Computer Science and Application 计算机科学与应用, 2024, 14(6), 149-156
Published Online June 2024 in Hans. https://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2024.146151

Hans汉斯

紧急医疗事件下的匿名访问控制方案

杨　鹏，岳笑含

沈阳工业大学信息科学与工程学院，辽宁 沈阳

收稿日期：2024年5月23日；录用日期：2024年6月22日；发布日期：2024年6月30日

摘　要

紧急医疗卫生事件的发生，使得各类公共场所成为了重点化防疫管控的对象，因此需要人们在出入公共场所时出示相应的防疫凭证。然而在防疫凭证验证过程中，伪造、冒充、篡改以及窃取个人隐私数据等恶意行为成为了公共医疗卫生事件溯源流调面临的最大挑战。针对这些挑战，本文提出了一种面向紧急医疗卫生事件的匿名认证方案：安全性方面，首先给出了该场景下所需的安全性需求；其次，结合密码学匿名凭证思想，利用区块链、生物特征验证等技术对方案进行了构建；性能方面，在解决了多源防疫凭证难以聚合的问题基础上，给出了方案的性能分析及在椭圆曲线下关键算法的性能测试，结果表明所提出的方案在安全性和性能两个方面都具有实际意义。综上，提出的方案可为紧急医疗事件下公共场所防疫提供一种隐私及安全的认证方案。

关键词

匿名认证，区块链，生物特征验证

An Anonymous Access Control for Emergency Health Events

Peng Yang, Xiaohan Yue

School of Information Science and Engineering, Shenyang University of Technology, Shenyang Liaoning

Received: May 23rd, 2024; accepted: Jun. 22nd, 2024; published: Jun. 30th, 2024

Abstract

The occurrence of emergency medical and health events has made all kinds of public places become the object of pandemic prevention and control (PPC), and people are required to show the corresponding epidemic prevention credentials when entering and leaving public places. However, in the process of PPC certificate verification, malicious behaviors such as forgery, impersonation, tampering and theft of personal privacy data have become the biggest challenges faced by the tra-

文章引用: 杨鹏, 岳笑含. 紧急医疗事件下的匿名访问控制方案[J]. 计算机科学与应用, 2024, 14(6): 149-156.
DOI: 10.12677/csa.2024.146151

ceability of public medical and health events. To solve these challenges, this paper proposes an anonymous authentication scheme for emergency medical and health events. In terms of security, the security requirements required in this scenario are first presented; Secondly, combined with the idea of cryptography anonymous credential, the scheme is constructed by using block chain, biometric verification and other technologies. In terms of performance, based on solving the problem of difficult aggregation of multi-source PPC credentials, the performance analysis of the scheme and the performance test of key algorithms under elliptic curve are given. The results show that the proposed scheme has practical significance in both security and performance. In summary, the proposed scheme can provide a privacy and safety certification scheme for PPC in public places under medical emergencies.

Keywords

Anonymous Authentication, Block Chain, Biometric Verification

1. 引言

新型冠状病毒(COVID-19)和猴痘疫情(mpox)等[1] [2]紧急公共医疗卫生事件所引发的全球持续性疫情，给全球经济、健康和人类生活带来了严重的影响。以新冠疫情为例，在全球防疫大背景下，为有效抑制病毒的传播以及对病毒传播的溯源，多类公共场所成为了各国防疫工作重点化、常态化管控的对象。各个国家/地区为此推出了相关的基于防疫凭证的认证技术[3] [4] [5] [6] [7]，但是目前存在的技术方案都存在着用户隐私泄漏[8]或者用户身份无法核验的问题。

因此，在公共场所下以用户防疫认证数据出示及防疫监管者验证为核心的应用场景中，存在以下安全及隐私挑战亟待解决：

1) 在用户侧，恶意用户可以通过篡改、伪造等行为欺骗验证者从而进入公共场所，这无疑会造成严重的防疫隐患。因此，如何在保障用户认证信息隐私的前提下，避免恶意用户的伪造、冒充等恶意行为是本文解决的问题之一；

2) 在防疫监管验证侧，恶意的监管人员会收集用户进入公共场所的相关信息，造成用户信息泄漏。因此，如何在保障防疫认证信息有效性可验证的基础上，对用户实现匿名性保护是本文解决的问题之二；

3) 在凭证颁发方侧，由于存在多个防疫凭证发行方，用户根据不同访问策略需要出示不同凭证。因此，在保证多源防疫凭证可聚合的基础上，出示相应的聚合后的防疫凭证，是本文需要解决的问题之三。

为应对上述挑战，在满足用户出入公共场所防疫展码可认证性基础上，且保证用户隐私安全以及确诊用户可追溯的核心需求下，本文利用“区块链 + 匿名认证 + 生物特征验证”相结合的技术提出了面向紧急医疗事件的高效匿名认证方案。本文从功能性、安全性、性能三个维度出发，文章贡献如下：

1) 在功能性方面，围绕公共场所防疫展码特点及功能需求，设计了方案的总体框架并给出了方案中各个实体及运行功能的形式化定义。

2) 在安全性方面，围绕公共场所防疫展码应用场景下的特点以及上述挑战，给出了方案的安全及隐私需求，包括匿名性、不可伪造性等。

3) 在性能方面，为确保方案在实际防疫展码场景下的可用性，利用具有线性同态的密码学算法实现

了基于场所访问策略的多源防疫属性凭证可聚合。

简而言之，本文所提出的匿名认证方案不但可以有效解决现有的紧急医疗卫生事件的公共场所匿名认证方案所存在的问题，而且结合区块链技术和生物认证可以实现有效溯源并保证用户身份的真实性，为防疫精准流调提供了数据支撑。

2. 相关工作

针对公共场所防疫所暴露出来的用户隐私安全问题，国内外政府、企业及研究机构提出了相关的解决方案。主要可以分为两类：第一类是以用户为中心的公共场所密接追踪方法，但该方法的前置条件太过理想不利于实际部署，因此本文后续不在讨论此类方案；第二类则是以公共场所为中心的防疫凭证匿名认证方法。

防疫凭证匿名认证方法相较于第一类密接追踪方法，匿名认证方法疫情防控效果更加精准有效，因此成为了世界各国选择的主要防疫方法。但文章开篇所提及的防疫凭证方案均存在不同程度安全性和隐私性挑战。因此，围绕这些挑战，各国专家学者给出了相应的解决方案。

Abid A 等人[9]提出数字健康证书解决方案能够实现对用户流调同时增强用户的隐私性，但文章为保证防疫凭证不可转移性，用户需要出示物理证件从而破坏了匿名性；Dima S M 等人[10]提出了一个结合区块链等技术的防疫证书签发和验证平台，然而该方案只采用了简单的数据脱敏方式保证用户隐私，这无法有效抵御数据推理和蛮力攻击。同样为了解决目前现存方案存在的安全隐私问题，Yao 等人[11]提出了一种基于区块链的多维可追溯隐私保护的健康码方案，然而该方案也不支持匿名状态下用户出示信息的可认证性，即无法确保用户给予验证者信息的真实性，类似的方案还有[12] [13]。

虽然上述方案对防疫展码场景下用户的隐私问题进行了阐述和解决，但围绕本文开篇提出的四个关键问题，现有的方案仍存在着一些共性不足。一是没有实现对多源防疫凭证的聚合出示；二是不支持非法用户系统访问权限的撤销，这无法阻止非法用户继续申请新的防疫凭证；三是现有方案都没有实现对用户真实身份的匿名认证(保证用户信息匿名且凭证与用户身份匿名绑定)，即未同时实现匿名和认证。

3. 方案的定义以及安全需求

围绕目前现有方案仍面临的不同挑战，本节首先设计了面向紧急医疗卫生事件的高效匿名认证方案的整体架构，并对架构中涉及的实体类型以及相关算法、协议进行了定义；其次，基于方案的整体架构给出了方案应具备的安全性及功能性需求。

3.1. 方案的定义

所提出方案的模型如图 1 所示。模型主要包含了五类实体，即注册中心、防疫凭证发行方、用户、公共场所防疫监管者和智能合约。注册中心颁发、更新和撤销令牌，并进行密接者溯源；防疫凭证发行方签发凭证；用户与注册中心和发行方交互获取令牌和凭证，并生成匿名认证信息展示给验证方；防疫监管者验证凭证有效性并上传信息给智能合约；智能合约验证事务并上传认证信息至区块链。方案包括六个阶段：初始化、注册、签发、认证阶段，详见表 1。在表 1 中对方案中涉及的主要变量符号进行了说明。

1) 初始化阶段

$\mathrm{Setup}\left(1^{\lambda}\right)\to pp$：输入为安全参数 λ，输出全局公开参数 pp。

$\mathrm{RKGen}\left(pp\right)\to\left(sk_{RA},vk_{RA},tsk_{RA},tpk_{RA}\right)$：注册中心执行，输出签发令牌密钥对 $\left(sk_{RA},vk_{RA}\right)$ 和密钥对 $\left(tsk_{RA},tpk_{RA}\right)$。

$\mathrm{IKGen}(pp)\to(isk_j,ivk_j)$：颁发方 Iss_j 运行，生成密钥对 (isk_j,ivk_j)。

$\mathrm{UKGen}(pp,\boldsymbol{u}_i)\to(usk_i,upk_i)$：用户 Usr_i 执行，输入用户的生物特征 $\boldsymbol{u}_i$，用户可以通过生物特征派生算法中的 FE.PkGen 与 FE.SkGen 计算出密钥对 (usk_i,upk_i)。

$\mathrm{VKGen}(pp)\to(vsk_{V_k},vvk_{V_k})$：算法由防疫监管者 V_k 执行，生成用于事务认证的签名密钥对 (vsk_{V_k},vvk_{V_k})。

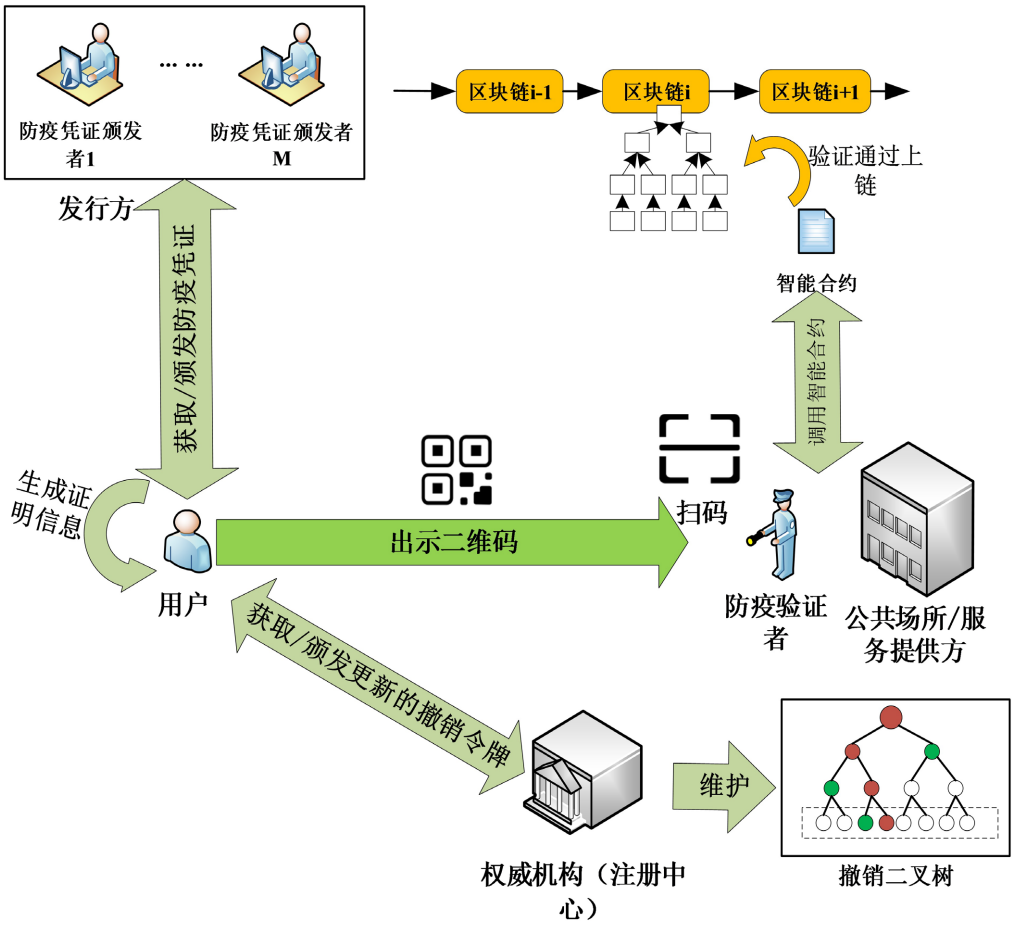

Figure 1. System model diagram
图 1. 系统模型图

2) 注册阶段

在注册阶段，用户与注册中心交互获取到身份令牌并验证。算法定义如下：

$\mathrm{UReg}(pp,usk_i,upk_i,vk_{RA})\to\pi_i^{\mathrm{tok}}$：由用户执行，生成身份令牌获取证明 π_i^{tok}。

$\mathrm{RReg}(pp,sk_{RA},t,\pi_i^{\mathrm{tok}})\to(tk_i,\rho_i)$：由注册中心执行，验证令牌获取证明 π_i^{tok}，若验证通过则为用户 Usr_i 分配一条完全二叉树上的路径 ρ_i 以及相应的令牌 $tk_i:=(tk_i^{\mathrm{tra}},tk_{i,n^*}^{\mathrm{rev}})$，其中 $n^*\in\rho_i\bigcap S_R^{(t)}$。RA 将 (ID_{Usr_i},tk_i,ρ_i) 存储至本地数据库 DB_{RA}，ID_{Usr_i} 包含在用户获取证明 π_i^{tok} 中。

$\mathrm{Verify}_{\mathrm{Usr}}^{\mathrm{tok}}(pp,vk_{RA},upk_i,tk_i,\rho_i,t)\to1/0$：由用户执行，输入注册中心验证公钥 vk_{RA}，用户公钥 upk_i 以及用户令牌 tk_i 和路径 ρ_i 进行验证，若验证通过输出 1，否则输出 0。

3) 签发阶段

在防疫凭证签发阶段，由于防疫凭证生成的非实时性，例如核酸、疫苗报告等，用户无法实时获取到新的防疫凭证。因此在该阶段颁发方将生成的防疫凭证利用用户注册时的公钥 upk_i 进行加密生成密文，并存储在本地凭证数据库 DB_{Iss_j}。当用户 Usr_i 请求时，颁发方查询相应的密文结果并返回给用户。算法定义如下：

$\mathrm{CIssue}\left(pp, upk_i, isk_j, ID_{Usr_i}\right) \to CT_{j,i}$：输入用户公钥 upk_i 以及身份标识 ID_{Usr_i} 和发行方私钥 isk_j，Iss_j 生成基于用户公钥加密的属性凭证 $CT_{j,i} \leftarrow \mathcal{E}.Enc\left(upk_i, cred_{j,i}\right)$，并存储 $\left(ID_{Usr_i}, CT_{j,i}\right)$ 到本地凭证数据库 DB_{Iss_j}，$\mathcal{E}$ 为公钥加密算法，例如 ElGamal 公钥加密算法。

$\mathrm{CObtain}\left(pp, isk_i, ivk_j, ID_{Usr_i}, CT_{j,i}\right) \to cred_{j,i} / \perp$：输入用户私钥 isk_j 以及身份标识 ID_{Usr_i}，加密的属性凭证 $CT_{j,i}$ 和验证公钥 ivk_j，用户解密出 $cred_{j,i} \leftarrow \mathcal{E}.Dec\left(isk_i, CT_{j,i}\right)$ 并验证 $cred_{j,i}$ 的有效性，如果有效输出 $cred_{j,i}$，否则输出 $\perp$。

4) 认证阶段

在认证阶段，根据访问属性策略集 $\mathcal{P}_{pub} := \{a_m\}_{m\in[N_{pub}]}$，其中 N_{pub} 表示所需属性的个数，用户利用令牌及符合 $\mathcal{P}_{pub}$ 的防疫凭证生成匿名认证信息并出示。防疫监管方对出示的认证信息进行验证，验证通过则表明该用户是未撤销用户且满足访问属性策略集 $\mathcal{P}_{pub}$。算法定义如下：

$\mathrm{Show}\left(pp, isk_i, vk_{RA}, tpk_{RA}, \{cred_{j,i}\}_{j\in[N_{Iss}]}, tk_i, \mathcal{P}_{pub}\right) \to \left(\pi_i^{\mathrm{show}}, \widehat{cred}_{agg}\right)$：输入用户通过生物特征恢复 isk_i，验证公钥 vk_{RA}，追踪公钥 tpk_{RA} 和满足 $\mathcal{P}_{pub}$ 的防疫凭证集合 $\{cred_{j,i}\}_{j\in[N_{Iss}]}$ 以及公共场所访问属性策略集 $\mathcal{P}_{pub}$，其中 N_{Iss} 表示防疫发行方的数量，算法输出匿名认证信息 π_i^{show} 和盲化后的聚合凭证 $\widehat{cred}_{agg}$。

$\mathrm{Verify}_{\mathrm{V}}^{\mathrm{Show}}\left(pp, vk_{RA}, \pi_i^{\mathrm{show}}, \widehat{cred}_{agg}, \mathcal{P}_{pub}\right) \to \sigma_V / \perp$：算法由公共场所防疫监管者 V_k 运行，用于验证用户所出示的认证信息是否有效。算法输入 RA 的验证公钥 vk_{RA}，用户的匿名认证信息 π_i^{show}，盲化后的聚合凭证 $\widehat{cred}_{agg}$ 以及访问属性策略集 $\mathcal{P}_{pub}$。若无效则输出 $\perp$。否则，V_k 生成签名值 $\sigma_{V_k} \leftarrow \Sigma.Sign\left(sk_{V_k}, m_{tx} := \left(\pi_i^{\mathrm{show}} \| msg\right)\right)$，其中 msg 包含认证场所信息以及时间戳等信息，并将验证事务 $tx := \left(\sigma_{V_k}, m_{tx}\right)$ 通过智能合约(SC)验证上传至区块链，Σ 为签名算法，例如 EdDSA 签名算法。

$\mathrm{SVerify}\left(pp, vvk_{V_k}, tx\right) \to 1/0$：智能合约使用验证算法 $\Sigma.Verify\left(vvk_{V_k}, tx\right)$ 对上传的事务进行验证，若验证通过则将数据上传至区块链中，并输出 1。否则，表示验证失败输出 0。

3.2. 方案的安全性以及功能性需求

本方案需要满足以下的安全性以及功能性需求：

匿名性：匿名性是指在凭证认证过程中，除了访问策略的属性值及认证结果外，攻击者无法从匿名认证信息中获取关于用户的任何有效个人信息。

不可伪造性：不可伪造性包含两方面，一是攻击者不能够伪造其它合法用户的匿名认证信息；二是攻击者无法伪造注册中心颁发的有效撤销令牌以及凭证发行方颁发的防疫凭证。

可撤销性：可撤销性是指注册中心能够对非法用户(例如隔离人员等)的身份令牌进行撤销，使其无法生成有效的匿名认证信息，从而保障方案的后向安全性。

不可转移性：不可转移性是指攻击者在认证阶段不能通过伪造用户私钥或派生出用户私钥进行匿名认证信息出示。

不可冒充性：不可冒充性是指攻击者在凭证认证阶段不能够冒充合法用户的身份出示匿名认证信息。

不可篡改性：不可篡改性是指单一的攻击者不能篡改用户进入公共场所的匿名认证信息以及相关公共场所信息。

选择性属性暴露：选择性属性暴露是指用户可以根据公共场所访问策略进行选择性的属性凭证聚合，而不需要出示所有用户的属性凭证。

4. 性能分析

在本节中，首先对部分算法性能进行了理论分析，如表 1 所示。在表 1 中，$\left(T_{\mathbb{G}_1}, T_{\mathbb{G}_2}, T_{\mathbb{G}_T}\right)$ 分别表示在群 $\left(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T\right)$ 上完成一次幂运算的时间；T_e 表示完成一次配对运算所消耗的时间，T_D 表示运行一次 FE.SkGen 算法所消耗的时间，N_{Iss} 指的是防疫凭证发行方的数量，$N_{Iss_j}^{att}$ 是防疫凭证发行方 Iss_j 为用户签发凭证中包含的属性数量，N_R 撤销后系统中根节点的数量，l 是完全二叉树的深度，K 表示公共场所数量与公共场所接受认证信息数量乘积(即 $K := I_{pub}^{ts} \cdot N_{pub_k}^{ts}$)。此外，在本文的性能分析中，仅考虑幂运算、FE.SkGen 算法和配对运算等计算代价较大的运算耗时。

表 1 给出了本方案中的实体在不同阶段运行各算法时的理论计算代价。为进一步测试本方案各个实体所涉及的算法在不同主流椭圆曲线，包含不同安全级别下的 BLS12_381 [14]和 BN462 [15]以及 BN254 [16]的实际性能(基准测试如表 2 所示)，本节利用密码学库 MCL 和区块链工具 HyperledgerFabric 框架[17]对本文所提出的匿名认证方案中较为频繁运行的 Show、$\text{Verify}_{\text{V}}^{\text{show}}$、Update 等算法进行了仿真实验，各个实验具体的相关测试平台配置信息如表 3 所示。

Table 1. Theoretical calculation cost table
表 1. 理论计算代价表

实体	注册中心	颁发方	验证方	用户
初始化阶段	$T_{\mathbb{G}_1} + 3T_{\mathbb{G}_2}$	$\left(N_{Iss}+1\right)T_{\mathbb{G}_2}$	-	-
注册阶段	$\left(2l+3\right)T_{\mathbb{G}_1}$		-	$\left(l+1\right)T_{\mathbb{G}_1} + \left(l+2\right)T_{\mathbb{G}_2} + \left(2l+2\right)T_e$
签发阶段	-	$T_{\mathbb{G}_1}$	-	$2T_e + \left(\sum_{j=1}^{N_{Iss}} N_{Iss_j}^{att}\right) \cdot T_{\mathbb{G}_2}$
认证阶段	-	-	$\left(\sum_{j=1}^{N_{Iss}} N_{Iss_j}^{att}\right)T_{\mathbb{G}_2} + 3T_{\mathbb{G}_1} + 9T_{\mathbb{G}_T} + 5T_e$	$6T_{\mathbb{G}_1} + \left(\sum_{j=1}^{N_{Iss}} N_{Iss_j}^{att}\right)T_{\mathbb{G}_2} + 7T_{\mathbb{G}_T} + 2T_e + T_D$

在认证阶段，验证方对接收的认证信息进行签名并调用智能合约上链。由于公有链，例如比特币、以太坊等，对事务处理速率较低，因此本方案采用了 Hyperledger Fabric 联盟链框架并编写智能合约(链码)进行了性能验证，通过实验表明批量验证 100 条签名事务平均耗时 0.031 s (吞吐量为 962 TPS)，能够实现高效的批量签名事务验证，满足实际需求。

Table 2. Different elliptic curve benchmarks
表 2. 不同椭圆曲线基准测试

	BN462		BLS12_381		BN254	
	Android	PC	Android	PC	Android	PC
$T_{\mathbb{G}_1}$	5.27 ms	0.82 ms	1.21 ms	0.19 ms	0.47 ms	0.074 ms
$T_{\mathbb{G}_2}$	12.01 ms	1.64 ms	3.35 ms	0.456 ms	1.29 ms	0.177 ms
$T_{\mathbb{G}_T}$	0.07 ms	0.005 ms	0.045 ms	0.0032 ms	0.025 ms	0.0017 ms
T_e	34.01 ms	2.5 ms	11.09 ms	0.814 ms	4.71 ms	0.346 ms

在通信代价方面，用户在认证阶段出示的认证信息 $Auth := \left(\widehat{cred}_{agg}, \pi_i^{show}, msg\right)$ 中需要 4 个 $\mathbb{G}_1$ 群元素和 7 个 $\mathbb{Z}_p$ 群元素以及信息字符串，即通信代价的理论值为 $4\mathbb{G}_1 + 7\mathbb{Z}_p + |msg|$。通过基准实验能够得出在 BN254 曲线上 $\mathbb{G}_1$ 群和 $\mathbb{Z}_p$ 群的元素长度分别是 192 字节和 64 字节。以用户出示包含 5 个属性的匿名凭证为例，在用户出示过程中需要耗费大约 371 ms，用户在 BN254 曲线下出示一个匿名凭证需要发送 1216 字节 $+|msg|$ 字节长度的信息，而常规的移动端可展示二维码信息容量最大为 4 KB，因此匿名凭证的内容能够以二维码的形式进行展示。

Table 3. The configuration of test platform
表 3. 测试平台配置

实体名称	平台信息		测试算法
User	CPU:Snapdragon 870 MEM:12.0GB OS:Android 12		Show
Verifier			$Verify_V^{show}$
RA	CPU: Intel(R) Core(TM) i7-7700HQ 2.80 GHz×8 RAM:16.0GB OS:Windows11 perfessional		RReg
SC (Fabric 链码)	区块链配置信息	Number of Channels: 1 Database: CouchDB Number of Nodes: 3 Consensus Mechanism: Kafka	SVerify
	平台配置信息	CPU: Intel(R) Xeon(R) Platinum 8369HB 3.30GHz×6 RAM:16.0GB OS: Debian GNU/Linux 11	

根据对上述实验过程中的理论计算代价和通信代价的分析可得，本文提出的匿名认证方案可以作为紧急医疗卫生事件场景下实际有效的隐私保护认证解决方案。

参考文献

[1] Isidro, J., Borges, V., Pinto, M., Sobral, D., Santos, J.D., Nunes, A., *et al*. (2022) Phylogenomic Characterization and Signs of Microevolution in the 2022 Multi-Country Outbreak of Monkeypox Virus. *Nature Medicine*, **28**, 1569-1572. https://doi.org/10.1038/s41591-022-01907-y

[2] Gorbalenya, A.E., Baker, S.C., Baric, R.S., de Groot, R.J., Drosten, C., Gulyaeva, A.A., *et al*. (2020) The Species Severe Acute Respiratory Syndrome-Related Coronavirus: Classifying 2019-nCoV and Naming It SARS-CoV-2. *Nature Microbiology*, **5**, 536-544. https://doi.org/10.1038/s41564-020-0695-z

[3] Covidpass. https://github.com/covidpass-org/covidpass

[4] The CovPassApp. https://digitaler-impfnachweis-app.de/en

[5] My Vaccine Pass. https://covid19.govt.nz/covid-19vaccines/vaccine-passes-and-certificates/proof-of-your-vaccination-status

[6] Al-Kuwari, M.G., Al Nuaimi, A.A., Semaan, S., *et al*. (2022) Effectiveness of Ehteraz Digital Contact Tracing App versus Conventional Contact Tracing in Managing the Outbreak of COVID-19 in the State of Qatar. *BMJ Innovations*, **8**. https://doi.org/10.1136/bmjinnov-2021-000879

[7] 胡凌. 健康码、数字身份与认证基础设施的兴起. 中国法律评论, 2021(2): 102-110.

[8] 付晓艺, 钟雨杉, 高慧茹, 张钟月, 肖怡凡, 李佳璐. 健康码应用中的个人信息保护研究[J]. 互联网周刊, 2022(18): 32-34.

[9] Abid, A., Cheikhrouhou, S., Kallel, S. and Jmaiel, M. (2021) NovidChain: Blockchain-Based Privacy-Preserving Platform for COVID-19 Test/Vaccine Certificates. *Software*: *Practice and Experience*, **52**, 841-867. https://doi.org/10.1002/spe.2983

[10] Dima, S.M., Hasikos, A., Kampakis, S., *et al*. (2021) Hygiea: A Secure, Smart, Privacy-Preserving and Interoperable Blockchain Solution for the Covid-19 Pandemic. https://arxiv.org/pdf/2107.09926.pdf

[11] Yao, S., Jing, P., Li, P. and Chen, J. (2022) A Multi-Dimension Traceable Privacy-Preserving Prevention and Control Scheme of the COVID-19 Epidemic Based on Blockchain. *Connection Science*, **34**, 1654-1677. https://doi.org/10.1080/09540091.2022.2077912

[12] Sugita, E., Abe, R., Suzuki, S., Uehara, K. and Nakamura, O. (2023). A System for Selective Disclosure of Information about a Patient with Intractable Disease. 2023 *IEEE* 47*th Annual Computers, Software, and Applications Conference* (*COMPSAC*), Torino, 26-30 June 2023, 1482-1487. https://doi.org/10.1109/compsac57700.2023.00228

[13] Duong, T., Gao, J., Phan, D.H., *et al*. (2023) Privacy-Preserving Digital Vaccine Passport. In: *International Conference on Cryptology and Network Security*, Springer Nature, Singapore, 137-161.

[14] Bowe, S. (2021) BLS12-381: New zk-SNARK Elliptic Curve Construction (2017). https://electriccoin.co/blog/new-snark-curve

[15] Barbulescu, R. and Duquesne, S. (2018) Updating Key Size Estimations for Pairings. *Journal of Cryptology*, **32**, 1298-1336. https://doi.org/10.1007/s00145-018-9280-5

[16] Nogami, Y., Akane, M., Sakemi, Y., *et al*. (2008) Integer Variable χ-Based Ate Pairing. In: *International Conference on Pairing-Based Cryptography*, Springer, Berlin, 178-191.

[17] Hyperledger Fabric. https://www.hyperledger.org/blog/2023/02/16/benchmarking-hyperledger-fabric-2-5-performance