



(12) 发明专利

(10) 授权公告号 CN 119722112 B

(45) 授权公告日 2025. 06. 06

(21) 申请号 202510237596.5

G06Q 50/02 (2024. 01)

(22) 申请日 2025. 03. 03

G06F 21/64 (2013. 01)

(65) 同一申请的已公布的文献号

申请公布号 CN 119722112 A

(56) 对比文件

CN 118246934 A, 2024. 06. 25

(43) 申请公布日 2025. 03. 28

审查员 王咏冬

(73) 专利权人 江苏天合云商有限公司

地址 210012 江苏省南京市雨花台区凤台

南路146号天合广场1幢2516室

(72) 发明人 陶尚平 周华飞 曾凡瑞 周明桥

吴妍秋

(74) 专利代理机构 南京九致知识产权代理事务

所(普通合伙) 32307

专利代理师 莫冬丽

(51) Int. Cl.

G06Q 30/018 (2023. 01)

权利要求书2页 说明书10页 附图3页

(54) 发明名称

一种全域信息化处理的产品追溯管理方法及电子设备

(57) 摘要

本发明提供了一种全域信息化处理的产品追溯管理方法及电子设备,涉及产品追溯管理技术领域,包括:在目标承包果树的追溯节点完成后,存储至承包数据库,并通过迭代加密同步至云端数据库,生成云端验证密钥和操作密钥,云端操作密钥进行动态切分,生成验证切分密钥并存储,剩余密钥通过安全方式发送给目标用户,将成熟果实包装并创建关联的追溯识别码,目标用户扫描识别码获取验证密钥,结合追溯切分密钥校验云端验证密钥,若校验通过,云端数据库提供数据验证结果。本发明解决了现有技术的产品追溯管理方法往往只依赖于单一的数据库存储,缺乏有效的加密技术手段,产品的追溯信息容易被篡改或伪造,导致存在安全隐患的技术问题。

在目标承包果树的P个追溯节点完成后,将P个追溯节点数据分别存储至承包数据库中P个独立存储单元的P个第一存储区域,并将P个追溯节点数据进行迭代关联加密后同步至云端数据库,获得P个云端验证密钥和P个云端操作密钥,P为正整数

对P个云端操作密钥进行动态切分,将获得的P个验证切分密钥存储至P个独立存储单元的P个第二存储区域和将获得的P个追溯切分密钥发送至目标用户

将目标承包果树的成熟果实打包装箱后,创建与承包数据库相关联的追溯识别码

目标用户在收到运输箱后,扫描追溯识别码获得P个验证切分密钥,结合P个追溯切分密钥对P个云端验证密钥进行校验,若校验通过,调用云端数据库对P个第一存储区域内的数据进行追溯验证,获得追溯验证结果

1. 一种全域信息化处理的产品追溯管理方法,其特征在于,所述方法包括:

在目标承包果树的P个追溯节点完成后,将P个追溯节点数据分别存储至承包数据库中P个独立存储单元的P个第一存储区域,并将P个追溯节点数据进行迭代关联加密后同步至云端数据库,获得P个云端验证密钥和P个云端操作密钥,P为正整数;

对P个云端操作密钥进行动态切分,将获得的P个验证切分密钥存储至P个独立存储单元的P个第二存储区域和将获得的P个追溯切分密钥发送至目标用户,包括:

利用随机数生成器生成P个随机数组合,其中,每个随机数组合包括第一随机数和第二随机数,每个随机数组合对应一个云端操作密钥;

分别将P个随机数组合中任意一个随机数组合中第一随机数比上该随机数组合中第一随机数和第二随机数的总和,获得P个动态切分比例;

利用所述P个动态切分比例分别对所述P个云端操作密钥进行切分,获得P个验证切分密钥和P个追溯切分密钥;

将目标承包果树的成熟果实打包装箱后,创建与承包数据库相关联的追溯识别码;

目标用户在收到运输箱后,扫描追溯识别码获得P个验证切分密钥,结合P个追溯切分密钥对P个云端验证密钥进行校验,若校验通过,调用云端数据库对P个第一存储区域内的数据进行追溯验证,获得追溯验证结果。

2. 如权利要求1所述的一种全域信息化处理的产品追溯管理方法,其特征在于,并将P个追溯节点数据进行迭代关联加密后同步至云端数据库,获得P个云端验证密钥和P个云端操作密钥,包括:

按照P个追溯节点的先后顺序,利用RSA算法依次对所述P个追溯节点数据进行加密,获得P个初始加密密钥对;

对所述P个初始加密密钥对进行两两组合,获得初始加密密钥对组合集合;

遍历所述初始加密密钥对组合集合进行相似度识别,获得初始相似度集合;

判断所述初始相似度集合中大于等于预设相似度阈值的初始相似度的数量是否满足预设数量阈值,若是,则触发密钥调整指令,根据所述密钥调整指令对P个初始加密密钥对进行迭代关联加密,获得P个调整加密密钥对;

基于所述P个调整加密密钥对获得所述P个云端验证密钥和P个云端操作密钥。

3. 如权利要求2所述的一种全域信息化处理的产品追溯管理方法,其特征在于,若是,则触发密钥调整指令,根据所述密钥调整指令对P个初始加密密钥对进行迭代关联加密,获得P个调整加密密钥对,包括:

从所述P个初始加密密钥对中提取加密顺序位于第一位和第二位的第一初始加密密钥对和第二初始加密密钥对;

获取第一初始加密密钥对的第一加密方式和第二初始加密密钥对的第二加密方式;

基于第一加密方式对所述第二加密方式进行方向性调整,获得第二调整加密方式;

再次从所述P个初始加密密钥对中提取加密顺序位于第三位的第三初始加密密钥对,获取所述第三初始加密密钥对的第三加密方式,并基于第一加密方式和第二调整加密方式对所述第三加密方式进行方向性调整,获得第三调整加密方式;

以此类推,直至从所述P个初始加密密钥对中提取加密顺序位于第P位的第P初始加密密钥对,获取所述第P初始加密密钥对的第P加密方式,并基于第一加密方式、第二调整加密

方式、第三调整加密方式直至第P-1调整加密方式对所述第P加密方式进行方向性调整,获得第P调整加密方式;

基于第一加密方式、第二调整加密方式、第三调整加密方式直至第P调整加密方式分别对所述P个初始加密密钥对中对应的初始加密密钥对重新进行加密,获得P个调整加密密钥对。

4.如权利要求3所述的一种全域信息化处理的产品追溯管理方法,其特征在于,基于第一加密方式对所述第二加密方式进行方向性调整,获得第二调整加密方式,包括:

计算所述第一加密方式和所述第二加密方式的相似度,将计算结果比上预设相似度阈值,获得第一调整带宽;

按照所述第一调整带宽对所述第二加密方式进行多次随机调整,获得第二初始调整加密方式集合;

遍历计算所述第二初始调整加密方式集合和第一加密方式的相似度,获得初始调整相似度集合;

将所述初始调整相似度集合中最小值对应的第二初始调整加密方式作为方向第二初始调整加密方式;

以所述方向第二初始调整加密方式为调整方向,按照所述第一调整带宽对所述第二初始调整加密方式集合中其余的第二初始调整加密方式进行调整,获得第二迭代调整加密方式集合;

计算所述第二迭代调整加密方式集合中与第一加密方式的迭代调整相似度集合,判断所述迭代调整相似度集合中是否存在小于等于方向第二初始调整加密方式对应的初始调整相似度,若是,则将迭代调整相似度集合中最小值对应的第二迭代调整加密方式更新为调整方向,继续对第二迭代调整加密方式集合中剩余的第二迭代调整加密方式进行方向性调整,直至满足预设最大调整次数,将最后一次调整获得的调整方向作为第二调整加密方式。

5.如权利要求4所述的一种全域信息化处理的产品追溯管理方法,其特征在于,若所述迭代调整相似度集合中存在大于方向第二初始调整加密方式对应的初始调整相似度,则再次按照所述第一调整带宽对所述第二加密方式进行多次随机调整,并根据调整结果对第二初始调整加密方式集合进行更新。

6.如权利要求3所述的一种全域信息化处理的产品追溯管理方法,其特征在于,所述第一加密方式包括第一初始素数组合、第一公钥指数和第一私钥指数。

7.一种电子设备,包括存储器和处理器,所述存储器存储有计算机程序,其特征在于,所述处理器对所述计算机程序进行执行,实现权利要求1至6中任一项所述的一种全域信息化处理的产品追溯管理方法的步骤。

一种全域信息化处理的产品追溯管理方法及电子设备

技术领域

[0001] 本发明涉及产品追溯管理技术领域,具体涉及一种全域信息化处理的产品追溯管理方法及电子设备。

背景技术

[0002] 在农业领域,果树种植、成熟、采摘、运输等各个环节的信息记录与追溯成为了保障农产品质量和安全的关键,然而,现有的追溯系统存在着数据存储方式不安全、信息篡改风险较高、验证环节繁琐等问题,尤其是在信息化处理和安全性方面的技术发展较为滞后。

[0003] 现有技术中,很多产品追溯系统采用云端存储来记录产品各个环节的数据信息,同时通过二维码、条形码等标识符来进行信息的读取与验证,这些技术通常利用扫描设备让消费者或者相关人员通过扫描识别码来查询产品的来源与流通情况,这类技术存在一些问题,一方面,很多现有的追溯系统中的数据往往只依赖于单一的数据库存储,缺乏有效的加密技术手段,一旦数据库遭遇攻击或数据泄露,产品的追溯信息容易被篡改或伪造;另一方面,一些现有技术采用简单的密钥或密码保护系统,但这些密钥未经过切分或加密处理,容易在传输过程中被拦截或者破解,导致整个追溯过程的安全性下降。

发明内容

[0004] 本申请通过提供一种全域信息化处理的产品追溯管理方法及电子设备,旨在解决现有技术的产品追溯管理方法往往只依赖于单一的数据库存储,缺乏有效的加密技术手段,一旦数据库遭遇攻击或数据泄露,产品的追溯信息容易被篡改或伪造,导致存在安全隐患的技术问题。

[0005] 本申请公开的第一个方面,提供了一种全域信息化处理的产品追溯管理方法,所述方法包括:在目标承包果树的P个追溯节点完成后,将P个追溯节点数据分别存储至承包数据库中P个独立存储单元的P个第一存储区域,并将P个追溯节点数据进行迭代关联加密后同步至云端数据库,获得P个云端验证密钥和P个云端操作密钥,P为正整数;对P个云端操作密钥进行动态切分,将获得的P个验证切分密钥存储至P个独立存储单元的P个第二存储区域和将获得的P个追溯切分密钥发送至目标用户;将目标承包果树的成熟果实打包装箱后,创建与承包数据库相关联的追溯识别码;目标用户在收到运输箱后,扫描追溯识别码获得P个验证切分密钥,结合P个追溯切分密钥对P个云端验证密钥进行校验,若校验通过,调用云端数据库对P个第一存储区域内的数据进行追溯验证,获得追溯验证结果。

[0006] 本申请公开的第二个方面,提供了一种电子设备,包括存储器和处理器,所述存储器存储有计算机程序,所述处理器对所述计算机程序进行执行,实现第一方面中一种全域信息化处理的产品追溯管理方法的步骤。

[0007] 本申请中提供的一个或多个技术方案,至少具有如下有益效果:

[0008] 通过将目标承包果树的P个追溯节点数据存储到承包数据库中,并将其加密后同步到云端数据库,确保了数据的安全性和隐私保护,每个追溯节点数据经过迭代加密,并生

成云端验证密钥和操作密钥,这种加密方法有效防止了数据泄露或被篡改的风险,同时为后续的追溯验证提供了可靠的加密基础;通过对P个云端操作密钥进行动态切分,并将切分后的密钥分别存储和传送给目标用户,这种方法增加了追溯验证过程中的安全性,通过将密钥切分成多个部分,避免了单一密钥丢失或泄露所带来的风险,同时确保密钥在传输过程中难以被拦截或破解;当目标用户收到包装箱并扫描追溯识别码时,他们可以通过验证切分密钥和追溯切分密钥对云端数据库中的数据进行验证,这一机制确保了用户能够从目标果树的种植过程、包装到最终运输过程中获得的所有信息,任何环节都可以通过云端验证与承包数据库进行匹配,从而实现全过程的透明和可信;在目标用户收到商品并扫描追溯识别码后,通过结合追溯切分密钥和验证切分密钥对云端验证密钥进行校验,进一步提高了安全性,由于密钥是分布式存储和切分的,攻击者需要破解多个部分才能获得完整的验证密钥,这使得整个追溯系统具有较高的抗攻击能力。

[0009] 上述说明仅是本申请技术方案的概述,为了能够更清楚了解本申请的技术手段,而可依照说明书的内容予以实施,并且为了让本申请的上述和其它目的、特征和优点能够更明显易懂,以下特举本申请的具体实施方式。

附图说明

[0010] 图1为本申请实施例提供了一种全域信息化处理的产品追溯管理方法流程图。

[0011] 图2为本申请实施例提供了一种全域信息化处理的产品追溯管理方法中获得P个云端验证密钥和P个云端操作密钥流程图示意图。

[0012] 图3为本申请实施例提供的示例性电子设备的结构示意图。

具体实施方式

[0013] 本申请通过提供一种全域信息化处理的产品追溯管理方法及电子设备,解决了现有技术的产品追溯管理方法往往只依赖于单一的数据库存储,缺乏有效的加密技术手段,一旦数据库遭遇攻击或数据泄露,产品的追溯信息容易被篡改或伪造,导致存在安全隐患的技术问题。

[0014] 在介绍了本申请基本原理后,下面将结合说明书附图来具体介绍本申请的各种非限制性的实施方式。

[0015] 实施例一,如图1所示,本申请实施例提供了一种全域信息化处理的产品追溯管理方法,所述方法包括:

[0016] 在目标承包果树的P个追溯节点完成后,将P个追溯节点数据分别存储至承包数据库中P个独立存储单元的P个第一存储区域,并将P个追溯节点数据进行迭代关联加密后同步至云端数据库,获得P个云端验证密钥和P个云端操作密钥,P为正整数。

[0017] 在目标承包果树的种植过程中,将每一个关键节点(如种植、浇水、施肥、采摘等)记录为一个追溯节点,每当某个追溯节点完成时,就会立即收集该节点的相关信息,并进行数据存储,这些节点数据包含果树各个成长阶段的详细信息,例如,浇水时间、浇水量、施肥情况、天气条件、农药使用等,这些信息是为了支持后续的全流程追溯,并确保数据的真实性。

[0018] 承包数据库用于存储目标承包果树的所有全域信息数据,这个数据库是果树管理过程中的核心数据存储中心,包含了所有从种植到最终产品的所有数据,承包数据库中的数据存储结构包括多个独立存储单元,每个追溯节点完成后,其相关数据分别存储到不同的存储单元中,这些存储单元有两个主要区域,其中,第一存储区域用于存储与果树成长各个阶段相关的节点数据和操作记录,这些数据包括但不限于每个成长阶段的数据,这些数据记录的是果树在各个阶段的实际操作和环境条件;第二存储区域用于存储与客户验证相关的验证切分密钥,这些密钥是为了后续的客户验证和防伪机制而存储的,支持客户对果树产品进行全流程追溯验证,在果树到达最终消费者之前,这些切分密钥将用于确保追溯信息的可靠性和防篡改。

[0019] 在将P个追溯节点数据存储到承包数据库后,对所有这些数据进行迭代关联加密,该加密方式是逐个节点对数据进行加密,并结合前一个节点的加密结果进行处理,从而形成一个加密链条,增加了数据的安全性。将加密后的追溯节点数据同步至云端数据库,通过将数据上传到云端,可以确保数据的冗余备份并提高数据的可访问性,同时,云端数据库能够提供高效的数据管理和查询服务。与承包数据库相比,云端数据库在数据的共享和存储容量上具有更大的优势。

[0020] 在数据上传至云端数据库的过程中,每个加密数据节点关联生成独立的云端验证密钥和云端操作密钥,其中,云端验证密钥用于在后续的追溯验证过程中,确保数据的真实性和完整性,防止数据被篡改;云端操作密钥用于支持云端数据库的操作,例如访问控制、数据查询等功能,是数据交互和操作的基础。

[0021] 对P个云端操作密钥进行动态切分,将获得的P个验证切分密钥存储至P个独立存储单元的P个第二存储区域和将获得的P个追溯切分密钥发送至目标用户。

[0022] 将生成的P个云端操作密钥进行动态切分,动态切分是将每个云端操作密钥进行切分,产生对应的验证切分密钥和一个追溯切分密钥,通过切分操作密钥,确保即使某部分密钥泄露,整个密钥系统仍能保持安全,因为完整的验证和追溯过程需要多个切分部分配合才能有效操作。

[0023] 将获得的P个验证切分密钥存储至P个独立存储单元中的第二存储区域,每个存储单元对应不同的切分密钥,追溯切分密钥则发送给目标用户,这样用户可以在产品的追溯和防伪验证过程中使用这些密钥,进一步加强产品的追溯可验证性,用户接收到这些密钥后,可以结合验证密钥对云端的验证信息进行检验。

[0024] 将目标承包果树的成熟果实打包装箱后,创建与承包数据库相关联的追溯识别码。

[0025] 当目标承包果树的成熟果实被打包装箱后,为这些果实生成一个追溯识别码,该识别码是一个唯一标识符,用于追踪该批次果实的整个生命周期,该识别码与承包数据库中的数据相关联,能够提供完整的追溯信息,消费者或供应链中的其他方可以通过扫描该识别码获取从果树种植到果实采摘、运输等每个环节的详细信息。追溯识别码的核心作用在于让消费者和相关人员能够通过扫描识别码,迅速查找到关于产品的详细信息,这不仅提高了消费者对产品质量和来源的信任,也有助于防伪和保障食品安全。

[0026] 目标用户在收到运输箱后,扫描追溯识别码获得P个验证切分密钥,结合P个追溯切分密钥对P个云端验证密钥进行校验,若校验通过,调用云端数据库对P个第一存储区域

内的数据进行追溯验证,获得追溯验证结果。

[0027] 目标用户是指承包目标承包果树的用户,当他们收到运输箱时,扫描运输箱上的追溯识别码,获取与该识别码相关的P个验证切分密钥。

[0028] 目标用户将收到的验证切分密钥与自己获得的追溯切分密钥相结合,对云端生成的P个云端验证密钥进行校验,这是第一重验证,其目的是确认运输箱中的商品是否与原计划一致,如果校验失败,说明可能存在问题,如运输箱可能被调换或伪造,此时将提示用户存在潜在的风险,该验证步骤确保了运输箱中的产品信息的正确性和防伪性。

[0029] 如果第一重验证通过,则进一步调用云端数据库,对存储在承包数据库中的P个第一存储区域内的数据进行追溯验证,这是第二重验证,目的是确认产品的所有追溯数据是否准确无误,如果数据与云端数据库中的信息不符,可能存在果实被调换或装错的情况,通过追溯验证,用户可以确保他们收到的果实是原始、未被篡改的,且符合所有的质量要求,如果验证失败,将会给出警告并标识出数据不符的具体问题。

[0030] 如果两重验证均通过,则生成并提供追溯验证结果,该结果表明运输的果实是正确且真实的,符合预期的追溯信息,用户可以通过追溯验证结果,获得关于果树种植、成长、采摘、运输等全程信息,增强对产品质量和来源的信任。

[0031] 进一步而言,如图2所示,并将P个追溯节点数据进行迭代关联加密后同步至云端数据库,获得P个云端验证密钥和P个云端操作密钥,包括:

[0032] 按照P个追溯节点的先后顺序,利用RSA算法依次对所述P个追溯节点数据进行加密,获得P个初始加密密钥对;对所述P个初始加密密钥对进行两两组合,获得初始加密密钥对组合集合;遍历所述初始加密密钥对组合集合进行相似度识别,获得初始相似度集合;判断所述初始相似度集合中大于等于预设相似度阈值的初始相似度的数量是否满足预设数量阈值,若是,则触发密钥调整指令,根据所述密钥调整指令对P个初始加密密钥对进行迭代关联加密,获得P个调整加密密钥对;基于所述P个调整加密密钥对获得所述P个云端验证密钥和P个云端操作密钥。

[0033] 使用RSA算法依次对P个追溯节点数据进行加密,RSA是一个常用的公钥加密算法,通过使用RSA算法,对每个追溯节点的数据进行加密,确保了数据在传输和存储过程中的保密性和完整性。具体地,对每个追溯节点的数据,使用RSA算法中的公钥对其进行加密,加密后的数据会生成一个密文,与每个追溯节点数据一一对应一个初始加密密钥对,RSA加密使用的是一对公钥和私钥,公钥用于加密,而私钥用于解密,通过这一过程,最终获得P个初始加密密钥对,其中每个密钥对与一个追溯节点数据相对应。

[0034] 将P个初始加密密钥对进行两两组合,即将每两个初始加密密钥对进行配对,生成一组密钥对组合,通过两两组合,获得初始加密密钥对组合集合,这个集合包含了所有的密钥对组合,每个组合都代表了两个追溯节点数据之间的加密密钥对,为接下来的相似度识别提供了基础。

[0035] 对初始加密密钥对组合集合进行相似度识别,相似度识别的目的是判断每对加密密钥对组合之间的相似度程度,相似度的高低可以通过对比加密方式、加密结果或者密钥本身的差异来衡量,将每一对组合的相似度进行计算,获得一组初始相似度值,相似度值用如余弦相似度、哈希相似度等度量标准表示,如果两者加密结果相似或具有相同的加密方式,则判定它们具有较高的相似度,反之,如果加密方式或者结果相差较大,则相似度较低。

最终获得的初始相似度集合中,每个相似度值都表示了对密钥对组合之间的相似程度。

[0036] 预设相似度阈值是一个预设的标准值,用于衡量两个密钥对的相似程度,如果两个密钥对的相似度大于等于该阈值,则判定这对密钥是相似的,需要进行进一步处理,除了相似度阈值,系统还设定了一个预设数量阈值,这意味着,如果在初始相似度集合中,满足相似度阈值的组合数量达到预设数量阈值,则触发密钥调整流程,触发密钥调整指令,这一指令将启动下一步的迭代关联加密,以优化或调整加密密钥的分布和结构,提高加密系统的安全性,其中,具体的迭代关联加密过程在后续步骤中详细展开,通过迭代关联加密,获得P个调整加密密钥对。

[0037] 基于P个调整加密密钥对获得P个云端验证密钥和P个云端操作密钥,其中,云端验证密钥属于公钥,即可以公开使用,不需要保密,公钥用于加密数据或进行验证操作,云端验证密钥将被用于产品追溯的验证过程,用户可以使用这些公钥来验证数据的真实性和完整性;云端操作密钥是私钥,用于解密或对数据进行操作,私钥需要严格保密,不应公开,它将被分发给目标用户,并存储在承包数据库中,目标用户需要通过这些私钥与公钥结合,才能对数据进行解密操作,验证追溯信息。通过这种密钥配对机制,确保了数据的安全性,防止了未经授权的访问和篡改。

[0038] 进一步而言,若是,则触发密钥调整指令,根据所述密钥调整指令对P个初始加密密钥对进行迭代关联加密,获得P个调整加密密钥对,包括:

[0039] 从所述P个初始加密密钥对中提取加密顺序位于第一位和第二位的第一初始加密密钥对和第二初始加密密钥对;获取第一初始加密密钥对的第一加密方式和第二初始加密密钥对的第二加密方式;基于第一加密方式对所述第二加密方式进行方向性调整,获得第二调整加密方式;再次从所述P个初始加密密钥对中提取加密顺序位于第三位的第三初始加密密钥对,获取所述第三初始加密密钥对的第三加密方式,并基于第一加密方式和第二调整加密方式对所述第三加密方式进行方向性调整,获得第三调整加密方式;以此类推,直至从所述P个初始加密密钥对中提取加密顺序位于第P位的第P初始加密密钥对,获取所述第P初始加密密钥对的第P加密方式,并基于第一加密方式、第二调整加密方式、第三调整加密方式直至第P-1调整加密方式对所述第P加密方式进行方向性调整,获得第P调整加密方式;基于第一加密方式、第二调整加密方式、第三调整加密方式直至第P调整加密方式分别对所述P个初始加密密钥对中对应的初始加密密钥对重新进行加密,获得P个调整加密密钥对。

[0040] 从P个初始加密密钥对中提取加密顺序位于第一位和第二位的初始加密密钥对,假设P个初始加密密钥对是按顺序排列的,例如,密钥对1、密钥对2、...、密钥对P,选择排在第一位和第二位的密钥对,获得第一初始加密密钥对和第二初始加密密钥对,用于后续的加密方式分析与调整。

[0041] 分别提取第一初始加密密钥对和第二初始加密密钥对的加密方式,对于第一初始加密密钥对,获取第一加密方式,包括第一初始素数组合、第一公钥指数和第一私钥指数;对于第二初始加密密钥对,获取第二加密方式,第二初始素数组合、第二公钥指数和第二私钥指数。通过这些要素,可以对加密过程进行更细致的控制和优化。

[0042] 方向性调整是指基于第一加密方式的特点,对第二加密方式进行调整,使其满足特定的加密需求或适应新的安全标准,此时,第二加密方式的调整是有方向性的,目的是确

保第二加密方式在某些特定条件下变得更安全、更稳定,具体的调整包括调整公钥指数、私钥指数,或者改变加密素数组合的方式,从而使得第二加密方式在加密强度或性能方面得以优化。经过方向性调整后,获得第二调整加密方式,它是基于第一加密方式的指导下所优化的加密方式,第二调整加密方式具有更高的安全性、可扩展性或者适应性,可以用于后续的密钥加密和解密过程。

[0043] 从P个初始加密密钥对中提取出加密顺序位于第三位的第三初始加密密钥对,这与之前的步骤类似,但是现在关注的是排在第三位的密钥对,提取第三初始加密密钥对后,获取其对应的第三加密方式,第三加密方式同样包括初始素数组合、公钥指数和私钥指数等元素,接下来,基于第一加密方式和第二调整加密方式,对第三加密方式进行方向性调整,这一调整并非简单的改变,而是确保第三加密方式朝着远离第一加密方式和第二加密方式的方向发展,这种调整的目的是为了避免在相似的加密方式之间出现重复或冗余,从而加强加密系统的多样性与安全性,通过远离第一加密方式和第二加密方式,获得的第三调整加密方式在加密过程中的表现更加独立、抗攻击性更强。

[0044] 以此类推,直至从P个初始加密密钥对中提取加密顺序位于第P位的第P初始加密密钥对,这一过程类似于之前步骤中的提取操作,直到提取到最后一个密钥对,即第P初始加密密钥对,获取与第P初始加密密钥对相对应的第P加密方式,基于第一加密方式、第二调整加密方式、第三调整加密方式,一直到第P-1调整加密方式,对第P加密方式进行方向性调整,这一方向性调整的目的是确保第P加密方式与之前的加密方式有所不同,并朝着一个独立且更安全的方向发展,最终,通过方向性调整,获得第P调整加密方式,这一加密方式是基于前面所有调整过的加密方式逐步优化得到的,具有较强的安全性,并且在整个加密链条中起到了重要的作用。

[0045] 基于第一加密方式、第二调整加密方式、第三调整加密方式直至第P调整加密方式,分别对P个初始加密密钥对中的每个初始加密密钥对进行重新加密,每一个初始加密密钥对会按照其对应的加密方式(包括第一加密方式、第二调整加密方式、第三调整加密方式等)进行加密操作,通过这种加密方式的迭代和调整,最终得到一组更加安全和优化的P个调整加密密钥对,这些密钥对比初始的密钥对更加安全、适应性更强,能够有效应对潜在的攻击和破解尝试。

[0046] 进一步而言,基于第一加密方式对所述第二加密方式进行方向性调整,获得第二调整加密方式,包括:

[0047] 计算所述第一加密方式和所述第二加密方式的相似度,将计算结果比上预设相似度阈值,获得第一调整带宽;按照所述第一调整带宽对所述第二加密方式进行多次随机调整,获得第二初始调整加密方式集合;遍历计算所述第二初始调整加密方式集合和第一加密方式的相似度,获得初始调整相似度集合;将所述初始调整相似度集合中最小值对应的第二初始调整加密方式作为方向第二初始调整加密方式;以所述方向第二初始调整加密方式为调整方向,按照所述第一调整带宽对所述第二初始调整加密方式集合中其余的第二初始调整加密方式进行调整,获得第二迭代调整加密方式集合;计算所述第二迭代调整加密方式集合中与第一加密方式的迭代调整相似度集合,判断所述迭代调整相似度集合中是否存在小于等于方向第二初始调整加密方式对应的初始调整相似度,若是,则将迭代调整相似度集合中最小值对应的第二迭代调整加密方式更新为调整方向,继续对第二迭代调整加

密方式集合中剩余的第二迭代调整加密方式进行方向性调整,直至满足预设最大调整次数,将最后一次调整获得的调整方向作为第二调整加密方式。

[0048] 计算第一加密方式与第二加密方式之间的相似度,相似度计算是衡量两个加密方式之间的相似程度,采用如余弦相似度、欧氏距离等度量方式来进行度量,具体地,第一加密方式和第二加密方式各自包含公钥指数、私钥指数和初始素数组合等元素,在比较时,根据这些元素的数值差异计算加密方式之间的相似度,如果两者的加密方式非常相似,则给出一个较高的相似度值;反之,如果两者的加密方式差异较大,则相似度值则较低。

[0049] 将计算结果与预设相似度阈值进行比较,预设相似度阈值是一个定义好的标准,用于判定两个加密方式是否相似到足以需要进行调整,如果计算结果高于或等于预设相似度阈值,说明这两个加密方式太过相似,需要进行调整,以避免加密过程中的冗余或弱点,计算相似度计算结果与预设相似度阈值的比值,将比值作为第一调整带宽,第一调整带宽表示对第二加密方式进行单次调整时的尺度或幅度,决定了调整的大小,例如,带宽越大,调整的幅度越大,反之则较小。

[0050] 根据第一调整带宽对第二加密方式进行多次随机调整,这些调整并非固定的,而是根据带宽的大小随机改变第二加密方式的某些参数,例如公钥指数、私钥指数,或者初始素数组合的选取方式,随机调整的目的是增加加密方式的多样性,同时避免在加密过程中产生过于相似的结果,从而提高加密系统的安全性,通过多次随机调整,生成多个不同的加密方式,每个加密方式与第二加密方式相比,都会有所变化,这些调整后的加密方式整合为第二初始调整加密方式集合。

[0051] 遍历第二初始调整加密方式集合,对于集合中的每一个加密方式,都采用与之前类似的相似度计算方法,计算其与第一加密方式的相似度,计算的结果反映出第二初始调整加密方式与第一加密方式之间的差异性,较低的相似度值表示两个加密方式差异较大,较高的相似度值则表示它们更为相似,经过遍历后,将每个计算出的相似度值存储到初始调整相似度集合中,这个集合包含了所有第二初始调整加密方式与第一加密方式的相似度值。

[0052] 遍历初始调整相似度集合,找出其中的最小值,最小值代表了与第一加密方式最为不同的第二初始调整加密方式,将最小相似度值所对应的第二初始调整加密方式选定为方向第二初始调整加密方式,这个加密方式是当前加密方式与第一加密方式差异最大的选择,因此它将作为后续加密调整的方向性参考,该加密方式的选择意味着在后续的加密过程中朝着与第一加密方式更为不同的方向进行调整,进一步增加系统的复杂度和安全性。

[0053] 将方向第二初始调整加密方式作为后续调整过程中的参考方向,意味着将根据这个加密方式的特点来调整其他加密方式,使得这些加密方式与第一加密方式的相似度进一步降低,基于方向第二初始调整加密方式和第一调整带宽,对第二初始调整加密方式集合中的其余加密方式进行调整,调整的过程涉及更改公钥指数、私钥指数,或者调整初始素数组合等,通过迭代的方法,可以逐步优化这些加密方式的安全性和独立性。经过多次调整后,得到一个新的集合,即为第二迭代调整加密方式集合,这个集合包含了所有经过调整后的加密方式,它们与第一加密方式的相似度更小,从而提升了系统的安全性。

[0054] 采用与之前类似的相似度计算方法,计算第二迭代调整加密方式集合中的每个加密方式与第一加密方式之间的相似度,获得迭代调整相似度集合,迭代调整相似度集合包

含所有这些加密方式与第一加密方式的相似度值,用于后续的选择和调整。

[0055] 检查迭代调整相似度集合中的所有相似度值,判断是否存在小于等于方向第二初始调整加密方式对应的初始调整相似度的值,该初始调整相似度是前述步骤选定的最小相似度值,相似度值低于或等于这个值的加密方式将作为目标进行进一步的优化,如果存在该情况,说明某些加密方式已经与第一加密方式有足够大的差异,可以继续调整以进一步增强加密方式的独立性,

[0056] 如果找到迭代调整相似度集合中小于等于上述初始调整相似度的值,将选择该加密方式对应的加密密钥对作为新的调整方向,并更新为第二迭代调整加密方式的调整方向,以此调整方向继续对第二迭代调整加密方式集合中剩余的加密方式进行方向性调整,这一过程会继续进行,直至所有的加密方式都朝着目标方向调整,这一调整过程是迭代的,也就是说,会反复进行调整,直到满足一个预设的最大调整次数,调整次数限制确保加密系统在保证安全性的同时,不会因为过多的调整导致计算效率过低,最后,经过多次调整后,选择最终一次调整中获得的调整方向,并将其作为第二调整加密方式,这个加密方式与第一加密方式之间有更大的差异,确保了加密密钥的多样性和抗攻击性。

[0057] 进一步而言,若所述迭代调整相似度集合中存在大于方向第二初始调整加密方式对应的初始调整相似度,则再次按照所述第一调整带宽对所述第二加密方式进行多次随机调整,并根据调整结果对第二初始调整加密方式集合进行更新。

[0058] 检查迭代调整相似度集合中的所有相似度值,判断是否存在大于方向第二初始调整加密方式对应的初始调整相似度的值,如果存在,则根据之前计算的第一调整带宽,对第二加密方式进行多次随机调整,这意味着重新调整第二加密方式,尝试通过不同的方式修改其参数,使其朝着更加安全或独立的方向发展,随机调整的过程意味着对第二加密方式进行的每次调整都是不确定的,因此可能得到多个不同的加密方式,在多次随机调整之后,根据调整后的加密方式结果,更新第二初始调整加密方式集合,更新后的集合包含更多具有不同特征的加密方式,为系统提供更大的灵活性和安全性选择。

[0059] 进一步而言,所述第一加密方式包括第一初始素数组合、第一公钥指数和第一私钥指数。

[0060] 第一加密方式包括第一初始素数组合、第一公钥指数和第一私钥指数,这些元素共同决定了RSA加密系统的工作原理和加密强度。

[0061] 在RSA加密算法中,初始素数组合指的是两个大素数(通常称为 p 和 q),它们是用来生成公钥和私钥的基础,通过这两个素数,RSA算法可以计算出模数 n (即 $n=p \times q$)以及其他相关的密钥参数,素数组合直接影响加密算法的安全性,初始素数组合是RSA加密系统中的核心元素,它决定了加密密钥对的强度,如果选择的素数较小或较容易被分解,则可能导致加密过程的破解。

[0062] 公钥指数是公钥的一部分,通常表示为一个整数 e (通常选取常用的数字如65537),它是一个小于 $\varphi(n)$ 的正整数,并且与 $\varphi(n)$ 互质,这样才能确保加密和解密过程正常工作,在RSA算法中,公钥指数的作用是在加密过程中用于加密消息。

[0063] 私钥指数是私钥的一部分,通常表示为 d ,在RSA算法中,私钥是用来解密加密消息的,私钥指数 d 是公钥指数 e 与 $\varphi(n)$ 的模逆,在解密过程中,使用私钥指数 d 来恢复原始明文。

[0064] 进一步而言,对P个云端操作密钥进行动态切分,将获得的P个验证切分密钥存储至P个独立存储单元的P个第二存储区域和将获得的P个追溯切分密钥发送至目标用户,包括:

[0065] 利用随机数生成器生成P个随机数组合,其中,每个随机数组合包括第一随机数和第二随机数,每个随机数组合对应一个云端操作密钥;分别将P个随机数组合中任意一个随机数组合中第一随机数比上该随机数组合中第一随机数和第二随机数的总和,获得P个动态切分比例;利用所述P个动态切分比例分别对所述P个云端操作密钥进行切分,获得P个验证切分密钥和P个追溯切分密钥。

[0066] 利用随机数生成器,例如rand函数,生成P个随机数组合,每个随机数组合由两个随机数组成,分别称为第一随机数和第二随机数,这些随机数组合用于后续的密钥切分过程,每个随机数组合对应着一个云端操作密钥,这些密钥用于云端与用户之间的操作验证。

[0067] 根据第一随机数和第二随机数计算动态切分比例,具体的计算方法是,对于任意一个随机数组合,计算第一随机数与该随机数组合中第一随机数和第二随机数的总和之比,将得到的比值作为一个动态切分比例,这一比例将决定后续云端操作密钥的切分方式,确保每个密钥部分的大小和分布是基于生成的随机数动态变化的。动态切分比例的计算确保了每个云端操作密钥被切分成多个部分,而且这些部分的大小会随着随机数的变化而变化,使得密钥的切分更加灵活且难以预测,从而增加了密钥系统的安全性。

[0068] 利用计算出的P个动态切分比例对每个云端操作密钥进行切分,每个云端操作密钥将根据对应的动态切分比例,分割成两个部分,一个是验证切分密钥,另一个是追溯切分密钥,具体来说,动态切分比例决定了云端操作密钥的切分比例,例如,如果一个切分比例为0.7,那么该云端操作密钥将70%作为验证密钥,30%作为追溯密钥,反之亦然。对每个云端操作密钥进行切分后,获得了P个验证切分密钥和P个追溯切分密钥,验证切分密钥用于后续的验证过程,而追溯切分密钥则帮助确保产品在追溯过程中能够确认其来源和真实性。

[0069] 综上所述,本申请实施例所提供的一种全域信息化处理的产品追溯管理方法具有如下技术效果:

[0070] 通过将目标承包果树的P个追溯节点数据存储到承包数据库中,并将其加密后同步到云端数据库,确保了数据的安全性和隐私保护,每个追溯节点数据经过迭代加密,并生成云端验证密钥和操作密钥,这种加密方法有效防止了数据泄露或被篡改的风险,同时为后续的追溯验证提供了可靠的加密基础;通过对P个云端操作密钥进行动态切分,并将切分后的密钥分别存储和传送给目标用户,这种方法增加了追溯验证过程中的安全性,通过将密钥切分成多个部分,避免了单一密钥丢失或泄露所带来的风险,同时确保密钥在传输过程中难以被拦截或破解;当目标用户收到包装箱并扫描追溯识别码时,他们可以通过验证切分密钥和追溯切分密钥对云端数据库中的数据进行验证,这一机制确保了用户能够从目标果树的种植过程、包装到最终运输过程中获得的所有信息,任何环节都可以通过云端验证与承包数据库进行匹配,从而实现全过程的透明和可信;在目标用户收到商品并扫描追溯识别码后,通过结合追溯切分密钥和验证切分密钥对云端验证密钥进行校验,进一步提高了安全性,由于密钥是分布式存储和切分的,攻击者需要破解多个部分才能获得完整的验证密钥,这使得整个追溯系统具有较高的抗攻击能力。

[0071] 实施例二,如图3所示,为本申请示例性电子设备的结构示意图。在图3中,总线架

构用总线300来代表,总线300可以包括任意数量的互联的总线和桥,总线300将包括由处理器302代表的一个或多个处理器和存储器304代表的存储器的各种电路连接在一起。总线300还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路连接在一起,这些都是本领域所公知的,因此,本文不再对其进行进一步描述。总线接口305在总线300和接收器301和发送器303之间提供接口。接收器301和发送器303可以是同一个元件,即收发机,提供用于在传输介质上与各种其他装置通信的单元。处理器302负责管理总线300和通常的处理,而存储器304可以被用于存储处理器302在执行操作时所使用的数据。

[0072] 对所公开的实施例的上述说明,使本领域专业技术人员能够实现或使用本申请。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的,本文中所定义的一般原理可以在不脱离本申请的精神或范围的情况下,在其它实施例中实现。因此,本申请将不会被限制于本文所示的这些实施例,而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

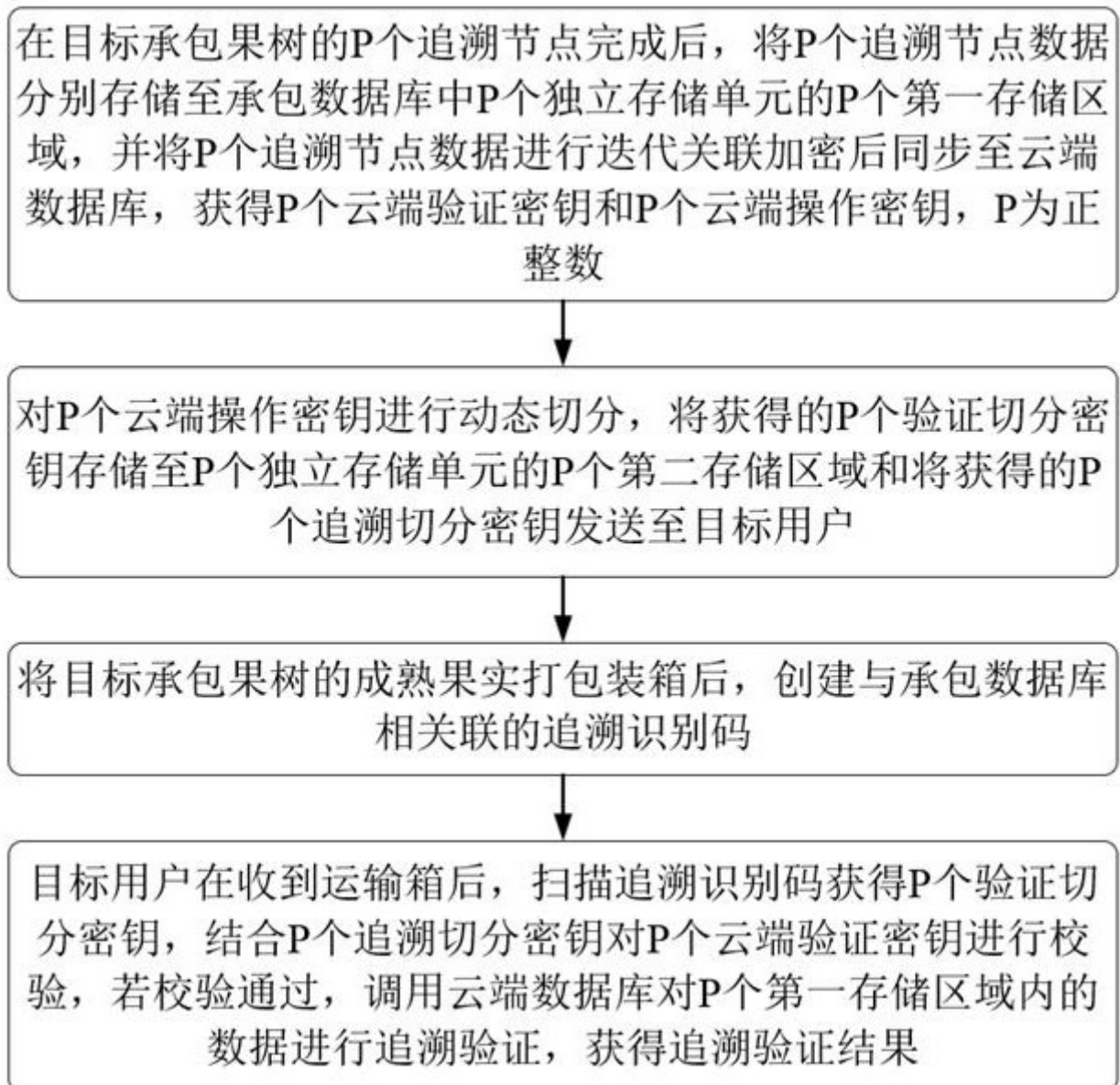


图 1

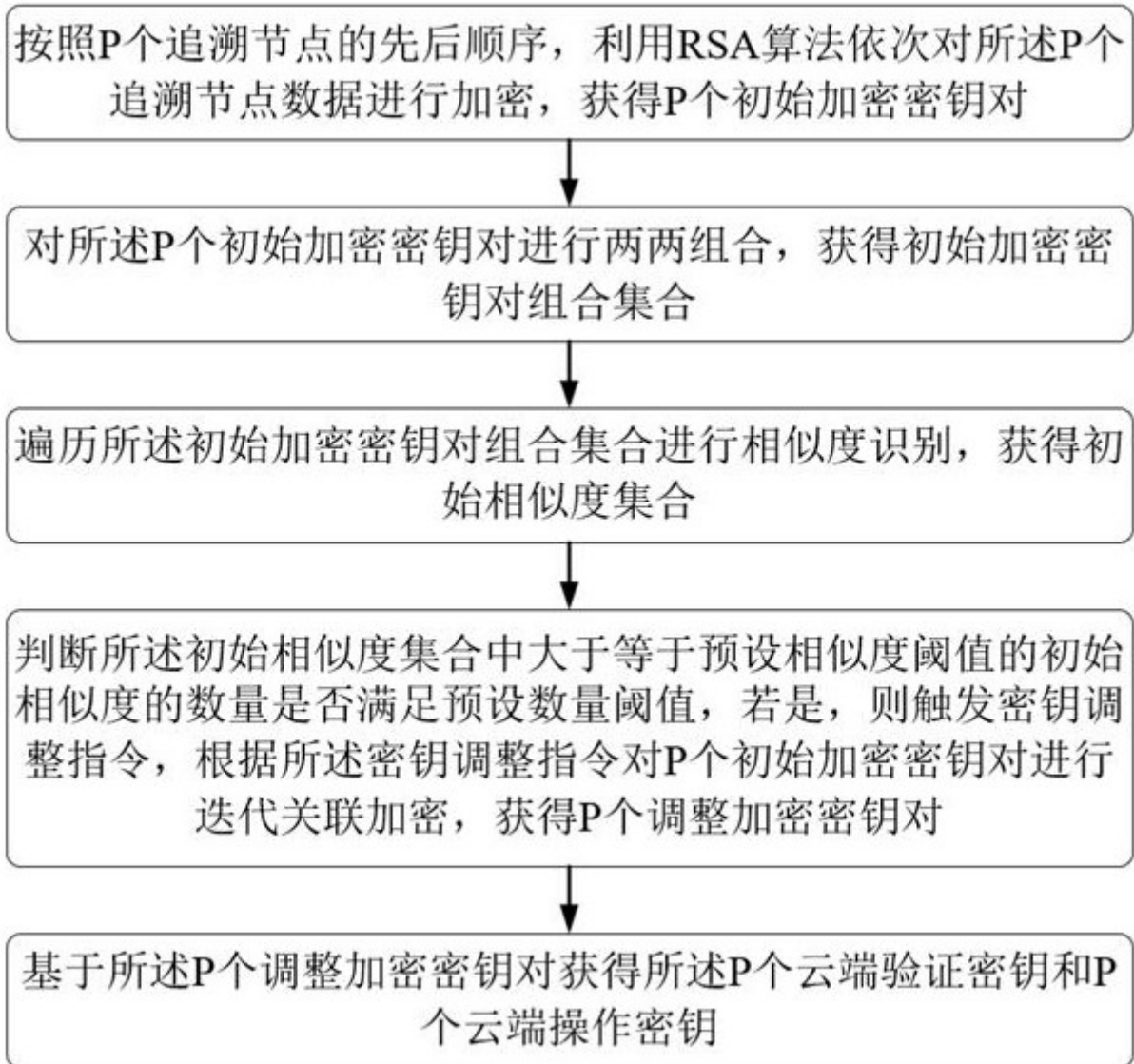


图 2

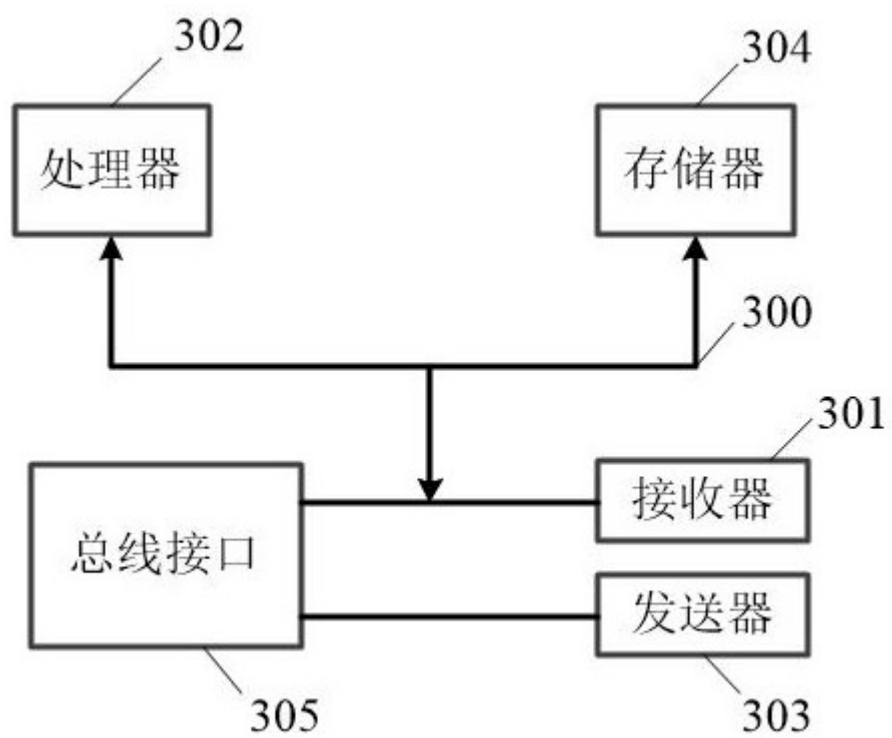


图 3