

doi:10.13682/j.issn.2095-6533.2026.05.002

区块链与可搜索加密的无人机 通信数据共享方案

李亚红, 魏 萱, 黄海燕

(兰州交通大学 电子与信息工程学院, 甘肃 兰州 730000)

摘 要: 针对低空无人机通信数据在存储、共享与访问过程中存在隐私泄露、数据篡改、访问控制困难及密文检索效率低等问题, 提出一种区块链与可搜索加密的无人机通信数据共享方案。该方案采用联盟链与边缘私有链协同的双链架构, 构建链上索引、链下密文存储模式, 在兼顾数据隐私保护的同时支持跨域共享。地面控制站负责数据采集、加密与索引生成, 边缘私有链记录密文哈希和关键词索引, 联盟链维护用户伪身份及共享索引, 并设计匿名索引构建机制, 实现用户身份匿名性和数据记录不可关联。最后, 结合代理重加密与可搜索加密技术, 给出轻量化重加密机制, 在不解密原始数据的条件下实现灵活授权访问与高效密文检索。安全性分析表明, 该方案满足选择密文攻击下的不可区分性, 能够保障用户身份匿名性、数据记录不可关联性 & 数据共享过程安全性。实验结果表明, 所提方案的加密、重加密和解密耗时分别为 16.0 ms、5.0 ms 和 6.0 ms, 重加密效率相较于同类方案最高提升约 78.3%, 能够在保障低空无人机通信数据全流程安全的同时满足实时共享需求。

关键词: 低空无人机网络; 通信数据共享; 区块链; 可搜索加密; 隐私保护

中图分类号: TP309.7

文献标志码: A

文章编号: 2095-6533(2026)05-0018-12

Blockchain and searchable encrypted UAV communication data sharing scheme

LI Yahong, WEI Xuan, HUANG Haiyan

(School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730000, China)

Abstract: Aiming at the problems of privacy leakage, data tampering, difficult access control and low ciphertext retrieval efficiency existing in the storage, sharing and access of low-altitude unmanned aerial vehicle (UAV) communication data, a UAV communication data sharing scheme integrating blockchain and searchable encryption is proposed. The scheme adopts a dual-chain architecture combining consortium blockchain and edge private blockchain, and constructs an on-chain index and off-chain ciphertext storage mode, which supports cross-domain data sharing while taking data privacy protection into account. Ground access stations are responsible for data collection, encryption and index generation. The edge private blockchain records ciphertext hashes and keyword indexes, while the consortium blockchain maintains user pseudonyms and shared indexes. An anonymous index construction mechanism is designed to realize user identity anonymity and unlinkability of data records. Finally, combined with proxy re-encryption and searchable encryption technologies, a lightweight re-encryption mechanism is proposed to realize flexible authorized access and efficient ciphertext retrieval without decrypting original data. Secu-

收稿日期: 2026-03-25

基金项目: 国家自然科学基金项目(62461032); 兰州交通大学-天津大学联合创新基金项目(LH2024003); 甘肃科技专员项目(26CXGA042)

引文格式: 李亚红, 魏萱, 黄海燕. 区块链与可搜索加密的无人机通信数据共享方案[J]. 西安邮电大学学报, 2026, 31(5): 18-29.

LI Yahong, WEI Xuan, HUANG Haiyan. Blockchain and searchable encrypted UAV communication data sharing scheme[J]. Journal of Xi'an University of Posts and Telecommunications, 2026, 31(5): 18-29.

rity analysis demonstrates that the scheme satisfies indistinguishability under chosen ciphertext attack, and can guarantee user identity anonymity, unlinkability of data records and the security of the entire data sharing process. Experimental results show that the time consumption of encryption, re-encryption and decryption of the proposed scheme is 16.0 ms, 5.0 ms and 6.0 ms respectively. Compared with similar schemes, the re-encryption efficiency is improved by up to approximately 78.3%. The proposed scheme can satisfy the real-time sharing requirement while ensuring the full-process security of low-altitude UAV communication data.

Keywords: low-altitude unmanned aerial vehicle networks; communication data sharing; blockchain; searchable encryption; privacy protection

随着低空经济和边缘计算技术的发展,无人机飞行共享状态数据逐渐成为现代智能空域管理系统中的重要组成部分。无人机飞行共享状态数据的使用不仅提高了空域信息的准确性和可靠性,简化了无人机运行记录管理,而且对空域协同、任务调度和低空智能服务具有积极意义^[1-2]。然而,传统的无人机飞行共享状态数据存储、共享与传输系统容易受到单点故障、恶意篡改等威胁,特别是在数据隐私、访问控制 and 安全性方面^[3]。因此,在保护无人机用户隐私的前提下,安全、有效地共享无人机飞行共享状态数据亟需得到完全解决。

区块链技术因其去中心化、不可篡改和可追溯的特性,能够有效保障无人机飞行共享状态数据在存储和共享过程中的数据完整性和安全性^[4-5]。通过智能合约实现精细的访问控制策略,确保仅授权用户能够访问特定数据,从而有效保护无人机用户隐私并提高数据处理效率^[6]。相关研究提出了基于区块链的数据管理模型,使数据拥有者能够对自身数据保持更高层次的控制权^[7]。也有研究探讨了区块链分布式账本技术在数据管理和共享中的应用,分析了区块链在提升数据管理系统安全性和透明度方面的作用^[8]。另有研究设计了基于区块链的数据共享框架,同样注重个人隐私保护^[9]。但是,区块链在处理无人机飞行共享状态数据时仍然面临诸多问题。首先,区块链的公开透明性与无人机飞行共享状态数据的隐私保护需求之间存在冲突,因此,在多个实体之间安全共享这些加密数据仍然是一个问题^[10]。其次,传统区块链对加密数据的查询缺乏灵活性,在不解密的情况下实现对目标数据的精确检索仍具有挑战性。

代理重加密(Proxy Re-Encryption, PRE)技术使得密文能够在不同用户之间进行共享^[11]。PRE在访问控制和密钥管理上具有较高的灵活性和效率。借助区块链的分布式网络,PRE能够在不同节点之间实现动态、安全的数据共享,从而支持跨节

点、跨域的数据协作^[12]。近年来,将PRE技术与区块链结合的研究逐渐增多。例如,Li等^[13]展示了基于区块链和PRE的数据共享方案,解决了多方协作中的访问控制问题。Remya等^[14]提出了基于无证书PRE的区块链数据共享方案,解决了证书托管问题,避免了传统服务器单点失效和存储容量受限的问题。Liu等^[15]提出了可跟踪匿名数据存储与区块链共享方案,通过链上链下模式缓解了区块链在大规模数据存储方面的压力。将PRE与区块链技术结合,有助于实现无人机飞行共享状态数据的安全授权共享,并提升跨域协同效率^[16]。

对于数据隐私保护,可搜索加密技术在区块链中的应用使得用户能够在数据保持加密状态的情况下,通过关键词检索访问特定数据^[17-18]。对于无人机飞行共享状态数据共享,无人机用户或授权数据请求者可以依据授权查询加密数据中的特定关键词,而无需暴露完整数据内容,这一过程极大降低了数据泄露的风险。李宇溪等^[19]提出了结合可搜索加密的区块链系统,能够在加密状态下实现有效查询,在保证数据隐私的同时提升了系统实用性。杨锐等^[20]的研究展示了区块链结合可搜索加密技术在加密信息检索中的优势,使得授权用户能够在加密数据中高效定位目标信息。结合PRE与可搜索加密技术后,既实现了无人机飞行共享状态数据灵活授权和安全共享,又支持加密数据的高效查询。近年来,深入探讨了PRE、可搜索加密与区块链的融合方案,为数据共享提供了更加完善的安全保障^[21-24]。

考虑到单一类型的区块链在处理无人机通信数据共享的隐私保护和跨节点协作时存在局限性^[25]。如果直接使用联盟链存储所有无人机飞行共享状态数据,可能会带来较高的存储成本,并且联盟链中的数据对所有参与节点都是可见的,这会增加数据泄露的风险。而私有链可以确保敏感数据只在特定节点内部可见,保障了更高的隐私性^[26]。

因此,联盟链和私有链的结合使用能够在实现数据共享的同时,确保数据的安全性和隐私保护^[27]。双链架构将联盟链和私有链结合应用于无人机飞行共享状态数据共享,进一步增强了数据安全性与访问控制的灵活性。相关研究表明,基于双链结构的数据共享系统能够在保障隐私的同时提高共享效率和系统安全性^[28-29]。

鉴于此,针对低空无人机通信数据在存储、共享与访问过程中存在的隐私泄露、数据篡改及访问控制困难等问题,本文拟提出一种区块链与可搜索加密的无人机通信数据共享方案。首先,构建联盟链与边缘私有链协同的双链架构改善单一区块链在隐私保护与跨域协同方面的不足,实现链上索引管理与链下密文存储。其次,引入匿名索引构建机制和代理重加密技术,在实现密文检索的基础上,进一步支持安全授权共享、身份隐私保护和数据记录不可关联。最后,设计轻量化重加密机制,降低授权共享过程中的计算开销,并通过安全性理论分析与计算性能验证,证明方案在安全性和效率方面的有效性。

1 预备知识

1.1 mCDH 假设

定义 1 改进的 CDH(Modified Computational Diffie-Hellman, mCDH)问题。设 G 是一个循环乘法群,其阶为素数 q ,且 g 是群 G 的生成元。从 $\mathbb{Z}_q^*$ 中随机选取未知数 a 和 b ,mCDH 问题是给定 $(g, g^{1/a}, g^a, g^b)$,计算 g^{ab} 。如果无法在一个概率多项式时间算法 P 能以不可忽略的概率求解 G 上的 mCDH 问题,则称 mCDH 问题是困难的。

1.2 代理重加密

PRE 是原始数据首先被用户 A 使用其公钥 p_A 加密,生成密文 c_A 发送给半可信的代理。然后,通过代理重加密技术,A 生成一个重加密密钥 R 给第三方,半可信的代理利用重加密密钥将加密的数据转换成另一个用户 B 的私钥 s_B 可以解密的形式 $c_B = \text{ReEncrypt}(R, c_A)$,其中 ReEncrypt 是重加密算法,而无需将原始数据解密成明文。这种转换通过重加密密钥实现,确保了即使在转换过程中,原始数据的明文也不会被暴露,从而保持了密文的机密性和安全性。

PRE 在选择密文攻击下具有不可区分性(Indistinguishability under Chosen Ciphertext Attacks

for Proxy Re-encryption, IND-PRE-CCA),即使攻击者可观察密文的转换过程并请求对非挑战密文的解密,也无法准确判断出一个特定密文的加密内容。

1.3 Schnorr 签名

Schnorr 签名是一种数字签名算法,由 Schnorr^[30] 在 1991 年提出,是公钥密码学中应用广泛的签名方法之一。Schnorr 签名算法因其高效性、安全性和较短的签名长度而受到认可。算法包括密钥生成、签名生成和签名验证,具体描述如下。

1) 密钥生成。选取大素数 p, q 和生成元 $g \in \mathbb{Z}_q^*$,其中 $p \geq 2^{512}, q | (p-1), q \geq 2^{160}, g^q = 1 \pmod{p}$,随机选择私钥 $x \in (1, q)$,计算公钥 $y = g^x \pmod{p}$ 。

2) 签名生成。输入用户的公钥 y 和消息 m ,用户选择随机数 $k \in (1, q)$, m 计算 $r = g^k \pmod{p}, u = H(r, m), s = xu + k \pmod{p}$,输出签名值 (u, s) 。

3) 签名验证。输入消息 m 和数字签名 (u, s) ,计算 $r' = g^u y^{-s} \pmod{p}$ 和 $H(r', m)$,并验证 $H(r', m) = u$ 是否成立,若成立输出 1,否则输出 0。

Schnorr 签名满足在选择消息攻击下存在不可伪造性(Existential Unforgeability under Chosen Message Attacks, EUF-CMA)。

2 方案设计

2.1 方案系统模型

低空无人机飞行状态数据共享系统由无人机用户、地面控制站(Ground Control Station, GCS)、边缘计算节点、第三方数据请求者以及区块链网络共同组成,系统模型如图 1 所示。

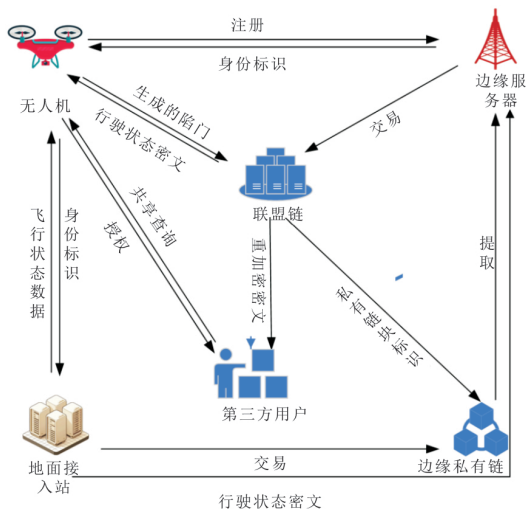


图 1 系统模型

1) 无人机用户。当无人机用户控制低空无人机通信网络执行飞行任务时,地面控制站根据无人机的飞行状态生成无人机飞行共享状态数据及相关关键词,并利用无人机用户提供的公钥对数据进行加密处理。若无人机在多个区域执行任务,可为其构建可搜索的数据索引并上传至联盟链,以便在后续数据共享过程中实现历史飞行信息的安全检索。

2) 地面控制站。地面控制站负责采集无人机飞行状态信息,并完成数据加密与索引生成操作。加密后的无人机飞行共享状态数据被上传至边缘节点存储,而数据密文的哈希值及相关索引信息被记录在边缘私有链上。同时,地面控制站可根据无人机用户的真实身份生成对应的匿名身份,用于后续数据共享过程中的隐私保护。

3) 第三方数据请求者。当相关管理机构或授权服务提供方需要获取无人机飞行共享状态数据时,必须首先获得无人机用户的授权。授权完成后,第三方数据请求者可通过联盟链获取加密的数据索引。联盟链节点利用代理重加密密钥对密文进行再次加密,使授权用户能够通过解密并访问目标数据。

4) 边缘计算节点。边缘节点负责存储加密后的无人机飞行共享状态数据,并从私有链中获取区块标识、数据哈希值以及无人机用户匿名身份等信息,在联盟链上构建新的交易记录,供联盟链节点进行验证与区块生成,从而实现数据的可信共享。

5) 边缘私有链。边缘私有链由各边缘节点独立维护,主要用于管理敏感无人机飞行共享状态数据的安全索引与完整性验证。地面控制站上传的数据哈希值及索引信息均记录在私有链中,并作为联盟链数据共享交易的重要依据。

6) 联盟链。联盟链由多个边缘节点及相关监管节点共同维护,主要用于实现跨区域无人机飞行共享状态数据共享及索引完整性审查。联盟链节点负责执行关键词搜索机制,以支持无人机用户或授权数据请求者对目标无人机飞行共享状态数据的安全查询与访问。在整个数据共享过程中,联盟链充当可信中介角色。

2.2 安全目标

在所提方案中,边缘服务器及地面控制站设备被定义为半信任节点。攻击者可能通过监听无线

链路窃取敏感信息,例如无人机飞行共享状态数据密文、索引信息及搜索密钥。针对上述安全威胁,所提方案将实现以下安全目标。

1) 数据安全与访问控制。通过对无人机飞行共享状态数据进行加密,并在边缘私有链中存储数据密文的哈希值,保证无人机飞行共享状态数据的安全性与不可篡改性。联盟链用于存储跨节点无人机飞行共享状态数据索引,而每次数据访问均需经过无人机用户授权并结合代理重加密机制实现,从而确保数据访问过程的安全性。

2) 保护隐私。为保护无人机用户隐私,系统通过引入匿名身份机制实现用户身份的匿名性与不可追踪性。不仅能够有效隐藏无人机用户的真实身份及敏感信息,还能防止攻击者通过数据关联分析识别不同数据记录是否来源于同一无人机用户,从而保障数据的不可关联性,并避免真实身份被追溯。

3) 安全搜索。系统设计安全搜索验证机制以确保检索过程的安全性。在搜索阶段,由无人机用户生成特定的搜索陷门并提交至联盟链,由联盟链节点执行密文检索操作。在整个搜索过程中,攻击者无法获取搜索关键词或相关查询信息,从而保证数据检索过程的隐私性与安全性。

2.3 共识机制

系统结合私有链和联盟链,每个链都有自己的一致性证明机制,以确保整个系统的完整性和同步。

1) 私有链的一致性证明机制。无人机用户首先在地面控制站完成控制注册与身份认证,从而获得唯一的无人机身份标识。随后,地面控制站根据无人机的飞行状态生成无人机飞行共享状态数据,并对数据进行加密处理。地面控制站将加密后的数据作为交易发布到边缘私有链上,私有链节点对该交易进行验证,以确保数据的生成与上传已获得无人机用户的授权。当超过 $2/3$ 的私有链节点验证通过后,边缘私有链将生成新的区块以记录相关交易,从而实现数据的可信存储与一致性维护。

2) 联盟链的一致性证明机制。该机制是确保索引管理一致性,首先在数据加密阶段定义关键字集合 $w = (w_1, w_2, \dots, w_n)$,所有加密关键字均从该集合中选择。其次系统通过关键字的哈希值构建多项式 $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$,用于验证关键字密文的合法性。当超过 $2/3$ 的验证者

确认关键字密文属于集合后,生成新区块。

3 方案描述

区块链与可搜索加密的无人机通信数据共享方案的具体实现主要包括系统建立、密钥设置、数据存储上传、匿名身份与区块构建、重加密密钥生成、陷门生成、密文重加密、检索验证及数据解密等关键环节,下面将完整说明数据从采集、加密、上链、授权检索到安全解密的全流程操作,明确各参与实体的交互逻辑与核心算法执行步骤。

1)系统建立 $\text{Setup}(\delta) \rightarrow m$ 。给定安全参数 δ ,输出双线性对 $\hat{e}: G \times G \rightarrow G_T$,其中 G 和 G_T 具有相同的素数阶数 q 的乘法群,选择生成元 $g \in G$,计算 $\varphi = e(g, g)$ 。定义哈希函数组 $H_1: \{0, 1\}^* \rightarrow G, H_2: \{0, 1\}^* \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*, H_3: G \rightarrow \{0, 1\}^*, H_4: \{0, 1\}^* \rightarrow \mathbb{Z}_q^*, H_5: \{0, 1\}^* \rightarrow G, H_6: \{0, 1\}^* \times G \rightarrow \mathbb{Z}_q^*$ 。无人机通信网络时,由地面控制站为无人机用户生成唯一的身份标识 $\alpha \in \mathbb{Z}_q^*$,计算 $\tau = H_4(\alpha)$ 并发送至边缘服务器,当通信时将给地面控制站,公布参数 $m = \{e, q, g, G, G_T, H_1, H_2, H_3, H_4, H_5, H_6\}$ 。

2)KeyGem(m) $\rightarrow (p_A, s_A, p_B, s_B, p_D, s_D, p_O, s_O)$ 。输入系统公开参数 m ,无人机用户 A 选择随机数 $x_A \in \mathbb{Z}_q^*$,公钥 $p_A = g^{x_A}$,私钥 $s_A = x_A$ 。地面控制站 B 选择随机数 x_B ,公钥 $p_B = g^{x_B}$,私钥 $s_B = x_B$ 。第三方用户 D 选择随机数 $x_D \in \mathbb{Z}_q^*$,公钥 $p_D = g^{x_D}$,私钥 $s_D = x_D$ 。联盟链上的节点 O 选择随机数 $x_O \in \mathbb{Z}_q^*$,公钥 $p_O = g^{x_O}$,私钥 $s_O = x_O$ 。输出所有公钥,私钥由生成者自己保管。

3)数据存储上传。GCS 首先对无人机飞行状态数据和关键词进行加密,然后对关键词进行签名以生成相应的索引数据,具体步骤如下。

步骤 1 $\text{Encrypt}(p_A, M, w) \rightarrow (C_1, C_2)$ 。输入用户 A 的公钥 p_A 、关键字 w 和无人机飞行状态的 $M \in \{0, 1\}^*$,选择随机数 $x \in \mathbb{Z}_q^*, s \in \mathbb{Z}_q^*, r \in \{0, 1\}^*$,计算 $y = H_2(M, r), U_1 = p_A^{x \cdot y}, U_2 = p_A^s, U_3 = H_3(g^s) \oplus M, U_4 = H_1(w) \cdot H_5(p_A^s), H_5(p_A^s), U_5 = s \cdot (y + H_4(U_1, U_2, U_3, U_4))$,输出密文 $C_1 = (U_1, U_2, U_3)$,关键词密文 $C_2 = (U_4, U_5)$,将 C_1 存储在边缘服务器。

步骤 2 签名 $\text{Sign}(s_B, w) \rightarrow C_3$ 。输入 GCS 的私钥 s_B 和关键词 w ,GCS 计算 $V_1 = g^{s \cdot H_4(w)}, V_2 = g^{s \cdot H_4(w)^2}, \dots, V_n = g^{s \cdot H_4(w)^n}$,其中向量 $\mathbf{V} = [V_1, V_2, \dots$

$V_n]$ 。计算 $s_0 = H_6(w, U_1), I = g^{s \cdot H_4(w) + s_0(s_B + H_4(w))}, J = \varphi^{s_0(s_B + H_4(w))}$,令 $C_3(I, J, \mathbf{V})$,GCS 将 C_1 的哈希值和 C_2, C_3 构成的关键字索引输出至私有链上。

4)匿名身份生成和区块构建。当身份为 Q 的无人机用户接入 GCS 时,GCS 随机选择 $e \in \mathbb{Z}_q^*$,计算出无人机的匿名身份 $I_Q = Q \oplus H_4(\alpha)^e$ 。为确保私有链上相同的数据记录,GCS 计算 $\alpha' = H_3(g^e) \oplus \alpha, \theta = g^{(e + s_B)/H_4(\alpha)}$ 。之后,GCS 将关键词索引、其身份和签名发布新的交易向私有链。当私有链的验证者接收到这一新交易时,首先查找 (θ, α') ,在边缘服务器上搜索 τ ,计算 $\alpha^* = H_3(\theta^e \cdot p_B^{-1}) \oplus \alpha'$,并核对等式 $\tau = H_4(\alpha^*)$ 。如果成功,表明交易有效。验证者广播一条成功的消息。当收到 $2/(3W)$ 的验证成功消息后,私有链就会生成新区块,其中 W 表示联盟链节点的数量。反之新区块将不会被加入到私有链中。正确性验证为

$$\begin{aligned} H_4(\alpha^*) &= H_4(H_3(\theta^e \cdot p_B^{-1}) \oplus \alpha') = \\ H_4(H_3(g^{H_4(\alpha) \cdot (e + s_B/H_4(\alpha))} \cdot g^{-s_B}) \oplus H_3(g^e) \oplus \alpha) &= \\ H_4(H_3(g^{e + s_B} \cdot g^{-s_B}) \oplus H_3(g^e) \oplus \alpha) &= \\ H_4(H_3(g^e) \oplus H_3(g^e) \oplus \alpha) &= H_4(\alpha) = \tau \end{aligned} \quad (1)$$

边缘服务器会从每个新区块中提取 I_Q 和 (C_2, C_3) ,并设定 $F = (I_Q, (C_2, C_3))$ 。服务器使用 F 、服务器的身份和签名创建新的交易,并将其传播到联盟链上。当联盟链的验证者接收到新交易时,为了保证交易的有效性,同时防止半可信的服务器传送假消息,首先验证两个等式 $e(\prod_{i=1}^n V_i^{t_i}, V_2) = e(V_1, V_1)$ 和 $e(I, g) = e(V_1, g)J$ 是否正确,其中 t_i 是 $g(x) = t_n x^n + \dots + t_1 x$ 的系数。如果验证通过,则说明 F 正确,此时交易无误,验证者会广播一个验证确认信息。如果接收到超过 $2/(3W)$ 的确认消息,联盟链将接纳新交易,并形成一个新的区块。如果不成,则新的区块将不会被加入到联盟链中。正确性验证分别为

$$\begin{aligned} e(\prod_{i=1}^n V_i^{t_i}, V_2) &= e(\prod_{i=1}^n g^{s_i H_4(w)^i}, g^{s H_4(w)^2}) = \\ e(\prod_{i=1}^n g^{s(t_n H_4(w)^n + \dots + t_1 H_4(w))}, g^{s H_4(w)^2}) &= \\ e(g^{s(t_n)}, g^{s H_4(w)^2}) &= e(g^s, g^{s H_4(w)^2}) = \\ e(g^{s H_4(w)}, g^{s H_4(w)}) &= e(V_1, V_1) \quad (2) \\ e(I, g) &= e(g^{s \cdot H_4(w) + s_0(s_B + H_4(w))}, g) = \\ e(g^{s \cdot H_4(w)}, g) e(g^{s_0(s_B + H_4(w))}, g) &= \\ e(V_1, g) e(g^{s_0(s_B + H_4(w))}, g) &= e(V_1, g)J \quad (3) \end{aligned}$$

5)设置重加密密钥。输入无人机用户 A 和第三方用户 D 的私钥 s_A 和 s_D ,生成重加密密钥的具体步骤如下。

步骤 1 无人机用户 A 选择随机数 $k \in \mathbb{Z}_q^*$, 计算 g^k 和 kx_A 通过安全信道发送到联盟链,同时将 k 通过安全信道发送给授权的第三方用户。

步骤 2 第三方用户接收 k 后,计算 g^k 和 kx_A , 并通过安全的信道传送给联盟链。

步骤 3 联盟链通过无人机用户和第三方用户分别发送的 g^k 进行对比,若相等,计算重加密密钥 $R=kx_D/kx_A$ 。

6)陷门生成 $\text{Trapdoor}(p_A, w) \rightarrow (T_1, T_2)$ 。输入无人机用户 A 的公钥 p_A 和关键词 w ,选择随机数 $\lambda \in \mathbb{Z}_q^*$, 计算 $T_1 = g^\lambda, T_2 = H_1(w)^{1/s_A} \cdot H_5(p_A^\lambda)$ 。输出到联盟链 $T_w = (T_1, T_2)$ 。

7)重加密 $\text{ReEncrypt}(C_1, C_2, R) \rightarrow (C'_1, C_2)$ 。输入重加密密钥 R 和 (C_1, C_2) 。联盟链验证等式 $p_B^{U_5} = U_1 U_2^{H_4(U_1, U_2, U_3, U_4)}$ 是否成立。不成立,输出 0。否则计算 $U'_2 = U_2^R = g^{s_A(kx_D/kx_A)} = g^{s_D}$, 输出新的密文 $(C'_1, C_2) = (U_1, U'_2, U_3, U_4, U_5)$ 。正确性验证为

$$\begin{aligned} p_A^{U_5} &= p^{s \cdot (y + H_4(U_1, U_2, U_3, U_4))} = \\ &= p^{s \cdot y} \cdot p^{s \cdot H_4(U_1, U_2, U_3, U_4)} = \\ &= U_1 \cdot U_2^{H_4(U_1, U_2, U_3, U_4)} \end{aligned} \quad (4)$$

8)测试 $\text{Test}(T_1, T_2) \rightarrow (0, 1)$ 。当无人机用户或数据使用者需要查看历史无人机飞行共享状态数据时,无人机用户会将搜索索引 $T_w = (T_1, T_2)$ 上传至联盟链,以进行关键字加密文本的测试。若测试成功,联盟链上节点将密文 (C_1, C_2) 或重加密密文 (C'_1, C_2) 发送给无人机用户或数据用户,用其私钥解密获得无人机用户的无人机飞行状态。输入联盟链上节点的私钥 s_0 、陷门 T_w 和密文 (C_1, C_2) , 计算 $R_1 = T_2 / H_4(T_1^o), R_2 = U_4 / H_4(T_1^o)$ 。验证等式 $e(R_1, U_2) = e(R_2, T_1)$ 是否成立。若等式成立则输出 1, 否则输出 0。正确性验证为

$$\begin{aligned} e(R_1, U_2) &= e\left(\frac{T_2}{H_4(T_1^o)}, g^{x_A \cdot s}\right) = \\ &= e\left(\frac{H_1(w)^{1/s_A} \cdot H_5(p_A^s)}{H_4(T_1^o)}, g^{x_A \cdot s}\right) = \\ &= e\left(\frac{H_1(w) \cdot H_5(p_A^s)}{H_4(T_1^o)}, g^s\right) = e(R_2, T_1) \end{aligned} \quad (5)$$

9)数据解密。输入无人机用户的私钥和密文 (C_1, C_2) , 执行以下步骤。

步骤 1 $\text{Decrypt}(s_A, C_1, C_2) \rightarrow M$ 。当无人机用户 A 需要访问无人机飞行状态 M 时,输入联盟链

上的节点发送的密文 (C_1, C_2) , 计算 $M = U_3 \oplus H_3(U_2^{1/x_A})$, 输出 M 。正确性验证为

$$\begin{aligned} U_3 \oplus H_3(U_2^{1/x_A}) &= H_3(g^s) \oplus M \oplus H_3(p_A^{s/x_A}) = \\ &= H_3(g^s) \oplus M \oplus H_3(g^s) = M \end{aligned} \quad (6)$$

步骤 2 $\text{Decrypt}(s_D, C'_1, C_2) \rightarrow M$ 。当第三方用户 D 共享数据时,输入用户 D 的私钥 s_D 和重加密密文 (C'_1, C_2) , 计算 $M = U_3 \oplus H_3(U_2'^{1/x_D})$, 输出 M 。正确性验证为

$$\begin{aligned} U_3 \oplus H_3(U_2'^{1/x_D}) &= H_3(g^s) \oplus M \oplus H_3(p_D^{s/x_D}) = \\ &= H_3(g^s) \oplus M \oplus H_3(g^s) = M \end{aligned} \quad (7)$$

4 安全性分析

下面将从密码学安全与隐私保护两个维度对所提方案进行严格安全性分析,基于 mCDH 困难假设与 Schnorr 签名的不可伪造性,证明方案满足选择密文攻击下的不可区分性;同时验证方案可实现无人机用户身份匿名性与数据记录不可关联性,确保在半可信环境与恶意攻击下,无人机飞行共享状态数据的机密性、完整性与用户隐私均能得到有效防护。

定理 1 所提方案在随机预言机模型下是 IND-PRE-CCA 安全的。

假设在群中满足 mCDH 假设,且存在 Schnorr 签名满足 EUF-CMA 的。如果存在一个敌手 $\mathcal{A}$, 最多向随机预言机 H_i 发出 q_{H_i} 次查询,若存在一个很小的数 ϵ , 其中 $i=1, 2, 3, 4, 5, 6$, 对于任何 $0 < v < \epsilon$, 能够以优势 v 破解所提方案的 $(t, q_u, q_c, q_{rk}, q_{re}, q_d, \epsilon)$ -IND-PRE-CCA 安全性,其中: q_u 表示询问密钥的次数; q_c 表示询问加密的次数; q_{rk} 表示询问重加密的次数; q_{re} 表示询问重加密的次数; q_d 表示询问解密的次数。那么,存在算法 $\mathcal{B}$ 可以在时间 t' 内解决群 G 中的 (t', ϵ') -mCDH 问题,其中 ϵ' 为敌手 $\mathcal{A}$ 解决 mCDH 的概率,或在时间 t' 内的优势为 v 破坏 Schnorr 签名的 EUF-CMA 安全性。 t' 和 ϵ' 应分别满足

$$\begin{aligned} t' &\leq \\ t + (q_{H_1} + q_{H_2} + q_{H_3} + q_{H_4} + q_u + q_c + q_{rk} + q_{re} + q_d) \mathcal{O}(1) + \\ &+ (q_u + q_c + 4q_{re} + 3q_d + (2q_d + q_{re})q_{H_1}) T_E \end{aligned} \quad (8)$$

$$\begin{aligned} \epsilon' &\geq \frac{1}{q_{H_2}} \left(2(\epsilon - v) - \right. \\ &\left. \frac{q_{H_1} + (q_{H_1} + q_{H_2})q_d}{2^{l_0 + l_1}} - \frac{q_{re} + 2q_d}{q} \right) \end{aligned} \quad (9)$$

式中: T_E 表示在群 G 中指数运算的运行时间;

l_0 表示消息长度; l_1 表示关键字的长度; $\mathcal{O}(1)$ 表示常数时间复杂度。

证明 假设 Schnorr 签名对于概率 $0 < v < \epsilon$ 是 (t', v) -EUF-CMA 安全的, 存在时间为 t 的敌手 $\mathcal{A}$ 可以以优势为 $(\epsilon - v)$ 破坏所提方案的 IND-PRE-CCA 安全性。随后构建一个算法 $\mathcal{B}$, 可解决群 G 中的 (t', ϵ') -mCDH 问题。

随机选取 $a, b \in \mathbb{Z}_q^*$, 假设算法 $\mathcal{B}$ 得到一个 mCDH 挑战元组 $(g, g^{1/a}, g^a, g^b) \in G^4$ 作为输入, 输出 g^{ab} , 并与敌手 $\mathcal{A}$ 进行 IND-PRE-CCA 游戏, 即 $\mathcal{B}$ 发送 $(q, G, g, H_1, H_2, H_3, H_4, l_0, l_1)$ 给 $\mathcal{A}$, 其中 $H_i (i = 1, 2, 3, 4)$ 是由 $\mathcal{B}$ 控制的随机预言机。

哈希预言 敌手 $\mathcal{A}$ 可以随时询问随机预言 $H_i (i = 1, 2, 3, 4)$ 。 $\mathcal{B}$ 维护初始为空的 4 个哈希表 $H_i^{\text{list}} (i = 1, 2, 3, 4)$, 并进行如下询问。

1) 询问 H_1 。在接收到 (m, w, p, r) 时, 如果该询问已经出现在元组 (m, w, p, r) 中的 H_1^{list} 上, 则返回预定义值 r 作为查询结果。否则, 选择随机数 $r \in \mathbb{Z}_q^*$, 将元组 (m, w, p, r) 添加到哈希表 H_1^{list} 并响应 $H_1(m, w, p, r) = r$ 。

2) 询问 H_2 。在接收到 $R \in G$ 时, 如果该询问已经出现在元组 (R, β) 中的 H_2^{list} 上, 则返回预定义值 β 作为查询结果。否则, 选择 $\beta \in \{0, 1\}^{l_0 + l_1}$, 将元组 (R, β) 添加到哈希表 H_2^{list} 并响应 $H_2(R) = \beta$ 。

3) 询问 H_3 。在接收到 (D, E, F) 时, 如果该询问已经出现在元组 (D, E, F, α) 中的 H_3^{list} 上, 则返回预定义值 α 作为查询结果。否则, 选择 $\alpha \in \mathbb{Z}_q^*$, 将元组 (D, E, F, α) 添加到哈希表 H_3^{list} 并响应 $H_3(D, E, F) = \alpha$ 。

4) 询问 H_4 。在接收到 (E', U) 时, 如果该询问已经出现在元组 (E', U, δ) 中的 H_4^{list} 上, 则返回预定义值 δ 作为查询结果。否则, 选择 $\delta \in \{0, 1\}^{l_0 + l_1}$, 将元组 (m, w, p, r) 添加到哈希表 H_4^{list} 并响应 $H_4(E', U) = \delta$ 。

阶段 1 敌手 $\mathcal{A}$ 在 IND-PRE-CCA 游戏中发出一系列询问。 $\mathcal{B}$ 维护初始为空的列表 K^{list} , 针对 $\mathcal{A}$ 的询问进行以下回答。

1) 密钥询问 $\langle i \rangle$ 。 $\mathcal{B}$ 选择随机数 $\eta_i \in \mathbb{Z}_q^*$, 定义 $p_i = (g^{1/a})^{\eta_i}, c_i = 0$ 。随后将元组 (p_i, η_i, c_i) 加入列表 K^{list} 并返回 p_i 给敌手 $\mathcal{A}$, c_i 表示私钥是否被损坏, 即 $c_i = 0$ 表示未损坏, $c_i = 1$ 表示已损坏。

2) 密钥询问 $\langle j \rangle$ 。选择随机数 $\eta_j \in \mathbb{Z}_q^*$, 定义 $p_j = g^{\eta_j}, c_j = 1$ 。随后将元组 (p_j, η_j, c_j) 加入列表

K^{list} 并返回 (p_i, η_j) 给敌手 $\mathcal{A}$ 。

3) 重加密密钥生成询问 $\langle p_i, p_j \rangle$ 。根据 IND-PRE-CCA 游戏, 需预先生成 p_i 和 p_j , 且两者都被破坏或两者都未被破坏。 $\mathcal{B}$ 首先恢复 K^{list} 中的元组 (p_i, η_i, c_i) 和 (p_j, η_j, c_j) , 然后返回重加密密钥 η_i/η_j 给 $\mathcal{A}$ 。

4) 重加密询问 (p_i, p_j, C_i) 。如果 $p_i^s \neq D \cdot E^{H_3(D, E, F)}$, 则输出 $\perp$ 。否则, $\mathcal{B}$ 根据如下步骤回应询问。

步骤 1 从 K^{list} 中恢复元组 (p_i, η_i, c_i) 和 (p_j, η_j, c_j) 。

步骤 2 若 $c_i = c_j$, 则计算 $E' = E^{\eta_j/\eta_i}, F' = F \oplus H_4(E', g^{\eta_j/\eta_i})$, 并将 (E', F') 作为第一级密文返回给 $\mathcal{A}$ 。

步骤 3 搜索是否存在元组 $(m, w, p_i, r) \in H_1^{\text{list}}$ 。若不存在, 则返回 $\perp$; 否则, 计算 $E' = p_j^r$ 。若 $c_i = 1 \wedge c_j = 0$, 定义 $F' = F \oplus H_4(E', g^{\eta_i a/\eta_j})$; 若 $c_i = 0 \wedge c_j = 1$, 定义 $F' = F \oplus H_4(E', g^{\eta_i/a\eta_j})$ 。最后, 将 (E', F') 作为第一级密文返回给 $\mathcal{A}$ 。

5) 解密询问 $\langle p, C \rangle$ 。 $\mathcal{B}$ 首先恢复 K^{list} 中的元组 (p, η, c) 。若 $c = 1$, $\mathcal{B}$ 运行 $\text{Decrypt}(C, \eta)$ 并将结果返回给 $\mathcal{A}$; 否则, $\mathcal{B}$ 按照以下情形进行。

情形 1 C 是第二级密文 $C = (D, E, F, s)$: 若 $p_i^s \neq D \cdot E^{H_3(D, E, F)}$, 则返回 $\perp$ 给 $\mathcal{A}$; 否则, 搜索列表 H_1^{list} 和 H_2^{list} 以查看是否存在 $(m, w, p, r) \in H_1^{\text{list}}$ 和 (R, β) , 使得 $p^r = E, \beta \oplus (m \parallel w) = F$ 且 $R = g^r$ 。若成立, 将 m 返回到 $\mathcal{A}$; 否则, 返回 $\perp$ 。

情形 2 C 是第一级密文 $C = (p'', E', F')$, $\mathcal{B}$ 执行以下步骤。

步骤 1 从 K^{list} 中恢复元组 (p, η, c) 和 (p'', η'', c'') 。

步骤 2 根据 3 种情况定义 U : 1) 若 $c = c''$, 定义 $U = g^{\eta/\eta''}$; 2) 若 $c = 0 \wedge c'' = 1$, 定义 $U = g^{\eta a/\eta''}$; 3) 若 $c = 1 \wedge c'' = 0$, 定义 $U = g^{\eta/\eta'' a}$ 。

步骤 3 搜索 H_1^{list} 和 H_2^{list} 以查看是否存在 $(m, w, p, r) \in H_1^{\text{list}}$ 和 (R, β) , 使得 $p^r = E', \beta \oplus (m \parallel w) \oplus H_4(E', U) = F'$ 和 $R = g^r$ 。若成立, 将 m 返回到 $\mathcal{A}$; 否则, 返回 $\perp$ 。

挑战 输出目标公钥 p_i 和两个等长消息 $m_0, m_1 \in \{0, 1\}^{l_0}$ 。从 K^{list} 中恢复元组 (p_i^*, η^*, c^*) , 根据 IND-PRE-CCA 游戏中的描述, K^{list} 应该包含此元组, 且 $c^* = 0$ (表示 $p_i^* = g^{\eta^*/a}$)。按以下步骤进行响应。

步骤 1 选取 $e^*, \lambda \in \mathbb{Z}_q^*$, 计算 $D^* = (g^b)^{-e^* \eta^*} \cdot (g^{1/a})^{\eta^* / \lambda^*}$ 和 $E^* = (g^b)^{\eta^*}$ 。

步骤 2 选取 $\sigma^* \in \{0, 1\}^{l_0 + l_1}$, 定义 $H_3(D^*, E^*, F^*) = e^*$ 。

步骤 3 选取 $u^* \in \{0, 1\}, w^* \in \{0, 1\}^{l_1}$, 定义 $H_2(g^{ab}) = (m_\mu \parallel w^*) \oplus F^*$ 和 $H_1(m_\mu, w^*, p_i^*) = ab$ 。

步骤 4 返回 $C^* = (D^*, E^*, F^*, \lambda^*)$ 作为被挑战的密文给敌手 $\mathcal{A}$ 。

令 $u^* = \lambda^* - abe^*, r^* = ab$, 挑战密文 C^* 分布与真实密文一致, 因为 H_2 充当随机预言机, 且有

$$D^* = (g^b)^{-e^* \eta^*} (g^{1/a})^{\eta^* \lambda^*} = (g^{\eta^* / a})^{\lambda^* - abe^*} = (p_i^*)^{\lambda^* - abe^*} = (p_i^*)^{u^*} \quad (10)$$

$$E^* = (g^b)^{\eta^*} = (g^{\eta^* / a})^{ab} = (p_i^*)^{ab} = (p_i^*)^{r^*} \quad (11)$$

$$F^* = H_2(g^{ab}) \oplus (m_\mu \parallel w^*) = H_2(g^{r^*}) \oplus (m_\mu \parallel w^*) \quad (12)$$

$$\lambda^* = (\lambda^* - abe^*) + abe^* = u^* + ab \cdot H_3(D^*, E^*, F^*) \quad (13)$$

阶段 2 $\mathcal{A}$ 继续阶段 1 中 IND-PRE-CCA 游戏的询问。

猜测 $\mathcal{A}$ 向 $\mathcal{B}$ 返回猜测 $\mu \in \{0, 1\}$ 。 $\mathcal{B}$ 从 H_2^{list} 中随机挑选元组 (R, β) , 并输出 R 作为给定 mCDH 实例的解。

分析 在随机预言机模型下, 所提方案通过模拟哈希预言机 H_3 和 H_4 , 验证了其 IND-PRE-CCA。如果攻击者 $\mathcal{A}$ 不向 H_1 提交关于 (m_μ, w^*, p_i^*) 的询问, 不向 H_2 提交关于 g^{ab} 的询问, 则可以保证 H_1 和 H_2 的模拟是完美的。事件 k_1^* 表示 (m_μ, w^*) 已向 H_1 提交询问, 而 k_2^* 表示元素 g^{ab} 已提交给 H_2 询问。根据模拟过程, 当 $\mathcal{A}$ 对的重加密密钥查询响应时, 也具备安全性。只有在 $\mathcal{A}$ 能够提交有效的第二级密文且不经 H_1 的情况下, 重加密密钥查询 R 的响应可能会停止。然而, 假设 H_1 作为一个随机预言机, 当攻击者在重加密询问中发起查询时, 有 $\Pr[R] \leq q_{re}/q$ 。因此, 所提方案具备关键词隐私和密文隐私安全性。

安全证明中, 该模拟整体有效, 特定条件下的密文拒绝错误不影响整体安全性, 具体如下。

假设存在有效密文 (p, C) , $C = (D, E, F, \lambda)$ 或 $C = (E, F)$ 被识别为有效, 但也可在未向 H_2 询问 g^r (其中 $r = H_1(m, w, p)$) 的前提下生成 C 。设事件 $\mathcal{K}$ 表示 C 有效性, 事件 k_1^* 表示 (m, w, p) 已向 H_1 发起过询问, 事件 k_2^* 表示 g^r 已向 H_2 发起过询问。对

于 $(E, F) = (p^r, H_2(g^r)) \oplus (m \parallel w)$, 有 $\Pr[V \mid \neg k_2] \leq$

$\frac{q_{H_1}}{2^{l_0 + l_1}} + \frac{1}{q}$, 故

$$\begin{aligned} \Pr[V \mid (\neg k_1^* \vee \neg k_2^*)] &\leq \\ \Pr[V \mid \neg k_1^*] + \Pr[V \mid \neg k_2^*] &\leq \\ \frac{q_{H_1} + q_{H_2}}{2^{l_0 + l_1}} + \frac{2}{q} &\quad (14) \end{aligned}$$

假设 D 表示在整个模拟期间预言机 $V \mid (\neg k_1^* \vee \neg k_2^*)$ 产生解密动作。由于 q_d 次解密预言被发布, 故有

$$\Pr[D] \leq \frac{(q_{H_1} + q_{H_2})q_d}{2^{l_0 + l_1}} + \frac{2q_d}{q} \quad (15)$$

若事件 G 表示为 $k_2^* \vee (k_1^* \mid \neg k_2^*) \vee R \vee D$ 没有发生, 考虑到 H_2 输出的随机性, $\mathcal{A}$ 不能在猜测 μ 中获得任何优势。即攻击者猜测正确的概率为 $\Pr[\mu = \mu' \mid G] = 1/2$, 猜测 $\mu' \in \{0, 1\}$ 。因此, 故有

$$\begin{aligned} \Pr[\mu = \mu'] &\geq \Pr[\mu = \mu' \mid G] \Pr[\neg G] = \\ \frac{1}{2}(1 - \Pr[G]) &= \frac{1}{2} - \frac{1}{2} \Pr[G] \quad (16) \end{aligned}$$

从而

$$\left| \Pr[\mu = \mu'] - \frac{1}{2} \right| \leq \frac{1}{2} \Pr[G] \quad (17)$$

定义 IND-PRE-CCA 敌手的优势为 $(\epsilon - v)$, 可知

$$\begin{aligned} (\epsilon - v) &= \left| \Pr[\mu = \mu'] - \frac{1}{2} \right| \leq \frac{1}{2} \Pr[k_2^*] + \\ \Pr[k_1^* \mid \neg k_2^*] + \Pr[R] + \Pr[D] &\quad (18) \end{aligned}$$

由于

$$\begin{aligned} \Pr[D] &\leq \frac{(q_{H_1} + q_{H_2})q_d}{2^{l_0 + l_1}} + \frac{2q_d}{q} \quad (19) \\ \Pr[k_2^*] &\geq 2(\epsilon - v) - \Pr[k_1^* \mid \neg k_2^*] - \Pr[R] - \Pr[D] \geq \\ 2(\epsilon - v) - \frac{q_{H_1}}{2^{l_0 + l_1}} - \frac{(q_{H_1} + q_{H_2})q_d}{2^{l_0 + l_1}} - \frac{2q_d}{q} - \frac{q_{re}}{q} &\geq \\ 2(\epsilon - v) - \frac{q_{H_1} + (q_{H_1} + q_{H_2})q_d}{2^{l_0 + l_1}} - \frac{2q_d + q_{re}}{q} &\quad (20) \end{aligned}$$

根据 $\Pr[k_1^* \mid \neg k_2^*] \leq \frac{q_{H_1}}{2^{l_0 + l_1}}, \Pr[R] \leq \frac{q_{re}}{q}$, 且事件 k_2^* 发生, 则 $\mathcal{B}$ 将能够求解 mCDH, 运行时间为 $t' \leq t + (q_{H_1} + q_{H_2} + q_{H_3} + q_{H_4} + q_u + q_c + q_{rk} + q_{re} + q_d) \mathcal{O}(1) + (q_u + q_c + 4q_{re} + 3q_d + (2q_d + q_{re}) + q_{H_1}) T_E$ (21)

则敌手 $\mathcal{A}$ 解决 mCDH 的概率为

$$\begin{aligned} \epsilon' &\geq \frac{1}{q_{H_2}} \left(2(\epsilon - v) - \right. \\ \left. \frac{q_{H_1} + (q_{H_1} + q_{H_2})q_d}{2^{l_0 + l_1}} - \frac{2q_d + q_{re}}{q} \right) &\quad (22) \end{aligned}$$

定理 2 所提方案实现了匿名性和不可关联性。

证明 无人机用户的匿名身份 $I_Q = Q \oplus H_1(\alpha)^e$ 。敌手无法得到 α 和随机数 e , 无法推导用户真实身份, 保障匿名性; 监听者无法关联加密记录归属, 实现数据不可关联性。

5 性能分析

5.1 功能性分析

将所提方案与文献[8]方案、文献[13]方案, 文献[15]方案和文献[22]方案进行功能性对比, 结果如表 1 所示。

表 1 不同方案功能性对比

方案	区块链	访问控制	隐私保护	安全搜索	数据共享
文献[8]	是	是	是	否	是
文献[13]	是	是	是	否	是
文献[15]	是	是	否	否	是
文献[22]	是	是	否	是	是
所提方案	是	是	是	是	是

由表 1 可以看出, 文献[8]方案、文献[13]方案和文献[15]方案未能实现数据搜索功能。文献[15]方案和文献[22]方案不能保证用户隐私保护。因此,

表 3 不同方案的计算开销对比

算法	文献[8]方案	文献[13]方案	文献[15]方案	文献[22]方案	所提方案
Encrypt	$2T_P + 8T_E + 7T_H$	$2T_P + 3T_E + 1T_M + 2T_H$	对称加密	$T_P + 7T_E + 4T_H + 3T_M$	$6T_E + 2T_M + 9T_H$
ReEncrypt	$T_P + 2T_E + T_M + T_H$	$1T_P + 1T_E + 1T_M$	$2T_P + 4T_E + 3T_M + T_H$	—	$4T_E + 4T_M$
Trapdoor	$T_P + 3T_E + T_M + T_H$	—	—	$T_P + 4T_E + T_M + 2T_H$	$3T_E + T_M + 2T_H$
Test	$T_P + T_H$	$2T_P$	—	$4T_P + T_E$	$2T_P + 2T_E + 2T_M + 2T_H$
Decrypt	$T_E + 2T_H$	$T_P + T_E + T_H + T_M$	$2T_P + 2T_E + 2T_M$	—	$2T_E + 2T_H$

由表 3 可以看出, 在 Encrypt 加密算法运算中, 所提方案的计算开销远低于文献[8]方案、文献[13]方案、文献[22]方案及文献[15]方案仅对无人机飞行状态加密, 并采用对称加密算法, 故效率较高于所提方案。在 ReEncrypt 重加密算法运算中, 所提方案计算开销与文献[8]方案、文献[13]方案及文献[15]方案相对比, 由于所提方案没有使用对运算, 因此开销较少。在 Trapdoor 陷门算法运算中, 所提方案均低于文献[8]方案和文献[22]方案。而 Test 测试算法运算中, 所提方案的计算开销高于文献[8]方案和文献[13]方案, 而低于文献[22]方案。在 Decrypt 解密算法运算中, 所提方案略高于文献[8]方案, 而低于文献[13]方案和文献[15]方案。因此, 所提方案整体在计算开销上有较明显的

所提方案在功能性上具有一定优势。

5.2 计算开销理论分析

使用 T_P 、 T_E 、 T_M 、 T_H 、 T_O 表示双线性配对运算、指数运算、乘法运算、哈希运算及异或运算, 基本操作的计算开销如表 2 所示。数值模拟实验在 I7-4700 CPU, 2.60 GHz 处理器、16 GiB 内存和 Window 10 操作系统的环境下运行。在 Linux 操作系统下利用 PBC(Paring-based Cryptography)库由 C 语言进行编写, 使用的椭圆曲线采用 PBC 库预定义的 Type-A 参数方程: $y^2 = x^3 + x$, 定义在 512 bit 的素数基域 F_p 上($p=512$)。实验结果 20 次运行结果取平均值。所提方案与文献[8]方案、文献[13]方案、文献[15]方案和文献[22]方案在 Encrypt 加密算法、ReEncrypt 重加密算法、Trapdoor 陷门算法、Test 测试算法和 Decrypt 解密算法上的计算开销对比如表 3 所示。

表 2 基本操作的计算开销

运算	定义	时间/ms
T_P	双线性对运算时间	5.217
T_E	指数运算执行时间	2.651
T_M	乘法运算执行时间	0.135
T_H	哈希运算执行时间	0.006

优势。

5.3 计算开销实验分析

所提方案与文献[8]方案、文献[13]方案和文献[22]方案在 Encrypt 加密算法的计算开销对比如图 2 所示。可以看出, 所提方案的计算开销为 16.0 ms, 均低于文献[22]方案的 24.5 ms、文献[8]方案的 31.5 ms 和文献[13]方案的 18.5 ms, 分别提升了约 34.7%、49.2% 和 13.5% 的效率。所提方案与文献[8]方案、文献[13]方案和文献[15]方案在 ReEncrypt 重加密算法的计算开销对比如图 3 所示。可以看出, 所提方案的计算开销为 5.0 ms, 均低于文献[15]方案的 12.0 ms、文献[8]方案的 23.0 ms 及文献[13]方案的 17.0 ms, 分别提升了约 58.3%、78.3% 和 70.6% 的效率。

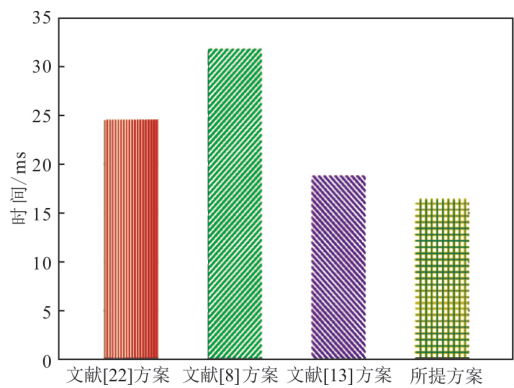


图 2 不同方案在 Encrypt 加密算法的计算开销对比

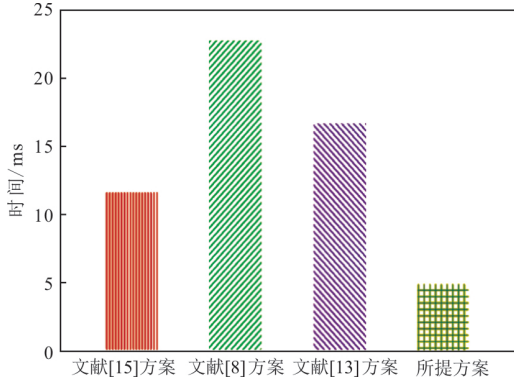


图 3 不同方案在 ReEncrypt 重加密算法的计算开销对比

所提方案与文献[8]方案、文献[13]方案和文献[22]方案在 Test 测试算法的计算开销对比如图 4 所示。可以看出,所提方案的计算时间为 10.0 ms,低于文献[22]的 23.0 ms、文献[8]的 20.0 ms 和文献[13]的 15.0 ms,分别提升了约 56.5%、50.0%、和 33.3%的效率。

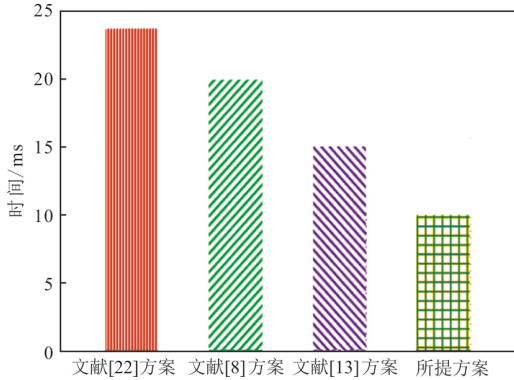


图 4 不同方案在 Test 测试算法的计算开销对比

所提方案与文献[8]方案、文献[13]方案和文献[15]方案在 Decrypt 解密算法的计算开销对比如图 5 所示。所提方案的计算开销为 6.0 ms,低于文献[15]的 16.0 ms 和文献[13]的 8.0 ms,但高于文献[8]的 3.0 ms。相较于文献[13]方案和文献[15]方案,所提方案分别提升了约 62.5% 和 25.0%的效率。

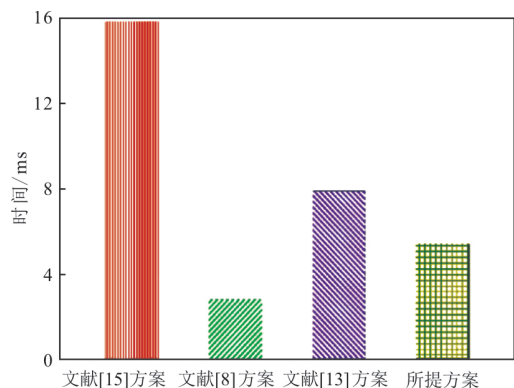


图 5 不同方案在 Decrypt 解密算法的计算开销对比

6 结语

区块链与可搜索加密的无人机飞行共享状态数据共享方案构建了联盟链与边缘私有链协同的双链架构,采用链上维护索引、链下存储密文的工作模式,由边缘私有链记录密文哈希与关键词索引,联盟链保存用户伪身份和跨域共享索引,以此平衡隐私保护与跨域数据共享的需求。方案融合代理重加密与可搜索加密技术,引入匿名索引构建机制,并设计轻量化重加密机制,能够在不解密原始密文的前提下完成灵活授权访问与关键词密文检索,实现用户身份匿名以及数据记录的不可关联,抵御攻击者通过关联分析还原用户敏感信息的攻击行为。安全性分析证明了所提方案满足选择密文攻击下的不可区分安全,能够有效保障无人机飞行共享状态数据的机密性、完整性以及用户隐私安全。实验结果表明,所提方案整体计算开销处于较低水平,适配边缘节点算力受限的应用特点,能够满足低空无人机通信场景下数据实时共享的安全性与时效性要求。

下一步工作将面向大规模无人机集群应用场景,进一步优化多关键词检索性能,提升方案的可扩展能力,研究实现更细粒度的访问权限管控,增强方案对于复杂低空业务场景的适配能力。

参 考 文 献

[1] Liu W Q, Zhang S, Ansari N. Joint laser charging and DBS placement for drone-assisted edge computing[J]. IEEE Transactions on Vehicular Technology, 2022, 71(1): 780-789.

[2] 赵旭东,姜晓东,张永波. 基于改进 YOLOv8 的无人机航拍图像目标检测[J]. 电子设计工程, 2026, 34(6): 176-182.

- Zhao Xudong, Jiang Xiaodong, Zhang Yongbo. UAV aerial image object detection based on improved YOLOv8[J]. *Electronic Design Engineering*, 2026, 34(6): 176-182.
- [3] 黄锐鸿, 黄烁, 黄毓琦, 等. 基于无人机云台角度自适应调整的无感智能督查技术[J]. *西安工程大学学报*, 2025, 39(6): 112-119.
- Huang Ruihong, Huang Shuo, Huang Yuqi, et al. Sensorless intelligent inspection technology based on adaptive adjustment of drone gimbal angle[J]. *Journal of Xi'an Polytechnic University*, 2025, 39(6): 112-119.
- [4] 陈浩, 张天予, 潘浩, 等. 无人机辅助边缘计算中基于多机协同的任务调度算法[J]. *西安邮电大学学报*, 2026, 31(4): 43-51.
- Chen Hao, Zhang Tianyu, Pan Hao, et al. Task scheduling algorithm based on multi-UAV collaboration in UAV-assisted edge computing[J]. *Journal of Xi'an University of Posts and Telecommunications*, 2026, 31(4): 43-51.
- [5] 毕昌兵, 田有亮, 李沓. 5G车联网中基于区块链的半分布式消息认证加密方案[J]. *软件学报*, 2026(2): 934-952.
- Bi Changbing, Tian Youliang, Li Ta. Blockchain-based semi-distributed message authentication and encryption scheme in 5G Internet of Vehicles[J]. *Journal of Software*, 2026(2): 934-952.
- [6] Jain A, Barke S, Garg M, et al. A walkthrough of blockchain-based Internet of drones architectures[J]. *IEEE Internet of Things Journal*, 2024, 11(21): 34924-34940.
- [7] 张瑶瑶, 周圆, 杨青林, 等. 区块链赋能数据存储安全服务研究进展[J]. *电子学报*, 2025, 53(10): 3794-3816.
- Zhang Yaoyao, Zhou Yuan, Yang Qinglin, et al. Research progress on blockchain-empowered data storage security service[J]. *Acta Electronica Sinica*, 2025, 53(10): 3794-3816.
- [8] Zhang A Q, Lin X D. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain[J]. *Journal of Medical Systems*, 2018, 42(8): 140-158.
- [9] 王少影, 赵建斌, 吴军英, 等. 基于同态加密与区块链的电力数据隐私保护方法研究[J]. *电子设计工程*, 2026, 34(7): 154-158.
- Wang Shaoying, Zhao Jianbin, Wu Junying, et al. Research on the privacy protection method for power data based on homomorphic encryption and blockchain[J]. *Electronic Design Engineering*, 2026, 34(7): 154-158.
- [10] 孟冬月, 黄玉钊, 韩国祥, 等. 基于前馈PID的应急救援四旋翼无人机安全控制研究[J]. *计算机科学*, 2025, 52(S2): 995-1003.
- Meng Dongyue, Huang Yuchuan, Han Guoxiang, et al. Research on emergency rescue quadcopter UAV safety control based on feedforward PID[J]. *Computer Science*, 2025, 52(S2): 995-1003.
- [11] Li Z C, Shi G Z. A CCA-secure puncturable attribute-based proxy re-encryption scheme[J]. *IEEE Internet of Things Journal*, 2025, 12(22): 47679-47690.
- [12] 张波, 李哲成, 徐兴帅. 云辅助工业物联网中基于区块链的用户友好型数据检索和共享方案[J]. *通信学报*, 2025, 46(S1): 56-68.
- Zhang Bo, Li Zhecheng, Xu Xingshuai. Blockchain-based user-friendly data retrieval and sharing scheme in cloud-assisted industrial Internet of Things[J]. *Journal on Communications*, 2025, 46(S1): 56-68.
- [13] Li W Z, Xie Z Y, Liu S L, et al. Controllable access control in permissioned blockchains via controllable threshold proxy re-encryption[J]. *IEEE Transactions on Information Forensics and Security*, 2025, 20: 9625-9640.
- [14] Remya S, Pillai M J, Ann Jacob P, et al. Security analysis and performance evaluation of certificateless proxy re-encryption for blockchain applications[J]. *IEEE Access*, 2025, 13: 162639-162667.
- [15] Liu J W, Jiang W Y, Sun R, et al. Conditional anonymous remote healthcare data sharing over blockchain[J]. *IEEE Journal of Biomedical and Health Informatics*, 2023, 27(5): 2231-2242.
- [16] George J, Chitra R. Securing health monitoring in IOT with blockchain-based proxy re-encryption[C]//2024 International Conference on Artificial Intelligence and Quantum Computation-based Sensor Application, Nagpur: IEEE, 2024: 1-6.
- [17] Wang S P, Zhang Y L, Zhang Y L. A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems[J]. *IEEE Access*, 2018, 6: 38437-38450.
- [18] Gao H M, Zhang Y H, Wang L B, et al. A searchable encryption scheme for blockchain-based digital twins[J]. *IEEE Internet of Things Journal*, 2025, 12(20): 42274-42289.
- [19] 李宇溪, 陈晶晶, 周福才, 等. 基于区块链索引的可验证布尔搜索加密方案[J]. *计算机研究与发展*, 2025, 62(11): 2855-2869.

Li Yuxi, Chen Jingjing, Zhou Fucui, et al. Verifiable Boolean searchable encryption scheme based on blockchain index[J]. Journal of Computer Research and Development, 2025, 62(11): 2855-2869.

[20] 杨锐, 张瑞婷, 翟社平. 电力数据多方共享的区块链可搜索加密方案[J]. 电力系统保护与控制, 2024, 52(22): 116-128.

Yang Rui, Zhang Ruiting, Zhai Sheping. Blockchain searchable encryption scheme for multi-user power data sharing[J]. Power System Protection and Control, 2024, 52(22): 116-128.

[21] Xu G X, Huang Y L, Ma C. Attribute-based searchable proxy re-encryption blockchain data sharing scheme[C]//2023 IEEE 12th International Conference on Cloud Networking. Hoboken: IEEE, 2023: 372-380.

[22] Banik M, Kumar S. Blockchain-based public key encryption with keyword search for medical data sharing in cloud environment[J]. Journal of Information Security and Applications, 2023, 78: 103626.

[23] Fugkeaw S, Deevijit J. SE-COLLAB: Achieving fine-grained and efficiently verifiable searchable encryption with Boolean multi-keyword search for collaborative IIoT data sharing[J]. IEEE Access, 2025, 13: 126012-126029.

[24] 牛淑芬, 刘文科, 陈俐霞, 等. 基于联盟链的可搜索加密电子病历数据共享方案[J]. 通信学报, 2020, 41(8): 204-214.

Niu Shufen, Liu Wenke, Chen Lixia, et al. Electronic medical record data sharing scheme based on searchable encryption via consortium blockchain[J]. Journal on Communications, 2020, 41(8): 204-214.

[25] Xie M Y, Chang Z, Li H W, et al. BASUV: A blockchain-enabled UAV authentication scheme for Internet of vehicles[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 9055-9069.

[26] Javed I T, Alharbi F, Margaria T, et al. PETchain: A blockchain-based privacy enhancing technology[J]. IEEE Access, 2021, 9: 41129-41143.

[27] Alamer A. A security and privacy-preserving consortium blockchain-based accessing control in mobile crowdsensing [J]. IEEE Access, 2025, 13: 53815-53834.

[28] Li T, Wang H Q, He D B, et al. Blockchain-based privacy-preserving and rewarding private data sharing for IoT[J]. IEEE Internet of Things Journal, 2022, 9(16): 15138-15149.

[29] Qiao Y, Xue Y, Zhai Y K, et al. A secure and efficient sharing scheme for medical IoT data based on consortium blockchain[J]. IEEE Internet of Things Journal, 2025, 12(23): 51422-51437.

[30] Schnorr C P. Efficient signature generation by smart cards [J]. Journal of Cryptology, 1991, 4(3): 161-174.

[作者简介]



李亚红(1984—),女,甘肃定西人,博士,兰州交通大学教授,主要研究方向为信息安全、密码学及无线网络安全。
E-mail: 359107023@qq.com



魏莹(2007—),女,甘肃天水人,兰州交通大学本科生,主要研究方向为可搜索加密、代理重加密、区块链数据共享。
E-mail: 3623372087@qq.com



黄海燕(1988—),女,甘肃高台人,博士,兰州交通大学教授、博士生导师,主要研究方向为无线通信可靠性与安全性、云网边端协同及无人机通信。
E-mail: 1633708306@qq.com

[责任编辑:祝 剑]