基于可截取签名的药品管理隐私保护方案

胡荣磊[1], 丁安邦[1], 李 莉[1], 段晓毅[1]

[1]北京电子科技学院电子与通信工程系 北京 中国 100070

摘要 药品的安全问题关乎民生健康与社会稳定, 而近年来我国药品安全事故频发, 保障药品的质量安全, 对人民群众来说至关重要。建设药品品种档案管理方案能够整合、统一管理药品的相关信息, 保证药品来源可查、去向可追、责任可究, 是减少药品质量安全事故发生的有效举措。为了解决药品品种档案在不同省市各部门之间共建共享以及隐私保护的问题, 本文提出了一种基于区块链的药品品种管理模型。该模型融合了 Fabric 联盟链、无证书密码体制、可截取签名等多种技术, 以实现药品档案数据的安全存储与共享。同时, 引入 Baas 区块链管理平台, 实时监控并动态配置区块链网络中的节点与链码, 并按照模型中功能性的不同设计了链上交易表单及其对应的智能合约存储字段。随后, 针对管理模型中的药品核查场景, 结合传统的数字签名方案, 设计了一种无证书可截取签名方案, 利用可截取签名技术实现对药企机密数据的隐私保护。安全性分析表明, 本文所提方案具有签名的不可伪造性、消息的保密性等特征。性能分析表明, 该方案的运算量明显降低, 相比于同类方案效率更高, 开销更低, 可满足药品品种档案管理场景下的各种需求, 为药品品种档案管理过程中进行数据验真提供了一种新的思路。

关键词 区块链; 药品档案; 可截取签名; 隐私保护; 数据共享

中图法分类号 TP309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2024.01.04

A Privacy Protection Scheme for Drug Management Based on Content Extraction Signature

HU Ronglei[1], DING Anbang[1], LI Li[1], DUAN Xiaoyi[1]

[1] Department of Electronics and Information Engineering, Beijing Electronic Science and Technology Institute, Beijing 100070, China

Abstract The safety of drugs is related to people's health and social stability. However, in recent years, our country's drug safety accidents have shown the characteristics of high incidence and frequent occurrence. It is very important to ensure the quality and safety of drugs for people. The establishment of drug variety archives management system can integrate and manage drug-related information uniformly. It ensures that drug sources can be found, whereabouts can be traced, and responsibilities can be investigated, which is an effective measure to reduce the occurrence of drug quality and safety accidents. In order to solve the problem of co-construction, sharing and privacy protection of drug product archives among various departments in different provinces and cities, a blockchain-based drug archives management model is proposed. The model integrates various technologies such as Fabric consortium chain, certificateless cryptosystem, and content extraction signature to realize the safe storage and sharing of drug archive data. At the same time, a blockchain management platform Baas is introduced to this paper to realize the real-time monitoring and dynamic configuration of nodes and chaincodes in the blockchain network. Also, according to the different functionalities in the model, this paper designs the transaction forms and its corresponding smart contract's storage fields. Subsequently, for the drug verification scenario in the management model, a certificateless content extraction signature scheme is designed combining traditional digital signature schemes, in which the content extraction signature technology is used to realize the privacy protection of confidential data within pharmaceutical companies. Security analysis shows that the proposed scheme has the features such as unforgeability of signatures and confidentiality of messages. Performance analysis shows that the computational complexity of this scheme is significantly reduced. It is more efficient and has lower overhead than similar schemes, which can meet the needs of drug archive management, providing a new idea for data verification in the process of drug variety file management.

Key words blockchain; drug product archives; CES; privacy protection; data sharing

通讯作者: 丁安邦, 硕士, Email: 526768549@qq.com。

本研究成果受以下项目资助: 中央高校基本科研业务费课题“针对有防御密码设备的能量分析攻击研究”(No. 328202207); 北京电子科技学院培育孵化教学类项目-一流本科专业建设-通信工程(No. jy202104); 北京高校“高精尖”学科建设项目; 国家自然科学基金资助项目(No. 62072014)。

收稿日期: 2022-04-20; 修改日期: 2022-07-12; 定稿日期: 2023-09-26

1 引言

通过建设药品的品种信息档案, 食品药品监督管理局可以汇总来自不同部门的药品数据, 整合包括药品基本信息、审评审批信息、上市监管信息、产品召回退市等药品的全生命周期信息, 实现“一品一档”, 为监督检查工作提供支持。然而当下药品档案管理体系均以中心化管理为主, 各个主体之间存在信息不对称、信任不足的问题, 并且药品的监管追溯难度较大。当中心节点发生故障, 或内部遭到恶意攻击时, 系统的稳定性及可靠性也将大打折扣。因此, 建立一个安全可靠的药品品种管理方案至关重要。

为了解决上述问题, 文献[1-4]将区块链技术应用于药品供应链的追溯和管理, 将药品的品种档案上传到区块链, 实现对相关数据的访问、共享和监督。刘天成等[1]分析了传统药品供应链溯源方式的不足, 将区块链技术用于药品溯源流程中, 提高了溯源过程中药品数据的完整性与可靠性。薛丹等[2]设计了一种基于区块链的药品供应追溯系统, 实现了药品数据的安全共享和实时管理, 但是缺少对隐私保护问题的深入探讨。古锐等[3]基于区块链对药品的质量安全追溯体系进行了改进, 一定程度上解决了伪造数据、身份认证以及药品辨伪追责等问题, 但对于供应链中涉及的各个阶段之间信息交换的困难性与复杂性没有很好地解决。牛淑芬等[4]通过构造联盟链与私有链, 提出了基于区块链的可搜索加密的数据共享方案, 利用代理重加密技术实现了其他数据用户对患者病历数据的共享, 解决了区块链上数据共享过程中数据安全与个人隐私的问题, 但却不能做到业务的实时共享与互相协作。

由此可见, 仅仅依靠区块链并不足以很好地保护药品相关隐私数据, 对于药企的商业机密, 只有避免隐私数据的上传与发布, 才能真正地实现药品信息的隐私保护。可截取签名[5](Content Extraction Signatures, CES)是较为有效的解决方案之一, 其最大的优势就在于支持删除部分已签名数据, 进而保护隐私信息。

自 2001 年起, 国内外学者就在积极探索可截取签名在隐私保护方面的应用前景。Bull 等[6]通过将可截取签名算法引入 XML 签名机制, 对 XML 签名体制进行了拓展并引入到数字图书馆的场景下。文献[7]结合可截取签名提出了一种可被修改签名方案, 该方案提出修改容忍度的概念, 扩展了数字签名方案的同时还保证了可修改签名的隐私。文献[8-9]是基于 RSA 的批签名方案, 提出了基于身份信息的可截取签名方案, 通过分组批量签名来提高签名效率, 但是使用了大量双线性对运算, 导致签名和验证的效率依然较低。文献[10]提出了一种前向安全的可截取签名方案, 通过固定公钥, 不断变化私钥的方式确保安全, 但是同样依赖于复杂的双线性对运算。之后, 文献[11]提出了一种基于二叉树的签名方案, 使用哈希函数构造二叉树, 将冗长的数据存储在树形结构中, 缩短了签名的长度, 也就克服了签名数量和长度的限制, 但并没有对涉及到的复杂计算进行改进。

可截取签名可以为数据带来可靠性与安全性, 而区块链又可以分散中心化系统的安全风险与维护成本, 将区块链和以可截取签名为基础的签名方案相结合, 可以有效地管理药品品种档案, 并帮助药企隐藏涉及机密档案的信息内容, 更好地实现药品档案相关的隐私保护。

对此, 本文以药品品种信息档案的安全存储、隐私保护和安全共享为目标, 基于区块链提出一种药品品种档案管理模型, 并就其中的隐私保护问题提出解决方案。该方案融合了可截取签名、Fabric 联盟链等多种技术, 最大程度保护药企私密数据的同时还能够满足食药监总局数据中心对药品品种相关信息的检查, 具有隐私保护、数据安全存储、不可伪造及数据保密性。同时, 按照该场景下功能性的不同分别对链码进行了设计, 并定义访问控制策略, 实现了药品档案数据的有效访问和共享。本文的主要贡献如下:

1) 建立了基于区块链的药品品种档案管理模型, 针对药品管理场景下功能需求的不同设计了三种不同的业务表单, 并以此开发相应的链上智能合约。

2) 将无证书密码体制与可截取签名相结合, 使用简单的标量乘与模逆运算代替复杂的双线性对与模幂运算, 保证方案安全性的同时还提高了运行效率。

3) 基于改进的可截取签名算法, 提出了区块链上药品品种档案监管过程中隐私保护方案的新设计, 便于药企申报和应检生产工艺相关数据的同时也做到了方案的隐私保护。

2 预备知识

2.1 区块链技术

区块链是一种采用链式存储结构的连续区块存储, 实际上是一个去中心化的分布式数据库系统, 由网络中的分布式节点通过共识机制参与数据处理。由于区块链具有去中心化、防篡改性、匿名性以及可溯源性等[12]特点, 使得它在金融机构、智能家

居、产业链等方面具有良好的应用前景。

根据成员加入方式的不同, 区块链可以分为公有链、私有链和联盟链[13]。公有链是完全去中心化的一种区块链, 各个节点均可自由加入或退出网络, 并参加链上数据的读写, 常见的应用如比特币、以太坊等。私有链是对单独的个人或实体进行开放的区块链系统, 由中心管理者进行统一管理限制, 一般认为跟传统中心化记账系统的差异不明显。联盟链是指由多个机构共同参与管理的区块链, 节点只有经过授权后才能加入或退出网络。

本文设计方案基于联盟链平台 Hyperledger Fabric, 各个实体在联盟链中进行药品品种信息的维护与共享, 也能够方便检查员在检查的过程中进行信息核对。国家食品药品监督管理总局数据中心拥有自己的数据库, 数据库里存储着有关药品品种工艺、成分及各种审查信息。多个数据源及调用方组成联盟并构建了一个联盟链来存储药品品种信息的安全索引。

2.2 可截取签名

Steinfeld 等人[5]在 2001 年首次提出可截取签名的概念。它能够解决在多方参与的情况下, 签名数据在签名者、签名持有者以及签名验证者之间多次传输、签名和验证过程中, 计算存储开销大, 同时可能存在安全风险的问题。

为了能从初始的签名中计算出截取签名, 一种实现方式是签名者将消息拆分为多个子消息, 然后依次对这些子消息进行签名, 再把签名传给截取者, 对子消息签名截取之后最终交给验证者进行验证。在这个过程中, 如果不能对消息的截取规则进行限制, 将很容易导致消息被截取者恶意截取进而泄露隐私。因此, 文献[5]又引入了内容截取访问结构(Content Extraction Access Structure, CEAS)来限制截取者对原消息的截取过程。截取访问结构中, 通过“1”来表示签名消息中的“必选”子段, 而用“0”来表示消息中的“可选”子段。截取者根据 *CEAS* 规则生成截取子集 $CI(M^{'})$ 及截取消息 $M^{'}$, 截取消息中的子消息排列顺序必须和原消息中的子消息一致, 并且合法的截取方式应该满足 $CEAS \subseteq CI(M^{'})$。例如 $M=(m_1,m_2,m_3,m_4,m_5)$, $CEAS=\{1,0,1,0,0\}$, $CI(M^{'})=\{1,0,1,0,0\}$ 和 $M^{'}=(m_1,m_2,m_3,m_4,m_5)$ 是合法的截取方式, 而 $CI(M^{'})=\{1,0,1,1,0\}$ 和 $M=(m_1,m_2,m_3,m_4,m_5)$ 也是合法的, 其中?是截取之后的任意填充消息。

一个通用的可截取签名方案共有签名方、截取方和验证方三个实体以及 4 个步骤组成:

1) 密钥生成(*Gen*): 输入安全参数 1^k, 生成并输出公私钥对 (PK,SK)。

2) 签名生成(*Sig*): 输入私钥 *SK*、消息 *M* 和截取访问规则 *CEAS*, 输出一个可截取的全局签名 σ_F。

3) 签名截取(*Ext*): 输入公钥 *PK*、原消息 *M*, 根据截取者给出的截取子集 $CI(M^{'})$, 输出截取消息 $M^{'}$ 的截取签名 σ_{EXT}。

4) 签名验证(*Ver*): 输入公钥 *PK*、截取消息 $M^{'}$ 和截取的签名 σ_{EXT}, 输出签名验证结果。

3 本文方案

本节介绍基于 Hyperledger Fabric 联盟链的药品品种管理模型设计, 给出区块链上的交易单结构, 并据此设计链上的智能合约, 最后基于该模型的安全目标提出本文方案。

3.1 基于区块链的药品品种管理模型

根据目前药品品种档案管理过程中的一般环节, 将管理模型参与方设定为药企、数据中心、核查中心、药审中心、受理中心和其他数据使用单位六大部分, 成员管理服务商 CA 中心给除了药企之外的五种角色进行注册并颁发证书, 药企不作为链中的节点加入联盟链。各节点之间的数据上链之后可以实时共享, 保证了数据真实性的同时还实现了数据的有效追溯。将基于联盟链的可信可控药品品种档案信息管理模型的整体架构主要分为三层, 分别是数据接入层、数据服务层和用户应用层, 整体架构如图 1 所示。

其中, 数据接入层的数据来源于药品审批报送、检查、调用的整个生命周期消息记录, 使用区块链上的格式进行封装后, 结合加密算法与时间戳的方式将数据上传至区块链中。

数据服务层引入 Hyperledger 社区的开源项目 Baas 区块链管理平台, 实时监控并动态配置区块链网络中的节点与链码, 其系统架构如图 2 所示。

该平台是基于 Spring Boot 后端框架和 fabric-java-sdk 1.4.0 开发的, 通过将构建的区块链网络文件路径及相关配置添加到 Baas 平台配置文件的中 fabric-path 路径下, 可以对区块的生成, 出块时间和出块大小进行设置。将前端界面编译部署到 Nginx 反向代理服务器上, 利用可视化界面对网络中的节点和链码进行管理。与此同时, 采用时间戳和非对称加密技术, 提高药品信息安全性的同时也确保了数字签名的归属性。

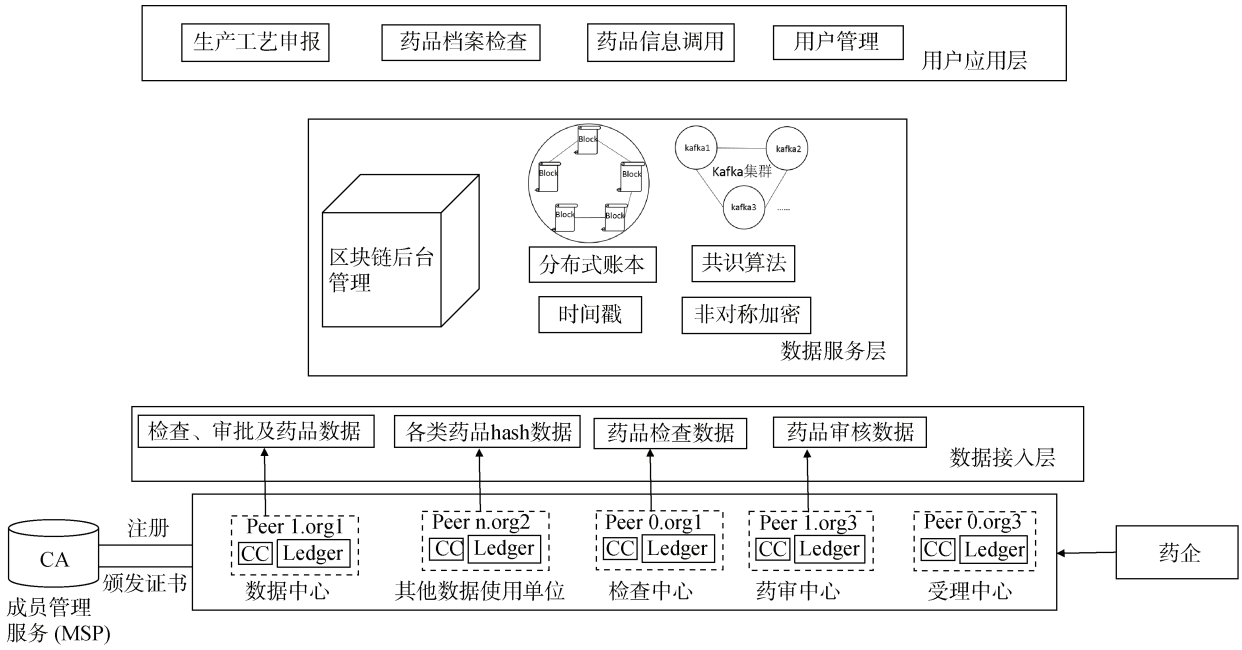


图 1　药品管理模型整体架构

Figure 1　The overall architecture of the drug management model

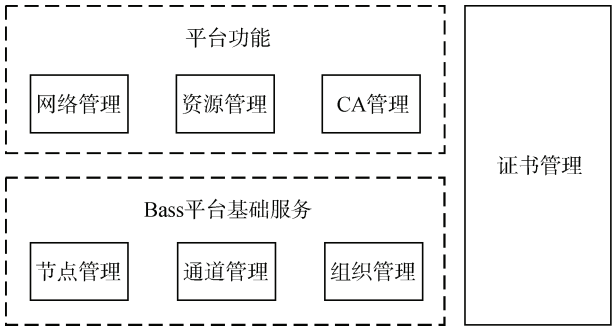


图 2　Bass 平台系统架构图

Figure 2　The architecture diagram of Bass platform

用户应用层的信息管理系统向药企、药审中心提供药品生产工艺的申报及其检查、药品信息的调用等服务支撑。这三层架构共同作用, 确保了药品信息档案的真实性以及安全性。

具体来看, 提出的药品档案模型中主要包括三类角色。首先是管理方, 本文方案中指国家食品药品监督管理总局数据中心; 其次是数据源以及数据调用方, 包括药企、核查中心、受理中心和各省市药审中心; 最后是业务人员, 本方案中为核查中心的检查员。除药企之外其余角色均能接入食药监区块链, 数据源即药企可以发起对药品数据的更新, 而总局数据中心能够限制模型中管理员对于数据的修改权限。药企自留的数据库中存有自己的药品生产工艺的原文件, 原文件不上链, 而食药监区块链中仅存储药品部分种类信息、生产工艺的 hash 值和相关品种药品的检查审批数据, 仅总局数据中心能够对数据进行最终的入库操作, 以此来避免错误或不完整的数据进入数据库。图 3 为药品品种档案管理模型总体业务流程。

药企。药企作为数据源, 是食药监区块链的核心, 但是其自身并不作为区块链节点加入。当有药品品种信息需要申报时, 首先需要将诸如批准文号、生产工艺、成分等相关信息交由受理中心受理, 受理中心必须在区块链 CA 中心提前注册并拿到证书。之后受理中心为其生产工艺生成 hash 值, 以药品的批准文号作为主键, 签名加密之后上传至食药监区块链, 并交由药审中心二次审核。

受理中心。受理中心需要在区块链 CA 中心注册身份, 有了合法的身份及证书之后, 才有权接收药企的申报请求。在收到药企的生产工艺原文件之后, 会生成 hash 值并上传至食药监区块链, 同时将生产工艺原文件传递给各省市药审中心进行下一步操作。

药审中心。药审中心扮演承上启下的角色, 对有错误或者不完整的数据进行过滤, 同时查询区块链上的 hash 值进行校验, 校验通过之后, 才会将生产工艺原文件报送至食品药品监管总局进行最后地校对入库。

核查中心。核查中心设立的目的是为了用一种快捷的方式来验证药企所提供的生产工艺文件的真实性。核查中心的高级管理员指派任务, 内容包括对生产工艺的验证和查询等给隶属于核查中心的检查员。检查员不需要接触到总局数据中心数据库的原

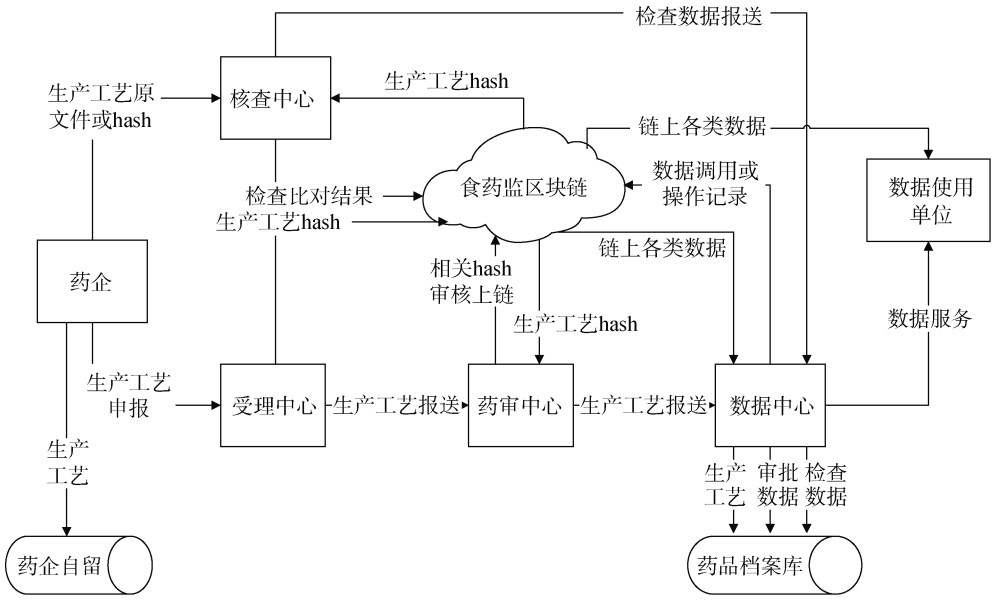


图 3　药品品种档案管理模型总体业务流程

Figure 3　The overall business process of the drug variety archives management model

文件就可以进行离线的验真操作, 如果有需要, 检查员还可以在一定程度受控的前提下, 下载药品的生产工艺数据进行更加详细地比对。

数据中心。整个食药监区块链中只有一个总局数据中心, 检查员、受理中心和药审中心将药企的相关药品品种信息上链后都会提交到数据中心, 由总局数据中心将生产工艺、审批数据和检查数据校验后存入药品档案数据库, 当有外网或专网用户调用档案库中的数据时, 数据中心会将数据操作记录和调用记录上链, 明确数据报送、入库、使用等相关操作经手人员的责任, 并保证涉及药企机密的重要数据不被非法篡改和删除。

其他数据用户。当其他数据用户需要获得有关链上的 hash 值时, 首先需要在区块链上注册得到合法身份, 然后才可以接入区块链。对于其他数据用户, 能够按多种方式查询到相应药品的档案数据, 既可以直接查询链上公开的数据, 也可以通过向总局数据中心进行数据调用申请, 必要的话, 数据中心能够向有权限的用户提供专网的数据下载服务。

3.2　区块链上交易表单结构及智能合约设计

区块链上的表单按照功能性的不同大致分为三类, 涵盖了药审中心、数据中心及核查中心这三类角色, 并按照这三类表单设计链上的智能合约。

第一类是药品数据报送与入库表单, 由四部分组成, 批准文号 *Id*(药监局提供), 生产工艺哈希值 *Hash*, 数据来源 *Operator*, 报送操作时间 *Time*, 如表 1 所示。为了保护生产工艺的私密性, 都是通过将原文件转换为 Hash 值的形式存储在链上的。

表 1　药品数据报送与入库表单

Table 1　Drug data submission and storage form

批准文号	哈希值	数据来源	操作时间
Id	*Hash*	*Operator*	*Time*

药品信息上传合约设计中的结构体存储字段即为上表 1 中所列的 4 种信息, 为了在各个机构之间共享真实的数据, 药审中心使用新增函数 put 将药品的档案数据上链, 链上的成员使用查询函数 query 获取链上已存在的药品信息, 总局数据中心使用背书函数 endorse 对药品相关信息进行二次验真并上链。

第二类是药品信息专网的调用表单, 由五部分组成, 药品的批准文号 *Id*, 调用数据的操作时间 *Time*, 调用数据的部门 *Dept* 和用户 *Operator*, 具体的操作内容 *Operation* 包括查询和下载等, 如表 2 所示。此类表单的主要目的是为了记录数据的使用情况。

表 2　药品信息专网调用表单

Table 2　The form of drug information call in the private network

批准文号	操作时间	部门	用户	操作内容
Id	*Time*	*Dept*	*Operator*	*Operation*

药品调用合约设计中的结构体存储字段即为表 2 所述的 5 部分信息, 为了记录药品档案数据的使用情况, 使用新增函数 create 将药品数据的初始记录上链, 当有链上成员调用或下载数据时, 使用追加函数 append 覆盖原有药品批准文号所对应的相关信息, 使用查询函数 query 可以获取药品档案的历史记录,

并提取批准文号所对应的各个版本的值。

第三类表单是用于药品核查过程，由六部分组成，分别是任务编号 *TaskId*，检查员 *Inspector*，药品的批准文号 *Id*，任务内容 *Operation*，任务截止时间和当前品种药品生产工艺的哈希值 *Hash*，如下表 3 所示。同时，对于检查员来说，需要将检查结果上链，因此也需要一个表单，包括任务编号，检查员，上传对比的 Hash 值，对比的结果一致或不一致，是否下载了原文件，以及任务的完成时间，如下表 4 所示。

表 3　药品核查过程使用的表单

Table 3　The form used in the drug verification process

任务编号	检查员	批准文号	任务内容	截止时间	当前 Hash
TaskId	*Inspector*	*Id*	*Operation*	*Deadline*	*Hash*

表 4　检查员上链的检查结果表单

Table 4　The inspection form uploaded by the inspector

任务编号	检查员	上传 Hash	对比结果	是否下载文件	完成时间
TaskId	*Inspector*	*DiffHash*	*DiffStatus*	*IsDownload*	*SubmitTime*

药品检查合约设计中涉及到的结构体存储字段即为表 3 和 4 所述的两类表单内容。为了验证药品档案数据上报的真实性，使用新增函数 create 新建任务，存储任务编号及其所对应的结构化数据，使用提交函数 submit 提交已完成的任务，并追加检查信息至对应的编号任务，使用查询函数 query 查看任务编号所对应的完整任务信息。

3.3　安全目标

可截取签名在药品监管场景下的应用如图 4 所示。签名持有者，此处为药企，可以对药监局已签署过的消息进行独立操作，而无需和签名方药监局交互。签名持有者能够出于个人的使用目的，截去不同部分的子消息，形成不同的可验证的截取消息及其签名，并且对于场景中其他的验证者来说，仍然可以从新的签名消息中验证其有效性。

针对上述应用场景，本文方案的安全目标如下。

数据的保密性和有效性。无论药品品种档案是存储在数据库还是通过外网传输到区块链上，其他数据使用单位均无法随意修改药品品种档案信息。在本文的可截取签名方案中，攻击者无法获取原消息中未被截取的部分。即使允许在截取消息中用不相关的信息填补没有被选中的子消息段，攻击者也无法通过此不相关消息计算出子消息的内容。因此，CES 签名方案可以保持消息的保密性与有效性。

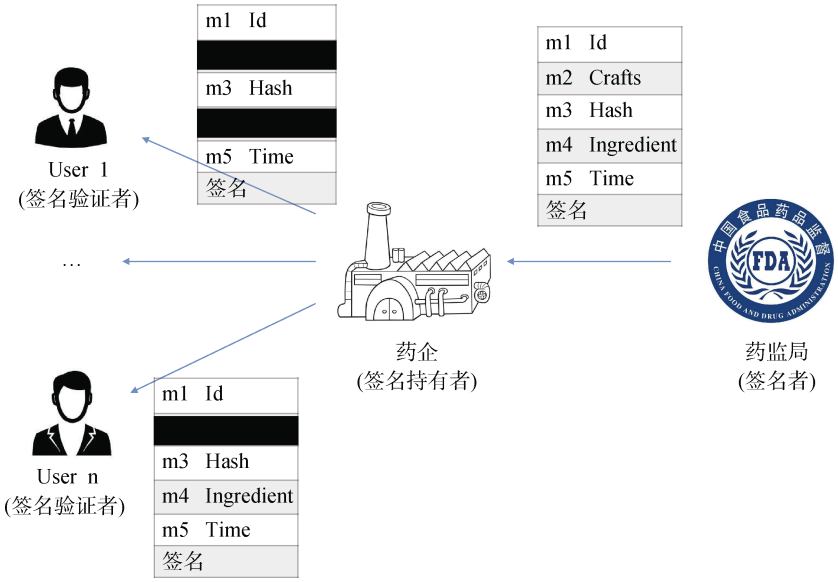


图 4　可截取签名在药品监管中的应用场景

Figure 4　Application scenarios of context extraction signature in drug supervision

访问控制。为防止未经授权的用户对药品的品种档案信息进行非法访问，对档案信息需要进行访问控制设置，使数据访问活动始终在总局数据中心的参与和监控之下进行。通过成员管理服务认证 CA 中心为不同身份、不同角色的有效用户进行身份认证、颁发证书，用这样的授权方式来实现访问控制。

隐私保护。由于药品品种档案信息中包含药品生产工艺、成分等一些隐私敏感的信息，因此在报送、检查药品信息的同时，也要注重保护药品相关的隐私。此外，原始的药品生产工艺、成分等信息不能

够透露给不相关的非法实体。

3.4 基于区块链的可截取药品品种管理方案

基于可截取签名方案和上述安全目标, 构建基于区块链的可截取签名药品隐私保护方案。本方案弃用了复杂耗时的双线性对运算和模幂运算, 参考无证书签名方案[17], 选择简单的标量乘与模逆运算来保证方案的安全, 大大减少了计算量, 显著提升了方案的运行效率。同时, 结合无证书密码体制, 避免了密钥托管带来的弊端, 更好地保障了方案的安全性。使用到的全局变量参数如表 5 所示。

表 5 全局变量参数

Table 5 Global variable parameter

参数	含义
l	方案的安全参数
p	有限域 F_q 中的大素数
s	方案的主密钥
$H(\bullet)$	单向抗碰撞 hash 函数
P_{pub}	方案中的公钥
R_i	NM 部分公钥
D_i	用户 ID_i 的部分私钥
x_i	用户 ID_i 选择的秘密值
SK_i	用户 ID_i 的私钥
PK_i	用户 ID_i 的公钥
M	所要签名的原消息
h_{1i}	原消息中每个子消息的哈希值
$\overline{M}$	签名原消息 M 的散列值
M'	M 被截取之后的截取消息
σ	原消息 M 的全局签名
σ_{EXT}	原消息 M 截取之后的截取签名
y_i	签名方选择的自己保存的随机数

基于可截取签名的药品管理隐私保护方案共可分为 3 个阶段: 方案初始化、信息上报、检查共享。

阶段 1 方案初始化

本阶段分为参数设置和成员注册相关 4 个步骤, 初始化主要由网络管理者(Network Manager, NM)负责生成方案的公共参数, 注册则由 Fabric 中的 CA 中心(Certificate Authority, CA)负责。如下图 5 所示, 详细描述如下:

1) 参数设置。给出一个安全参数 l, NM 选择一条在有限域 F_q 上的椭圆曲线, 生成一个阶为 p 的域上的加法群 G, 其中 q 为 l 位比特的大素数, 群 G 的生成元为 P。随后再随机选择主密钥 $s\in Z_q^*$ 和 5 个抗碰撞哈希函数: $H_0\sim H_4$, 其中 $H_0:\{0,1\}^*\times G^2\to Z_q^*$, $H_1:\{0,1\}^*\to\{0,1\}^k$, $H_2:\{0,1\}^*\to\{0,1\}^k$, $H_3:\{0,1\}^*\times\{0,1\}^*\times G^2\to Z_q^*$, $H_4:\{0,1\}^*\times\{0,1\}^*\times G^2\to Z_q^*$, 然后计算 $P_{pub}=sP$ 作为方案中的公钥。主密钥 s 由网络管理者 NM 秘密保存, 同时公开参数 $params=\{F_q,G,P_{pub},P,H_0,H_1,H_2,H_3,H_4\}$

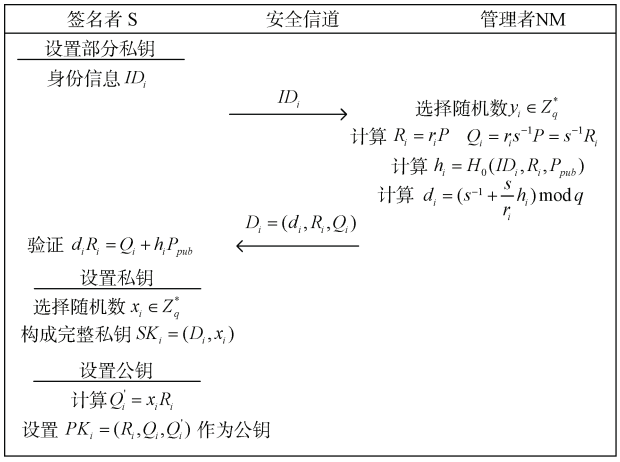


图 5 所提方案中方案初始化的密钥设置阶段

Figure 5 The key setting phase of the scheme initialization in the proposed scheme

2) 数据中心向 NM 注册

a) 输入公开参数 $params$, 主密钥 s 和食药监总局数据中心(以下简称总局数据中心)的身份信息 ID_i, 网络管理者 NM 产生一个随机数 $r_i\in Z_q^*$, 计算 $R_i=r_iP$, 称之为 NM 部分公钥, 计算 $h_i=H_0(ID_i,R_i,P_{pub})$, $Q_i=r_is^{-1}P=s^{-1}R_i$, $d_i=(s^{-1}+\frac{s}{r_i}h_i)\bmod q$, 并将生成的部分私钥 $D_i=(d_i,R_i,Q_i)$ 秘密的发送给总局数据中心 ID_i。

b) 随后, 总局数据中心 ID_i 会选择一个随机数 $x_i\in Z_q^*$ 作为自身的秘密值, 计算 $Q_i'=x_iR_i$, 将 $PK_i=(R_i,Q_i,Q_i')$ 作为自身的完整公钥并连同自己的身份信息 ID_i 一同发送给网络管理方 NM。

c) 对于接收到的部分私钥 D_i, 总局数据中心 ID_i 会验证等式 $d_iR_i=Q_i+h_iP_{pub}$ 是否正确。若正确, 则接收部分私钥, 并设置数据中心的完整私钥 $SK_i=(D_i,x_i)$; 否则, 终止算法。

3) 总局数据中心向 CA 中心注册。

CA 中心首先会验证接收到的总局数据中心的完整公钥和身份信息 ID_i, 验证通过后将会为其颁发

有效的注册证书 $ECert_i=(ID_i,PK_i,Sig_i)$，其中 Sig_i 为 CA 中心结合用户信息给请求证书的用户所颁发的签名，链上的用户均需要如此向 CA 注册。

4) 药企向网络管理者 NM 注册。

药企选择有限域上的一个随机数 $z_i\in Z_q^*$，并将其作为自己的私钥 $SK=z_i$，同时计算公钥 $PK=z_iP$，形成公私钥对用来安全地传递药品品种信息。

阶段 2　药品品种信息上报

本阶段分为药品品种信息的创建和签名截取 2 个步骤，药企在对药品品种信息进行申报或更新时，会将信息通过受理中心传递给药审中心，由药审中心为其创建药品的品种信息，包括数据来源、药品通用名称、药品批准文号、生产单位、药品成分、生产工艺、生产工艺文件哈希值、上链时间、上链状态等等，记为 $M=\{m_1,m_2,\cdots,m_n\}$。当药审中心需要将收到的药品信息上链时，首先要向 CA 中心的 MSP 提供申请，MSP 通过注册证书 $ECert_i$ 来为其生成匿名交易证书 $TCert_i$ 及派生公私钥对 (PK_{FID_i},SK_{FID_i})，以此来完成以交易假名 FID_i 为身份的匿名化，保证用户交易过程中的隐私。

本方案采用改进可截取签名算法对原始药品品种信息进行签名，再通过安全信道传递给药企。这样，作为签名的唯一持有者，只有药企可以在不破坏签名合法性的情况下，对药品数据中的隐私信息进行截取，保证了药品品种信息在检查过程中诸如药品生产工艺、药品成分等隐私信息不被泄露。当然，为了避免药企进行恶意截取，作为签名方的总局数据中心可以设定适当的内容截取规则 *CEAS*，固定保留数据来源、药品批准文号等重要的字段信息。签名生成和截取的具体过程如下图 6 所示，详细描述如下:

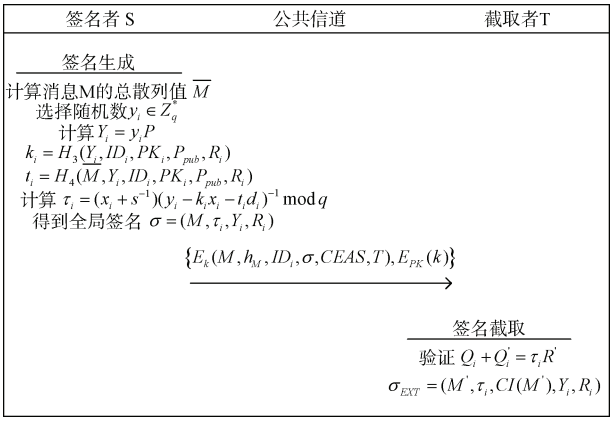


图 6　所提方案中签名生成与截取阶段

Figure 6　The signature generation and interception stage in the proposed scheme

1) 签名生成

假设签名方总局数据中心 ID_i 要为消息 $M=\{m_1,m_2,\cdots,m_n\}$ 签名，执行的操作如下:

a) 首先需要计算消息 M 的所有子段消息 $m_i(i\in[1,n])$与内容截取访问结构 *CEAS* 组成的哈希值 $h_{1i}=H_1(m_i\|CEAS)$，然后将他们按照编号依次异或级联 $h_{11}\oplus h_{12}\oplus\cdots\oplus h_{1n}$，最后计算级联后完整消息总的散列值 $\overline{M}=H_2(h_{11}\oplus h_{12}\oplus\cdots\oplus h_{1n})$。

b) 作为签名者的总局数据中心得到散列值 $\overline{M}$ 之后，随机选择 $y_i\in Z_q^*$ 并计算 $Y_i=y_iP$。

c) 计算签名所需参数

$$k_i=H_3(Y_i,\ ID_i,\ PK_i,P_{pub,}R_i)$$

$$t_i=H_4(\overline{M},Y_i,ID_i,PK_i,P_{pub},R_i)$$

d) 计算部分签名 $\tau_i=(x_i+s^{-1})(y_i-k_ix_i-t_id_i)^{-1}\bmod q$，如果 $\tau_i=0$，则重新选取 y_i 并返回最初的步骤 a)；否则，输出消息 M 的全局签名 $\sigma=(M,\tau_i,Y_i,R_i)$。

2) 签名截取。

全局签名并不会直接发送给药企，总局数据中心会选择一个随机数 $k\in Z_q^*$ 作为自己的对称密钥，对签名进行加密，同时通过药企的公钥加密 k 以安全传送给药企。利用对称密钥加密的信息包括原始的品种档案信息 M 及其 *hash* 值 $h_M=H_1(M\|ID_i)$，总局数据中心的身份信息 ID_i，消息 M 的全局签名 σ，截取访问结构 *CEAS* 及发送时间 *T*，即最后发的消息为 $\{E_k(M,h_M,ID_i,\sigma,CEAS,T),E_{PK}(k)\}$。

药企在收到总局数据中心发来的两个密文之后，会先用自己的私钥 *SK* 解密 $E_{PK}(k)$ 得到加密信息所用的对称密钥，然后用对称密钥解密得到药品的档案信息，并进行数据的有效性和正确性分析。首先，计算 $h_M'=H_1(M\|ID_i)$，判断 $h_M'=h_M$ 是否成立，据此可判断原档案信息有无被篡改。然后，计算散列值 $\overline{M}$，哈希值 k_i 和 t_i，最后验证等式 $Q_i+Q_i'=\tau_iR'$ 是否成立，其中 $R'=Y_i-k_iQ_i'-t_iQ_i-t_ih_iP_{pub}$。如果不成立，则终止操作；如果成立，则药企作为截取者继续以下操作:

a) 根据内容截取访问结构 *CEAS* 构造截取子集 $CI(M')$。

b) 构造完截取子集 $CI(M')$ 之后，结合原消息

$M=\{m_1,m_2,\cdots,m_n\}$ 构造截取消息 $M^{'}=\{m_1^{'},m_2^{'},\cdots,m_n^{'}\}$。对属于截取子集中的子段, 即 $i\in CI(M^{'})$ 时, 令 $m_i^{'}=m_i$, 而未被截取的子段, 则用 $m_i^{'}=H_1(m_i\|CEAS)$ 表示。

c) 之后生成截取消息 $M^{'}$ 的截取签名 $\sigma_{EXT}=(M^{'},\tau_i,CI(M^{'}),Y_i,R_i)$。

阶段 3　信息检查及共享

本阶段主要是检查员作为验证者, 根据截取签名来恢复验证消息的合法性并将检查结果上链, 如下图 7 所示, 详细描述如下:

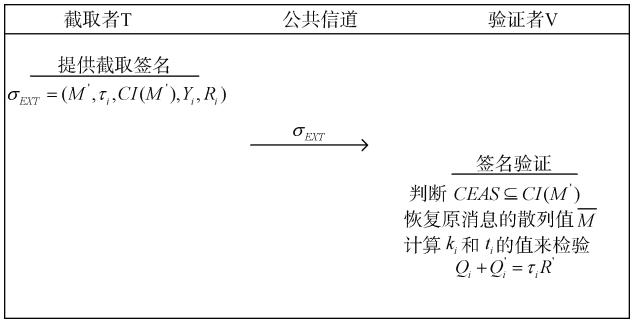


图 7　所提方案中签名验证阶段

Figure 7　The signature verification stage in the proposed scheme

核查中心的检查员作为验证者来到药企之后, 对企业提供的截取签名 σ_{EXT} 需要先判定其合法性。首先判断内容截取访问结构 $CEAS$ 是否包含于截取子集 $CI(M^{'})$, 即 $CEAS\subseteq CI(M^{'})$, 若不包含, 则终止算法, 否则继续。然后根据截取子集 $CI(M^{'})$ 和截取消息 $M^{'}$ 来恢复原消息的散列值 $\overline{M}$, 方法如下: 当 $i\in CI(M^{'})$, 那么 $m_i=H_1(m_i^{'}\|CEAS)$, 否则保留原来截取消息中的 $m_i^{'}$ 即令 $m_i=m_i^{'}$, 按截取消息从左往右的顺序异或即可得到原消息的散列值 $\overline{M}=H_2(H_1(m_1\|CEAS)\oplus H_1(m_2\|CEAS)\oplus\cdots\oplus H_1(m_n\|CEAS))$。最后按照签名生成阶段的算法计算 k_i 和 t_i 的值, 通过这两个哈希值检验 $Q_i+Q_i^{'}=\tau_i R^{'}$ 正确与否, 其中 $R^{'}=Y_i-k_iQ_i^{'}-t_iQ_i-t_ih_iP_{pub}$。若不正确, 则认为 σ_{EXT} 是无效的, 上报总局数据中心, 并申请生产工艺原文件下载, 进行进一步检查。若正确, 则截取签名 σ_{EXT} 有效, 此时展开检查, 对比药品品种信息中的 hash 值与链上查询得到的 hash 值是否一致, 不管一致与否, 都会将此次的检查结果上传至联盟链, 若不一致, 有权向总局数据中心申请下载原文件, 进行进一步检查。

由此, 针对管理模型中的不同身份, 利用区块链上的智能合约和可截取签名的新型设计为他们分别指定了不同的操作方式, 如下表 6 所示。

表 6　本文方案中药品品种档案的操作类型

Table 6　Operation types of drug variety archives in our scheme

档案数据	操作者	操作
药品信息	药企	更新、查询
	受理中心	查询
	数据中心	查询
	药审中心	查询、下载
	数据中心	查询
调用记录	药审中心	更新、查询
	核查中心	更新、查询
检查数据	药企	查询
	核查中心	更新、查询
	数据中心	查询、下载

4　安全性分析

4.1　方案的正确性

截取过程中使用以下关系进行原消息 M 的每个子段消息 m_i 的替换:

$$m_i^{'}=\begin{cases}m_i, & i\in CI(M^{'})\\ H_1(m_i\|CEAS), & i\notin CI(M^{'})\end{cases}$$

而在验证过程中使用的是以下关系来恢复截取消息 $M^{'}$ 中的每个子段 m_i:

$$m_i=\begin{cases}H_1(m_i^{'}\|CEAS), & i\in CI(M^{'})\\ m_i^{'}, & i\notin CI(M^{'})\end{cases}$$

由以上这两个关系式可以得出验证阶段的值均为 $H_1(m_i\|CEAS)$, 这与截取阶段的值是一致的, 也就保证了两个阶段的总散列值 $\overline{M}$ 是相等的。

上述方案中用于验证截取签名有效性的验证等式是可以确保是正确的, 推导过程如下:

$$\begin{aligned}R^{'}&=Y_i-k_iQ_i^{'}-t_iQ_i-t_ih_iP_{pub}\\&=y_iR_i-k_ix_iR_i-t_is^{-1}r_iP-t_ih_isP\\&=y_iR_i-k_ix_iR_i-r_it_i(s^{-1}-h_i\frac{s}{r_i})P\\&=y_iR_i-k_ix_iR_i-t_id_iR_i\\&=(y_i-k_ix_i-t_id_i)R_i\end{aligned}$$

因此, $\tau_iR^{'}=(x_i+s^{-1})R_i=Q_i+Q_i^{'}$ 等式是可验证的, 由此也说明了上述基于可截取签名的药品隐私保护方案中采用的可截取签名是正确的。

4.2 敌手模型

通常, 基于可截取签名的隐私保护方案中存在两种类型的攻击模型[14], 第一类型攻击和第二类型攻击。第一类型的攻击者是普通的恶意用户, 无法获得方案中的主密钥 s, 但是可以自己选择某个特定的值替换一个实体的公钥。第二类型的攻击者是某个恶意的CA中心, 能够知道方案的主密钥 s 值的大小, 但是不能够随意替换其他实体的公钥。对于可截取签名方案的安全性讨论, 一般会分别以攻击者在以下两种挑战中的不同表现来判断:

挑战 1: 敌手 α_1 进行此项挑战的目的是通过构建挑战者 β 破解签名方案的安全性。α_1 与 β 相互配合, α_1 会提交一些询问给 β, β 会返回相应的回答, α_1 结合这些回答能够破解签名方案的安全机制。大致的流程如下:

初始化阶段: 一开始, NM 使用安全参数 l 产生一些公共参数、主密钥 s 及其对应的公钥 P_{pub}, 敌手 α_1 能够掌握的只有公共参数。

询问阶段: 敌手 α_1 不仅可以查询到任何输入数据的哈希值, 而且能够针对性的选择以下事件进行询问, 包括部分私钥询问、秘密值询问、公钥询问、公钥替换询问、签名询问以及签名截取询问。

输出阶段: 最终, 敌手 α_1 生成对所选身份的伪造签名 (ID_i, M', σ'), 若满足以下两个条件, 那么即视作获得本次挑战的胜利:

(1) 关于目标身份的部分私钥询问和伪造消息的签名询问从来没有被提交过;

(2) 在公钥被替换的情况下, 伪造消息的签名验证依然能够通过。

定义 1。抗第一类型攻击安全: 对于可截取签名方案, 在任意多项式时间内, 第一类型敌手赢得挑战 1 的概率不可忽略的, 则认为该签名方案对于第一类型攻击是安全、不可伪造的。

挑战 2: 挑战 2 和挑战 1 类似, 除了敌手模型不同, 挑战 2 的敌手 α_2 知道 CA 中心主密钥的值, 同时也可以计算任意用户的部分私钥, 挑战 2 的大致流程如下:

初始化阶段: NM 使用安全参数 l 产生一些公共参数、主密钥 s 及其对应的公钥 P_{pub}, 敌手 α_2 知道主密钥 s 以及公开参数。

询问阶段: 敌手 α_2 同样可以查询到任何输入数据的哈希值, 每次可以执行一次相关询问, 包括部分私钥询问、秘密值询问、公钥询问、签名询问以及签名截取询问, 但不能提交公钥替换的询问。

输出阶段: 最终, 敌手 α_2 生成选定身份的伪造签名 (ID_i, M', σ'), 如果满足以下条件, 则视为获得本次挑战的胜利:

(1) 关于目标身份的秘密值和伪造消息的签名询问从来没有执行过;

(2) 伪造消息的签名是有效的, 可以通过验证。

定义 2。抗第二类型攻击安全: 对于可截取签名方案, 在任意多项式时间内, 第二类型敌手赢得挑战 2 的概率是不可忽略的, 则认为该签名方案对于第二类型攻击是安全、不可伪造的。

定义 3。可截取签名方案安全: 在任意多项式时间内, 一个无证书可截取签名方案可以同时抵御第一类挑战的敌手和第二类挑战的敌手, 则认为该签名方案对于选择消息和身份的攻击是安全、不可伪造的。

4.3 安全性证明

(1) 不可伪造性

定理 1: 本文提出来的隐私保护方案能够在给定随机数据模型的情况下抵御第一类攻击, 考虑到求解椭圆曲线离散对数问题(ECDLP)的困难性。

证明 1: 假设存在一个攻击者 α_1, 能够在多项式时间内以一个不可忽略的概率 ε_1 破解本文中的签名方案。目标是 α_1 利用挑战者 β 能够解决 ECDLP 困难问题, 即给出一个 β 已知的 ECDLP 实例 $\psi = (P, P_{pub})$, α_1 通过构建一个挑战者 β 求解出 s 满足 $P_{pub} = sP$。

初始化阶段。在此阶段, 当攻击者 α_1 发起对 ECDLP 元组 ψ 的挑战时, 它首先会创建两个状态机列表, 在 L_C 中记录 $(ID_i, R_i, Q_i, Q_i', x_i, d_i)$, 在 L_H 中记录 $(ID_i, R_i, Q_i, Q_i', h_i)$。一开始, 列表 L_C 和 L_H 中是空的。随后, 挑战者 β 模拟方案初始化过程, 生成一系列公共参数 $params = \{G, P_{pub}, P, H_0, H_1, H_2, H_3, H_4\}$, 然后把参数传递给 α_1, 并随机选取一个参与第一类攻击的挑战身份 ID^*, 且不会泄露给 α_1。至此, 攻击者 α_1 将通过挑战者 β 来解决 ECDLP 问题。

询问阶段。在这个阶段, 攻击者 α_1 会进行一系列的询问, 而 β 维护着一些初始值为空的询问机列表 $L_{H_0} \sim L_{H_4}$ 和上一阶段中的列表 L_C、L_H, 以此来实现算法的快速响应并保持数据一致性。

(1) 创建用户询问。当 α_1 提交一个对身份 ID_i 的询问时, 挑战者 β 会做出以下回应:

若 $ID_i = ID^*$，β 选取随机数 $r_i, x_i, h_i \in Z_q^*$ 并计算 $R_i = r_i P$，$Q_i = h_i P_{pub}$，$Q_i^{'} = x_i R_i$，令 $h_i = H_0(ID_i, R_i, P_{pub})$，$D_i = (d_i, R_i, Q_i)$。

若 $ID_i \neq ID^*$，β 选取随机数 $x_i, r_i, a, b \in Z_q^*$，令 $d_i = a$，$h_i = H_0(ID_i, R_i, P_{pub}) = -b \bmod q$，然后计算 $R_i = r_i P$，$Q_i = aR_i + bP_{pub}$，$Q_i^{'} = x_i R_i$，可以看到，此处的 (d_i, R_i, h_i) 总是满足 $d_i R_i = Q_i + h_i P_{pub}$。

最后，β 更新状态机列表 L_H 和 L_C，在列表 L_C 中记录 $(ID_i, R_i, Q_i, Q_i^{'}, x_i, d_i)$，在列表 L_H 中记录 $(ID_i, R_i, Q_i, Q_i^{'}, h_i)$。

(2) H_0 询问。对于 α_1 询问的回复，β 先查看自己维护的列表 $list_{H_0}$ 中是否有表项 (ID_i, R_i, Q_i, h_i)，如果有，直接返回 h_i 给 α_1；如果没有，选择一个随机数 $h_i \in Z_q^*$ 给 α_1，并且把 (ID_i, R_i, Q_i, h_i) 添加到 $list_{H_0}$ 表项。

(3) H_1 询问。β 维护一个存储着 $(m_i, CEAS, h_{1i})$ 的列表 $list_{H_1}$，当收到 α_1 的询问时，β 先查看 $list_{H_0}$ 中有无表项 $(m_i, CEAS, h_{1i})$，如果有，直接返回 h_{1i} 给 α_1；否则，选择一个随机数 $h_{1i} \in Z_q^*$ 给 α_1，并且把 $(m_i, CEAS, h_{1i})$ 添加到 $list_{H_1}$ 中。

(4) H_2 询问。对于 α_1 询问的回复，β 先查看自己维护的列表 $list_{H_2}$ 中是否有表项 $(h_{1i}, \overline{M})$，如果有的话，直接返回 $\overline{M}$ 给 α_1；否则，取任意的 $\overline{M} \in Z_q^*$，并将 $(h_{1i}, \overline{M})$ 添加到列表 $list_{H_2}$ 中。

(5) H_3 询问。β 维护一个存储着 $(Y_i, ID_i, PK_i, P_{pub}, R_i, k_i)$ 的列表 $list_{H_3}$，当收到 α_1 的询问时，β 先查看 $list_{H_3}$ 中有无表项 $(Y_i, ID_i, PK_i, P_{pub}, R_i, k_i)$，如果有，返回 k_i；否则，随机选择 $k_i \in Z_q^*$ 并添加 $(Y_i, ID_i, PK_i, P_{pub}, R_i, k_i)$ 到 $list_{H_3}$。

(6) H_4 询问。对于 α_1 询问的回复，β 先查看自己维护的列表 $list_{H_4}$ 中是否有表项 $(\overline{M}, Y_i, ID_i, PK_i, P_{pub}, R_i, t_i)$，如果有，返回 t_i；否则，随机选择 $t_i \in Z_q^*$ 并将 $(\overline{M}, Y_i, ID_i, PK_i, P_{pub}, R_i, t_i)$ 添加到 $list_{H_4}$。

(7) 部分私钥询问。攻击者 α_1 以身份 ID_i 发起此询问，β 会做出以下回应，如果 $ID_i = ID^*$，默认失败并终止模拟过程；若 $ID_i \neq ID^*$，β 查看创建用户中的表项 L_C，并返回 (d_i, R_i, Q_i) 给 α_1。

(8) 秘密值询问。α_1 发起询问时，β 将表 L_C 中对应的表项 $(ID_i, R_i, Q_i, Q_i^{'}, x_i, d_i)$ 里的秘密值 x_1 返回给 α_1。

(9) 公钥询问。攻击者 α_1 以身份 ID_i 查询公钥，首先 β 在自己的表项 L_C 中查看是否存在对应身份的信息，若有，则直接返回 $PK_i = (R_i, Q_i, Q_i^{'})$；如果没有，那么 β 执行创建用户询问，输出 $PK_i = (R_i, Q_s, Q_s^{'})$ 到 α_1，然后添加表项 $(ID_i, R_i, Q_i, Q_i^{'}, x_i, d_i)$ 到 L_C。

(10)公钥替换询问。如果攻击者 α_1 想用部分公钥 $Q_i^{''}$ 替换 ID_i 的部分公钥 $Q_i^{'}$，那么 β 会先查看自己的列表 L_C 和 L_H 中是否存在 (ID_i, PK_i)，若存在，则令 $Q_i^{'} = Q_i^{''}$，$Q_i = Q_i^{'}$，$x_i = x_i^{'}$，$R_i^{'} = r_i^{'} P$，然后将列表 L_C 和 L_H 中相应的表项更新为 $(ID_i, R_i^{'}, x_i^{'}, Q_i^{'}, Q_i^{''})$；若不存在，则执行一次关于公钥查询的询问，然后用 $(ID_i, R_i^{'}, x_i^{'}, Q_i^{'}, Q_i^{''})$ 覆盖列表 L_C 和 L_H 中相应的表项。

(11) 签名询问。当 β 收到从 α_1 发出的签名询问 $(ID_i, M, \tau_i, Y_i, R_i)$ 时，β 先查看列表 $list_{H_2}$ 找到表项消息的散列值 $\overline{M}$，然后查询身份 ID_i 的公钥是否被替换。若没有被替换，则 β 执行方案中的签名算法，并把签名 (M, τ_i, Y_i, R_i) 传递给 α_1；若已经被替换，β 选取随机数 $a, b, c \in Z_q^*$，然后令 $\tau = a$，$k_i = H_3(Y_i, ID_i, PK_i, P_{pub}, R_i) = b$ $t_i = H_4(\overline{M}, Y_i, ID_i, PK_i, P_{pub}, R_i) = c$，并且计算 $Y_i = (a^{-1} + c)Q_s + (a^{-1} + b)x_i R_i + ch_i P_{pub}$，更新列表 $list_{H_3}$ 和 $list_{H_4}$，然后将签名 (M, τ_i, Y_i, R_i) 传递给 α_1。

(12) 签名截取询问。α_1 接收到签名 (M, τ_i, Y_i, R_i) 之后，首先按照方案中的截取签名过程检验等式 $Q_i + Q_i^{'} = \tau_i R^{'}$ 是否成立，其中 $R' = Y_i - k_i Q_i^{'} - t_i Q_i - t_i h_i P_{pub}$。若不成立则终止模拟过程；若成立，$\alpha_1$ 根据内容截取访问结构 $CEAS$ 构建截取子集 $CI(M^{'})$，同时用方案中的替换方法得到截取消息 M'。然后返回消息 M' 的截取签名 $\sigma_{EXT} = (M^{'}, \tau_i, CI(M^{'}), Y_i, R_i)$。

伪造阶段。 α_1 在经过与 β 的询问交互之后，生成一个关于 (ID_i^*, M^*) 伪造的签名消息 $(M^*, \tau_i^*, Y_i^*, R_i^*)$，其中身份 ID_i^* 的伪造公钥是 $PK_i^* = (R_i^*, Q_i^{'}, Q_i^{''})$。当 $ID_i^* \neq ID^*$ 时，则 β 输出不合法并终止模拟过程；否

则, β 从列表 L_C 和 L_H 中取出相应的表项, 利用分叉引理[15](Forking Lemma)实现上述模拟过程的重放, β 可以构造另外两组相应有效的签名 $\sigma_1=(M^*,\tau_i^{'},CI(M^{'}),Y_i,R_i)$, $\sigma_2=(M^*,\tau_i^{''},CI(M^{'}),Y_i,R_i)$, 同时也意味着以下等式始终都成立:

$$Q_i+Q_i^{'}=\tau_i(Y_i-k_iQ_i^{'}-t_iQ_i-t_ih_iP_{pub})$$

等式可以被写作

$$r_is^{-1}P+x_ir_iP=\tau_i(y_iP-k_ix_ir_iP-t_ir_is^1P-t_ih_isP)$$

$$(r_is^{-1}+x_ir_i)P=\tau_i(y_i-k_ix_ir_i-t_ir_is^{-1}-t_ih_is)P$$

两边约去 P 可得:

$$r_is^{-1}+x_ir_i=\tau_i(y_i-k_ix_ir_i-t_ir_is^{-1}-t_ih_is)$$

$$(\tau_it_i+1)r_is^{-1}+(x_i+\tau_ik_ix_i)r_i+\tau_it_ih_is=\tau_iy_i$$

令 $A_i=(\tau_it_i+1)$, $\delta=r_is^{-1}$, $B_i=(x_i+\tau_ik_ix_i)$, $C_i=\tau_it_ih_i$, 则上述等式可以被写作 $A_i\delta+B_ir_i+C_is=\tau_iy_i$。

β 可以利用列表 L_C 和 L_H 解出方程。可以看到, 对于方程 $A_i\delta+B_ir_i+C_is=\tau_iy_i$ 只需要执行两次重放攻击就可以得到三个等式解决上述一次三元未知数方程, 从而解出未知的 s、δ 和 r_i。因此, β 解出了 s 作为 ECDLP 实例 $\psi=(P,P_{pub})$ 的解, 这与椭圆曲线离散对数问题的困难性定义不符合, 所以该方案对于一类攻击是安全的。**证毕。**

破解概率分析

成功解决上述 ECDLP 实例, 需要同时满足三个条件:

θ_1: 挑战者 β 能成功执行上述模拟过程

θ_2: 攻击者 α_1 能生成一个身份合法的伪造签名

θ_3: 伪造签名能满足 $ID_i=ID^*$ 的各种检验条件

因此, 对于第一类攻击能够成果解决 ECDLP 困难性问题实例总的概率为 $P(\theta_1\wedge\theta_2\wedge\theta_3)$=$P(\theta_1)\cdot P(\theta_2\mid\theta_1)\cdot P(\theta_3\mid\theta_1\wedge\theta_2)$。

部分私钥询问会在创建用户询问失败的时候终止模拟, 而创建用户询问会因为 Hash 询问中有关 $h_i=H_0(ID_i,R_i,P_{pub})$ 值的不一致而失效。假设上述 Hash 询问的情况发生的概率最大不超过 $\frac{n_H}{q}$, 其中 n_H 是 Hash 询问发生的次数, 那么部分私钥询问成功的概率至少为 $(1-\frac{n_H}{q})^{n_{KE}}$, 其中 n_{KE} 是部分私钥询问发起的次数。同理, 挑战者 β 获取秘密值成功的概率至少为 $(1-\frac{n_H}{q})^{n_{SV}}$, 其中 n_{SV} 是公钥询问发起的次数。攻击者 α_1 在签名询问阶段成功生成一个有效签名且满足 $ID_i=ID^*$ 的概率是 $(1-\frac{1}{q})$, 因此, 当有 n_s 次签名询问被认为有效的概率至少为 $(1-\frac{1}{q})^{n_s}$。攻击者 α_1 在签名询问之后成功伪造一个有效签名且满足 $ID_i=ID^*$ 的概率是 $\frac{1}{n_H}$, 假设挑战者 β 生成一个身份合法的伪造签名的概率是 ε, 那么有以下概率:

$$P(\theta_1)=(1-\frac{n_H}{q})^{(n_{KE}+n_{SV})}(1-\frac{1}{q})^{n_s}$$

$$\geqslant(1-\frac{n_H(n_{KE}+n_{SV})}{q})(1-\frac{n_s}{q})$$

$$P(\theta_2\mid\theta_1)\geqslant\varepsilon$$

$$P(\theta_3\mid\theta_1\wedge\theta_2)\geqslant\frac{1}{n_H}$$

综上所述, 可以计算出挑战者成功破解 ECDLP 困难性问题的概率为:

$$P(\theta_1\wedge\theta_2\wedge\theta_3)=P(\theta_1)\cdot P(\theta_2\mid\theta_1)\cdot P(\theta_3\mid\theta_1\wedge\theta_2)$$

$$\varepsilon^{'}\geqslant(1-\frac{n_H(n_{KE}+n_{SV})}{q})(1-\frac{n_s}{q})\varepsilon(\frac{1}{n_H})$$

因此, 如果攻击者 α_1 成功伪造签名的概率 ε 是不可忽略的, 那么当 n_H、n_{KE}、n_{SV}、n_s 和 q 都是常数时, $\varepsilon^{'}$ 也是无法忽略的。

定理 2: 本文提出来的隐私保护方案能够在给出随机数据模型的情况下抵御第二类攻击, 考虑到求解椭圆曲线离散对数问题(ECDLP)的困难性。

证明 2: 假设存在一个攻击者 α_2, 能够在多项式时间内以一个不可忽略的概率 ε_2 破解本文中的签名方案。目标是攻击者 α_2 利用一个挑战者 β 能够解决 ECDLP 困难问题, 即给出一个随机的 ECDLP 实例 $\psi=(P,x\cdot P)$, 攻击者 α_2 能够求出 x。

初始化阶段和询问阶段与第一类攻击过程类似, 不同之处在于此时攻击者是知道主密钥 s 的值的。因此, 在创建用户询问阶段, 若 $ID_i\neq ID^*$ 时不需要通过 $Q_i=aR_i+bP_{pub}$ 计算。而是由 β 随机选择 $r_i,h_i\in Z_q^*$, 计算 $R_i=r_iP$, $Q_i=s^{-1}R_i$ 和 $d_i=s^{-1}+r_i^{-1}sh_i$, 然后将相应的值输出给 α_2, 同时更新到列表 L_C 和 L_H 中。

在最后阶段, 攻击者 α_2 能够成功地在多项式时间内以一个不可忽略的概率 ε_1 输出一个关于

(ID_i, M) 的签名消息 (M, τ_i, Y_i, R_i)，从而挑战者 β 能够以一个不可忽略的概率 ε' 解决ECDLP困难性问题，其中，$\varepsilon' \geqslant (1-\frac{n_H(n_{KE}+n_{SV})}{q})(1-\frac{n_s}{q})\varepsilon_1(\frac{1}{n_H})$。这与椭圆曲线离散对数问题 ECDLP 的困难性定义不符合，所以本文提出的方案是安全的。 **证毕。**

(2) 保密性

定理 3: 在本文提出的隐私保护方案中，攻击者无法获取原消息中未被截取的消息，对未截取消息具有较强的保密性。

证明 3: 假设 σ_0 是用户 ID_i 为消息 $M_0 = \{m_1, \cdots, m_{i-1}, m', m_{i+1}, \cdots, m_n\}$ 的截取子消息 D_0 生成的签名，其截取子集 $CI(D_0)$ 满足 $i \notin CI(D_0)$，即 D_0 包含消息 M_0 中除 m' 以外的所有子消息。σ_1 是用户 ID_i 为消息 $M_1 = \{m_1, \cdots, m_{i-1}, m'', m_{i+1}, \cdots, m_n\}$ 的截取子消息 D_1 生成的签名，其截取子集 $CI(D_1)$ 满足 $i \notin CI(D_1)$，即 D_1 包含消息 M_1 中除 m'' 以外的所有子消息，因此 $D_0 = D_1$。由于截取部分的签名独立于未截取部分，与未截取签名无关，因此即使攻击者能够选择 (m', m'')，截取子集 $CI(D_0)$，$CI(D_1)$ 及其余子消息 m_i，也无法区分签名 σ_0 与 σ_1，也就无法获得任何未截取的 m' 和 m'' 有关信息。所以，该方案对于未截取消息具有保密性。

5 性能分析

本节首先对本文提出的基于区块链的药品品种管理方案与其他类似的区块链药品管理方案进行功能上的对比，随后，分别从理论与实验仿真两个方面对方案的计算效率进行分析，并且与已有的可截取签名改进方案进行比较，以此来对方案进行总体的评估。

5.1 功能性分析

基于区块链的药品或电子病历的信息管理与本文方案在功能上的对比情况如下表 7 所示。可以看到，文献[16]不能实现对于参与签名过程中的身份进行认证管理，文献[4]不能实现对于签名之后的档案数据进行远程访问，而本文所提方案基本上实现了最初提出的访问控制、安全存储及隐私保护等目标。

5.2 方案效率分析

通过对方案中涉及的基本运算和其他几种已有的方案进行分析对比，分别从计算复杂度和仿真运行时间上对不同方案进行评估。为了方便表示，用 par 表示双线性对运算, has 表示哈希函数运算, exp 表示指数运算，sca 表示椭圆曲线上的标量乘法运算以及 inv 表示模逆运算，其他简单的普通四则运算过程可忽略不计。

表 7 与其他方案的功能性对比情况

Table 7 Functional comparison with other solutions

方案	访问控制	安全存储	身份认证	远程访问
文献[1]方案	✓	✓	×	×
文献[4]方案	✓	✓	✓	×
文献[16]方案	✓	✓	×	✓
本文方案	✓	✓	✓	✓

理论分析方面，表 8 展示了不同方案计算效率消耗的对比，其中 n 指的是待签消息 M 中子消息的个数，m 指的是截取消息的个数。由该表可知，方案[8-10, 17]在验签的过程中均使用了非常耗时的双线性对运算，因此消耗普遍偏高。而方案[7]虽没有涉及双线性对运算，但是涉及一定量的指数运算导致方案的效率不高。而本文方案中没有涉及到双线性对或是指数运算等较为耗时的运算，只使用了一些标量乘法以及模逆运算，故而在效率上有较为明显地提升。此外，使用无证书密码体制，省去了密钥托管的步骤，使得方案的安全性得到更进一步的提升。

表 8 各个方案的效率与安全性对比

Table 8 Efficiency and safety comparison of different scheme

方案	签名及截取算法消耗	验签消耗
方案[10]	(2n+3)has+2exp+1par+4sca	(m+3)has+1par+2sca
方案[8]	(2n+4)has+2par+5sca	(m+2)has+4par+7sca
方案[9]	(2n+4)has+1par+3sca+2exp	(m+2)has+2par+5sca+3exp
方案[7]	(2n+3)has+5exp	(m+3)has+3exp
方案[17]	(2n+2)exp+1par	(m+3)par+2exp
本方案	(2n+5)has+2sca+1inv	(m+2)has+2sca

实验仿真方面，对上述方案中各个阶段涉及的算法用 C 语言进行实际运行时间的测试。模拟实验环境的硬件平台是 Intel Core I7-7700@3.6GHz 的处理器和 16GB 的运行内存，软件环境是 Centos7 版本的 Linux 操作系统，选用 Miracl 密码库，椭圆曲线使用安全性高、速度快的 A 类椭圆曲线 $y^2 = x^3 + x$。

为了避免结果的偶然性，实验结果取以上方案中涉及到的 5 种运算分别重复运行 30 次的平均值，结果如下表 9 所示。

方案的总体运行时间主要取决于签名、截取算法以及签名验证所消耗的时间。因此，综合表 8 和表 9 的数据就可以计算出算法的实际运行时间函数，结果如表 10 所示。

表 9 方案中各运算的实际执行时间

Table 9 The actual execution time of each operation in the scheme

运算	哈希运算 has	双线性对运算 par	指数运算 exp	标量乘运算 sca	模逆运算 inv
运行时间 (ms)	2.01	8.02	3.31	1.42	0.71

表 10 不同方案中各阶段消耗的运行时间

Table 10 The runnisng time consumed by each stage in different schemes

方案	签名及截取算法消耗	验签消耗
方案[10]	4.02n+26.35	2.01m+16.89
方案[8]	4.02n+31.18	2.01m+46.04
方案[9]	4.02n+26.94	2.01m+37.09
方案[7]	4.02n+22.58	2.01m+15.96
方案[17]	6.62n+14.64	8.02m+30.68
本方案	4.02n+13.6	2.01m+6.86

采用图 8、图 9 所示的点线图来表示实验结果。可以看到, 随着待签名消息 M 的子消息数目和截取消息数目的增加, 不同的方案在两个阶段的消耗均有所增加。并且不同方案在签名及截取阶段的运行时间差别不大, 这主要是因为只要是可截取签名, 在签名和截取阶段就一定会涉及到计算待签名消息整体散列值 $\overline{M}$ 和截取以及相对应的后续还原整体散列值 $\overline{M}$ 过程。由于避免了耗时相对过多的双线性对运算和指数运算, 可以看到, 本文提出的方案各阶段运行时间要明显低于其他比较的方案, 这与之前理论分析的结果是一致的。对比其他方案, 本文提出的无证书可截取签名隐私保护方案, 能够很好地降低运算量, 提高签名验签的效率。

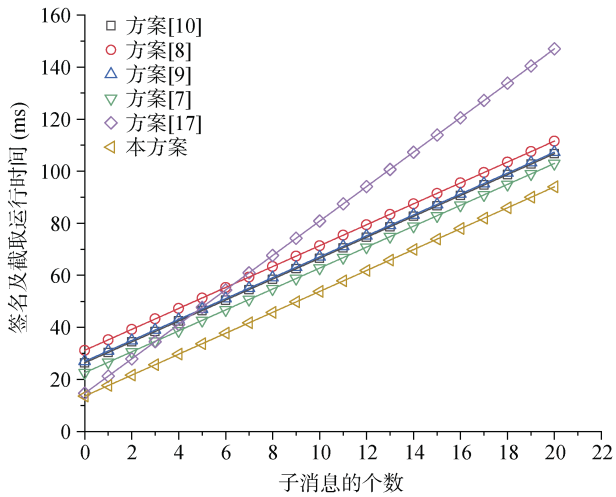


图 8 不同方案中签名及截取阶段消耗时间

Figure 8 Time consumption of signature and interception in different schemes

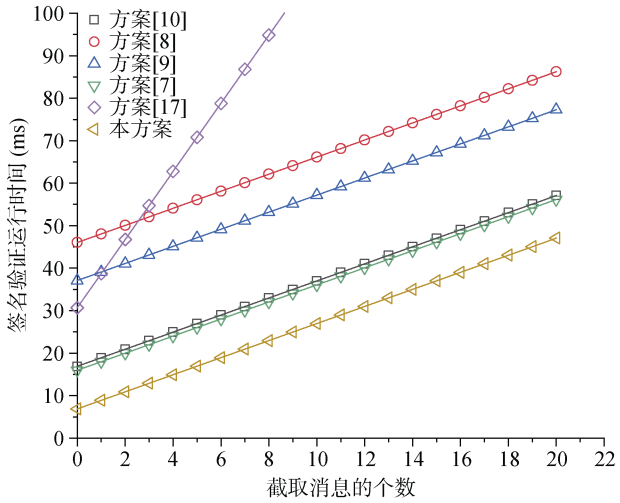


图 9 不同方案中签名验证阶段消耗时间

Figure 9 Time consumption of signature verification phase in different schemes

6 结束语

本文基于改进的无证书可截取签名算法, 提出了区块链上一种具有安全存储和隐私保护的药品品种信息共享审查方案, 解决了药品品种信息审查过程中数据安全及全过程跟踪监管等关键问题。在本文提出的药品信息档案管理模型中, 药品的品种档案信息由药企直接提交给上级受理中心, 再逐级提交至总局数据中心, 层层通过之后才会最终进入数据中心的线下数据库。而各种审批、检查数据由各级业务中心提交至联盟链中, 数据中心直接从链上获取这部分数据并保存到自己的线下数据库中, 实现了药品档案数据的安全存储与共建共享。其次, 考虑到药品品种档案中涉及的许多诸如生产工艺、药品成分等一些药企并不想公开传播的数据, 利用可截取签名技术在检查员审核的时候删去部分隐私数据, 从而既能保证检查流程的正常进行, 也保护了药企的机密数据不被轻易泄露, 为区块链环境下, 提供了一种更为安全、灵活的药品档案隐私保护机制。最后, 安全性证明和性能分析表明, 本方案不仅达到了最初的设计目标而且相比于同类方案效率更高。

参考文献

[1] Liu T C, Chen Z G, Song X X. Research and Application of Drug Traceability System Based on Blockchain Technology[J]. *Journal of Zhejiang Wanli University*, 2021, 34(2): 78-85.
(刘天成, 陈智罡, 宋新霞. 基于区块链技术的药品溯源系统研究与应用[J]. *浙江万里学院学报*, 2021, 34(2): 78-85.)

[2] Xue D. *Design and implementation of drug supply chain traceability system based on blockchain*[D]. Xi'an: Xidian University, .
(薛丹. 基于区块链的药品供应链追溯系统设计与实现[D]. 西

安: 西安电子科技大学.)

[3] Gu R. Research on the Construction of Drug Quality and Safety Traceability System Based on Blockchain Technology[J]. *Computer Knowledge and Technology*, 2020, 16(2): 230-231.
(古锐. 基于区块链技术的药品质量安全追溯系统构建研究[J]. *电脑知识与技术*, 2020, 16(2): 230-231.)

[4] 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.
(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.)

[5] Steinfeld R, Bull L, Zheng Y L. Content Extraction Signatures[C]. *The 4th International Conference Seoul on Information Security and Cryptology*, 2001: 285-304.

[6] Bull L, Stanski P, Squire D M. Content Extraction Signatures Using XML Digital Signatures and Custom Transforms On-Demand[C]. *The 12th international conference on World Wide Web*, 2003: 170-177.

[7] Idalino T B, Moura L, Adams C. Modification Tolerant Signature Schemes: Location and Correction[C]. *International Conference on Cryptology in India*, 2019: 23-44.

[8] Li X, Du X N, Wang C F, et al. Improved Scheme of Content Extraction Signatures Based on RSA[J]. *Computer Engineering and Applications*, 2014, 50(24): 96-99.
(李旭, 杜小妮, 王彩芬, 等. 基于 RSA 的可截取签名改进方案[J]. *计算机工程与应用*, 2014, 50(24): 96-99.)

[9] Yin X C, Ye S Y, Ou F N, et al. An ID-Based Content Extraction Signatures without Trusted Party[C]. *2010 5th IEEE Conference on Industrial Electronics and Applications*, 2010: 1801-1804.

[10] Wang C F, Li Y H, Huang S Y, et al. A New Forward Secure Content Extraction Signature Scheme[C]. *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery*, 2016: 1698-1702.

[11] Pavlovski C J. Efficient Batch Signature Generation Using Tree Structures[C]. *The International Workshop on Cryptographic Techniques and E-Commerce*, 1999: 70-77.

[12] Yli-Huumo J, Ko D, Choi S, et al. Where is Current Research on Blockchain Technology? -a Systematic Review[J]. *PLoS ONE*, 2016, 11(10): e0163477.

[13] Swan M. Blockchain: Blueprint for a new economy[M]. "O'Reilly Media, Inc.", 2015.

[14] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[C]. *International conference on the theory and application of cryptology and information security*, 2003: 452-473.

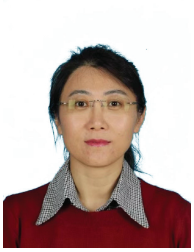
[15] Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures[J]. *Journal of Cryptology*, 2000, 13(3): 361-396.

[16] Yue X, Wang H J, Jin D W, et al. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control[J]. *Journal of Medical Systems*, 2016, 40(10): 218.

[17] Shim K A. A New Certificateless Signature Scheme Provably Secure in the Standard Model[J]. *IEEE Systems Journal*, 2019, 13(2): 1421-1430.

胡荣磊 于 2009 年在北京航空航天大学通信与信息系统专业获得博士学位。现任北京电子科技学院电子与通信工程系副教授。研究领域为密码学, 区块链技术。研究兴趣包括无线通信, 信息安全等。Email: huronglei@sina.com

丁安邦 于 2019 年在河海大学物联网工程专业获得学士学位。现在北京电子科技学院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。研究兴趣包括区块链技术, 信息安全等。Email: 526768549@qq.com



李莉 于 2018 年在西安电子科技大学密码学专业获得博士学位。现任北京电子科技学院电子与通信工程系教授。研究领域为密码学。研究兴趣包括区块链技术, 信息安全等。Email: laury_li@126.com

段晓毅 于 2009 年在北京航空航天大学通信与信息系统专业获得博士学位。现任北京电子科技学院电子与通信工程系副教授。研究领域为密码学。研究兴趣包括区块链技术, 侧信道分析, 信息安全等。Email: xiaoyi_duan@sina.co