

基于区块链的个人健康护照存储、共享与验证方案

高汉成^{1,2}, 吉浩宇^{1,2}, 高晨昊^{1,2}, 黄海平^{1,2}

(1.南京邮电大学计算机学院,江苏 南京 210023; 2.江苏省无线传感网高技术研究重点实验室,江苏 南京 210023)

摘要: 随着人们对出境需求的增加,个人健康护照成为确认旅行者健康状况、满足入境要求的重要工具。针对个人健康护照全球共享所面临“信息孤岛”、隐私保护和易伪造等难题,提出了一种基于区块链的个人健康护照存储、共享与验证方案。方案在采用链上链下协同存储的同时,通过结合可搜索加密和区块链技术,优化了区块链上的存储方式,减少区块链的存储压力,同时实现用户个人数据的可靠存储及安全共享。方案对弱共识机制进行了优化,优化后的算法达成共识只需要2个阶段,从而减小了节点间达成共识的通信复杂度,提高了整个区块链系统的吞吐量。为适应多用户场景,方案引入并改进了聚合签名技术,减轻了签名验证的计算负担,使方案能够快速追溯恶意伪造者。方案给出了全面的安全性分析,证明方案是安全可靠的。最后,仿真实验结果表明,相较于现有方案,在多用户场景下方案的计算开销最高优化了49.89%,通信开销最高优化了25.81%,所提出的共识机制在不同节点数量下效率也有较大的优势。

关键词: 区块链; 共识算法; 聚合签名; 可搜索加密

中图分类号: TN918

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024015

Individual health passport storage, sharing and verification scheme based on blockchain

GAO Hancheng^{1,2}, JI Haoyu^{1,2}, GAO Chenhao^{1,2}, HUANG Haiping^{1,2}

1.School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210003, China

2.Jiangsu High Technology Research Key Laboratory for Wireless Sensor Networks, Nanjing 210023, China

Abstract: As the demand for international travel escalates, the individual health passport has emerged as an essential instrument for verifying the health status of travelers and fulfilling entry criteria. To tackle the challenges associated with the global sharing of individual health passports, including information fragmentation, privacy concerns, and the risk of counterfeiting, a blockchain-based scheme for the secure storage, sharing, and verification of individual health

收稿日期: 2023-12-15; 修回日期: 2024-02-29

通信作者: 黄海平, hhp@njupt.edu.cn

基金项目: 国家自然科学基金(No.62072252); 江苏省科研与实践创新计划(No.KYCX22_1016)

Foundation Items: The National Natural Science Foundation of China (No.62072252), The Postgraduate Research and Practice Innovation Program of Jiangsu Province (No.KYCX22_1016)

引用格式: 高汉成, 吉浩宇, 高晨昊, 等. 基于区块链的个人健康护照存储、共享与验证方案[J]. 网络与信息安全学报, 2024, 10(02): 95-105.

Citation Format: GAO H C, JI H Y, GAO C H, et al. Individual health passport storage, sharing and verification scheme based on blockchain[J]. Chinese Journal of Network and Information Security, 2024, 10(02): 95-105.

passports was developed. This scheme employed a hybrid on-chain and off-chain storage methodology and incorporated searchable encryption with blockchain technology. This integration aimed to streamline blockchain storage, alleviating the storage load while guaranteeing the dependable archiving and secure dissemination of user-sensitive data. The scheme also refined the weak consensus mechanism, with an improved algorithm that achieved consensus in merely two stages. This innovation significantly diminished the communication complexity among nodes and amplified the throughput capacity of the blockchain system. To cater to multi-user environments, the scheme introduced and enhanced aggregate signature technology. This enhancement minimized the computational load associated with signature verification and facilitated the swift identification of potential malicious forgers. An exhaustive security analysis was conducted to substantiate the scheme's security and dependability. Subsequent simulation outcomes indicate that, in comparison to existing solutions, the proposed scheme realizes substantial optimizations of up to 49.89% in computational overhead and 25.81% in communication overhead within multi-user contexts. Moreover, the proposed consensus mechanism demonstrates significant efficiency benefits across varying node counts.

Keywords: blockchain, consensus algorithm, aggregate signature, searchable encryption

0 引言

随着社会的不断发展,人们对于出境旅行、学术访问和国际交流需求不断增加。然而,不同国家和地区对疾病的预防措施与要求存在巨大差异,导致出入境健康标准的差异性。在这种情况下,许多国家和地区纷纷制定了严格的健康政策,以确保公共健康和安全。在此背景下,个人健康护照成为一种有力工具,可用于确认旅行者的健康状态,满足不同国家和地区的健康入境要求。个人健康护照可以容纳个人的健康信息和疫苗接种记录,以便对公共健康进行有效管理和监测^[1-2]。

传统的纸质健康护照可以追溯到15世纪欧洲鼠疫大流行期间发行的“健康通行证”,旨在免除旅行者隔离措施。然而,传统的纸质健康护照存在容易伪造和篡改的隐患,导致了不安全性和可信度的问题。特别是在数字化时代,信息的流动性和易受攻击性进一步加剧了这些问题。在此背景下,一些国家和国际组织相继推出电子健康护照或免疫护照,允许在不损害个人或公共健康的情况下出国工作和旅行。随着电子健康护照的引入,个人信息的隐私泄露问题也日益凸显,传统的中心存储架构往往将用户数据存储在第三方平台,一旦第三方被恶意攻击者攻破或者与其合谋,用户的隐私安全将难以得到保障。因此,个人敏感数据的保护和隐私风险管理成为亟待解决的问题。同时,各个医疗机构乃至各国之间的医疗数据并不互通,导致了“信息孤岛”的形成,令健康护照在全球范围内的共享受到了极大限制。

区块链技术因其所固有的难以篡改、透明和去中心化等优势特性被广大学者引入于智慧医疗领域,为健康护照的管理和验证带来了全新的可能性^[3-4]。然而,传统区块链吞吐量和效率低与实际中健康护照应用场景所需要的高效性存在的矛盾并未得到解决。其次,可搜索加密技术虽然可以使用户将数据加密后上传至云服务器并可以进行密文的检索,但用户所使用的往往是资源受限的移动设备,无法满足现有方案所带来的大量密码学计算负担。

综上,亟须一种安全、高效的、用于跨国之间的个人健康护照共享方案。为了应对以上挑战,本文提出了一种基于区块链的个人健康护照存储、共享与验证方案,本文主要贡献如下。

(1) 方案创新地采用链上链下协同存储的方式,通过结合可搜索加密技术和区块链技术,在区块链上存储索引,在星际文件系统(inter planetary file system, IPFS)中存储密文;优化了区块链上的存储方式,减少了区块链的存储压力,同时实现了用户个人数据的可靠存储及安全共享。

(2) 针对多用户场景,方案采用聚合签名技术,大幅减少了签名验证的计算负担。此外,本文对聚合签名做了进一步改进,使方案能够快速追溯到恶意伪造者,增强方案的安全性。

(3) 为提升区块链系统的吞吐量和整体效率,本文对弱共识机制进行了优化。优化后的算法达成共识只需要2个阶段,从而大大减小了节点间达成共识的通信复杂度,提高了整个区块链系统的吞吐量。

(4) 本文给出了全面的安全性分析, 证明所提方案是安全可靠的, 同时, 给出了计算开销、通信开销和共识算法的对比实验。实验结果表明, 本文方案相较于其他方案, 在效率和可靠性上有较大优势。

1 相关工作

区块链技术作为一种分散式数据库已在医疗健康、金融服务和供应链管理等领域广泛应用^[5-6]。针对个人健康护照的共享与验证问题, 学者提出了许多基于区块链的解决方案。Xin^[7]基于区块链技术实现了个人健康数据管理应用程序 GreenPass, 虽然提及了应用的健康状况调查功能, 但却未深入介绍其系统模型和详细方案细节。Bansal 等^[8]提出由政府管理的区块链来存储新冠疫苗接种凭证, 强调了生物特征认证的使用, 以增强用户的匿名性和隐私保护。Angelopoulos 等^[9]提出基于私有链的数字健康护照, 该护照包含抗体测试结果以及时间戳, 但私有链并不适用于国际出入境的场景。Haque 等^[10]的方案 VacciFi 考虑了通用数据保护标准 (general data protection regulation, GDPR), 该体系结构是可扩展的。同时, 该方案致力于使用许可区块链保障个人健康信息的可用性、可追溯性和完整性, 但该方案未能很好地应对内部攻击问题。Lee 等^[11]提供一个全球性的架构, 该架构利用区块链来完成不同疫苗接种凭证的验证和分发, 具有低成本、高安全性和可验证性等优势。Chaudhari 等^[12]提出一个在线护照系统来报告公民的健康状况。该方案利用用户的生物特征信息 (如虹膜扫描) 来实现对每个用户的唯一识别, 同时区块链存储用户的历史病历等健康信息。Chen 等^[13]设计一个基于可追踪区块链的疫苗接种记录存储和共享系统, 接种记录被保存在区块链上, 保证了数据的可追溯性, 同时, 通过相互认证, 数据的完整性和不可否认性也得到了保证。

共识算法作为区块链系统的重要组成部分, 影响区块链系统的整体运行效率。目前主流的共识算法有工作证明^[14-15]、抵押证明^[16]、资产证明^[17]、拜占庭容错 (Byzantine fault tolerance, BFT) 协议^[18-19]等。而联盟链中的共识算法大多使

用了实用拜占庭容错 (practical BFT, PBFT)^[20]共识, 但 PBFT 作为一种强一致性的共识机制, 网络等外部因素必定会影响一条消息在整个系统中完成共识的时间, 而对等 (peer-to-peer, P2P) 网络中各节点等待所有节点达成共识的时间也因此延长。显然, 世界范围的健康护照信息上链必定对区块链的吞吐量有极高要求, 这是传统的 PBFT 共识机制难以满足的。因此, 选择适合当前方案的共识机制十分重要。Wang 等^[21]通过弱化共识过程中对强一致性的要求, 提出了一种弱一致性 BFT 共识方法, 该方法基于异步 BFT 算法, 只保证每个节点收到并共识的消息的相对位置, 而不要求每个节点的消息顺序完全一致, 从而达到整个系统的一致性, 这样也大大提高了整个区块链的吞吐量。本文方案对弱一致性 BFT 共识方法进行了改进, 进一步提高了效率。

综上所述, 尽管学者针对健康护照的共享和验证问题提出了解决方案, 然而现有方案将大量数据存储在区块链的做法却使区块链节点负担加重, 从而降低整体方案的效率。尤其在多用户场景下, 频繁的验证操作更会进一步增加方案的时间成本^[22]。同时, 对于健康护照这种需要频繁更新和验证信息的使用场景, 现有方案未能充分考虑传统区块链的吞吐量低, 无法处理短时间内大量的用户请求, 从而影响了健康信息的实时性和准确性。因此, 迫切需要寻求一种更加高效和可持续的方法, 以在确保安全性的前提下提升方案的效率, 并且应该能够同时兼顾机密性、完整性和多用户场景等多个维度。为了更直观地表现本文方案与传统方案的不同, 将本文方案与一些具有代表性的方案^[7, 9-10, 13, 22]从多个维度进行了对比。

2 预备知识

2.1 双线性映射

设 G_1 和 G_2 是 2 个具有素数阶的乘法循环群, g 为 G_1 的生成元, G_2 是一个双线性映射 $e: G_1 \times G_1 \rightarrow G_2$, 该双线性映射具有以下 3 个属性^[23]。

(1) 双线性: 对于所有 $u, v \in G_1$ 和 $a, b \in \mathbb{Z}_p$, 有 $e(u^a, v^b) = e(u, v)^{ab}$ 。

(2) 非退化性: $e(u, v) \neq 1$ 。

(3) 可计算性: 对于所有 $u, v \in G_1$, 可以

有效计算 $e(u, v)$ 。

如果 G_1 中双线性映射和群运算是可有效计算的, 则可以说 G_2 是一个双线性群。值得注意的是, 映射 e 是对称的, 即 $e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)$ 。

2.2 计算 Diffie-Hellman 问题

在给定 $P, xp, yp \in G$, 且 $x, y \in Z_q^*$ 前提下, 并不存在一个可行的算法能够通过 P, x, y 计算得到 xyp , 即无法找到一个算法在可实现的时间复杂度内完成该计算任务^[24]。

2.3 判定 Diffie-Hellman 问题

在给定 $P, xp, yp, Z \in G$, 且 $x, y \in Z_q^*$ 前提下, 并不存在一个可行的算法能够通过 P, xp, yp 和 Z 从而判断等式 $Z = xyP \pmod{p}$ 是否成立, 即无法找到一个算法在可实现的时间复杂度内完成该计算任务^[25]。

3 系统模型

本节首先重点介绍系统模型和实体功能, 然后给出本文建立的威胁模型及模型的安全目标。

3.1 系统模型和实体功能

本文方案模型如图1所示。假设每个国家的各医疗机构作为联盟链节点, 合作维护一条联盟链。方案包含用户、医疗机构、IPFS、联盟链、海关、密钥生成中心 (key generation center, KGC) 6 个实体。主要的交互流程为: 首先, 由 KGC 完成

系统的初始化, 并分发各实体的公私钥对; 然后, 由医疗机构为用户生成健康护照; 最后, 将健康护照密文上传至 IPFS, 同时将关键字索引和签名作为交易上传至联盟链。在用户需要再次就诊或出国时, 用户生成查询陷门, 并向联盟链发起请求。联盟链返回文档存储标识给 IPFS 或向海关提供验证结果, 从而完成护照的更新与验证操作。

(1) 用户: 用户注册个人健康护照, 用以前往医疗机构就诊或出国海关检查。同时, 多个用户可组成旅行团或学术交流团, 在检查时完成多用户验证。

(2) 医疗机构: 为用户提供就诊服务后生成或更新个人健康护照, 并将数据加密后存储于 IPFS。最后, 针对护照生成关键字索引, 并将其作为交易上传联盟链。

(3) IPFS: IPFS 是一个分散的文件存储网络, 用于存储医疗机构生成的个人健康护照密文数据。

(4) 联盟链: 每个国家选取医疗机构代表构成联盟链节点, 共同完成交易的发布与共识工作。此外, 联盟链负责根据用户生成的陷门查询密文存储索引或向海关返回护照验证结果。

(5) 海关: 海关工作人员需要获得联盟链关于用户护照的验证结果。

(6) KGC: 负责生成系统参数并为所有实体部分私钥。

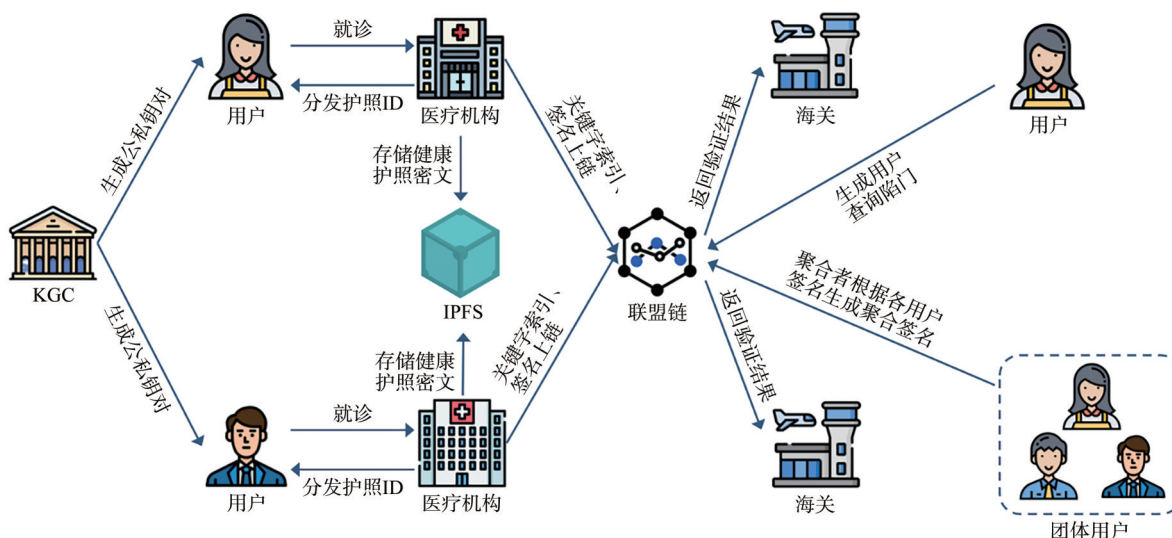


图1 方案模型
Figure 1 System model

3.2 威胁模型

本文建立的威胁模型如下。

(1) 在联盟链接收到搜索请求后，联盟链节点可能会为了节省计算资源而向用户返回无效的检索结果。

(2) IPFS存储网络是诚实但好奇的，可以诚实地执行用户的指令，但会根据用户提供的关键词索引等信息进行猜测行为。

3.3 安全目标

假设所有区块链节点和海关检查人员皆为半诚实方，攻击者可能在用户与其他实体间窃听通信。基于这种假设，本文提出了以下安全目标。

(1) 机密性：健康护照数据中包含用户的个人隐私信息，共享过程中可能存在泄露风险。因此，确保健康护照数据的机密性成为本文方案的目标之一。

(2) 可追溯性和不可否认性：为解决医患间的争议以及就诊后可能出现的责任问题，方案应能有效防范恶意攻击者对健康护照数据记录的篡改。因此，要求该方案在具有可追溯性（追溯后不可否认）的同时，也具备难以篡改的特性。

(3) 不可伪造性：在海关进行防疫检查时，恶意攻击者可能会伪造合法用户的健康护照以欺骗检查人员。因此，要求该方案能够防止攻击者对健康护照进行伪造。

4 方案设计

为解决当下健康护照在共享、验证过程中面临的隐私泄露问题，以及区块链吞吐量低、无法与智慧医疗实时性相匹配的难题，本节给出具体的方案设计。方案考虑用户在出行时以团体为主的多用户场景，将方案分为了单用户与多用户两个场景。方案主要包含系统初始化、健康护照加密与存储、健康护照的更新、健康护照的验证共4个阶段，符号说明如表1所示。

4.1 系统初始化

在此阶段，由密钥生成中心生成系统参数和各实体的公私钥对。

(1) 系统建立：输入安全参数 λ ，KGC选择阶数为 p 的两个乘法循环群 G_1 和 G_2 ，定义双线性映射 $e: G_1 \times G_1 \rightarrow G_2$ ，其中， G_1 的生成元为

g 。随机选择 $s \in Z_p^*$ ，设置主密钥 $SK = s$ ，计算 $P_{pub} = g^s$ 。选取6个防碰撞的哈希函数 $H_0: \{0, 1\}^* \times G_1 \rightarrow Z_p^*$ ， $H_1: \{0, 1\}^* \times G_1^2 \rightarrow Z_p^*$ ， $H_2: \{0, 1\}^* \rightarrow Z_p^*$ ， $H_3: \{0, 1\}^* \rightarrow G_1$ ， $H_4: G_2 \rightarrow \{0, 1\}^*$ ， $H_5: G_2^2 \times \{0, 1\}^* \rightarrow \{0, 1\}^*$ ，发布公共参数CP如下。

$$CP = \{p, g, e, SK, P_{pub}, H_0, H_1, H_2, H_3, H_4, H_5\} \quad (1)$$

表1 符号说明

Table 1 Notation description

参数	含义	参数	含义
SK	主密钥	$index_f$	密文检索标识
CP	公共参数	T_c	交易
(pk_i, sk_i)	用户公私钥对	SToken	搜索陷门
$passport_i$	个人健康护照	δ	聚合签名
C_{p_i}	健康护照密文	index	区块序列号
δ_i	用户签名	OID	区块节点编号
PUID _i	健康护照编号	M	打包的交易
I_K	关键字索引	D	消息摘要

(2) 生成部分密钥：根据主密钥SK和用户身份 $ID \in \{0, 1\}^*$ ，KGC随机选择 $r_i \in Z_p^*$ ，计算 $R_i = g^{r_i}$ ， $k_i = H_0(ID_i || R_i)$ ， $d_i = g^{r_i + k_i s}$ 。KGC通过安全信道将部分私钥 $D_i = (R_i, d_i)$ 给用户 i 。

(3) 生成完整公私钥对：用户 i 随机选择 $x_i \in Z_p^*$ ，计算 $X_i = g^{x_i}$ 。生成完整的公钥 $pk_i = (R_i, X_i)$ 和私钥 $sk_i = (x_i, d_i)$ 。

(4) 系统中其他实体按照上述步骤生成自己的公私钥对，医院 h 与联盟链节点C的公私钥对分别表示为 $\{pk_h = (R_h, X_h), sk_h = (x_h, d_h)\}$ 和 $\{pk_c = (R_c, X_c), sk_c = (x_c, d_c)\}$ 。

4.2 健康护照加密与存储

用户首次就诊后，医疗机构为其生成健康护照，将护照密文数据存储在IPFS上。然后，将相关的关键字索引、用户签名和密文检索标识作为交易上传至联盟链。联盟链节点负责将这些交易打包，执行改进后的弱共识机制，确保交易成功地被记录在链上。

(1) 用户就诊：用户 i 在医院 h 就诊后，医院 h 为用户 i 生成健康护照 $passport_i$ ，包括用户的个人信息、健康护照编号PUID_i和就诊信息。其中就诊信息包含就诊时间、就诊地点和个人病历等。

(2) 护照加密: 医院 h 随机选择一个秘密值 $\theta_i \in Z_p^*$, 计算 $A_i = X_i^{\theta_i}$, $= e(g^{\theta_i}, H_3(\text{PUID}_i))$, $B_i = k \cdot \text{passport}_i$, $C_{p_i} = (A_i, B_i)$ 为健康护照 passport_i 的密文。

(3) 护照存储: 将护照密文 C_{p_i} 上传至 IPFS, 返回相应的密文检索标识 index_f 。

(4) 护照签名: 用户随机选择 $u_i \in Z_p^*$, 计算 $U_i = g^{u_i}$, $h_i = H_1(\text{ID}_i \| U_i \| X_i)$, $V_i = g^{h_i x_i + h_i u_i} d_i$ 。其中 (x_i, d_i) 为用户 i 的私钥, $\delta_i = (U_i, V_i)$ 为用户 i 对护照的签名。

(5) 交易上传: 医院 h 利用健康护照编号 PUID_i 生成关键字索引 $I_k = H_3(e(H_3(\text{PUID}_i), g) \| \text{PUID}_i)$, 结合签名 δ_i 和密文检索标识 index_f 构建交易 $T_c = \{\delta_i, I_k, \text{index}_f\}$ 。最后, 医院将交易 T_c 上传联盟链, 交易结构如图2所示。

区块头	时间戳	区块ID	大小	父块哈希
	t	ID_c	size	hash
交易	产生者	关键字索引	用户签名	检索标识
	ID_h	I_k	δ_i	index_f

图2 交易结构
Figure 2 Transaction structure

(6) 联盟链共识: 联盟链节点收到医院上传的交易 T_c , 通过改进的弱共识机制对其进行共识并将其打包上链。改进后的共识机制的具体方案如下。

1) 交易 T_c 被提交至联盟链, 并在各医院节点构成的 P2P 网络中广播。

2) 当某个节点 A 收到客户端发来的交易 T_c 后, 该节点首先验证 T_c 的签名与完整性, 然后将交易存储至本地交易池中。待存储的交易数量达到预设的阈值时, 节点对交易进行打包写入新的区块中, 为新区块生成 Prepare 消息 $\langle \text{Prepare}, \text{index}, \text{OID}, M, D, \text{proof} \rangle$, 并广播 Prepare 消息至 P2P 网络中。其中 index 为由当前节点生成的区块的有序序列号, OID 为生成此区块的节点编号, M 为打包的交易, D 为消息摘要, Proof 为 A 节点已经将区块插入本地链中的证明。

3) 假设另一个随机节点 B 收到了生成这条消息的 A 节点发来的 Prepare 消息, 该节点将会

验证这条 Prepare 消息的签名与完整性, 验证通过后生成一条 Commit 消息 $\langle \text{Commit}, \text{index}, D, \text{OID}, \text{NID} \rangle$ 。只广播该消息的摘要 D , NID 为发送这条 Commit 消息的节点, 同时将该消息广播至 P2P 网络中。

4) 当 B 节点收到来自其他节点的 $2f+1$ 条 Commit 消息后, 表明该交易已经在共识节点内达成共识, 可以上链。节点将该区块更新至本地链, 并确保区块序号 index 与其他节点生成的区块序号有序递增, 实现各节点生成的区块间的相对一致性。

4.3 健康护照的更新

用户再次就诊时需要获取护照数据, 由医疗机构更新并存储护照数据, 步骤如下。

(1) 生成陷门: 用户 i 随机选择秘密值 $l_i \in Z_p^*$, 计算 $\tau_1 = H_3(\text{PUID}_i)^{\frac{1}{x_i}} \cdot X_c^{l_i}$, $\tau_2 = g^{l_i}$, 记 $\text{SToken} = \langle \tau_1, \tau_2 \rangle$ 为查询陷门。用户 i 向联盟链节点提交 SToken , 发起搜索请求。

(2) 数据检索: 联盟链节点 C 收到请求后, 验证等式 $I_k = H_5(e(\frac{\tau_1}{\tau_2^{x_c}}, X_i) \| \text{PUID}_i)$ 是否成立。若等式成立, 节点提取对应交易中的 index_f , 从 IPFS 中搜索密文 C_{p_i} 并返回给用户。

(3) 解密与验证: 用户计算健康护照明文数据如式 (2) 所示。

$$\text{passport}_i = \frac{B_i}{e(A_i, H_3(\text{PUID}_i))^{\frac{1}{x_i}}} \quad (2)$$

(4) 就诊与更新: 医疗机构提供医疗服务后, 更新用户健康护照数据, 并将其重新存储上链。

4.4 健康护照的验证

4.4.1 单用户验证

当个体用户计划出国旅行或进行国际交流, 海关对其进行健康状态检查, 仅允许健康状态良好的用户通行, 主要步骤如下。

(1) 生成陷门: 用户基于健康护照编号 PUID_i 生成查询陷门, 并向联盟链发起请求以检索用户签名, 流程细节与第4.3节步骤 (1) 一致。

(2) 获取签名: 联盟链节点获取交易 T_c 中的关键字索引 I_k 后, 验证等式 $I_k = H_5\left(e\left(\frac{\tau_1}{\tau_2^{x_c}}, X_i\right) \| \right)$

PUID_i)是否成立。若等式成立,获得交易中的用户签名 δ_i 。

(3) 验证签名: 由联盟链节点调取验证智能合约, 根据用户签名 $\delta_i = (U_i, V_i)$ 和公钥 $\text{pk}_i = (R_i, X_i)$, 计算 k_i 和 h_i 。验证等式 $H_2(e(V_i, g)) = H_2(e(R_i \cdot P_{\text{pub}}^{k_i} \cdot X_i^{h_i}, g) \cdot e(U_i^{h_i}, g))$ 是否成立。若成立, 则确认用户护照状态正常, 返回结果给海关工作人员。

4.4.2 多用户验证

为提高验证效率, 团体用户 (如国际旅行团、学术交流团等) 计划出国旅行或进行国际交流时, 团队聚合签名, 以接受海关的健康状态检查。

(1) 获取个人签名: 团体中的 n 个用户根据自己的护照编号生成查询陷门, 以检索各自的签名 $\delta_i (1 < i \leq n)$ 。流程与第4.4.1节中一致。

(2) 生成聚合签名: 团队中聚合者根据签名集合 $\{\delta_1, \delta_2, \dots, \delta_n\}$ 计算哈希集合 $\text{Hash} = \{\text{hash}_1, \text{hash}_2, \dots, \text{hash}_n\}$, 其中 $\text{hash}_i = H_2(\text{hash}_{i-1} + e(V_i, g))$, $1 < i \leq n$ 。记 $t = \text{hash}_n$, 得到聚合签名 $\delta = (U, U_2, \dots, U_n, t)$, 并向联盟链发起验证请求。

(3) 验证聚合签名: 由联盟链节点调取验证智能合约, 对所有的 $1 < i \leq n$, 计算 k_i 和 h_i 。验证 $t = H_2(H_2(H_2(H_2(e(R_i \cdot P_{\text{pub}}^{k_i} \cdot X_i^{h_i}, g) \cdot e(U_i^{h_i}, g)) + e(R_2 \cdot P_{\text{pub}}^{k_2} \cdot X_2^{h_2}, g) \cdot e(U_2^{h_2}, g)) \dots) + e(R_n \cdot P_{\text{pub}}^{k_n} \cdot X_n^{h_n}, g) \cdot e(U_n^{h_n}, g))$ 是否成立。若成立, 说明团体中用户护照状态正常, 返回结果给海关工作人员; 若不成立, 说明团体中存在恶意用户, 有人伪造了疫苗接种凭证。为找出恶意用户, 对于 $1 < i \leq n$ 依次计算 $t_i = H_2(\text{hash}_{i-1} + e(R_i \cdot P_{\text{pub}}^{k_i} \cdot X_i^{h_i}, g) \cdot e(U_i^{h_i}, g))$ 。判断 $t_i = \text{hash}_i$ 是否成立, 若等式不成立, 则用户 i 的护照状态异常。

5 安全性分析

5.1 正确性

(1) 检索正确性

针对第4.3节步骤(2)中等式 $I_k = H_5$

$\left(e\left(\frac{\tau_1}{\tau_2^{x_c}}, X_i\right) \parallel \text{PUID}_i\right)$, 推导过程如式(3)所示。

$$\begin{aligned} & H_5\left(e\left(\frac{\tau_1}{\tau_2^{x_c}}, X_i\right) \parallel \text{PUID}_i\right) = \\ & H_5\left(e\left(\frac{H_3(\text{PUID}_i)^{\frac{1}{x_i}} \cdot X_c^{l_i}}{(g^{l_i})^{x_c}}, \right) \parallel \text{PUID}_i\right) = \\ & H_5\left(e\left(\frac{H_3(\text{PUID}_i)^{\frac{1}{x_i}} \cdot (g^{x_c})^{l_i}}{(g^{l_i})^{x_c}}, g^{x_i}\right) \parallel \text{PUID}_i\right) = \\ & H_5\left(e\left(H_3(\text{PUID}_i), g\right) \parallel \text{PUID}_i\right) = I_k \end{aligned} \quad (3)$$

(2) 解密正确性

针对第4.3节步骤(3)中 $\text{passport}_i =$

$$\begin{aligned} & \frac{B_i}{e(A_i, H_3(\text{PUID}_i))^{\frac{1}{x_i}}}, \text{推导过程如式(4)所示。} \\ & \frac{B_i}{e(A_i, H_3(\text{PUID}_i))^{\frac{1}{x_i}}} = \\ & \frac{k \cdot \text{passport}_i}{e(X_i^{\theta_i}, H_3(\text{PUID}_i))^{\frac{1}{x_i}}} = \\ & \frac{k \cdot \text{passport}_i}{e(X_i^{\theta_i}, H_3(\text{PUID}_i))^{\frac{1}{x_i}}} = \\ & \frac{e(g^{\theta_i}, H_3(\text{PUID}_i))}{e((g^{x_i})^{\theta_i}, H_3(\text{PUID}_i))^{\frac{1}{x_i}}} \cdot \text{passport}_i = \\ & \text{passport}_i \end{aligned} \quad (4)$$

(3) 签名正确性

针对第4.4.1节中等式 $H_2(e(V_i, g)) = H_2(e(R_i \cdot P_{\text{pub}}^{k_i} \cdot X_i^{h_i}, g) \cdot e(U_i^{h_i}, g))$, 具体推导证明如式(5)所示。

$$\begin{aligned} & e(V_i, g) = e(g^{h_i x_i + h_i u_i} \cdot d_i, g) = \\ & e(g^{h_i x_i + h_i u_i} \cdot g^{r_i + k_i s}, g) = \\ & e(g^{r_i} \cdot g^{h_i x_i} \cdot g^{h_i u_i} \cdot g^{k_i s}, g) = \\ & e(g^{r_i} \cdot (g^{x_i})^{h_i} \cdot (g^{u_i})^{h_i} \cdot (g^{s_i})^{k_i}, g) = \\ & e(R_i \cdot X_i^{h_i} \cdot U_i^{h_i} \cdot P_{\text{pub}}^{k_i}, g) = \\ & e(R_i \cdot P_{\text{pub}}^{k_i} \cdot X_i^{h_i}, g) \cdot e(U_i^{h_i}, g) \end{aligned} \quad (5)$$

(3) 聚合签名正确性

针对第4.4.2节中 $t = H_2(H_2(H_2(e(R_1 \cdot P_{\text{pub}}^{k_1} \cdot X_1^{h_1}, g) \cdot e(U_1^{h_1}, g)) + e(R_2 \cdot P_{\text{pub}}^{k_2} \cdot X_2^{h_2}, g) \cdot e(U_2^{h_2}, g)) \cdots) + e(R_n \cdot P_{\text{pub}}^{k_n} \cdot X_n^{h_n}, g) \cdot e(U_n^{h_n}, g))$, 其证明过程与签名正确性验证类似。

5.2 机密性

本文方案使用用户的公钥对健康护照数据进行加密, 只有拥有私钥才能对数据进行解密。健康护照密文数据存储在 IPFS, 即使 IPFS 遭到黑客攻击, 攻击者也无法获取有效数据。同时, KGC 仅保留部分私钥 $D_i = (R_i, d_i)$, 完整私钥 $\text{sk}_i = (x_i, d_i)$ 由用户自己生成, 从而加强了数据的机密性。

5.3 可追溯性和不可否认性

本文方案依赖于区块链难以篡改的特性, 用户护照的索引与签名均被上传至联盟链, 每笔交易中包含交易生成者的身份标识 ID_h 。如用户的健康状态出现问题, 可追溯至相关的医疗机构, 而交易中包含的医院的签名 sig_h , 则可以防止医院否认事实。

5.4 不可伪造性

在将交易上传至联盟链前, 用户使用私钥对健康护照进行签名。恶意攻击者无法获取用户私钥, 因此无法伪造有效签名。无效签名无法通过等式 $e(V_i, g) = e(R_i \cdot P_{\text{pub}}^{k_i} \cdot X_i^{h_i}, g) \cdot e(U_i^{h_i}, g)$ 验证, 从而保证了健康护照的不可伪造性。

6 性能分析

本节首先将本文方案与相关健康护照方案进行了功能比较; 然后从理论角度分析本文方案的计算开销, 并与现有方案进行了比较; 最后通过

仿真实验对方案性能进行评估。

6.1 功能比较

本文方案与其他健康护照方案^[7, 9-10, 13, 22]的功能比较如表2所示。由表2可以看出, 所有的方案都实现了机密性与完整性。文献[7, 9]方案无法保证数据的不可否认性; 文献[13]方案没有考虑健康护照被伪造的问题; 文献[10, 22]方案很好地实现了上述功能, 但不能提供多人场景下高效的健康护照验证。而本文方案很好地实现了这些功能。

6.2 计算开销

为了比较计算开销, 本文在一台操作系统为 Windows10, CPU 为 Intel Core i3-10100 CPU, 3.60 GHz, 16 GB 内存的个人计算机上进行仿真实验。方案中各运算操作的执行时间如表3所示。本文方案的计算开销主要在健康护照检索阶段与签名验证阶段, 本文方案与文献[13, 22]方案的计算开销比较如表4所示, 其中 n 为用户人数。(文献[7]方案未提供具体方案细节, 因此不进行计算开销比较)。

表3 运算操作的执行时间
Table 3 Execution time of operations

符号	运算操作	执行时间/ms
T_h	哈希函数运算	0.04
T_m	点乘运算	0.07
T_e	指数运算	10.56
T_p	双线性运算	4.98

不同阶段的计算开销比较如图3所示。方案的健康护照检索阶段计算开销如图3(a)所示, 文献[13, 22]方案的计算开销优于本文方案单用户情形的计算开销, 但弱于多用户情形的计算开销, 且会随用户人数的增多使差距逐渐增大。这

表2 功能比较
Table 2 Functional comparison

功能	文献[7]方案	文献[9]方案	文献[10]方案	文献[13]方案	文献[22]方案	本文方案
机密性	√	√	√	√	√	√
可追溯	√	√	√	√	√	√
完整性	√	√	√	√	√	√
不可否认	×	×	√	√	√	√
不可伪造	√	√	√	×	√	√
多人场景	×	×	×	×	×	√

表4 计算开销比较
Table 4 Comparison of computation overhead

方案	检索阶段计算开销	签名验证阶段计算开销	总计
文献[13]方案	$3nT_h + 5nT_m + 3nT_e + 2nT_p$	$3nT_h + 5nT_m + 3nT_e + 2nT_p$	$6nT_h + 10nT_m + 6nT_e + 4nT_p$
文献[22]方案	$nT_h + 3nT_e + nT_p$	$2nT_h + 3nT_m + 3nT_e + 3nT_p$	$3nT_h + 3nT_m + 4nT_e + 4nT_p$
本文方案(单用户)	$2nT_h + nT_m + 4nT_e + nT_p$	$4nT_h + 3nT_m + 3nT_e + 3nT_p$	$5nT_h + 3nT_m + 4nT_e + 4nT_p$
本文方案(多用户)	$2T_h + T_m + 4T_e + T_p$	$3nT_h + 3nT_m + 3nT_e + 2nT_p$	$(3n+2)T_h + (3n+1)T_m + (3n+4)T_e + (2n+1)T_p$

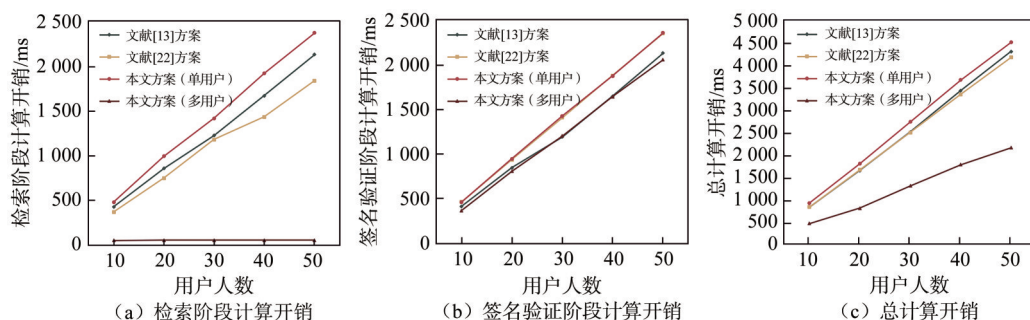


图3 不同阶段的计算开销比较
Figure 3 Comparison of computation overhead at different stages

是因为本文方案引入了聚合签名技术，只需要进行一次检索；而其他方案需要对每位用户的接种凭证一一进行检索，用户人数越多，检索阶段计算开销越大。方案在签名验证阶段的计算开销如图3(b)所示，本文方案单用户情形的签名验证计算开销与文献[22]方案的计算开销大体一致，但大于文献[13]方案的计算开销，并且文献[22]方案的签名验证阶段计算开销也大于本文方案在多用户情形下的计算开销，这是因为文献[13]方案和本文方案的签名验证过程相较于文献[22]方案减少了1个双线性运算操作，在一定程度上降低了签名验证的计算开销。同时，本文方案相较于文献[13]方案减少了2个乘法运算操作，具有微弱的优势。方案的总计算开销如图3(c)所示，可以看出，本文方案在多用户情形下总计算开销显著优于现有方案，最高优化了49.89%，这是因为本文方案相较于现有方案考虑了在进行检索和验证时可以将复杂的计算（如双线性映射与指数运算）合并。为实现多用户场景下计算的合并，增加了单用户场景下的计算操作。虽然这会导致本文方案在单用户情形下计算开销高于其他现有方案，但由图3(a)~图3(c)可以看出，其他现有方案无论是数据的检索还是验证阶段，计算开销均高于本文方案的多用户场景。

因此，本文方案在实际应用中的效率更具有优势，更适用于国际旅行或国际交往场景。

方案中可能会存在恶意攻击者伪造合法用户的健康护照的情况，这会导致签名验证失败。签名一旦验证失败，只有重新获得每个用户的签名并依次进行验证，才能找出恶意伪造者。而本文提出的聚合签名方案不需要重新上链查询每个用户的签名来验证，就可以追溯到恶意伪造者；同时，追溯验证的计算开销也有了一定降低。

6.3 共识开销

为了评估本文改进的弱共识算法效率，本文使用Java作为编程语言对PBFT算法^[20]、弱共识算法^[21]和改进的弱共识算法流程进行模拟仿真，通过WebSocket的不同端口间通信分别模拟了4~64个节点的P2P网络环境，对每个实验进行10次仿真实验并取平均值作为最终结果。实验在1台操作系统为Windows11，CPU为AMD Ryzen 75800H，16 GB内存的笔记本电脑上进行。区块链中的吞吐量由每秒能够上链的交易来表示每秒交易数(transaction per second, TPS)，即 $TPS = \frac{N_{T_s}}{t}$ ，其中 t 为时间， N_{T_s} 为 t 时间内上链的交易数，本文对比了传统的PBFT算法、弱共识算法以及本文改进的弱共识算法，共识效率比较如图4所示。

由图4可以看出, PBFT的共识算法在节点越多时, 吞吐量越低。相较于PBFT算法^[20]和弱共识算法^[21], 本文改进的弱共识算法的吞吐量在节点数较少时, 远高于另外2个共识算法。同时, 在节点数较多时, 仍有较好的表现。改进的弱共识算法达成共识只需要2个阶段, 从而大大减小了节点间达成共识的通信复杂度, 提高了整个区块链系统的吞吐量。

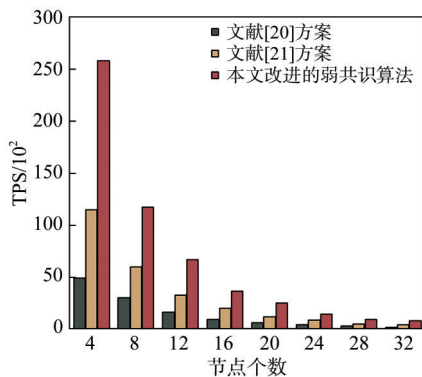


图4 共识效率比较

Figure 4 Comparison of consensus efficiency

6.4 通信开销

假设索引、陷门、哈希值、密钥对的长度为256 bit, 健康护照数据密文信息的长度为512 bit, 签名信息的长度为1 024 bit, 身份ID的长度为128 bit, 时间戳的长度为64 bit, 则存储阶段, 通信开销比较如图5所示, 在健康护照数据存储阶段, 文献[13]方案需要发送1 984 bit, 文献[22]方案需要发送1 792 bit, 而本文方案只需要发送1 664 bit; 检索阶段, 通信开销比较如图6所示, 文献[13]方案需要发送1 984 bit, 文献[22]方案需要发送1 536 bit, 而本文方案只需要发送1 280 bit。与文献[13, 22]方案相比, 本文方案通信开销较小, 最高优化了25.81%, 这归功于减少了不必要的传输(如时间戳和密钥)。

7 结束语

本文针对个人健康护照全球共享所面临“信息孤岛”、隐私保护和易伪造等难题, 设计了基于区块链的健康护照存储、共享与验证方案, 主要解决安全、隐私和效率问题。本文方案利用可搜索加密技术和区块链技术相结合, 同时改进聚合签名和弱共识算法, 实现了多用户情形下健康

护照的安全、高效和共享。但本文方案还存在一定的局限性, 在单用户情形下, 方案的检索开销和签名验证开销高于现有方案的计算开销。未来将继续改进方案中的聚合签名验证方法, 降低单用户情形下的计算开销。

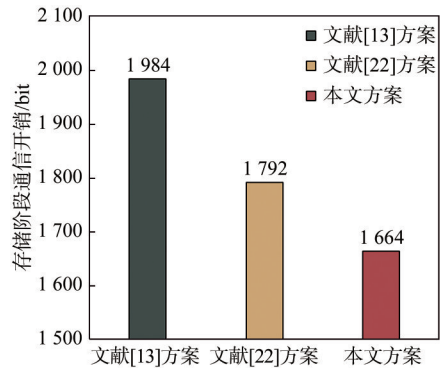


图5 存储阶段通信开销比较

Figure 5 Comparison of communication overhead at storage

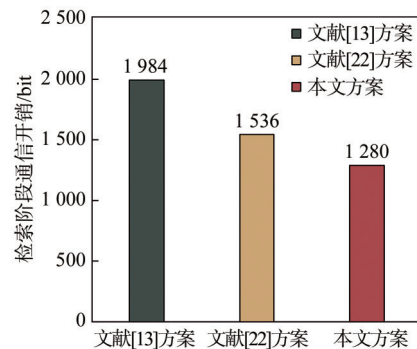


图6 检索阶段通信开销比较

Figure 6 Comparison of communication overhead at retrieval

参考文献:

- [1] JECKER N S. Vaccine passports and health disparities: a perilous journey[J]. Journal of Medical Ethics, 2022, 48(12): 957-960.
- [2] NIU S F, CHEN L X, WANG J F, et al. Electronic health record sharing scheme with searchable attribute-based encryption on blockchain[J]. IEEE Access, 2019(8): 7195-7204.
- [3] GAI K K, GUO J N, ZHU L H, et al. Blockchain meets cloud computing: a survey[J]. IEEE Communications Surveys & Tutorials, 2020, 22(3): 2009-2030.
- [4] 陈友荣, 陈浩, 韩蒙, 等. 基于信用等级划分的医疗数据安全共识算法[J]. 电子与信息学报, 2022, 44(1): 279-287.
CHEN Y R, CHEN H, HAN M, et al. Security consensus algorithm of medical data based on credit rating[J]. Journal of Electronics & Information Technology, 2022, 44(1): 279-287.
- [5] 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 S F, LIU W K, CHEN L X, et al. Electronic medical record data sharing scheme based on searchable encryption via consortium

- blockchain[J]. Journal on Communications, 2020, 41(8): 204-214.
- [6] 张海波, 徐蓬勃, 王汝言, 等. 区块链下基于蛛网模型的新能源汽车能源交易机制研究[J]. 电子与信息学报, 2023, 45(12): 4245-4253.
- ZHANG H B, XU P B, WANG R Y, et al. Research on energy trading mechanism of new energy vehicles based on cobweb model under blockchain[J]. Journal of Electronics & Information Technology, 2023, 45(12): 4245-4253.
- [7] XIN W M. Fighting COVID-19 and helping economy reopen by using blockchain technology[C]//Proceedings of the 2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops). 2020: 102-105.
- [8] BANSAL A, GARG C, PADAPPAYIL R P. Optimizing the implementation of COVID-19 'immunity certificates' using blockchain[J]. Journal of Medical Systems, 2020, 44(9): 140.
- [9] ANGELOPOULOS C M, DAMIANOU A, KATOS V. DHP framework: digital Health Passports Using Blockchain: use case on international tourism during the COVID-19 pandemic[J]. arXiv preprint, arXiv: 2005.08922. 2020.
- [10] HAQUE A B, NAQVI B, ISLAM A K M N, et al. Towards a GDPR-compliant blockchain-based COVID vaccination passport[J]. Applied Sciences, 2021, 11(13): 6132.
- [11] LEE H A, WU W C, KUNG H H, et al. Design of a vaccine passport validation system using blockchain-based architecture: development study[J]. JMIR Public Health and Surveillance, 2022, 8(4): e32411.
- [12] CHAUDHARI S, CLEAR M, BRADISH P, et al. Framework for a DLT based COVID-19 passport[M]. Cham: Springer International Publishing, 2021: 108-123.
- [13] CHEN J S, CHEN X F, CHEN C L. A traceable blockchain-based vaccination record storage and sharing system[J]. Journal of Healthcare Engineering, 2022: 2211065.
- [14] BONNEAU J, MILLER A, CLARK J, et al. SoK: research perspectives and challenges for Bitcoin and cryptocurrencies[C]//Proceedings of the 2015 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2015: 104-121.
- [15] NAKAMOTO S, BITCION A. A peer-to-peer electronic cash system[J]. Bitcoin, 2008, 4(2): 15.
- [16] KIAYIAS A, RUSSELL A, DAVID B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol[C]//Proceeding of the Advances in Cryptology-CRYPTO 2017. 2017: 357-388.
- [17] TOYODA K, MACHI K, OHTAKE Y, et al. Function-level bottleneck analysis of private proof-of-authority ethereum blockchain[J]. IEEE Access, 2020(8): 141611-141621.
- [18] XU X L, ZHU D W, YANG X X, et al. Concurrent practical Byzantine fault tolerance for integration of blockchain and supply chain[J]. ACM Transactions on Internet Technology, 21(1): 7.
- [19] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 20(4): 398-461.
- [20] CASTRO M, LISKOV B. Practical Byzantine fault tolerance [C]//Proceedings of the third symposium on Operating systems design and implementation. 1999: 173-186.
- [21] WANG Q, LI R J. A weak consensus algorithm and its application to high-performance blockchain[C]//Proceedings of the IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. 2021: 1-10.
- [22] GAO H C, JI H Y, HUANG H P, et al. An immunity passport scheme based on the dual-blockchain architecture for international travel[J]. Wireless Communications and Mobile Computing, 2022, 2022: 5721212.
- [23] ZHANG F G, SAFARI-NAINI R, SUSILO W. An efficient signature scheme from bilinear pairings and its applications[C]//Proceedings of the International Workshop on Public Key Cryptography. 2004: 277-290.
- [24] JOUX A, NGUYEN K. Separating decision Diffie-Hellman from computational Diffie-Hellman in cryptographic groups[J]. Journal of Cryptology, 2003, 16(4): 239-247.
- [25] 袁承昊, 李勇, 任爽. 多关键词动态可搜索加密方案[J]. 网络与信息安全学报, 2023, 9(2): 143-153.
- YUAN C H, LI Y, REN S. Dynamic multi-keyword searchable encryption scheme[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 143-153.

[作者简介]



高汉成 (1998-), 男, 河南洛阳人, 南京邮电大学博士生, 主要研究方向为区块链和数据隐私保护。



吉浩宇 (1997-), 男, 辽宁建昌人, 南京邮电大学硕士生, 主要研究方向为区块链和隐私保护。



高晨昊 (1997-), 男, 安徽马鞍山人, 南京邮电大学硕士生, 主要研究方向为区块链技术。



黄海平 (1981-), 男, 福建三明人, 南京邮电大学教授、博士生导师, 主要研究方向为物联网、信息安全、数据隐私保护。