基于区块链的农产品云数据可搜索加密研究

张 震[1]
ZHANG Zhen

摘 要 随着全社会对农产品数字化监管的推进，使用区块链和云存储已经成为趋势，但是其中的数据安全问题也越发突出。采用对称可搜索加密农产品云数据中的隐私文件进行快速加密，用智能合约技术和非对称可搜索加密管理对称密钥，不仅实现了农产品云数据机密性，还能让数据使用者在不解密的情况下对密文库进行搜索。结合区块链技术，提出一种基于区块链的农产品云数据可搜索加密方案，基于层次机构设计了引用层的数据查询、数据分析、溯源服务和数据共享功能。

关键词 区块链；可搜索加密；智能合约；农产品；云存储

doi：10.3969/j.issn.1672-9528.2024.10.035

0 引言

农产品质量安全关系着国计民生，但是在农产品数据溯源和共享过程中，现有的中心化处理方案面临着数据被篡改、隐私泄露、数据孤岛等问题。为了解决这些问题，将数据迁移到云服务器上是一种较为常见的方案，其在存储和处理效率方面有所提升，却也引入了数据安全、访问控制和高效搜索等新的难题[1]。区块链技术具有去中心化、不可篡改、透明可追溯等特性，是对农产品数据管理的一种新方案[2]。然而，仅仅依靠区块链技术仍无法完全解决农产品云数据的隐私保护和高效搜索问题。因此，结合可搜索加密技术，通过对数据进行加密存储，同时支持加密状态下的关键词搜索，确保数据的隐私保护和高效检索。通过构建基于区块链的农产品云数据可搜索加密方案，在对隐私数据保护的前提下，仍可以实现数据的高效搜索和有效共享。这两者的有机结合，降低了整体溯源和管理成本，为农产品云数据的管理提供了一个安全、可靠、高效的解决方案。

1 相关技术概述

1.1 区块链技术

区块链的本质是一个分布式账本，由一个又一个的区块按照时间戳顺序链接而成，被系统内的所有节点所记录[3]。区块是一种包含了多个交易的数据结构，后一个区块把前一个区块的哈希值纳入到本区块哈希函数输入，这样就形成了一种不断生长的链条结构。由于哈希函数的单向性和密码学特点，区块链具有了不可篡改的特性。共识算法是区块链技术的灵魂，它规定了系统内共识节点之间达成数据一致性的条件，设计了系统抵抗恶意节点的机制，实现了区块链技术中数据的可追溯性和透明性。区块链技术在数据共享、隐私保护和多方协作等方面具有较大的优势，已经被广泛应用到数字金融、医疗健康、物联网管理和司法存证等领域。

区块链的类型可以依据进入权限的不同、开放的程度和所处阶段进行分类。权限指的是对一个普通节点被接纳为区块链节点的限制，没有限制的区块链类型被称为非许可链，反之，如果某个节点需要被审核之后才能进入区块链系统成为节点，那么则称之为许可链。可见，是否有审核环节是该类型判断的核心。开放程度指的是共识节点的身份是否被严格指定。具体来说，任何一个区块链节点都可以成为共识节点，那么这种类型的区块链被称为公有链，比如比特币和以太坊。如果共识节点被圈定在一小部分节点范围内，甚至于指定特定节点，那么这种类型的区块链被称为联盟链，常见于多个平等实体之间，比如 Fabric 和 Ripple。如果区块链系统仅存在于单一的实体之内，如公司或者某个组织，那么这种类型的区块链就被称为私有链。区块链第一阶段是 1.0 时代，它的代表是比特币，目的是实现金融功能，强调区块链的去中心化、安全和匿名等特性。随着智能合约和去中心化应用的引入，区块链技术进入了第二阶段，也就是 2.0 时代，它的代表是以太坊。区块链的 3.0 时代在 2.0 的基础之上强调满足更多的需求，更加注重整体性能的提升，对于互操作性和隐私保护等方面有深刻的技术安排。

1.2 可搜索加密技术

可搜索加密（searchable encryption，SE）是一种为了解决云存储环境下加密数据检索困难问题，实现用户基于密文

1. 河南工业贸易职业学院信息工程学院 河南郑州 450053

[基金项目] 2024 年度河南省科技厅科技攻关项目“基于云计算和区块链融合的农产品质量安全控制技术研究”（242102210188）

关键词安全搜索的技术[4]。在使用过程中，用户只需要输入特定关键词，服务器就可以返回其需要的加密后的文件，解决了传统明文搜索的数据泄密问题，有效保护了用户数据的隐私安全。根据加密方式的不同，可搜索加密技术分为对称可搜索加密（symmetric searchable encryption，SSE）和非对称可搜索加密（asymmetric searchable encryption，ASE）[5]。

1.2.1 对称可搜索加密

对称可搜索加密的核心是使用同样的密钥进行加密数据和解密数据。用户一般可以使用密码学安全随机数生成器等方法生成密钥，然后使用某些方法将密钥传递给其他节点。因为只涉及一个密钥，所以该方法具有加密速度快、密钥管理简单和查询效率高等优良特性，但也因此存在着密钥安全性较低、密钥轮换困难和仅适合数据上传者检索数据的局限性，不能应用于访问控制和多用户搜索等场景[6]。

对称可搜索加密方案主要包含密钥生成算法、密文和索引生成算法、陷门生成算法、搜索算法以及文件解密算法五个算法。数据所有者执行 KeyGen 得到密钥 K，然后使用 K 对本地文件 D 进行 Enc 运算得到加密后的文件 C，同时生成加密索引 I，并将两者传输至服务器。数据使用者，也就是数据所有者，需要在加密后文件中进行搜索的时候，先执行 Trapdoor 算法生成陷门 tk，上传至服务器进行加密搜索操作。云服务器根据陷门 tk 和机密索引 I 匹配后，将匹配的密文结果 C' 交给数据使用者。数据使用者用密钥 K 对密文结果 C' 解密即可得到明文文件。

1.2.2 非对称可搜索加密

与对称可搜索加密不同的是，非对称可搜索加密技术在进行加密和解密的时候使用的是不同的密钥，分别称之为公钥和私钥，非对称可搜索加密也被称为公钥可搜索加密。这样的设计解决了对称可搜索加密在密钥泄露后面临重大数据安全的窘境，不同实体分别保存公钥和密钥，能更灵活地应对可搜索加密需求，在访问控制和多用户搜索等场景中较为适用。但因为计算复杂度更高，所以该算法具有需要更多的计算资源、密钥管理复杂和速度较慢等缺点，难以应用在效率要求较高的应用场景[7]。

非对称可搜索加密方案模型中包含数据所有者、数据使用者、云服务器和密钥管理中心四个实体，包含系统初始化算法 Setup、加密关键字和密文生成算法 KeyGen、陷门生成算法 Trapdoor、搜索算法 Search 和文件解密算法 Dec 五个算法组成。

密钥管理中心首先执行 Setup 算法获得主密钥 MK 和公共参数 PP，然后将其输入 KeyGen 算法得到公钥 pk 和私钥 sk。数据所有者执行 Enc 算法对本地文件进行加密，提取本地文件的关键字 w，并对其加密生成加密关键字 cw，最后将 cw 密文提交至云服务器。当数据使用者需要在加密后的文件中进行搜索的时候，他首先需要输入私钥 sk 和关键字 w，执行 Trapdoor 算法，得到陷门 tk，然后将其提交至云服务器进行搜索。云服务器将收到的陷门 tk 和加密关键字 cw 进行运算，然后将匹配到的加密后的文件 C' 传输给数据使用者。数据使用者用密文对应的密钥 sk 对密文 C' 进行解密，最终可以解析出相应的明文内容。在这个过程中，云服务器并不会泄露任何明文信息。

2 一种基于区块链的农产品云数据可搜索加密方案

2.1 方案模型

在本方案中共有数据所有者、数据使用者、云服务器和密钥管理中心四种角色，生产者、加工厂、运输商、经销商和用户均可以是数据所有者和数据使用者。如图 1，基于区块链的农产品云数据可搜索加密方案采用分层结构设计，由下向上依次是数据采集层、数据加密层、区块链层和应用层。

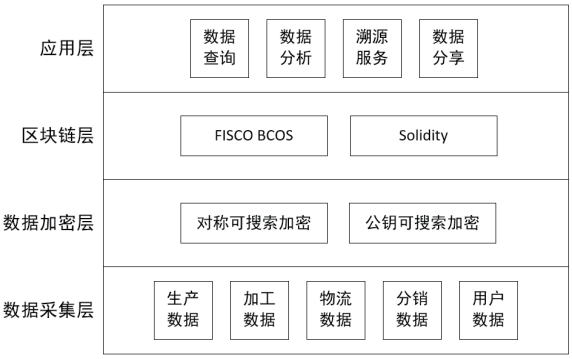

图 1 基于区块链的农产品云数据可搜索加密方案架构图

2.1.1 数据采集层

参与数据采集的主要参与方包括生产者、加工厂、运输商、经销商和用户。数据采集层负责从农产品的生产、加工、运输和存储等环节中，通过传感器、手持设备和物联网设备等手段，采集相关数据。这些数据主要包括环境温度、空间湿度、光照强度、地理位置和运输时间等[8]。数据采集层对原始数据进行清洗、分类和结构化处理，进而确保数据具有较高的质量和一致性，为接下来的数据加密和存储环节做好基础工作。

2.1.2 数据加密层

数据加密层将对称可搜索加密和公钥可搜索加密相进行有效结合，进而实现隐私数据的机密性和可搜索性。具体而言，使用对称可搜索加密方案对农产品涉及的隐私数据进行加密，从而保证数据在云环境中的隐私保护和可搜索性。与此同时，为了避免对称可搜索加密的缺点，安全地管理其密钥，该层使用公钥可搜索加密对对称可搜索加密的密钥进行加密和保护。通过这种组合方式，数据加密层能够在确保数

据隐私的同时，实现对加密数据的高效检索和安全访问控制。

2.1.3 区块链层

区块链层的技术平台是 FISCO BCOS[8]，它具备并行处理、分布式存储和较高安全控制等特性，是一个开源的企业级联盟链。农产品处理流程中的生产者、加工厂、运输商、经销商、用户和监管方被设置为共识节点，存储系统中的所有数据，参与共识算法，对系统内的事务进行统一决策，这些节点被部署在云服务器中。FISCO BCOS 支持部署智能合约 [9]。系统将帮助各方用户编写基于业务规则的智能合约，用来高效公平处理各种数据，过滤不规范的数据，为其他层打好数据基础。

2.1.4 应用层

应用层位于整个系统的最上层，可以为使用者提供便捷直观的操作界面，帮助其使用相应的功能。该层通过调用底层区块链和数据加密层的接口，整合并展示经过加密和验证的数据，满足不同角色用户（包括生产者、加工厂、运输商、经销商、用户和监管方）的特定需求。

应用层功能划分为数据查询、数据分析、溯源服务和数据共享。数据查询功能帮助用户在密文条件下搜索相关文件。数据分析功能帮助用户对特定领域的数据进行分析，运用大数据等技术挖掘其潜在的价值，指导用户优化业务。溯源服务是一项基本服务，保证了农产品的可查可信可追溯。数据共享功能建立了多方主体之间的数据传递原则，能够有力推动相关领域的科研探索和商业价值 [10]。

2.2 基于区块链的农产品云数据可搜索加密流程

基于区块链的农产品云数据可搜索加密流程整体上分为两部分，分别是使用对称可搜索加密方案对农产品隐私数据进行加密，以及使用非对称可搜索加密方案对对称密钥加密。

2.2.1 对农产品隐私数据进行加密

（1）密钥生成阶段

数据采集层的数据所有者节点（生产者、加工厂、运输商、经销商和用户）执行密钥生成算法 KeyGen 得到密钥 K。

（2）密文和索引生成阶段

数据采集层的数据所有者节点运行 Enc 算法，使用密钥 K 对涉及农产品隐私数据的文件进行加密获得密文文件 C，根据待加密文件的关键词生成加密索引 I，将两者上传到区块链网络所在的云服务器中。

（3）构造搜索陷门阶段

系统内的数据使用者节点运行陷门生成算法 Trapdoor，将密钥 K 和搜索关键字 w 进行运算获得陷门 tk。

（4）加密文件搜索阶段

智能合约收到数据使用者节点提交的陷门 tk 后，按照预定的规则执行搜索算法 Search，将匹配于加密索引 I 的密文文件 C' 返回给数据使用者。

（5）文件解密阶段

数据使用者节点执行解密算法 Dec，使用密钥 K 对智能合约返回的 C' 进行解密，最终完成对加密文件的搜索。

2.2.2 对对称可搜索加密密钥的加密

针对对称加密方案存在的密钥容易泄露问题，本方案将结合公钥加密可搜索方案和区块链技术实现对称加密密钥的有效管理。

（1）系统初始化阶段

本方案中由监管方承担密钥管理中心节点职责，借助智能合约的自动化执行的特性，将系统初始化算法 Setup 部署在区块链上。当初始化功能被调用者触发后，密钥管理中心节点生成对应的主密钥 MK 和公共参数 PP。

（2）公私钥生成阶段

密钥管理中心节点根据 KeyGen 算法为调用者生成公钥 pk 和私钥 sk。

（3）加密对称密钥阶段

对称密钥作为关键字 w 参与本阶段运算，数据所有者节点使用公钥 pk 对其进行加密后获得加密关键字 cw，然后将 w 和 cw 发送至由 FISCO BCOS 搭建的区块链网络中。

（4）密文搜索阶段

数据使用者节点使用自己的私钥 sk 和要搜索的关键字 w 作为算法 Trapdoor 输入，进而得到该函数输出的陷门 tk，然后将其提交给对应的智能合约，由其在加密数据库中搜索，最终得到对应的加密文件 C' 并交还给数据使用者节点。

（5）还原对称密钥阶段

数据使用节点运行解密算法 Dec，将得到的加密文件 C' 还原为对称密钥。

3 结语

针对云存储环境下的农产品数据安全问题，本文提出了一种基于区块链的农产品云数据可搜索加密方案。它解决了当前区块链的明文存储问题，为注重数据隐私的用户设计了密文条件下的搜索方案，保护了产品生产、交易、运输等环节的机密性。采用智能合约实现了数据的高效处理。应用层的多种功能为农产品的全流程处理提供了较大的便捷性。下一步的研究重点是探索可编辑区块链在该领域的应用，进一步克服区块链上数据不可变的局限性，给用户更大的操作权限，完善相关领域的业务流程。

参考文献：

[1] 翟社平，张瑞婷，杨锐，等．多用户环境的区块链可搜索加密方案 [J/OL]. 西安电子科技大学学报 ,1-18[2024-06-24]. https://doi.org/10.19665/j.issn1001-2400.20240205.

单源多播网络视域下的安全网络编码技术探究

杨 浩[1]
YANG Hao

摘 要 研究了单源多播网络视域下的安全网络编码技术，旨在提高数据传输的安全性和效率。研究内容包括网络模型的构建、污染攻击的防御、自适应验证机制的设计及其性能分析。通过引入线性子空间签名和自适应验证机制，实现了对数据包的完整性和正确性的有效保障。仿真结果显示，所提出的方案在不同攻击环境下均能显著提高数据包验证成功率，并且通过动态调整验证策略，降低了计算和带宽开销。研究成果表明，所提出的方案不仅增强了网络抗攻击能力，还提高了数据传输的整体效率，具有重要的理论价值和实际应用价值。

关键词 安全网络；编码技术；单源多播网络；信源节点；自适应验证

doi：10.3969/j.issn.1672-9528.2024.10.036

0 引言

随着网络通信技术的迅速发展，网络安全问题日益凸显。特别是在单源多播网络中，数据传输的完整性和安全性面临着严峻挑战。污染攻击、重放攻击和窃听攻击等威胁不断升级，对网络数据的正确性和保密性构成了巨大威胁。因此，研究一种能够有效防御这些攻击的安全网络编码技术具有重要意义。本文旨在探讨一种基于线性子空间签名的自适应安全网络编码方案，着重分析了方案在防御各种攻击方面的有效性，还通过仿真验证了其在不同网络环境下的性能表现，为网络安全提供了新的解决方案和理论依据。

1. 辽宁省烟草公司葫芦岛市公司 辽宁葫芦岛 125000

1 方案构建

1.1 信源节点编码

信源节点编码过程依赖于以下参数。

大素数 q 和 p：满足 $p \mid (q-1)$ 的关系，用于有限域和群的生成[1]。

生成元 g：有限域 F_q 上阶为 p 的群 G 的生成元。

私钥 prK：随机选择的私钥集合 $\{\alpha_i \mid i=1,2,...,m+n\}$。

公钥 puK：通过 $h_i=g^{\alpha i}$ 生成的公钥集合，向网络中所有

[2] 黄宁，谷茂春，王敬红．基于区块链＋物联网的农产品溯源解决方案研究 [J]. 无线互联科技，2022,19(20): 158-161+165.

[3] 孙国梓，王钰，李兆维，等．基于区块链的可搜索加密技术研究综述 [J]. 南京邮电大学学报 (自然科学版), 2024, 44(1): 65-78.

[4] 郑智健，郑清杰，林钒．可搜索加密的区块链气象数据保护研究 [J]. 技术与市场，2023,30(1):32-35.

[5] 马彩霞．动态对称可搜索加密的隐私保护研究 [D]. 保定：河北大学，2023.

[6] 张洪骜．面向区块链的可搜索加密方案研究 [D]. 北京：北京工业大学，2024.

[7] 卢俊成．基于区块链的可搜索加密方案研究 [D]. 兰州：兰州理工大学，2024.

[8] 王桂兰，张成，周国亮．结合 FISCO BCOS 与拓扑优化一致性算法的配电网多目标经济调度 [J/OL]. 计算机工程：1-16 [2024-03-01].https://doi.org/10.19678/j.issn.1000-3428.0069274.

[9] 查凯金．基于区块链的食品溯源关键技术研究及应用 [D]. 抚州：东华理工大学，2023.

[10] 王诗卉．云存储中支持验证的可搜索加密技术研究 [D]. 南京：东南大学，2022.

【作者简介】

张震（1993—），男，河南三门峡人，硕士，助教，研究方向：区块链、云计算。

（收稿日期：2024-07-01）