(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 116484398 B
(45)授权公告日 2024.04.02

(21)申请号 202310269454.8
(22)申请日 2023.03.15
(65)同一申请的已公布的文献号
申请公布号 CN 116484398 A
(43)申请公布日 2023.07.25
(73)专利权人 香港理工大学深圳研究院
地址 518057 广东省深圳市南山区粤海街道高新技术产业园南区粤兴一道18号香港理工大学产学研大楼205室
(72)发明人 刘立昊 肖斌
(74)专利代理机构 深圳市君胜知识产权代理事务所(普通合伙) 44268
专利代理师 李可
(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
(56)对比文件
CN 109413178 A,2019.03.01
CN 109918925 A,2019.06.21
CN 110995408 A,2020.04.10
CN 111400753 A,2020.07.10
CN 111741031 A,2020.10.02
CN 112185535 A,2021.01.05
CN 112565223 A,2021.03.26
CN 113312574 A,2021.08.27
CN 113536389 A,2021.10.22
CN 114491576 A,2022.05.13
CN 115567247 A,2023.01.03
审查员 范广坡

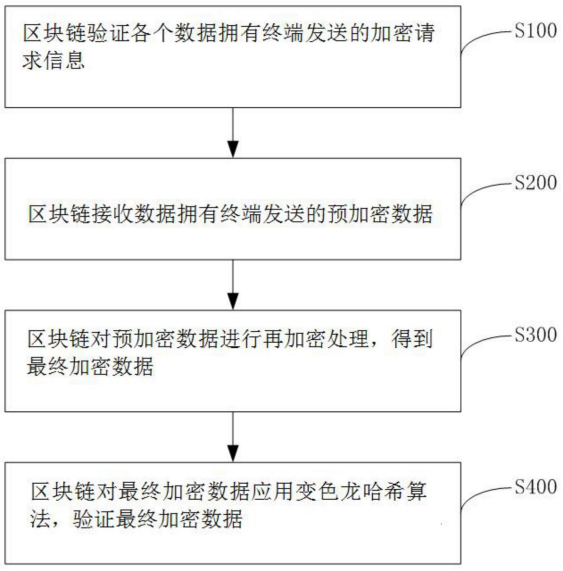
权利要求书2页 说明书9页 附图2页

(54)发明名称

一种基于变色龙哈希的加密验证方法和系统

(57)摘要

本发明涉及数据加密技术领域,具体是涉及一种基于变色龙哈希的加密验证方法和系统。本发明只将算力较小的初加密处理放在数据拥有终端上进行,而将算力较大的剩余加密工作放在区块链上进行。在数据拥有终端上执行数据的初加密,赋予了数据一定的安全性,将具有一定安全性的预加密数据再在开源的区块链上进一步加密就能够充分保证数据的安全性。而且本发明将对算力要求低的初加密处理放在数据拥有终端上执行,而将对算力要求高的再加密处理放在区块链上执行,能够借助区块链的算力提升加密速度。综上所述,本发明既保证了加密数据的安全性又保证了加密速度,从而提升了数据加密性能。



CN 116484398 B

1.一种基于变色龙哈希的加密验证方法,其特征在于,包括:

接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据;

对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力;

对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据;

所述对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力,包括:

将所述预加密数据结合原始外包数据进行再加密处理,得到最终加密数据,所述预加密数据所对应的原始数据所需的保密性大于所述原始外包数据所需的保密性,所述原始外包数据为所述数据拥有终端所持有的数据中除所述预加密数据所对应的原始数据之外而需要加密的数据。

2.如权利要求1所述的基于变色龙哈希的加密验证方法,其特征在于,所述数据拥有终端为密钥验证通过的所述数据拥有终端,所述接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据,之前还包括:

接收所述数据拥有终端发送的加密请求消息;

通过各个所述数据拥有终端所对应的哈希私钥,检查所述加密请求消息中所涵盖的所述数据拥有终端的个人私钥,得到针对各个所述数据拥有终端的密钥检查结果,所述哈希私钥为对所述个人私钥进行哈希处理得到的密钥;

依据各个所述数据拥有终端的所述密钥检查结果和所述个人私钥的绝限期,验证各个所述数据拥有终端,得到密钥验证通过的所述数据拥有终端。

3.如权利要求2所述的基于变色龙哈希的加密验证方法,其特征在于,所述依据各个所述数据拥有终端的所述密钥检查结果和所述个人私钥的绝限期,验证各个所述数据拥有终端,得到密钥验证通过的所述数据拥有终端,包括:

确定所述密钥检查结果中的检查合格所对应的所述数据拥有终端,记为初选合格终端,所述检查合格为所述数据拥有终端的所述个人私钥吻合于所述哈希私钥;

从各个所述初选合格终端中筛选出所述绝限期小于设定期限所对应的终端,得到密钥验证通过的所述数据拥有终端。

4.如权利要求1所述的基于变色龙哈希的加密验证方法,其特征在于,所述对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据,包括:

对所述最终加密数据、随机参数、公钥应用变色龙哈希算法,得到哈希值,所述公钥为初始化所述数据拥有终端时而生成的密钥;

依据所述哈希值,验证所述最终加密数据。

5.如权利要求1所述的基于变色龙哈希的加密验证方法,其特征在于,还包括:

当所述最终加密数据验证合格时,获取激励,所述验证合格用于表征所述最终加密数据满足所述数据拥有终端针对所述最终加密数据设定的条件,所述激励用于表征被所述数据拥有终端下一次分配所述预加密数据的概率;

当所述最终加密数据验证不合格时,扣除押金,所述押金与所述激励相对应。

6.一种基于变色龙哈希的加密验证系统,其特征在于,包括如下组成部分:

数据拥有终端,用于基于原始数据进行初加密处理生成预加密数据;

数据控制端,用于给所述数据拥有终端分配密钥;

区块链,用于对密钥验证通过的所述数据拥有终端发送的所述预加密数据进行再加密处理,得到最终加密数据,并验证所述最终加密数据;

数据使用终端,用于存储所述最终加密数据;

所述预加密数据进行再加密处理,得到最终加密数据,包括:

将所述预加密数据结合原始外包数据进行再加密处理,得到最终加密数据,所述预加密数据所对应的原始数据所需的保密性大于所述原始外包数据所需的保密性,所述原始外包数据为所述数据拥有终端所持有的数据中除所述预加密数据所对应的原始数据之外而需要加密的数据。

7.一种基于变色龙哈希的加密验证装置,其特征在于,所述装置包括如下组成部分:

数据接收模块,用于接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据;

加密模块,用于对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力;

验证模块,用于对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据;

所述对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力,包括:

将所述预加密数据结合原始外包数据进行再加密处理,得到最终加密数据,所述预加密数据所对应的原始数据所需的保密性大于所述原始外包数据所需的保密性,所述原始外包数据为所述数据拥有终端所持有的数据中除所述预加密数据所对应的原始数据之外而需要加密的数据。

8.一种终端设备,其特征在于,所述终端设备包括存储器、处理器及存储在所述存储器中并可在所述处理器上运行的基于变色龙哈希的加密验证程序,所述处理器执行所述基于变色龙哈希的加密验证程序时,实现如权利要求1-5任一项所述的基于变色龙哈希的加密验证方法的步骤。

9.一种计算机可读存储介质,其特征在于,所述计算机可读存储介质上存储有基于变色龙哈希的加密验证程序,所述基于变色龙哈希的加密验证程序被处理器执行时,实现如权利要求1-5任一项所述的基于变色龙哈希的加密验证方法的步骤。

一种基于变色龙哈希的加密验证方法和系统

技术领域

[0001] 本发明涉及数据加密技术领域,具体是涉及一种基于变色龙哈希的加密验证方法和系统。

背景技术

[0002] 银行、医院等机构将用户的一些数据保存在终端(数据拥有终端)上,当机构需要将这些数据传输给需要使用这些数据的用户时,需要先对数据进行加密,以确保安全传输这些数据,然后借助区块链将加密之后的数据传输给需要使用数据的用户。现有技术为了确保数据的安全性,在数据拥有终端对数据进行完全加密,而区块链仅仅只符合加密数据的传输,导致了数据拥有终端承担了加密所需的全部算力,从而降低了加密数据的处理速度。或者,现有技术将数据加密完全放在算力高的区块链上进行,而区块链是一个开放的系统,会导致影响数据的安全性。从上述分析可知,现有技术的数据加密难以兼顾安全性和加密处理速度,从而降低了数据加密的性能。

[0003] 综上所述,现有技术降低了数据加密性能。

[0004] 因此,现有技术还有待改进和提高。

发明内容

[0005] 为解决上述技术问题,本发明提供了一种基于变色龙哈希的加密验证方法和系统,解决了现有技术降低数据加密性能的问题。

[0006] 为实现上述目的,本发明采用了以下技术方案:

[0007] 第一方面,本发明提供一种基于变色龙哈希的加密验证方法,其中,包括:

[0008] 接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据;

[0009] 对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力;

[0010] 对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据。

[0011] 在一种实现方式中,所述数据拥有终端为密钥验证通过的所述数据拥有终端,所述接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据,之前还包括:

[0012] 接收所述数据拥有终端发送的加密请求消息;

[0013] 通过各个所述数据拥有终端所对应的哈希私钥,检查所述加密请求消息中所涵盖的所述数据拥有终端的个人私钥,得到针对各个所述数据拥有终端的密钥检查结果,所述哈希私钥为对所述个人私钥进行哈希处理得到的密钥;

[0014] 依据各个所述数据拥有终端的所述密钥检查结果和所述个人私钥的绝限期,验证各个所述数据拥有终端,得到密钥验证通过的所述数据拥有终端。

[0015] 在一种实现方式中,所述依据各个所述数据拥有终端的所述密钥检查结果和所述

个人私钥的绝限期,验证各个所述数据拥有终端,得到密钥验证通过的所述数据拥有终端,包括:

[0016] 确定所述密钥检查结果中的检查合格所对应的所述数据拥有终端,记为初选合格终端,所述检查合格为所述数据拥有终端的所述个人私钥吻合于所述哈希私钥;

[0017] 从各个所述初选合格终端中筛选出所述绝限期小于设定期限所对应的终端,得到密钥验证通过的所述数据拥有终端。

[0018] 在一种实现方式中,所述对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力,包括:

[0019] 将所述预加密数据结合原始外包数据进行再加密处理,得到最终加密数据,所述预加密数据所对应的原始数据所需的保密性大于所述原始外包数据所需的保密性,所述原始外包数据为所述数据拥有终端所持有的数据中除所述预加密数据所对应的原始数据之外而需要加密的数据。

[0020] 在一种实现方式中,所述对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据,包括:

[0021] 对所述最终加密数据、随机参数、公钥应用变色龙哈希算法,得到哈希值,所述公钥为初始化所述数据拥有终端时而生成的密钥;

[0022] 依据所述哈希值,验证所述最终加密数据。

[0023] 在一种实现方式中,还包括:

[0024] 当所述最终加密数据验证合格时,获取激励,所述验证合格用于表征所述最终加密数据满足所述数据拥有终端针对所述最终加密数据设定的条件,所述激励用于表征被所述数据拥有终端下一次分配所述预加密数据的概率;

[0025] 当所述最终加密数据验证不合格时,扣除押金,所述押金与所述激励相对应。

[0026] 第二方面,本发明实施例还提供一种基于变色龙哈希的加密验证系统,其中,包括如下组成部分:

[0027] 数据拥有终端,用于基于原始数据进行初加密处理生成预加密数据;

[0028] 数据控制端,用于给所述数据拥有终端分配密钥;

[0029] 区块链,用于对密钥验证通过的所述数据拥有终端发送的所述预加密数据进行再加密处理,得到最终加密数据,并验证所述最终加密数据;

[0030] 数据使用终端,用于存储所述最终加密数据。

[0031] 第三方面,本发明实施例还提供一种基于变色龙哈希的加密验证装置,其中,所述装置包括如下组成部分:

[0032] 数据接收模块,用于接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据;

[0033] 加密模块,用于对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力;

[0034] 验证模块,用于对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据。

[0035] 第四方面,本发明实施例还提供一种终端设备,其中,所述终端设备包括存储器、处理器及存储在所述存储器中并可在所述处理器上运行的基于变色龙哈希的加密验证程

序,所述处理器执行所述基于变色龙哈希的加密验证程序时,实现上述所述的基于变色龙哈希的加密验证方法的步骤。

[0036] 第五方面,本发明实施例还提供一种计算机可读存储介质,所述计算机可读存储介质上存储有基于变色龙哈希的加密验证程序,所述基于变色龙哈希的加密验证程序被处理器执行时,实现上述所述的基于变色龙哈希的加密验证方法的步骤。

[0037] 有益效果:本发明首先在数据拥有终端上对原始数据进行初加密处理,得到预加密数据,然后区块链再基于预加密数据进行加密处理,得到最终加密数据,最后区块链验证最终加密数据是否正确,如果正确,区块链就开始传输最终加密数据。从上述分析可知,本发明只将算力较小的初加密处理放在数据拥有终端上进行,而将算力较大的剩余加密工作放在区块链上进行。在数据拥有终端上执行数据的初加密,赋予了数据一定的安全性,将具有一定安全性的预加密数据再在开源的区块链上进一步加密就能够充分保证数据的安全性。而且本发明将对算力要求低的初加密处理放在数据拥有终端上执行,而将对算力要求高的再加密处理放在区块链上执行,能够借助区块链的算力提升加密速度。综上所述,本发明既保证了加密数据的安全性又保证了加密速度,从而提升了数据加密性能。

附图说明

[0038] 图1为本发明的整体流程图;

[0039] 图2为本发明实施例中的加密验证系统结构图;

[0040] 图3为本发明实施例提供的终端设备的内部结构原理框图。

具体实施方式

[0041] 以下结合实施例和说明书附图,对本发明中的技术方案进行清楚、完整地描述。基于本发明中的实施例,本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0042] 经研究发现,银行、医院等机构将用户的一些数据保存在终端(数据拥有终端)上,当机构需要将这些数据传输给需要使用这些数据的用户时,需要先对数据进行加密,以确保安全传输这些数据,然后借助区块链将加密之后的数据传输给需要使用数据的用户。现有技术为了确保数据的安全性,在数据拥有终端对数据进行完全加密,而区块链仅仅只符合加密数据的传输,导致了数据拥有终端承担了加密所需的全部算力,从而降低了加密数据的处理速度。或者,现有技术将数据加密完全放在算力高的区块链上进行,而区块链是一个开放的系统,会导致影响数据的安全性。从上述分析可知,现有技术的数据加密难以兼顾安全性和加密处理速度,从而降低了数据加密的性能。

[0043] 为解决上述技术问题,本发明提供了一种基于变色龙哈希的加密验证方法和系统,解决了现有技术降低数据加密性能的问题。具体实施时,首先区块链接收数据拥有终端发送的预加密数据,预加密数据为数据拥有终端对数据拥有终端持有的原始数据进行初加密处理而得到的加密数据;然后区块链对预加密数据进行再加密处理,得到最终加密数据,再加密处理所需的算力大于初加密处理所需的算力;最后区块链对最终加密数据应用变色龙哈希算法,验证最终加密数据。本发明能够提升加密数据的性能。

[0044] 举例说明,如图2所示,以医院为例,数据拥有者(数据拥有终端)保存者医院里的

病人信息(年龄、性别等属性数据A)以及病人的病历数据等原始数据B,当数据拥有终端需要将上述原始数据传输至数据使用者(比如疾病控制中心)时,数据拥有终端先对A进行加密(加密A所需要的算力很小),得到加密数据C。然后数据拥有终端将加密数据C和原始数据B发送给区块链中的各个背书节点(服务器),各个背书节点分别对加密数据C和原始数据B进行加密,各个背书节点将加密数据C和原始数据B加密成最终加密数据D、E、F,然后区块链对最终加密数据D、E、F分别应用变色龙哈希算法,得到D的哈希值D′、E的哈希值E′、F的哈希值F′,最后区块链比较哈希值D′、哈希值E′、哈希值F′,如果这三个哈希值中哈希值E′与另外两个哈希值不相等,那么最终加密数据E则为错误的加密数据,另外两个最终加密数据D和最终加密数据F则为正确的加密数据。

[0045] 示例性系统

[0046] 本实施例提供一种基于变色龙哈希的加密验证系统,如图2所示,该系统包括如下组成部分:

[0047] 数据拥有终端,用于基于原始数据进行初加密处理生成预加密数据;

[0048] 数据控制端,用于给所述数据拥有终端分配密钥;

[0049] 区块链,用于对密钥验证通过的所述数据拥有终端发送的所述预加密数据进行再加密处理,得到最终加密数据,并验证所述最终加密数据;

[0050] 数据使用终端,用于存储所述最终加密数据。

[0051] 数据拥有终端、数据控制端(图2中的银行、医院、物联网系统所在的终端为控制端)、区块链、数据使用终端构成了本实施例的加密验证系统。

[0052] 本实施例的加密验证系统对数据实施加密验证的流程依次包括初始化阶段、用户注册阶段、数据加密阶段、加密正确性的验证阶段、奖惩阶段。下面分别介绍上述五个阶段:

[0053] 初始化阶段:图2中的银行、医院、物联网系统所在的终端生成公密钥PK对以及其他系统所需要的加密参数。

[0054] 向密钥生成算法(现有技术)输入一个素数p的双线性群G_0、生成器g、两个随机指数α和β(α,β∈Z_p,Z_p为由素数P组成的集合),算法输出公密钥PK:

[0055] $PK=G_0,g,h=g^{\beta},e(g,g)^{\alpha}$

[0056] e为双线性映射算法,h是一种双线性群G_0的元素,它由生成元g和随机指数β的幂次计算得到。g^{β}和$e(g,g)^{\alpha}$连接(,代表连接)得到公密钥PK。

[0057] 用户注册阶段:数据控制端生成主密钥MK(MK为(β,g^{α}),数据控制端使用随机数α和β以及生成器g产生主密钥MK),数据控制端基于主密钥MK生成个人私钥SK(数据控制端使用MK和用户属性集为用户生成个人私钥SK。密钥生成算法输入一组属性S并输出与S关联的个人私钥SK,比如属性S为医院里的病人年龄、性别等属性数据A),数据控制端将个人私钥SK分发给数据拥有终端。数据控制端对个人私钥SK进行哈希处理得到哈希私钥SK′,数据控制端再将哈希私钥SK′发送给区块链中的各个节点,以进行密钥管理。

[0058] $SK=\left(D=g^{(\alpha+d)/\beta},\forall j\in S:D_j=g^{d}\cdot H(j)^{d_j},D_j'=g^{d_j}\right)$

[0059] 式中,随机数d∈Z p,随机数d_j∈Z_,对于每个属性j∈S。

[0060] 哈希私钥SK′为数据控制端在SK上执行散列函数得到的结果。

[0061] SK′=哈希$_{md5}$[SK]

[0062] 哈希md5用于将SK转换成128位元的函数,哈希md5可以用来验证档案的完整性或

加密敏感资料。

[0063] 初始化阶段和用户注册阶段的密钥生成算法包括如下的三种:

[0064] 第一种:使用素数o并在空间Zo设置陷门x_{ch}。通过gmod o将公钥设置为PK_{ch}。

[0065] 第二种:使用公钥PK_{ch}、消息M_{ch}和随机参数r_{ch}生成变色龙哈希值H_{ct}。

[0066] 第三种:使用陷门x_{ch},随机参数r_{ch},消息M_{ch},伪造消息M'_{ch}来计算原变色龙哈希值H_{ct}。$Hash_{ch}(M'_{ch},r'_{ch},PK_{ch})=Hash_{ch}(M_{ch},r_{ch},PK_{ch})=H_{ct}$。

[0067] 数据加密阶段:以属性加密作为例子,但不局限在属性加密,可以用任何其他的加密方式进行替代:数据拥有端首先执行部分加密,并将自定义策略和加密文件发送给两个背书节点(位于区块链中的两个节点)。背书节点然后执行基于属性的加密。本实施例使用部分加密并利用功能加密的弱密钥属性来构造的部分加密(在数据拥有终端上已执行部分加密的数据)和待加密的外包数据加密。外包加密的随机参数在部分加密中预先定义,区块链的各个节点再对部分加密和最终加密数据待加密的外包数据进行加密,得到最终加密数据。

[0068] 加密正确性的验证阶段:背书节点对密文(最终加密数据)生成哈希值。共识机制通过比较来自选定背书节点的两个哈希值来验证加密结果的正确性。正确的加密结果(最终加密数据)将被批准并上传到去中心化云存储,即将正确的最终加密数据发送给数据使用终端。

[0069] 数据使用终端在解密操作期间或之后发现错误数据,数据使用终端先检查加密结果CT(最终加密数据)的最终大小,或者对加密结果进行解密,找出错误的外包操作。

[0070] 奖惩阶段又包括加密工作的激励阶段和加密不正确情况下的退款机制。

[0071] 加密工作的激励阶段:数据拥有终端向区块链中的任意两个节点发送由预加密数据、属性(原始外包数据)、变色龙哈希随机数(个人私钥SK)组成的加密请求消息M。之后两个背书节点分别对加密请求消息M进行属性加密,得到两个最终加密数据CT,两个背书节点再对各自生成的最终加密数据CT应用变色龙哈希函数,两个背书节点分别得到最终加密数据CT的哈希值CT′。变色龙哈希将由区块链社区进行比较(区块链中的控制器对各个背书节点对应的哈希值CT′进行比较)。如果两个哈希值CT′“相等”,则最终加密数据CT被批准,并且上述两个背书节点获得奖励(所谓获得奖励就是当数据拥有者下次再发送需要加密的数据时,首先选择这两个背书节点)。奖励是数据拥有者给予的交易费用。如果多数决定是“不相等”,则最终加密数据CT将被丢弃。然后,系统会将加密请求消息M转发给其它两个随机背书节点。

[0072] 背书节点需要支付一定押金才能加入背书池。押金将进一步用于退款机制。外包加密成功后,被选中的背书节点可以获得80%的交易手续费。交易费用的20%将分配给批准加密结果的背书节点。

[0073] 此验证过程消除了中心化的需要,并激励背书节点执行外包属性加密加密。

[0074] 加密不正确情况下的退款机制:数据拥有终端将它的押金存入智能合约(加密验证系统的智能合约),并与两个随机选择的背书节点一起启动外包加密过程。通过密钥验证后,背书节点将押金存入智能合约。然后,这个外包加密的智能合约启动一个押金定时器。该计时器将保留数据拥有终端和背书节点的押金,直到最终退款决定或限时结束。退款机制始于数据拥有者在解密操作期间或之后发现不正确的数据。数据拥有者可以检查加密结

果的最终大小或解密加密结果以查找错误。之后,数据拥有者通过发出验证请求,识别错误的加密结果。先生成消息密文和随机数r'_{ch}的哈希碰撞,证明外包加密是错误的。与此同时,数据拥有者向随机背书节点发出另一个加密请求。背书节点会用密文回应数据拥有终端,并将一个变色龙哈希发送给退款法官。之后,法官将输入密文和生成一个变色龙散列r'_{ch},然后将结果与背书节点的密文进行比较。如果两个结果相同且与前一个背书节点不同,数据拥有终端证明它的正确性和对真实数据和变色龙哈希暗门的所有权。然后数据拥有终端从错误加密的背书节点的押金中取回付款。剩余的押金将分配给参与此验证的第三方法官和其他背书节点。上述退款机制中,数据拥有终端通过提供哈希碰撞来进行高隐私保护的验证,不会泄露信息和依赖中心化来进行验证。本实施例的加密验证系统具有安全性、可行性和高效能。

[0075] 示例性方法

[0076] 本实施例的基于变色龙哈希的加密验证方法可应用于终端设备中,所述终端设备可为具有数据处理功能的终端产品,比如电脑等。在本实施例中,如图1中所示,所述基于变色龙哈希的加密验证方法具体包括如下步骤:

[0077] S100,区块链验证各个数据拥有终端发送的加密请求信息。

[0078] 如图2所示,数据拥有终端将加密请求信息M发送给区块链,区块链会解析加密请求信息M中所涵盖的个人私钥SK,如果个人私钥SK与区块链之前保存的哈希私钥SK′相匹配,则区块链对该数据拥有终端发送的加密请求信息M内所涵盖的需要加密的数据进行加密。

[0079] 在一个实施例中,步骤S100包括如下的步骤S101、S102、S103、S104:

[0080] S101,区块链接收所述数据拥有终端发送的加密请求消息。

[0081] 构成区块链中的各个背书节点接收数据拥有终端发送的加密请求消息。

[0082] S102,区块链通过各个所述数据拥有终端所对应的哈希私钥,检查所述加密请求消息中所涵盖的所述数据拥有终端的个人私钥,得到针对各个所述数据拥有终端的密钥检查结果,所述哈希私钥为对所述个人私钥进行哈希处理得到的密钥。

[0083] S103,确定所述密钥检查结果中的检查合格所对应的所述数据拥有终端,记为初选合格终端,所述检查合格为所述数据拥有终端的所述个人私钥吻合于所述哈希私钥。

[0084] 检查合格即数据拥有终端发送的个人私钥SK与区块链之前保存的哈希私钥SK′相匹配,那么这些数据拥有终端就是初选合格终端。

[0085] S104,从各个所述初选合格终端中筛选出所述绝限期小于设定期限所对应的终端,得到密钥验证通过的所述数据拥有终端。

[0086] 区块链中保存了各个哈希私钥SK′的绝限期(绝限期即哈希私钥SK′的有效时间,如果哈希私钥SK′不在有效时间内,那么即使与哈希私钥SK′所匹配的数据拥有终端发送需要加密的数据,区块链也不对其进行加密处理)。本实施例中的设定期限为有效时间所对应的期限。

[0087] S200,区块链接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据。

[0088] 在一个实施例中的预加密数据为经过数据拥有终端加密之后的数据。在另一个实施例中,预加密数据包括经过数据拥有终端加密之后的数据和数据拥有终端发送给区块链

的未经数据拥有终端加密的数据。

[0089] S300,区块链对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力。

[0090] 当S200中的预加密数据为后者时,区块链将所述预加密数据结合原始外包数据进行再加密处理,得到最终加密数据。

[0091] 数据拥有终端定义了一个策略树T将其内部的数据划分为T_{BC}和T_{DO}。

[0092] T_{DO}只包含一个属性(包含了医院的病人的属性信息,DO可以随机指定1次多项式$q_R(x)$并设置$s=q_R(0)$、$s_1=q_R(1)$和$s_2=q_R(2)$。然后数据拥有终端DO发送s_1至背书节点),数据拥有终端只需要很小的计算能力就可以对其进行预加密,得到预加密数据CT_{DO}。T_{BC}为包含大量数据的原始外包数据,比如T_{BC}为医院里病人的病历信息。

[0093] $$CT_{DO}=(\forall y\in Y_{DO}:C_y=g^{q_y(0)},C_{y'}=H(att(y))^{q_y(0)})$$

[0094] $\tilde{C}=Me(g,g)^{\alpha s}$,$C=h^s$

[0095] Y_{DO}为数据拥有者DO的属性信息,$H(att(y))_{qy(0)}$为数据拥有者执行的部分加密。

[0096] 区块链中的各个背书节点再对预加密数据CT_{DO}和T_{BC}进行加密得到最终加密数据CT(以下公式展示了CT的计算公式):

[0097] $$CT=(T=T_{BC}\cap T_{DO},C\approx=^{Me}(g,g)^{\alpha s},\forall y\in Y_{BC}\cup Y_{DO}:C_y=g^{q_y(0)},C_{y'}=H(att(y))^{q_y(0)})$$

[0098] $$CT_{BC}=(\forall y\in Y_{BC}:C_y=g^{q_y(0)},C_{y'}=H(att(y))^{q_{y(0)}})$$

[0099] 其中CT为最终的加密数据,CT_{BC}为在区块链节点中的外包加密中产生的加密数据。

[0100] S400,区块链对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据。

[0101] 在一个实施例中,对所述最终加密数据CT、随机参数r_{ch}、公钥应用变色龙哈希算法,得到哈希值,所述公钥PK为初始化所述数据拥有终端时而生成的密钥;依据所述哈希值,验证所述最终加密数据。

[0102] 随机参数r_{ch}为医院对应的数据控制端发送给背书节点的。

[0103] 哈希值$=$哈希$_{ch}(CT,r_{ch},PK)=g_{CT}*PKr_{ch}$ modo

[0104] 式中,modo为素数o的模运算。

[0105] 在数据加密阶段中,背书节点对密文(最终加密数据CT)生成哈希值。共识机制通过比较来自选定背书人的两个哈希值来验证加密结果的正确性。正确的加密结果将被批准并上传到去中心化云存储。

[0106] 在另一个实施例中,数据拥有终端DO也可以发起验证请求,识别出错误的结果H_{old}(最终加密数据CT),并生成消息CT'和随机数的哈希碰撞r'_{ch}。

[0107] $x_{ch}=(CT-CT')/(r_{ch}-r'_{ch})\bmod_o$

[0108] 此外,DO向随机背书节点发出另一个加密请求。背书节点会用CT回应DO并发送一个变色龙哈希H_{new}给第三方法官。之后,法官生成一个变色龙散列CT′and r'_{ch},然后将结果与背书节点的哈希H_m进行比较。如果两个结果相等,DO证明了他对真实数据和变色龙哈希参数的正确性和所有权。

[0109] 综上,本发明首先在数据拥有终端上对原始数据进行初加密处理,得到预加密数据,然后区块链再基于预加密数据进行加密处理,得到最终加密数据,最后区块链验证最终加密数据是否正确,如果正确,区块链就开始传输最终加密数据。从上述分析可知,本发明只将算力较小的初加密处理放在数据拥有终端上进行,而将算力较大的剩余加密工作放在

区块链上进行。在数据拥有终端上执行数据的初加密,赋予了数据一定的安全性,将具有一定安全性的预加密数据再在开源的区块链上进一步加密就能够充分保证数据的安全性。而且本发明将对算力要求低的初加密处理放在数据拥有终端上执行,而将对算力要求高的再加密处理放在区块链上执行,能够借助区块链的算力提升加密速度。综上所述,本发明既保证了加密数据的安全性又保证了加密速度,从而提升了数据加密性能。

[0110] 另外,背书方收到加密请求或数据请求后,首先验证私钥的正确性和有效期。背书节点执行基于属性的加密并将加密文件上传到分布式云存储或将请求的数据返回给数据拥有人。在这个过程中,没有固定的背书节点接受加密请求。这使得加密更加安全,因为它消除了对中心化第三方的需求。区块链存储访问记录、智能合约状态和用户余额。分布式云存储用于存储数据使用者的共享文件。它保留了传统云平台的优势,并消除了集中存储的风险,例如删除、篡改或未经授权的访问。

[0111] 本发明的属性授权机构(数据控制终端)将一组散列私钥、客户的智能合约地址和到期日期发送到区块链以进行密钥管理。分发后,每个背书节点在密钥管理表中存储和维护私钥、客户智能合约地址和密钥到期日期的组合。密钥管理表将定期更新每个背书节点都有相同的资料。散列的私钥和智能合约地址不会泄漏隐私信息。密钥到期日期将在属性加密之前由背书人的智能合约检查。带有过期私钥的加密请求将不会被执行。这种方法自动高效,解决了传统属性加密方案的局限性。这种方法是安全的,因为散列可以保护私钥不泄露属性信息。此外,密钥管理表是分布式的,恶意攻击者无法修改。

[0112] 示例性装置

[0113] 本实施例还提供一种基于变色龙哈希的加密验证装置,所述装置包括如下组成部分:

[0114] 数据接收模块,用于接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据;

[0115] 加密模块,用于对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力;

[0116] 验证模块,用于对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据。

[0117] 基于上述实施例,本发明还提供了一种终端设备,其原理框图可以如图3所示。该终端设备包括通过系统总线连接的处理器、存储器、网络接口、显示屏、温度传感器。其中,该终端设备的处理器用于提供计算和控制能力。该终端设备的存储器包括非易失性存储介质、内存储器。该非易失性存储介质存储有操作系统和计算机程序。该内存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该终端设备的网络接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种基于变色龙哈希的加密验证方法。该终端设备的显示屏可以是液晶显示屏或者电子墨水显示屏,该终端设备的温度传感器是预先在终端设备内部设置,用于检测内部设备的运行温度。

[0118] 本领域技术人员可以理解,图3中示出的原理框图,仅仅是与本发明方案相关的部分结构的框图,并不构成对本发明方案所应用于其上的终端设备的限定,具体的终端设备以包括比图中所示更多或更少的部件,或者组合某些部件,或者具有不同的部件布置。

[0119] 在一个实施例中,提供了一种终端设备,终端设备包括存储器、处理器及存储在存

储器中并可在处理器上运行的基于变色龙哈希的加密验证程序,处理器执行基于变色龙哈希的加密验证程序时,实现如下操作指令:

[0120] 接收数据拥有终端发送的预加密数据,所述预加密数据为所述数据拥有终端对所述数据拥有终端持有的原始数据进行初加密处理而得到的加密数据;

[0121] 对所述预加密数据进行再加密处理,得到最终加密数据,所述再加密处理所需的算力大于所述初加密处理所需的算力;

[0122] 对所述最终加密数据应用变色龙哈希算法,验证所述最终加密数据。

[0123] 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程,是可以通过计算机程序来指令相关的硬件来完成,所述的计算机程序可存储于一非易失性计算机可读取存储介质中,该计算机程序在执行时,可包括如上述各方法的实施例的流程。其中,本发明所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用,均可包括非易失性和/或易失性存储器。非易失性存储器可包括只读存储器(ROM)、可编程ROM(PROM)、电可编程ROM(EPROM)、电可擦除可编程ROM(EEPROM)或闪存。易失性存储器可包括随机存取存储器(RAM)或者外部高速缓冲存储器。作为说明而非局限,RAM以多种形式可得,诸如静态RAM(SRAM)、动态RAM(DRAM)、同步DRAM(SDRAM)、双数据率SDRAM(DDRSDRAM)、增强型SDRAM(ESDRAM)、同步链路(Synchlink)DRAM(SLDRAM)、存储器总线(Rambus)直接RAM(RDRAM)、直接存储器总线动态RAM(DRDRAM)、以及存储器总线动态RAM(RDRAM)等。

[0124] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

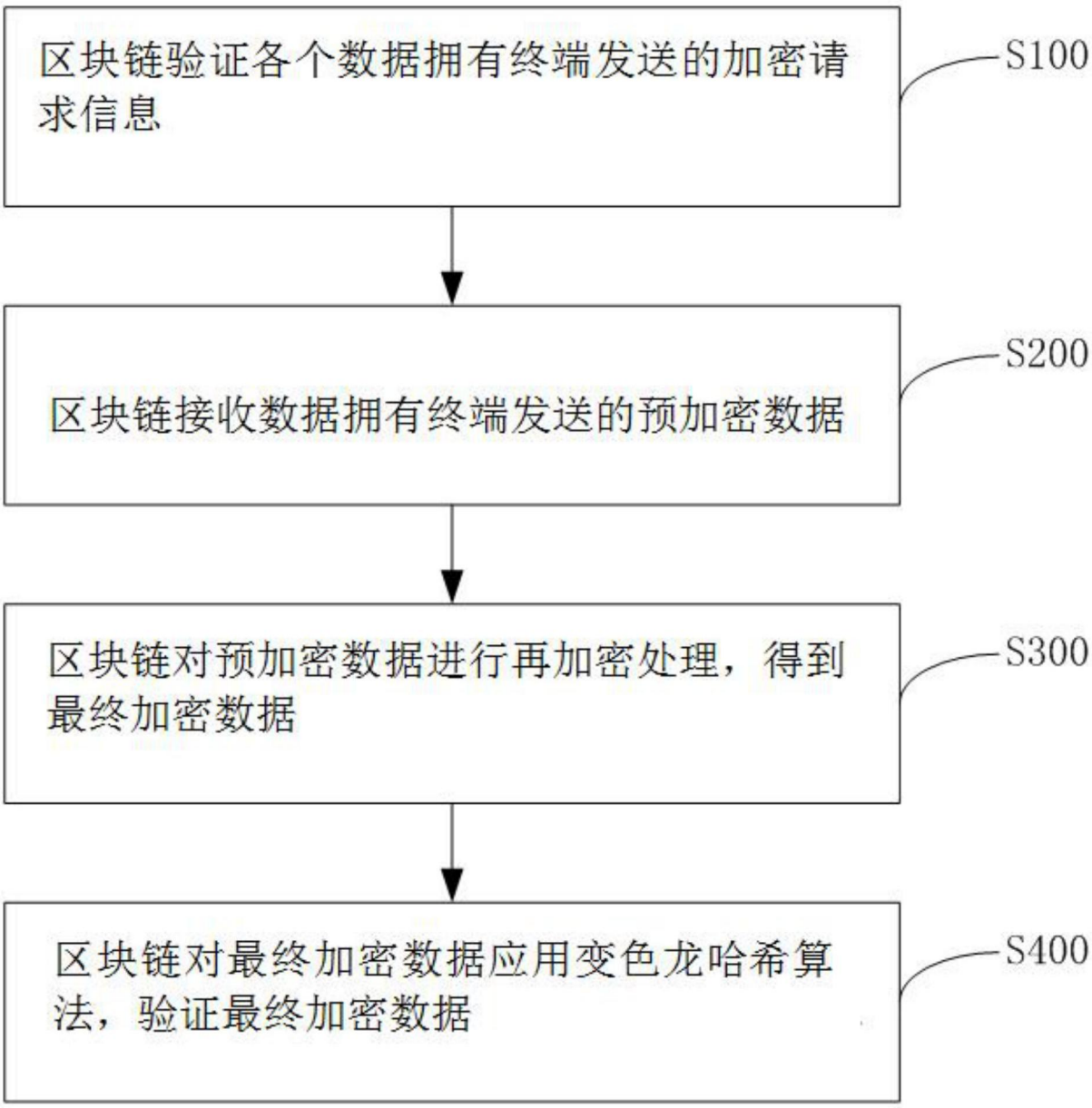

区块链验证各个数据拥有终端发送的加密请求信息
S100
区块链接收数据拥有终端发送的预加密数据
S200
区块链对预加密数据进行再加密处理，得到最终加密数据
S300
区块链对最终加密数据应用变色龙哈希算法，验证最终加密数据
S400

图1

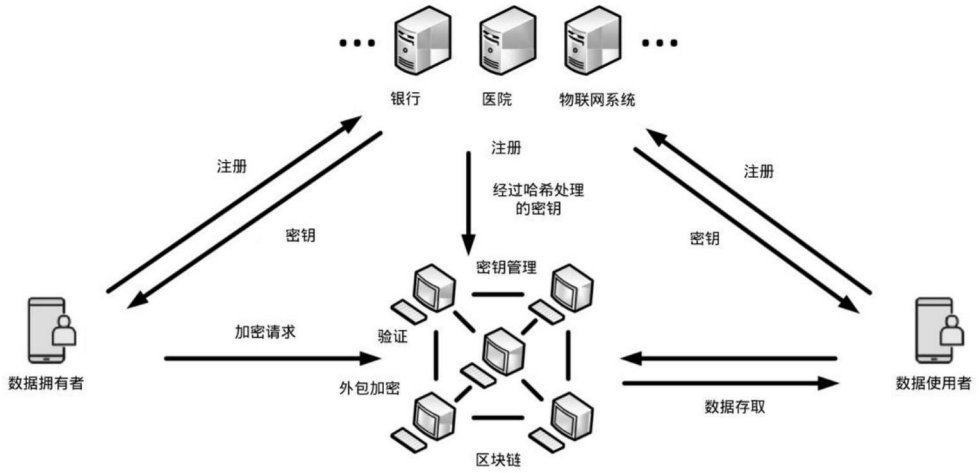

银行
医院
物联网系统
注册
密钥
注册
经过哈希处理的密钥
注册
密钥
密钥管理
加密请求
验证
外包加密
数据拥有者
数据使用者
数据存取
区块链

图2

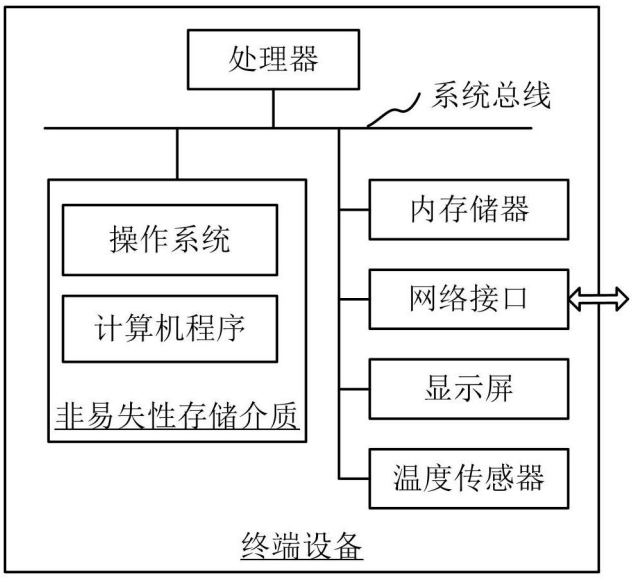

处理器
系统总线
操作系统
计算机程序
非易失性存储介质
内存储器
网络接口
显示屏
温度传感器
终端设备

图3