w'_2}=\dfrac{M_\beta}{Q}=\dfrac{M_\beta}{g^{ab}}$。由此可得, $\mathcal{B}$ 拥有 g^a,g^b 攻破 DDH 困难问题等同于 $\mathcal{A}$ 拥有 $pk_{\mathrm{CS}},T^*_{w'_1}$ 区分 β, 所以 $\mathcal{B}$ 输出 1 当且仅当 $\mathcal{A}$ 成功, 所以 $\Pr[B(T)=1|T_D]=\Pr[\mathrm{succ}]$。此外, succ 意味着 $\mathcal{A}$ 攻击成功。由此:

$$\begin{aligned}\Pr[B(T)=1]&=\Pr[T_D]\Pr[B(T)=1|T_D]+\\&\quad\Pr[T_R]\Pr[B(T)=1|T_R]\\&=1/2\Pr[\mathrm{succ}]+1/2\times1/2\\\Pr[B(T)=0]&=\Pr[T_D]\Pr[B(T)=0|T_D]+\\&\quad\Pr[T_R]\Pr[B(T)=0|T_R]\\&=1/2[1-\Pr[\mathrm{succ}]]+1/2\times1/2\end{aligned}$$

$$|\Pr[B(T)=1]-\Pr[B(T)=0]|=|\Pr[\mathrm{succ}]-1/2|,$$

$$|\Pr[B(T_R)=1]-\Pr[B(T_D)=1]|=|\Pr[\mathrm{succ}]-1/2|。$$

等式左边为敌手 $\mathcal{B}$ 攻破 DDH 困难问题的优势, 等式右边为敌手 $\mathcal{A}$ 区分 $T^*_{w'_2}$ 的优势, 由于 DDH 问题是困难的, 所以敌手 $\mathcal{B}$ 区分 $Q=g^{ab}$ 和 $Q=g^z$ 的优势是可以忽略的。故敌手 $\mathcal{A}$ 攻破本方案的优势是可以忽略的。所以本方案的关键词陷门在选择明文攻击下是不可区分的。 证毕

6 功能对比与性能分析

6.1 功能对比

将本文方案与文献[17,18,21,23,32]的方案进行对比, 对比结果如表 2 所示。

由表 2 对比可以看出, 本文方案在安全性方面不仅可以保证关键词密文和陷门的不可区分性, 还支持在群组内进行一对多的可搜索加密。在系统功能性方面支持匿名搜索, 使云服务器无法获得用户的身份信息, 且在系统中引入了区块链机制, 保证了用户与服务器间的公平支付。

6.2 性能分析

本文进行仿真实验的硬件环境与软件环境为: 处理器为 AMD Ryzen 5 3550H with Radeon Vega Mobile Gfx 2.10GHz, 运行内存 4GB, 操作系统是运行 64 位的 Ubuntu 18.04, 编程语言是 Python3.6, 测试工具为 PyCharm 2019.3.3, 使用的密码库为 Charm-crypto-0.50, 其中本文采用的是对称椭圆曲线群(SS512), 该曲线群的阶数为 160bit。

在表 3 中列举了群上元素和域上元素的字节数与大小, 记 $|G|$ 为群上的元素大小, 记 $|Z^*_q|$ 为域上的元素大小, 将本文方案与文献[18,23]进行通信量对比, 分别对比 1 次关键词密文与关键词陷门传输过程中的通信量, 对比结果如表 3 所示。其中 *PEKS* 代表关键词密文传输过程中的通信量, *Trapdoor* 代表关键词陷门传输过程中的通信量。

由表 4 可以看出, 在 *PEKS* 阶段, 各方案通信量由大到小依次是文献[23]、文献[18]、本文方案, 其中本方案的计算开销最小, 为 0.127KB; 在 *Trapdoor* 阶段, 本方案与文献[18,23]的通信量相同, 均为 0.25KB。

本文在表 5 中分别列举了常用密码操作及其含义, 表 6 中列举了常用密码操作的运行时间。

表 2 不同方案的功能对比

Table 2 Function comparison of different schemes

方案	密文不可区分性	陷门不可区分性	多用户环境	匿名性	公平支付
[17]	√	√	×	×	×
[18]	√	√	×	×	×
[21]	√	√	√	×	×
[23]	√	×	×	×	×
[32]	√	√	√	×	√
本方案	√	√	√	√	√

(注: √代表包含此功能, ×代表不包含此功能。)

表 3 不同元素的字节数及大小

Table 3 Number and size of bytes of different elements

元素	字节数(bytes)	大小(KB)
G	128	0.125
Z_q^*	20	0.020

表 4 不同方案通信量比较

Table 4 Traffic volume Comparison of different schemes

方案	*PEKS*(KB)	*Trapdoor*(KB)
[18]	0.375	0.25
[23]	0.5	0.25
本方案	0.127	0.25

表 5 常用密码操作及其含义

Table 5 The meanings of common cryptographic operations

密码操作	含义
T_c	指数运算的时间
T_p	双线性对运算的时间
$T_{H\to G}$	哈希到群 G 的时间
$T_{H\to Z_q^*}$	哈希到 Z_q^* 的时间
T_m	乘法运算的时间
T_i	逆运算的时间

表 6 常用密码操作的运行时间

Table 6 The elapsed time of common cryptographic operations

密码操作	T_c	T_p	$T_{H\to G}$	$T_{H\to Z_q^*}$	T_m	T_i
时间(ms)	1.14	0.89	2.26	0.0008	0.004	0.00015

由表 6 可以看出, $T_{H\to G} > T_c > T_p > T_m > T_{H\to Z_q^*} > T_i$, 且哈希到 Z_q^* 的时间, 乘法运算时间, 逆运算时间远小于其他的密码操作的运行时间。

本文同时对本方案进行了计算开销测试, 其中 *PEKS* 代表关键词密文生成算法, *Trapdoor* 代表关键词陷门生成算法, *Test* 代表匹配算法。本文同时对文献[18,23]进行了计算开销对比, 对比结果如表 7 所示。

实验仿真中分别测试了生成 1~100 个关键词密文, 1~100 个关键词陷门与 1~100 次匹配所用的计算开销。对比图如图 6~图 8 所示, 其中图 6 表示关键词密文的计算开销, 图 7 表示关键词陷门的计算开销, 图 7 表示匹配的计算开销。

由图 6 的对比可知, 在关键词密文产生所用的时间上, 本文与文献[23]中的方案相差不大, 但是与文献[18]的方案相比较具有一定优势, 且随着关键词的增多所产生的差距也越来越大。因此本方案在关键词密文产生上有较高的计算效率。

由图 7 的对比可知, 在关键词陷门产生所用的时间上本方案与文献[18,23]的方案相比有较大的优势, 原因在于本方案产生关键词陷门时仅用到 2 次指数运算与 1 次哈希到群 G 上的运算, 而文献[18]用到 4 次指数运算, 1 次双线性对运算, 2 次哈希到群 G 上的运算, 文献[23]用到 4 次指数运算与 1 次哈希到群 G 上的运算。因此本方案在关键词密文产生上有较高的计算效率。

由图 7 的对比可知, 本方案在匹配的时间上略高于文献[23]的方案, 但是本方案在关键词密文与关键词陷门的产生时间上均小于其方案。相比于文献[18]的方案具有较大优势, 原因是因为本方案在匹配时使用了 1 次指数运算与 1 次双线性对运算, 而文献[18]的方案使用了 2 次指数运算与 2 次双线性对运算。由上述分析可得出结论, 本方案在保证安全的情况下, 具有较强的实用性。

7 总结

本文针对群组内用户进行密文安全搜索的需求, 基于广播加密的思想, 以群组为单位进行明文加密与密钥封装, 将公钥可搜索加密与基于身份的加密相结合, 提出了群组内匿名可搜索加密方案, 并给出了算法的形式化定义与实现过程, 实现了只有合法的授权用户才可以进行安全搜索并解密数据。此外, 在方案

表 7 计算开销比较

Table 7 Comparison of computing costs

方案	*PEKS*	*Trapdoor*	*Test*
[18]	$3T_c + 2T_p + 2T_{H\to G}$	$4T_c + T_p + 2T_{H\to G} + 4T_m$	$2T_c + 2T_p + T_m$
[23]	$5T_c + T_p + T_{H\to G} + T_{H\to Z_q^*} + T_m$	$4T_c + T_{H\to G} + T_{H\to Z_q^*} + 4T_m$	$2T_p + T_m$
本方案	$2T_c + 2T_p + 2T_{H\to G} + T_{H\to Z_q^*}$	$2T_c + T_{H\to G} + 2T_m + T_i$	$T_c + T_p + T_{H\to Z_q^*} + T_m$

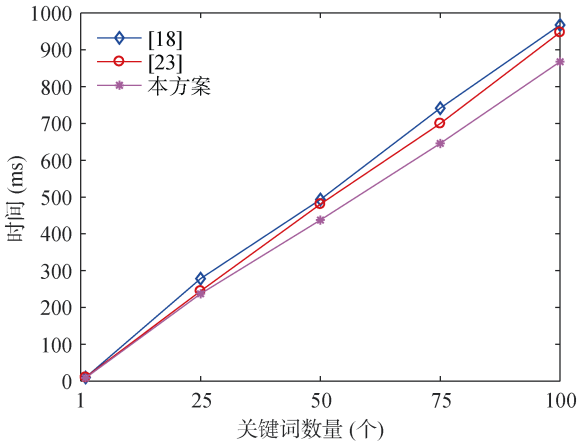

图 6 关键词密文计算开销

Figure 6 The computing costs of *PEKS*

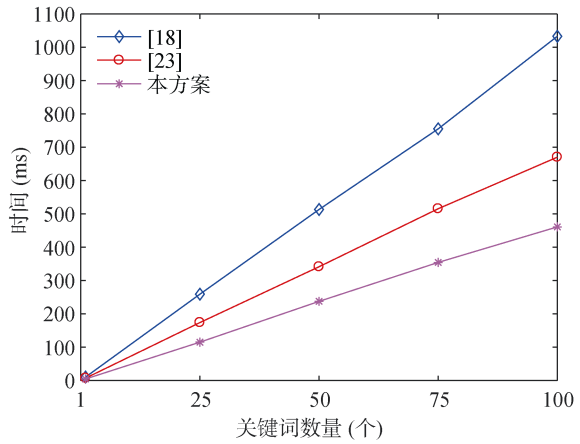

图 7 关键词密文计算开销

Figure 7 The computing costs of *Trapdoor*

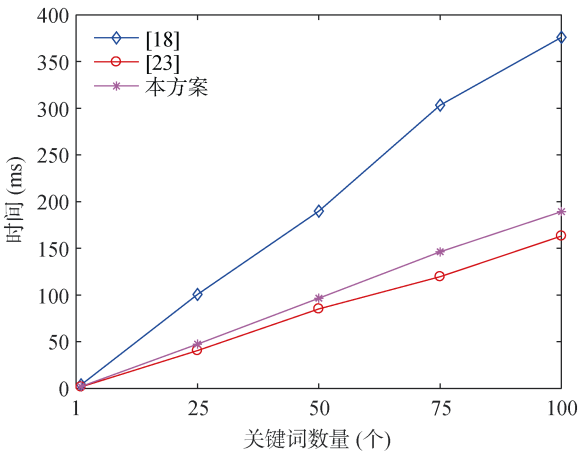

图 8 匹配计算开销

Figure 8 The computing costs of *Test*

中引入区块链机制, 利用智能合约作为可信第三方, 在用户验证搜索结果正确后支付搜索费用, 保证了云服务器与用户之间的公平支付。基于判定性双线性 Diffie-Hellman 问题与判定性 Diffie-Hellman 问题进行安全性分析, 证明本文方案在选择明文攻击下满足关键词密文与关键词陷门的不可区分性。利用 Charm-crypto 密码库进行性能分析表明本文方案在关键词密文与关键词陷门生成时具有较低的计算开销。

参考文献

[1] Sun P J. Security and Privacy Protection in Cloud Computing: Discussions and Challenges[J]. *Journal of Network and Computer Applications*, 2020, 160: 102642.

[2] Qin Z G, Xu J, Nie X Y, et al. A Survey of Public-Key Encryption with Keyword Search[J]. *Journal of Cyber Security*, 2017, 2(3): 1-12.
(秦志光, 徐骏, 聂旭云, 等. 公钥可搜索加密体制综述[J]. *信息安全学报*, 2017, 2(3): 1-12.)

[3] Song D X, Wagner D, Perrig A. Practical Techniques for Searches on Encrypted Data[C]. *2000 IEEE Symposium on Security and Privacy. S&P 2000*, 2000: 44-55.

[4] Boneh D, Di Crescenzo G, Ostrovsky R, et al. Public key encryption with keyword search[C]. *International conference on the theory and applications of cryptographic techniques*, 2004: 506-522.

[5] Baek J, Safavi-Naini R, Susilo W. Public Key Encryption with Keyword Search Revisited[C]. *Computational Science and Its Applications – ICCSA 2008*, 2008: 1249-1259.

[6] Park D J, Kim K, Lee P J. Public Key Encryption with Conjunctive Field Keyword Search[C]. *Information Security Applications*, 2005: 73-86.

[7] Boneh D, Waters B. Conjunctive, Subset, and Range Queries on Encrypted Data[C]. *Theory of Cryptography*, 2007: 535-554.

[8] Tang Q, Chen L Q. Public-Key Encryption with Registered Keyword Search[C]. *Public Key Infrastructures, Services and Applications*, 2010: 163-178.

[9] 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.

[10] Xu P, Jin H, Wu Q H, 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.

[11] Qin B D, 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.

[12] Lu H N. Searchable Symmetric Encryption with Hidden Search Pattern[J]. *Netinfo Security*, 2017(1): 38-42.
(陆海宁. 可隐藏搜索模式的对称可搜索加密方案[J]. *信息网络安全*, 2017(1): 38-42.)

[13] Boneh D, Franklin M. Identity-Based Encryption from the Weil Pairing[C]. *Advances in Cryptology — CRYPTO 2001*, 2001: 213-229.

[14] 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.

[15] Wu T Y, Tsai T T, Tseng Y M. Efficient Searchable ID-Based Encryption with a Designated Server[J]. *Annals of Telecommunications - Annales Des Télécommunications*, 2014, 69(7/8): 391-402.

[16] Wang S H, Han Z J, Xiao F, et al. Identity-Based Searchable Encryption Scheme with a Designated Tester[J]. *Journal on Communications*, 2014, 35(7): 22-32.
(王少辉, 韩志杰, 肖甫, 等. 指定测试者的基于身份可搜索加密方案[J]. *通信学报*, 2014, 35(7): 22-32.)

[17] Wei J, Qin L L. Secure identity-Based Searchable Encryption Scheme for Designated Sender[J]. *Computer Applications and Software*, 2020, 37(4): 285-289.
(魏晶, 秦璐璐. 安全的指定发送者的基于身份的可搜索加密方案[J]. *计算机应用与软件*, 2020, 37(4): 285-289.)

[18] Niu S F, Xie Y Y, Yang P P, et al. Identity-Based Searchable Encryption Scheme for Encrypted Email System[J]. *Journal of Electronics & Information Technology*, 2020, 42(7): 1803-1810.
(牛淑芬, 谢亚亚, 杨平平, 等. 加密邮件系统中基于身份的可搜索加密方案[J]. *电子与信息学报*, 2020, 42(7): 1803-1810.)

[19] Ma M M, He D B, Kumar N, et al. Certificateless Searchable Public Key Encryption Scheme for Industrial Internet of Things[J]. *IEEE Transactions on Industrial Informatics*, 2018, 14(2): 759-767.

[20] Zhang Y L, Liu X Z, Lang X L, et al. Certificateless Multi-Server Searchable Encryption Scheme in Cloud Environment[J]. *Netinfo Security*, 2019(3): 72-80.
(张玉磊, 刘祥震, 郎晓丽, 等. 云环境下基于无证书的多服务器可搜索加密方案[J]. *信息网络安全*, 2019(3): 72-80.)

[21] Tan L M. *Research on Searchable Encryption Scheme for Multi-User Data Sharing*[D]. Shanghai: East China Normal University, 2018.
(谭柳梅. 多用户数据共享可搜索加密方案的研究[D]. 上海: 华东师范大学, 2018.)

[22] Delerablée C. Identity-based broadcast encryption with constant size ciphertexts and private keys[C]. *International Conference on the Theory and Application of Cryptology and Information Security*, 2007: 200-215.

[23] Zhu M H, Chen Y L, Hu Y Y. Identity-Based Searchable Encryption Scheme Supporting Proxy re-Encryption[J]. *Computer Engineering*, 2019, 45(1): 129-135, 140.
(朱敏惠, 陈燕俐, 胡媛媛. 支持代理重加密的基于身份可搜索加密方案[J]. *计算机工程*, 2019, 45(1): 129-135, 140.)

[24] Xia Y M, Xu C G, Dou B N. An Anonymous Identity-Based Encryption Scheme in the Standard Model[J]. *Netinfo Security*, 2018(4): 72-78.
(夏逸珉, 许春根, 窦本年. 一种标准模型下基于身份的匿名加密方案[J]. *信息网络安全*, 2018(4): 72-78.)

[25] Mughal A, Joseph A. Blockchain for Cloud Storage Security: A Review[C]. *2020 4th International Conference on Intelligent Computing and Control Systems*, 2020: 1163-1169.

[26] Li H G, Zhang F G, He J J, et al. A Searchable Symmetric Encryption Scheme Using BlockChain[EB/OL]. 2017: arXiv: 1711.01030[cs.CR]. https://arxiv.org/abs/1711.01030

[27] Du R Z, Tan A L, Tian J F. Public Key Searchable Encryption Scheme Based on Blockchain[J]. *Journal on Communications*, 2020, 41(4): 114-122.
(杜瑞忠, 谭艾伦, 田俊峰. 基于区块链的公钥可搜索加密方案[J]. *通信学报*, 2020, 41(4): 114-122.)

[28] Fan K, Wang S Y, Ren Y H, et al. MedBlock: Efficient and Secure Medical Data Sharing via Blockchain[J]. *Journal of Medical Systems*, 2018, 42(8): 136.

[29] Chen L X, Lee W K, Chang C C, et al. Blockchain Based Searchable Encryption for Electronic Health Record Sharing[J]. *Future Generation Computer Systems*, 2019, 95: 420-429.

[30] Weng X Y, You L, Lan T T. Blockchain-Based Result-Traceable Searchable Encryption Scheme[J]. *Telecommunications Science*, 2019, 35(9): 98-106.
(翁昕耀, 游林, 蓝婷婷. 基于区块链的结果可追溯的可搜索加密方案[J]. *电信科学*, 2019, 35(9): 98-106.)

[31] Hei Y M, Liu J W, Zhang Z Y, et al. Blockchain-Based Distributed Cloud Storage System with Public Verification[J]. *Netinfo Security*, 2019(3): 52-60.
(黑一鸣, 刘建伟, 张宗洋, 等. 基于区块链的可公开验证分布式云存储系统[J]. *信息网络安全*, 2019(3): 52-60.)

[32] Yan X X, Yuan X H, Tang Y L, et al. Verifiable Attribute-Based Searchable Encryption Scheme Based on Blockchain[J]. *Journal on Communications*, 2020, 41(2): 187-198.
(闫玺玺, 原笑含, 汤永利, 等. 基于区块链且支持验证的属性基搜索加密方案[J]. *通信学报*, 2020, 41(2): 187-198.)

[33] Ni Y D, Zhang C, Yin T T. A Survey of Smart Contract Vulnerability Research[J]. *Journal of Cyber Security*, 2020, 5(3): 78-99.
(倪远东, 张超, 殷婷婷. 智能合约安全漏洞研究综述[J]. *信息安全学报*, 2020, 5(3): 78-99.)

王泽锐 于 2019 年在西安邮电大学信息安全专业获得学士学位。现在西安邮电大学电子与通信工程专业攻读硕士研究生学位。研究领域为密码学。研究兴趣包括: 云计算安全, 可搜索加密等。Email: wangzr0730@163.com

郑东 于 1999 年在西安电子科技大学获得密码学博士学位。现在西安邮电大学网络空间安全学院教授。研究领域为密码学, 云计算安全, 云存储安全。研究兴趣包括: 密码学, 云存储安全。Email: zhengdong@xupt.edu.cn

郭瑞 于 2014 年在北京邮电大学获得信息安全专业博士学位。现在西安邮电大学网络空间安全学院副教授。研究领域为云计算安全, 区块链技术。研究兴趣包括密码学, 区块链等。Email:guorui@xupt.edu.cn

朱天泽 于 2019 年在西安邮电大学信息安全专业获得学士学位。现在西安邮电大学网络空间安全专业攻读硕士研究生学位。研究领域为密码学。研究兴趣包括云计算安全, 可搜索加密等。Email: xiyouztz@163.com