(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 4 月 7 日 (07.04.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/068237 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2021/097120

(22) 国际申请日: 2021 年 5 月 31 日 (31.05.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011054352.7 2020年9月29日 (29.09.2020) CN

(71) 申请人: 平安科技（深圳）有限公司 (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(72) 发明人: 贾牧 (JIA, Mu); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。 陆陈一帆 (LU, Frank YiFan Chen); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。 谢丹力 (XIE, Danli); 中国广东省深圳市福田区福田街道福安社区益田路5033号平安金融中心23楼, Guangdong 518000 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

(54) **Title:** INFORMATION PROCESSING METHOD AND APPARATUS FOR GENERATING KEY ON THE BASIS OF ATTRIBUTE OF INFORMATION, AND DEVICE

(54) 发明名称: 基于信息的属性生成密钥的信息处理方法、装置及设备

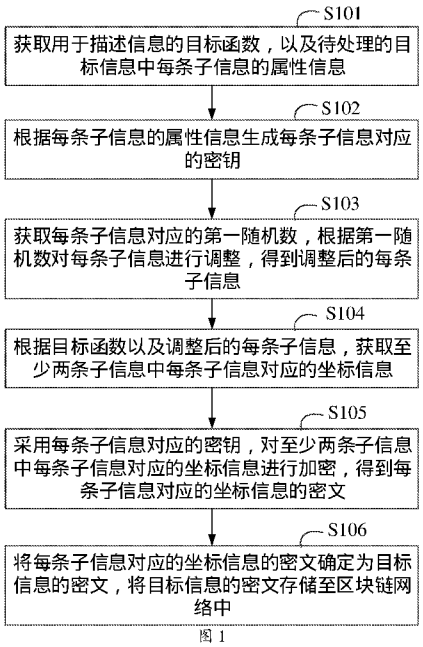


图 1

S101 Acquire a target function for describing information and attribute information of each piece of sub-information in target information to be processed

S102 Generate a key of each piece of sub-information according to the attribute information of each piece of sub-information

S103 Acquire a first random number corresponding to each piece of sub-information, and adjust each piece of sub-information according to the first random number, so as to obtain each piece of adjusted sub-information

S104 According to the target function and each piece of adjusted sub-information, acquire coordinate information corresponding to each piece of sub-information among at least two pieces of sub-information

S105 Encrypt the coordinate information of each piece of sub-information among at least two pieces of sub-information by using the key of each piece of sub-information, so as to obtain a ciphertext of the coordinate information corresponding to each piece of sub-information

S106 Determine the ciphertext of the coordinate information corresponding to each piece of sub-information as a ciphertext of the target information, and store the ciphertext of the target information into a block chain network

(57) **Abstract:** An information processing method and apparatus for generating a key on the basis of attribute of information, and a device. Said method comprises: acquiring a target function for describing information and attribute information of each piece of sub-information in target information to be processed (S101); generating a key of each piece of sub-information according to the attribute information of each piece of sub-information (S102); acquiring a first random number corresponding to each piece of sub-information,

WO 2022/068237 A1

[见续页]

BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

一 包括国际检索报告(条约第21条(3))。

and adjusting each piece of sub-information according to the first random number, so as to obtain each piece of adjusted sub-information (S103); according to the target function and each piece of adjusted sub-information, acquiring coordinate information corresponding to each piece of sub-information (S104); encrypting the coordinate information of each piece of sub-information by using the key of each piece of sub-information, so as to obtain a ciphertext of the coordinate information (S105); and determining the ciphertext of the coordinate information corresponding to each piece of sub-information as a ciphertext of the target information, and storing the ciphertext of the target information into a block chain network (S106). The invention improves the security of information.

(57) 摘要：一种基于信息的属性生成密钥的信息处理方法、装置及设备，其中，方法包括：获取用于描述信息的目标函数和待处理的目标信息中每条子信息的属性信息（S101）；根据每条子信息的属性信息生成每条子信息的密钥（S102）；获取每条子信息对应的第一随机数，根据第一随机数对每条子信息进行调整，得到调整后的每条子信息（S103）；根据目标函数和调整后的每条子信息，获取每条子信息对应的坐标信息（S104）；采用每条子信息的密钥，对每条子信息的坐标信息进行加密，得到坐标信息的密文（S105）；将每条子信息对应的坐标信息的密文确定为目标信息的密文，将目标信息的密文存储至区块链网络中（S106）。提高了信息的安全性。

基于信息的属性生成密钥的信息处理方法、装置及设备

本申请要求于2020年9月29日提交中国专利局、申请号为202011054352.7，发明名称为“基于信息的属性生成密钥的信息处理方法、装置及设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及区块链技术领域，尤其涉及基于信息的属性生成密钥的信息处理方法、装置及设备。

背景技术

在这个网络发展较为迅速的时代，越来越多的信息都是通过网络进行交互、存储。发明人意识到，现有的信息存储方式一般为终端本地存储，例如，医疗平台中会使用终端对每个患者的病历信息、患者信息等信息进行存储，该种信息存储方式存在较大的风险，非法终端容易获取到本地存储的信息，导致信息的泄露，以及，非法用户可以对本地存储的信息进行篡改，导致信息安全性较低，并且，当本地存储出现故障时，导致信息无法找回，从而造成损失。因此，如何确保信息存储过程中信息的安全性，防止信息泄露是亟待解决的问题。

发明内容

本申请实施例提供基于信息的属性生成密钥的信息处理方法、装置及设备，可以实现对信息进行加密，提高信息的安全性，防止信息泄露。

本申请实施例一方面提供基于信息的属性生成密钥的信息处理方法，包括：

获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，该目标信息包括至少两条子信息，该每条子信息的属性信息包括该每条子信息所属的机构、该每条子信息的生成地址以及该每条子信息的数据类型中的至少一种；

根据该每条子信息的属性信息生成该每条子信息对应的密钥；

获取该每条子信息对应的第一随机数，根据该第一随机数对该每条子信息进行调整，得到调整后的每条子信息；

根据该目标函数以及该调整后的每条子信息，获取该至少两条子信息中每条子信息对应的坐标信息；

采用该每条子信息对应的密钥，对该至少两条子信息中的对应子信息的坐标信息进行加密，得到该每条子信息对应的坐标信息的密文；

将该每条子信息对应的坐标信息的密文确定为该目标信息的密文，将该目标信息的密文存储至区块链网络中。

本申请实施例一方面提供基于信息的属性生成密钥的信息处理装置，包括：

函数获取模块，用于获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，该目标信息包括至少两条子信息，该每条子信息的属性信息包括该每条子信息所属的机构、该每条子信息的生成地址以及该每条子信息的数据类型中的至少一种；

密钥生成模块，用于根据该每条子信息的属性信息生成该每条子信息对应的密钥；

信息调整模块，用于获取该每条子信息对应的第一随机数，根据该第一随机数对该每条子信息进行调整，得到调整后的每条子信息；

坐标获取模块，用于根据该目标函数以及该调整后的每条子信息，获取该至少两条子信息中每条子信息对应的坐标信息；

信息加密模块，用于采用该每条子信息对应的密钥，对该至少两条子信息中的对应子信息的坐标信息进行加密，得到该每条子信息对应的坐标信息的密文；

信息存储模块，用于将该每条子信息对应的坐标信息的密文确定为该目标信息的密文，将该目标信息的密文存储至区块链网络中。

本申请一方面提供了一种计算机设备，包括：处理器、存储器、网络接口；

上述处理器与存储器、网络接口相连，其中，网络接口用于提供数据通信功能，上述存储器用于存储计算机程序，上述处理器用于调用上述计算机程序，以执行以下方法：

获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，所述目标信息包括至少两条子信息，所述每条子信息的属性信息包括所述每条子信息所属的机构、所述每条子信息的生成地址以及所述每条子信息的数据类型中的至少一种；

根据所述每条子信息的属性信息生成所述每条子信息对应的密钥；

获取所述每条子信息对应的第一随机数，根据所述第一随机数对所述每条子信息进行调整，得到调整后的每条子信息；

根据所述目标函数以及所述调整后的每条子信息，获取所述至少两条子信息中每条子信息对应的坐标信息；

采用所述每条子信息对应的密钥，对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文；

将所述每条子信息对应的坐标信息的密文确定为所述目标信息的密文，将所述目标信息的密文存储至区块链网络中。

本申请实施例一方面提供了一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，该计算机程序包括程序指令，该程序指令当被处理器执行时使该处理器执行以下方法：

获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，所述目标信息包括至少两条子信息，所述每条子信息的属性信息包括所述每条子信息所属的机构、所述每条子信息的生成地址以及所述每条子信息的数据类型中的至少一种；

根据所述每条子信息的属性信息生成所述每条子信息对应的密钥；

获取所述每条子信息对应的第一随机数，根据所述第一随机数对所述每条子信息进行调整，得到调整后的每条子信息；

根据所述目标函数以及所述调整后的每条子信息，获取所述至少两条子信息中每条子信息对应的坐标信息；

采用所述每条子信息对应的密钥，对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文；

将所述每条子信息对应的坐标信息的密文确定为所述目标信息的密文，将所述目标信息的密文存储至区块链网络中。

本申请实施例通过将目标信息的密文信息存储至区块链网络中，基于区块链不可篡改且不易丢失的特性，可以提高信息的安全性；此外，将目标信息的密文存储至区块链网络中，可以减少终端本地存储空间的资源占用。

附图说明

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本申请实施例提供的一种基于信息的属性生成密钥的信息处理方法的流程示意图；

图 2 是本申请实施例提供的一种基于信息的属性生成密钥的信息处理方法的流程示意图；

图 3 是本申请实施例提供的一种基于信息的属性生成密钥的信息处理装置的组成结构示意图；

图4是本申请实施例提供的一种计算机设备的组成结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

本申请的技术方案可涉及区块链技术领域，比如本申请涉及的数据如坐标信息的密文和/或目标信息的密文等存储于区块链中。可选的，本申请可应用于金融科技如对金融数据加密等场景中，还可应用于数字医疗如对患者信息加密等场景中，以提高信息安全性。

本申请所涉及的区块链是一种分布式数据存储、点对点传输（P2P 传输）、共识机制、加密算法等计算机技术的新型应用模式，其本质上是一个去中心化的数据库，是一串使用密码学方法相关联产生的数据块，每一个数据块中包含了一批次网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块。区块链可以包括区块链底层平台、平台产品服务层以及应用服务层；区块链可由多个借由密码学串接并保护内容的串连交易记录（又称区块）构成，用区块链所串接的分布式账本能让多方有效纪录交易，且可永久查验此交易（不可篡改）。其中，共识机制是指区块链网络中实现不同节点之间建立信任、获取权益的数学算法；也就是说，共识机制是区块链各网络节点共同认可的一种数学算法。

本申请适用于医疗平台中，则目标信息例如可以为患者的病历信息、患者信息等等，通过对患者的病历信息、患者信息以及医疗平台的其他信息进行加密，并将加密后的信息存储至区块链网络中，有利于对患者的病历信息、患者信息等进行管理，提高患者的信息的安全性。

请参见图 1，图 1 是本申请实施例提供的一种基于信息的属性生成密钥的信息处理方法的流程示意图，该方法应用于区块链网络中的节点，该节点可以是独立的一个物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、内容分发网络（Content Delivery Network，CDN）、以及大数据和人工智能平台等基础云计算服务的云服务器。或者，该节点可以是指计算机设备，包括手机、平板电脑、笔记本电脑、掌上电脑、智能音响、移动互联网设备（MID，mobile internet device）、POS（Point Of Sales，销售点）机、可穿戴设备（例如智能手表、智能手环等）等。如图 1 所示，该方法包括：

S101，获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息。

这里，目标函数可以是指椭圆曲线对应的函数，目标函数也可以是指其他曲线对应的函数。目标信息包括至少两条子信息，目标信息可以是指某机构的交易数据、营业数据、该机构的内部资料等数据。目标信息中每条子信息的属性信息包括每条子信息所属的机构、每条子信息的生成地址以及每条子信息的数据类型中的至少一种。

S102，根据每条子信息的属性信息生成每条子信息对应的密钥。

这里，每条子信息的属性信息每条子信息所属的机构、每条子信息的生成地址以及每条子信息的数据类型中的至少一种。计算机设备可以根据每条子信息所属的机构、每条子信息的生成地址以及每条子信息的数据类型中的至少一种生成每条子信息对应的密钥。由于每条子信息的属性信息不同，因此根据每条子信息的属性信息生成每条子信息对应的密钥不同，在后续对每条子信息进行加密时，使用每条子信息对应的密钥对每条子信息进行加密，即使非法终端获取到某一条子信息对应的密钥，也无法根据该密钥计算出其他子信息对应的密钥，因此无法实现对目标信息的密文的解密，可以提高目标信息的安全性。

其中，每条子信息所属的机构可以是指生成每条子信息的终端所属的机构，或者，每

条子信息所属的机构可以是指拥有每条子信息的所有权的机构，例如，每条子消息为某银行机构一天内的营业数据，则该每条子消息所属的机构为该银行机构。每条子信息的生成地址可以包括生成每条子信息的终端的 IP 地址、MAC 地址或者其他地址。每条子信息的数据类型可以是指每条子信息的业务类型。例如，每条子信息的业务类型可以包括转账业务、充值业务等实时性较高的业务，以及婚姻登记业务、证件办理业务等实时性较低的业务，等等。计算机设备根据每条子信息的属性信息生成每条子信息对应的密钥，通过使用每条子信息对应的密钥对每条子信息进行加密，从而实现对目标信息进行加密，可以提高目标信息的安全性。

S103，获取每条子信息对应的第一随机数，根据第一随机数对每条子信息进行调整，得到调整后的每条子信息。

这里，由于每条子信息对应的数值大于第一阈值时，不能实现将每条子信息映射到目标函数的曲线上，则无法根据目标函数的曲线计算得到每条子信息对应的坐标点。因此可以使用第一随机数对每条子信息进行调整，使得调整后的每条子信息对应的数值小于或等于第一阈值，从而实现将每条子信息映射到目标函数的曲线上，根据目标函数的曲线计算得到每条子信息对应的坐标点。通过使用第一随机数对每条子信息进行调整，可以提高获取每条子信息对应的坐标点的概率，从而提高加密成功的概率。第一阈值可以是根据目标函数对应的曲线参数确定的，如该曲线参数为曲线长度 c，则第一阈值为(2^256)-w，其中，w 为一个极小的数值。

具体实现中，可以采用随机数生成算法生成随机数，例如中心极限定理和 Box Muller（坐标变换法）、蒙特卡洛算法、数值概率算法、拉斯维加斯算法或者其他算法生成随机数，并将该生成的随机数确定为每条子信息对应的第一随机数。或者，可以调用 C 语言中的 rand 函数生成随机数。

在一种可能的情况下，若每条子信息不为数值类型的数据，则可以对每条子信息进行编码，得到数值类型的编码数据，根据每条子信息对应的第一随机数对每条子信息对应的编码数据进行调整，得到调整后的每条子信息。

在另一种可能的情况下，若每条子信息为数值类型的数据，则根据每条子信息对应的第一随机数对每条子信息进行调整，得到调整后的每条子信息。可知，调整后的每条子信息包括该条子信息和该条子信息对应的第一随机数。

S104，根据目标函数以及调整后的每条子信息，获取至少两条子信息中每条子信息对应的坐标信息。

这里，例如可以对调整后非数值类型的每条子信息进行编码，得到调整后数值类型的每条子信息对应的编码数据，将调整后数值类型的每条子信息对应的编码数据映射至目标函数对应的曲线上得到对应的坐标点，从而根据该坐标点得到每条子信息对应的坐标信息。

在一种可能的实现方式中，可以获取目标函数对应的曲线，将调整后的每条子信息映射至该目标函数对应的曲线上的目标点的第一坐标；根据该第一坐标以及该目标函数，确定该目标函数对应的曲线上的目标点的第二坐标；将该第一坐标以及该第二坐标确定为每条子信息对应的坐标信息，从而获取到至少两条子信息中每条子信息对应的坐标信息。

举例来对获取至少两条子信息中任意一条子信息 c 对应的坐标信息进行说明，可以根据第一坐标和目标函数，确定该目标函数对应的曲线上的目标点的第二坐标，将该第一坐标以及该第二坐标确定为子信息 c 对应的坐标信息。例如，目标函数对应的曲线可以如公式（1-1）所示：

$$y^2 = x^3 + ax + b \quad (1\text{-}1)$$

其中，a 和 b 均为已知的实数，x 和 y 均为参数，通过确定 x 或者 y 中的任意一个参数

的值，则可以通过公式（1-1）计算得到另一个参数的值，例如，通过确定 x 的值，根据公式（1-1）可计算得到 y 的值。

例如，a 为 1，b 为-1，子信息 c 映射至该目标函数对应的曲线上的目标点的第一坐标（例如该目标点的横坐标）为 1，将 a，b 以及该第一坐标作为 x 代入公式（1-1）中，得到 y 为 1，即该目标函数对应的曲线上的目标点的第二坐标为 1，则子信息 c 对应的坐标信息为（1,1），通过该方法，可以获取到至少两条子信息中其他子信息对应的坐标信息，从而获取到至少两条子信息中每条子信息对应的坐标信息。

S105，采用每条子信息对应的密钥，对至少两条子信息中每条子信息对应的坐标信息进行加密，得到每条子信息对应的坐标信息的密文。

这里，由于步骤 S102 中根据每条子信息的属性信息生成每条子信息对应的密钥，因此，计算机设备可以采用每条子信息对应的密钥，对至少两条子信息中每条子信息对应的坐标信息进行加密，得到每条子信息对应的坐标信息的密文。具体实现中，计算机设备可以获取目标信息所属的终端的私钥，根据该终端的私钥和每条子信息对应的密钥，对至少两条子信息中每条子信息对应的坐标信息进行加密，得到每条子信息对应的坐标信息的密文。可知，子信息对应的坐标信息的密文为对子信息加密后的得到的密文，在未对其进行解密的情况下，即使获取到该密文也无法获知该密文对应的子信息的内容。通过使用目标信息所属的终端的私钥和每条子信息对应的密钥对目标信息对应的每条子信息进行加密，可以提高目标信息的安全性。

S106，将每条子信息对应的坐标信息的密文确定为目标信息的密文，将目标信息的密文存储至区块链网络中。

这里，上述步骤中，对于至少两条子信息中的每条子信息，都会得到每条子信息对应的坐标信息的密文，因此，将每条子信息对应的坐标信息的密文确定为目标信息的密文，也就是说，目标信息的密文包括至少两条子信息中的每条子信息对应的坐标信息的密文，至此，可以实现对目标信息进行加密得到目标信息的密文，可以将目标信息的密文存储至区块链网络中。通过将目标信息发送至区块链网络中进行加密以及存储，可以减少终端本地存储空间的资源占用，以及，可以避免目标信息存储在终端本地被非法用户篡改，提高目标信息的安全性。

可选的，在将目标信息的密文存储至区块链网络后，后续当存在需要获取目标信息的终端时，计算机设备可以验证该需要获取目标信息的终端的合法性，在确定获取该终端具有合法性的情况下，对目标信息的密文解密后得到目标信息，并将目标信息发送至需要获取目标信息的终端，从而实现获取目标信息。或者，也可以将目标信息的密文发送至该目标信息所属的终端，通过目标信息所属的终端对目标信息的密文进行解密后，将解密后的目标信息发送至需要获取目标信息的终端，从而实现获取目标信息。

本申请实施例中，根据每条子信息的属性信息生成每条子信息对应的密钥，由于每条子信息的属性信息不同，生成的每条子信息对应的密钥不同，因此采用每条子信息对应的密钥进行加密后，非法终端难以获取每条子信息对应的密钥，因此难以实现对密文进行解密，可以提高密文破解的难度，提高信息的安全性。通过对至少两条子信息中每条子信息进行调整，有利于根据调整后的每条子信息生成调整后的每条子信息对应的坐标信息，提高获取调整后的每条子信息对应的坐标信息的成功率。通过对目标信息中的每条子信息进行加密，避免非法终端对该密文进行破解，从而提高每条子信息的安全性，进而提高目标信息的安全性。通过将目标信息的密文信息存储至区块链网络中，基于区块链不可篡改且不易丢失的特性，可以提高信息的安全性；此外，将目标信息的密文存储至区块链网络中，可以减少终端本地存储空间的资源占用。

在一个实施例中，上述每条子信息的属性信息包括上述每条子信息所属的机构，上述

步骤 S102 中包括如下步骤 s11~s13。

s11，获取每条子信息所属的机构向区块链网络中写入信息的时间以及写入信息的条数。

其中，该机构向区块链网络中写入信息包括所有该机构向区块链网络写入的所有信息，写入信息的条数包括该机构向区块链网络写入的所有信息的条数。例如该机构去年向区块链网络写入 80 条信息、且该机构今年向区块链写入 100 条信息，则该机构向区块链网络中写入信息的条数为 180 条，则获取 180 条信息中每条信息写入区块链的时间。

s12，根据写入信息的时间以及写入信息的条数确定每条子信息所属的机构的活跃度。

这里，活跃度例如可以为 0-1 以内的数值，或者，活跃度也可以为 0-10 以内的数值，或者 0-100 以内的数值，等等。例如活跃度为 0-100 以内的数值，则活跃度对应的数值越大，表示该机构的活跃度越大；活跃度对应的数值越小，表示该机构的活跃度越小。

例如，根据写入信息的时间以及写入信息的条数确定每条子信息所属的机构的活跃度的方法可以包括：写入信息的周期越短且写入信息的条数越多，活跃度越高；写入信息的周期越长且写入信息的条数越少，活跃度越低。根据写入信息的时间可以确定属于同一个周期内的信息。例如，周期为每星期，该机构每星期向区块链网络写入信息的条数为第一数量阈值，对应的活跃度为活跃度 1，该机构每月向区块链网络写入信息的条数为第一数量阈值，对应的活跃度为活跃度 2，该机构每季度向区块链网络写入信息的条数为第一数量阈值，对应的活跃度为活跃度 3，则活跃度 1 大于活跃度 2 大于活跃度 3。或者，该机构每星期向区块链网络写入信息的条数为第一数量阈值，对应的活跃度为活跃度 1，该机构每月向区块链网络写入信息的条数为第二数量阈值，对应的活跃度为活跃度 2，该机构每季度向区块链网络写入信息的条数为第三数量阈值，对应的活跃度为活跃度 3，则活跃度 1 大于活跃度 2 大于活跃度 3。其中，第一数量阈值大于第二数量阈值，第二数量阈值大于第三数量阈值。第一数量阈值、第二数量阈值以及第三数量阈值可以根据具体的情况进行设置，本申请实施例对此不做限定。

或者，可以根据该机构每个月向区块链网络写入信息的条数确定该机构的活跃度。若该机构每个月向区块链网络写入信息的条数大于第一数量阈值，则该机构的活跃度为 80-100 以内的数值；若该机构每个月向区块链网络写入信息的条数大于第二数量阈值且小于第一数量阈值，则该机构的活跃度为 60-79 以内的数值；若该机构每个月向区块链网络写入信息的条数大于第三数量阈值且小于第二数量阈值，则该机构的活跃度为 0-59 以内的数值。也就是说，机构每个月向区块链网络写入信息的条数越多，该机构的活跃度对应的数值越大，则活跃度越大。

可选的，可以获取每条子信息所属的机构向区块链网络中写入信息的种类以及写入信息的条数，根据写入信息的种类以及写入信息的条数确定每条子信息所属的机构的活跃度。

这里，写入信息的种类越多且写入信息的条数越多，则每条子信息所属的机构的活跃度越高；写入信息的种类越少且写入信息的条数越少，则每条子信息所属的机构的活跃度越低。例如，该机构向区块链网络中写入信息的种类大于第一数值，且写入信息的条数大于第一数量阈值，对应的活跃度为活跃度 1；该机构向区块链网络中写入信息的种类大于第二数值且小于第一数值，且写入信息的条数大于第二数量阈值且小于第一数量阈值，对应的活跃度为活跃度 2；该机构向区块链网络中写入信息的种类大于第三数值且小于第二数值，且写入信息的条数大于第三数量阈值且小于第二数量阈值，对应的活跃度为活跃度 3。其中，活跃度 1 大于活跃度 2 大于活跃度 3，第一数量阈值大于第二数量阈值大于第三数量阈值。

s13，分别对每条子信息所属的机构的活跃度进行哈希运算，得到每条子信息对应的密钥。

这里，例如某一条子信息所属的机构的活跃度为 k，则根据哈希函数对该条子信息所

属的机构的活跃度进行哈希运算，即 hash（k）=k1，则 k1 为该条子信息对应的密钥。计算机设备通过分别使用哈希函数对每条子信息所属的机构的活跃度进行哈希运算，得到每条子信息对应的密钥。由于每条子信息所属的机构对应的活跃度不同，因此根据活跃度得到的每条子信息对应的密钥不同，因此，在后续加密过程中，采用每条子信息对应的密钥进行加密，得到的密文不同，即使非法终端获取到目标信息对应的密文，也难以获取到每条子信息对应的密钥，因此无法实现对每条子信息的密文进行解密，从而无法实现对目标信息的密文进行解密，进而提高目标信息的安全性。

在一个实施例中，上述每条子信息的属性信息包括上述每条子信息的生成地址，上述步骤 S102 中包括如下步骤 s21~s22。

s21，对每条子信息的生成地址进行编码，得到每条信息对应的第二随机数。

s22，分别对每条信息对应的第二随机数进行哈希运算，得到每条子信息对应的密钥。

在步骤 s21~s22 中，每条子信息的生成地址可以为每条子信息所属终端的 IP 地址、每条子信息所属终端的 MAC 地址、每条子信息所属终端的具体地理位置，例如可以包括经纬度，等等。计算机设备通过对每条子信息的生成地址进行编码，得到每条信息对应的第二随机数，分别对每条信息对应的第二随机数进行哈希运算，得到每条子信息对应的密钥。例如，计算机可以使用上述步骤 S103 中的随机数生成算法生成某一条子信息对应的第二随机数 p，则对该第二随机数 p 进行哈希运算，即 hash（p）=p1，则 p1 为该条子信息对应的密钥。由于每条子信息的生成地址可能不同，因此根据生成地址得到的每条子信息对应的密钥不同，因此，在后续加密过程中，采用每条子信息对应的密钥进行加密，得到的密文不同，即使非法终端获取到目标信息对应的密文，也难以获取到每条子信息对应的密钥，因此无法实现对每条子信息的密文进行解密，从而无法实现对目标信息的密文进行解密，进而提高目标信息的安全性。

在一个实施例中，上述每条子信息的属性信息包括上述每条子信息的数据类型，上述步骤 S102 中包括如下步骤 s31~s33。

s31，根据每条子信息的数据类型，确定处理每条子信息的实时性等级。

s32，根据每条子信息的实时性等级生成每条子信息对应的第三随机数。

s33，分别对每条信息对应的第三随机数进行哈希运算，得到每条子信息对应的密钥。

在步骤 s31~s33 中，每条子信息的数据类型可以是指每条子信息的业务类型，业务类型可以包括转账业务、充值业务等实时性较高的业务类型，以及婚姻登记业务、证件办理业务等实时性较低的业务类型，等等。对于转账业务、充值业务等类型的业务需要的实时性较高，则该类型业务对应的每条子信息的实时性等级较高；对于婚姻登记业务、证件办理业务等类型的业务需要的实时性较低，则该类型业务对应的每条子信息的实时性等级较低。例如，可以将在第一时间阈值内完成的子信息确定为第一实时性等级、将在第二时间阈值内完成的子信息确定为第二实时性等级、将在第三时间阈值内完成的子信息确定为第三实时性等级，等等。根据每条子信息的实时性等级生成每条子信息对应的第三随机数，分别对每条信息对应的第三随机数进行哈希运算，得到每条子信息对应的密钥。例如根据某一条子信息的实时性等级生成第三随机数 m，则对该第三随机数 m 进行哈希运算，即 hash（m）=m1，则 m1 为该条子信息对应的密钥。

由于每条子信息的数据类型可能不同，因此根据数据类型得到的每条子信息对应的密钥不同，因此，在后续加密过程中，采用每条子信息对应的密钥进行加密，得到的密文不同，即使非法终端获取到目标信息对应的密文，也难以获取到每条子信息对应的密钥，因此无法实现对每条子信息的密文进行解密，从而无法实现对目标信息的密文进行解密，进而提高目标信息的安全性。

在一种可能的实现方式中，每条子信息的属性信息可以包括每条子信息包含的标的额，

根据每条子信息中包含的标的额生成每条子信息对应的第五随机数；分别对每条信息对应的第五随机数进行哈希运算，得到每条子信息对应的密钥。

这里，标的额是指每条子信息中包含的标的物（货物）的金额，即表示每条子信息中货物的总价值。如某一条子信息为购买某货物的买卖合同，则标的额为购买该货物支付的总金额。由于每条子信息中的标的物的单价和数量不相同，因此每条子信息包含的标的额不同。例如，根据某一条子信息包含的标的额生成第五随机数 n，则对该第五随机数 n 进行哈希运算，即 hash（n）=n1，则 n1 为该条子信息对应的密钥。由于每条子信息包含的标的额可能不同，因此根据每条子信息包含的标的额得到的每条子信息对应的密钥不同，因此，在后续加密过程中，采用每条子信息对应的密钥进行加密，得到的密文不同，即使非法终端获取到目标信息对应的密文，也难以获取到每条子信息对应的密钥，因此无法实现对每条子信息的密文进行解密，从而无法实现对目标信息的密文进行解密，进而提高目标信息的安全性。

在一个实施例中，上述步骤 S103 中包括如下步骤 s41~s42。

s41，将第一随机数与每条子信息进行拼接，得到拼接后的每条子信息。

s42，若拼接后的每条子信息小于信息阈值，则将拼接后的每条子信息确定为调整后的每条子信息。

在步骤 s41~s42 中，若拼接后的每条子信息小于信息阈值，则认为将该条子信息映射至目标函数对应的曲线上的目标点的第一坐标，可以根据该第一坐标以及该目标函数，计算得到该目标函数对应的曲线上的目标点的第二坐标，即可以得到每条子信息对应的坐标信息。若拼接后的每条子信息大于或等于信息阈值，则认为将该条子信息映射至目标函数对应的曲线上的目标点的第一坐标，无法根据该第一坐标以及该目标函数，计算得到该目标函数对应的曲线上的目标点的第二坐标，即无法得到每条子信息对应的坐标信息。其中，每条子信息对应的第一随机数可以相等，也可以不相等。其中，信息阈值例如可以为（2^256），也可以小于（2^256）。通过将第一随机数与每条子信息进行拼接，可以得到拼接后的每条子信息，从而根据拼接后的每条子信息与信息阈值的大小关系，将拼接后的每条子信息确定为调整后的每条子信息。

在一种可能的实现方式中，若拼接后的每条子信息大于或等于信息阈值，则可对第一随机数进行调整，具体方法包括如下步骤 s51~s53。

s51，若拼接后的每条子信息大于或等于信息阈值，则调整第一随机数。

S52，将调整后的第一随机数与每条子信息进行拼接，得到候选的每条子信息。

S53，若候选的每条子信息小于信息阈值，则将候选的每条子信息确定为调整后的每条子信息。

在步骤 s51~s53 中，由于拼接后的每条子信息大于或等于信息阈值时，将该条子信息映射至目标函数对应的曲线上的目标点的第一坐标，无法根据该第一坐标以及该目标函数，计算得到该目标函数对应的曲线上的目标点的第二坐标，即无法得到每条子信息对应的坐标信息。因此，需要对每条子信息对应的第一随机数进行调整，并将调整后的第一随机数与每条子信息进行拼接，得到候选的每条子信息。

可知，若候选的每条子信息小于信息阈值，将该条子信息映射至目标函数对应的曲线上的目标点的第一坐标，可以根据该第一坐标以及该目标函数，计算得到该目标函数对应的曲线上的目标点的第二坐标，即可以得到每条子信息对应的坐标信息。若候选的每条子信息大于或等于信息阈值，则认为将该条子信息映射至目标函数对应的曲线上的目标点的第一坐标，无法根据该第一坐标以及该目标函数，计算得到该目标函数对应的曲线上的目标点的第二坐标，即无法得到每条子信息对应的坐标信息。也就是说，若候选的每条子信息大于或等于信息阈值，则继续调整第一随机数，直到对调整后的第一随机数与候选的每

条子信息进行拼接，拼接后的候选的每条子信息小于信息阈值，则将拼接后的候选的每条子信息确定为调整后的每条子信息。通过对每条子信息对应的第一随机数与子信息进行拼接，以及不断调整每条子信息对应的第一随机数，可以得到调整后的每条子信息，提高后续对每条子信息进行加密的成功率。

在一个实施例中，上述步骤 S105 中包括如下步骤 s61~s62。

s61，获取目标信息所属的终端的私钥，以及每条子信息对应的密钥。

这里，目标信息所属的终端为上传目标信息至区块链网络中进行加密以及存储等处理的终端，目标信息所属的终端的私钥为通过该终端生成的私钥。

具体实现中，例如可以获取该目标信息所属终端的标识，采用 SECP256K1 算法生成第四随机数，对第四随机数进行填充，得到终端的私钥，该终端的私钥可以是指包括 256 位的数。这里，终端的标识可以是指终端的出厂编号，或者其他用于唯一指示该终端的标识。

s62，根据终端的私钥以及每条子信息对应的密钥，对至少两条子信息中每条子信息对应的坐标信息进行加密，得到每条子信息对应的坐标信息的密文。

具体实现中，可以采用加密算法对每条子信息对应的坐标信息进行加密，得到每条子信息对应的坐标信息的密文，加密算法例如可以包括 Elgamal 算法（一种非对称加密算法）、Rabin 算法（一种非对称加密算法）、Diffie-Hellman 算法（一种非对称加密算法）、ECC 算法（椭圆曲线加密算法）。计算机设备根据终端的私钥以及每条子信息对应的密钥，对至少两条子信息中每条子信息对应的坐标信息进行加密，得到每条子信息对应的坐标信息的密文，可以实现对每条子信息进行加密，得到对应的密文，终端获取到每条子信息对应的密文后，需要进行解密，才能获知每条密文对应的子信息。

具体实现中，根据终端的私钥以及每条子信息对应的密钥，对至少两条子信息中每条子信息对应的坐标信息进行加密，得到每条子信息对应的坐标信息的密文的方法如图 2 所示，图 2 是本申请实施例提供的一种基于信息的属性生成密钥的信息处理方法的流程示意图，该方法应用于区块链网络中的节点，该节点可以是指计算机设备；如图 2 所示，该方法包括：

s71，获取目标函数的曲线的基点坐标。

s72，获取基点坐标与终端的私钥的乘积，得到候选坐标。

s73，根据每条子信息对应的密钥对候选坐标进行加密，得到候选坐标的密文。

s74，对每条子信息对应的坐标信息与对应的候选坐标的密文进行融合，得到每条子信息对应的坐标信息的密文。

在步骤 s71~ s74 中，通过获取目标函数的曲线，以及目标函数的曲线参数，可以获取该目标函数的曲线的基点坐标。例如基点为 G，对应的基点坐标为（x1,y1），终端的私钥为 h，则可以根据公式（1-2）计算得到候选坐标：

$$H = h * G \quad (1\text{-}2)$$

其中，候选坐标为 H，基点为 G，终端的私钥为 h。

例如，目标信息对应的子信息的数量为 n 条，子信息 i 为 n 条子信息中的任意一条子信息，可以通过公式（1-3）的方式对候选坐标进行加密，得到候选坐标的密文，以及对子信息 i 对应的坐标信息与候选坐标的密文进行和融合，得到子信息 i 对应的坐标信息的密文。

$$Ci = Mi + ki * H \quad (1\text{-}3)$$

其中，候选坐标为 H，Ci 为子信息 i 对应的坐标信息的密文，Mi 为子信息 i 对应的坐标信息，ki 为子信息 i 对应的密钥。ki*H 表示根据子信息 i 对应的密钥对候选坐标进行加密，得到候选坐标的密文。可知，对于 n 条子信息中的其他子信息，也可以通过公式（1-3）进行加密和融合，得到其他子信息对应的坐标信息的密文。对于每一条子信息，通过公式（1-3）进行加密和融合可以得到该条子信息对应的坐标信息的密文，也就是说，一条子信

息对应一条子信息对应的坐标信息的密文的数量，即对于 n 条子信息，最终得到的子信息对应的坐标信息的密文的数量为 n。

通过对每条子信息进行加密，即使非法终端获取到子信息对应的密文，由于无法实现解密，也无法获取到子信息的内容，因此可以保证每条子信息的安全性，从而保证目标信息的安全性。

上面介绍了本申请实施例的方法，下面介绍本申请实施例的装置。

参见图 3，图 3 是本申请实施例提供的一种基于信息的属性生成密钥的信息处理装置的组成结构示意图，上述基于信息的属性生成密钥的信息处理装置可以是运行于计算机设备中的一个计算机程序（包括程序代码），例如该基于信息的属性生成密钥的信息处理装置为一个应用软件；该装置可以用于执行本申请实施例提供的方法中的相应步骤。该装置 30 包括：

函数获取模块 301，用于获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，该目标信息包括至少两条子信息，该每条子信息的属性信息包括该每条子信息所属的机构、该每条子信息的生成地址以及该每条子信息的数据类型中的至少一种；

密钥生成模块 302，用于根据该每条子信息的属性信息生成该每条子信息对应的密钥；

信息调整模块 303，用于获取该每条子信息对应的第一随机数，根据该第一随机数对该每条子信息进行调整，得到调整后的每条子信息；

坐标获取模块 304，用于根据该目标函数以及该调整后的每条子信息，获取该至少两条子信息中每条子信息对应的坐标信息；

信息加密模块 305，用于采用该每条子信息对应的密钥，对该至少两条子信息中的对应子信息的坐标信息进行加密，得到该每条子信息对应的坐标信息的密文；

信息存储模块 306，用于将该每条子信息对应的坐标信息的密文确定为该目标信息的密文，将该目标信息的密文存储至区块链网络中。

可选的，该每条子信息的属性信息包括该每条子信息所属的机构；该密钥生成模块 302，具体用于：获取该每条子信息所属的机构向该区块链网络中写入信息的时间以及写入信息的条数；根据该写入信息的时间以及该写入信息的条数确定该每条子信息所属的机构的活跃度；分别对该每条子信息所属的机构的活跃度进行哈希运算，得到该每条子信息对应的密钥。

可选的，该每条子信息的属性信息包括该每条子信息的生成地址；该密钥生成模块 302，具体用于：对该每条子信息的生成地址进行编码，得到该每条信息对应的第二随机数；分别对该每条信息对应的第二随机数进行哈希运算，得到该每条子信息对应的密钥。

可选的，该每条子信息的属性信息包括该每条子信息的数据类型；该密钥生成模块 302，具体用于：根据该每条子信息的数据类型，确定处理该每条子信息的实时性等级；根据该每条子信息的实时性等级生成该每条子信息对应的第三随机数；分别对该每条信息对应的第三随机数进行哈希运算，得到该每条子信息对应的密钥。

可选的，该信息调整模块 303，具体用于：将该第一随机数与该每条子信息进行拼接，得到拼接后的每条子信息；若该拼接后的每条子信息小于信息阈值，则将该拼接后的每条子信息确定为调整后的每条子信息。

可选的，该信息加密模块 305，具体用于：获取该目标信息所属的终端的私钥，以及该每条子信息对应的密钥；根据该终端的私钥以及该每条子信息对应的密钥，对该至少两条子信息中每条子信息对应的坐标信息进行加密，得到该每条子信息对应的坐标信息的密文。

可选的，该信息加密模块 305，具体用于：获取该目标函数的曲线的基点坐标；获取

该基点坐标与该终端的私钥的乘积，得到候选坐标；根据该每条子信息对应的密钥对该候选坐标进行加密，得到该候选坐标的密文；对该每条子信息对应的坐标信息与对应的候选坐标的密文进行融合，得到该每条子信息对应的坐标信息的密文。

需要说明的是，图 3 对应的实施例中未提及的内容可参见方法实施例的描述，这里不再赘述。

根据本申请的一个实施例，图 1 所示的基于信息的属性生成密钥的信息处理方法所涉及的步骤可由图 3 所示的基于信息的属性生成密钥的信息处理装置中的各个模块来执行。例如，图 1 中所示的步骤 S101 可由图 3 中的函数获取模块 301 来执行，图 1 中所示的步骤 S102 可由图 3 中的密钥生成模块 302 来执行；图 1 中所示的步骤 S103 可由图 3 中的信息调整模块 303 来执行；图 1 中所示的步骤 S104 可由图 3 中的坐标获取模块 304 来执行；图 1 中所示的步骤 S105 可由图 3 中的信息加密模块 305 来执行；图 1 中所示的步骤 S106 可由图 3 中的信息存储模块 306 来执行。根据本申请的一个实施例，图 3 所示的基于信息的属性生成密钥的信息处理中的各个模块可以分别或全部合并为一个或若干个单元来构成，或者其中的某个（些）单元还可以再拆分为功能上更小的多个子单元，可以实现同样的操作，而不影响本申请的实施例的技术效果的实现。上述模块是基于逻辑功能划分的，在实际应用中，一个模块的功能也可以由多个单元来实现，或者多个模块的功能由一个单元实现。在本申请的其它实施例中，基于信息的属性生成密钥的信息处理装置也可以包括其它单元，在实际应用中，这些功能也可以由其它单元协助实现，并且可以由多个单元协作实现。

根据本申请的另一个实施例，可以通过在包括中央处理单元（CPU）、随机存取存储介质（RAM）、只读存储介质（ROM）等处理元件和存储元件的例如计算机的通用计算机设备上运行能够执行如图 1 和图 2 中所示的相应方法所涉及的各步骤的计算机程序（包括程序代码），来构造如图 3 中所示的基于信息的属性生成密钥的信息处理装置，以及来实现本申请实施例的基于信息的属性生成密钥的信息处理方法。上述计算机程序可以记载于例如计算机可读记录介质上，并通过计算机可读记录介质装载于上述计算设备中，并在其中运行。

本申请实施例中，根据每条子信息的属性信息生成每条子信息对应的密钥，由于每条子信息的属性信息不同，生成的每条子信息对应的密钥不同，因此采用每条子信息对应的密钥进行加密后，非法终端难以获取每条子信息对应的密钥，因此难以实现对密文进行解密，可以提高密文破解的难度，提高信息的安全性。通过对至少两条子信息中每条子信息进行调整，有利于根据调整后的每条子信息生成调整后的每条子信息对应的坐标信息，提高获取调整后的每条子信息对应的坐标信息的成功率。通过对目标信息中的每条子信息进行加密，避免非法终端对该密文进行破解，从而提高每条子信息的安全性，进而提高目标信息的安全性。通过将目标信息的密文信息存储至区块链网络中，基于区块链不可篡改且不易丢失的特性，可以提高信息的安全性；此外，将目标信息的密文存储至区块链网络中，可以减少终端本地存储空间的资源占用。

参见图 4，图 4 是本申请实施例提供的一种计算机设备的组成结构示意图。如图 4 所示，上述计算机设备 40 可以包括：处理器 401，网络接口 404 和存储器 405，此外，上述计算机设备 40 还可以包括：用户接口 403，和至少一个通信总线 402。其中，通信总线 402 用于实现这些组件之间的连接通信。其中，用户接口 403 可以包括显示屏（Display）、键盘（Keyboard），可选用户接口 403 还可以包括标准的有线接口、无线接口。网络接口 404 可选的可以包括标准的有线接口、无线接口（如 WI-FI 接口）。存储器 405 可以是高速 RAM 存储器，也可以是非易失性的存储器（non-volatile memory），例如至少一个磁盘存储器。存储器 405 可选的还可以是至少一个位于远离前述处理器 401 的存储装置。如图 4 所示，

作为一种计算机可读存储介质的存储器 405 中可以包括操作系统、网络通信模块、用户接口模块以及设备控制应用程序。

在图 4 所示的计算机设备 40 中，网络接口 404 可提供网络通讯功能；而用户接口 403 主要用于为用户提供输入的接口；而处理器 401 可以用于调用存储器 405 中存储的设备控制应用程序，以实现：

获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，该目标信息包括至少两条子信息，该每条子信息的属性信息包括该每条子信息所属的机构、该每条子信息的生成地址以及该每条子信息的数据类型中的至少一种；

根据该每条子信息的属性信息生成该每条子信息对应的密钥；

获取该每条子信息对应的第一随机数，根据该第一随机数对该每条子信息进行调整，得到调整后的每条子信息；

根据该目标函数以及该调整后的每条子信息，获取该至少两条子信息中每条子信息对应的坐标信息；

采用该每条子信息对应的密钥，对该至少两条子信息中的对应子信息的坐标信息进行加密，得到该每条子信息对应的坐标信息的密文；

将该每条子信息对应的坐标信息的密文确定为该目标信息的密文，将该目标信息的密文存储至区块链网络中。

应当理解，本申请实施例中所描述的计算机设备 40 可执行前文图 1 以及图 2 所对应实施例中对上述基于信息的属性生成密钥的信息处理方法的描述，也可执行前文图 3 所对应实施例中对上述基于信息的属性生成密钥的信息处理装置的描述，在此不再赘述。另外，对采用相同方法的有益效果描述，也不再进行赘述。

本申请实施例中，根据每条子信息的属性信息生成每条子信息对应的密钥，由于每条子信息的属性信息不同，生成的每条子信息对应的密钥不同，因此采用每条子信息对应的密钥进行加密后，非法终端难以获取每条子信息对应的密钥，因此难以实现对密文进行解密，可以提高密文破解的难度，提高信息的安全性。通过对至少两条子信息中每条子信息进行调整，有利于根据调整后的每条子信息生成调整后的每条子信息对应的坐标信息，提高获取调整后的每条子信息对应的坐标信息的成功率。通过对目标信息中的每条子信息进行加密，避免非法终端对该密文进行破解，从而提高每条子信息的安全性，进而提高目标信息的安全性。通过将目标信息的密文信息存储至区块链网络中，基于区块链不可篡改且不易丢失的特性，可以提高信息的安全性；此外，将目标信息的密文存储至区块链网络中，可以减少终端本地存储空间的资源占用。

本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，该计算机程序包括程序指令，该程序指令当被计算机执行时使该计算机执行如前述实施例该的方法，该计算机可以为上述提到的计算机设备的一部分。例如为上述的处理器 401。作为示例，程序指令可被部署在一个计算机设备上执行，或者被部署位于一个地点的多个计算机设备上执行，又或者，在分布在多个地点且通过通信网络互连的多个计算机设备上执行，分布在多个地点且通过通信网络互连的多个计算机设备可以组成区块链网络。

可选的，本申请涉及的存储介质如计算机可读存储介质可以是非易失性的，也可以是易失性的。

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，该的程序可存储于计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，该的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）或随机存储记忆体（Random Access Memory，RAM）等。

以上所揭露的仅为本申请较佳实施例而已，当然不能以此来限定本申请之权利范围，因此依本申请权利要求所作的等同变化，仍属本申请所涵盖的范围。

权利要求

1、一种基于信息的属性生成密钥的信息处理方法，包括：

获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，所述目标信息包括至少两条子信息，所述每条子信息的属性信息包括所述每条子信息所属的机构、所述每条子信息的生成地址以及所述每条子信息的数据类型中的至少一种；

根据所述每条子信息的属性信息生成所述每条子信息对应的密钥；

获取所述每条子信息对应的第一随机数，根据所述第一随机数对所述每条子信息进行调整，得到调整后的每条子信息；

根据所述目标函数以及所述调整后的每条子信息，获取所述至少两条子信息中每条子信息对应的坐标信息；

采用所述每条子信息对应的密钥，对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文；

将所述每条子信息对应的坐标信息的密文确定为所述目标信息的密文，将所述目标信息的密文存储至区块链网络中。

2、根据权利要求 1 所述的方法，其中，所述每条子信息的属性信息包括所述每条子信息所属的机构；所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

获取所述每条子信息所属的机构向所述区块链网络中写入信息的时间以及写入信息的条数；

根据所述写入信息的时间以及所述写入信息的条数确定所述每条子信息所属的机构的活跃度；

分别对所述每条子信息所属的机构的活跃度进行哈希运算，得到所述每条子信息对应的密钥。

3、根据权利要求 1 所述的方法，其中，所述每条子信息的属性信息包括所述每条子信息的生成地址；所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

对所述每条子信息的生成地址进行编码，得到所述每条信息对应的第二随机数；

分别对所述每条信息对应的第二随机数进行哈希运算，得到所述每条子信息对应的密钥。

4、根据权利要求 1 所述的方法，其中，所述每条子信息的属性信息包括所述每条子信息的数据类型；所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

根据所述每条子信息的数据类型，确定处理所述每条子信息的实时性等级；

根据所述每条子信息的实时性等级生成所述每条子信息对应的第三随机数；

分别对所述每条信息对应的第三随机数进行哈希运算，得到所述每条子信息对应的密钥。

5、根据权利要求 1 所述的方法，其中，所述根据所述第一随机数对所述每条子信息进行调整，得到调整后的每条子信息，包括：

将所述第一随机数与所述每条子信息进行拼接，得到拼接后的每条子信息；

若所述拼接后的每条子信息小于信息阈值，则将所述拼接后的每条子信息确定为调整后的每条子信息。

6、根据权利要求 1 所述的方法，其中，对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文，包括：

获取所述目标信息所属的终端的私钥，以及所述每条子信息对应的密钥；

根据所述终端的私钥以及所述每条子信息对应的密钥，对所述至少两条子信息中每条子信息对应的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文。

7、根据权利要求 6 所述的方法，其中，所述根据所述私钥以及所述每条子信息对应的密钥，对所述至少两条子信息中每条子信息对应的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文，包括：

获取所述目标函数的曲线的基点坐标；

获取所述基点坐标与所述终端的私钥的乘积，得到候选坐标；

根据所述每条子信息对应的密钥对所述候选坐标进行加密，得到所述候选坐标的密文；

对所述每条子信息对应的坐标信息与对应的候选坐标的密文进行融合，得到所述每条子信息对应的坐标信息的密文。

8、一种基于信息的属性生成密钥的信息处理装置，包括：

函数获取模块，用于获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，所述目标信息包括至少两条子信息，所述每条子信息的属性信息包括所述每条子信息所属的机构、所述每条子信息的生成地址以及所述每条子信息的数据类型中的至少一种；

密钥生成模块，用于根据所述每条子信息的属性信息生成所述每条子信息对应的密钥；

信息调整模块，用于获取所述每条子信息对应的第一随机数，根据所述第一随机数对所述每条子信息进行调整，得到调整后的每条子信息；

坐标获取模块，用于根据所述目标函数以及所述调整后的每条子信息，获取所述至少两条子信息中每条子信息对应的坐标信息；

信息加密模块，用于采用所述每条子信息对应的密钥，对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文；

信息存储模块，用于将所述每条子信息对应的坐标信息的密文确定为所述目标信息的密文，将所述目标信息的密文存储至区块链网络中。

9、一种计算机设备，包括：处理器、存储器以及网络接口；

所述处理器与所述存储器、所述网络接口相连，其中，所述网络接口用于提供数据通信功能，所述存储器用于存储程序代码，所述处理器用于调用所述程序代码，以执行以下方法：

获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，所述目标信息包括至少两条子信息，所述每条子信息的属性信息包括所述每条子信息所属的机构、所述每条子信息的生成地址以及所述每条子信息的数据类型中的至少一种；

根据所述每条子信息的属性信息生成所述每条子信息对应的密钥；

获取所述每条子信息对应的第一随机数，根据所述第一随机数对所述每条子信息进行调整，得到调整后的每条子信息；

根据所述目标函数以及所述调整后的每条子信息，获取所述至少两条子信息中每条子信息对应的坐标信息；

采用所述每条子信息对应的密钥，对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文；

将所述每条子信息对应的坐标信息的密文确定为所述目标信息的密文，将所述目标信息的密文存储至区块链网络中。

10、根据权利要求 9 所述的计算机设备，其中，所述每条子信息的属性信息包括所述每条子信息所属的机构；执行所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

获取所述每条子信息所属的机构向所述区块链网络中写入信息的时间以及写入信息的

条数；

根据所述写入信息的时间以及所述写入信息的条数确定所述每条子信息所属的机构的活跃度；

分别对所述每条子信息所属的机构的活跃度进行哈希运算，得到所述每条子信息对应的密钥。

11、根据权利要求 9 所述的计算机设备，其中，所述每条子信息的属性信息包括所述每条子信息的生成地址；执行所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

对所述每条子信息的生成地址进行编码，得到所述每条信息对应的第二随机数；

分别对所述每条信息对应的第二随机数进行哈希运算，得到所述每条子信息对应的密钥。

12、根据权利要求 9 所述的计算机设备，其中，所述每条子信息的属性信息包括所述每条子信息的数据类型；执行所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

根据所述每条子信息的数据类型，确定处理所述每条子信息的实时性等级；

根据所述每条子信息的实时性等级生成所述每条子信息对应的第三随机数；

分别对所述每条信息对应的第三随机数进行哈希运算，得到所述每条子信息对应的密钥。

13、根据权利要求 9 所述的计算机设备，其中，执行所述对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文，包括：

获取所述目标信息所属的终端的私钥，以及所述每条子信息对应的密钥；

根据所述终端的私钥以及所述每条子信息对应的密钥，对所述至少两条子信息中每条子信息对应的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文。

14、根据权利要求 13 所述的计算机设备，其中，执行所述根据所述私钥以及所述每条子信息对应的密钥，对所述至少两条子信息中每条子信息对应的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文，包括：

获取所述目标函数的曲线的基点坐标；

获取所述基点坐标与所述终端的私钥的乘积，得到候选坐标；

根据所述每条子信息对应的密钥对所述候选坐标进行加密，得到所述候选坐标的密文；

对所述每条子信息对应的坐标信息与对应的候选坐标的密文进行融合，得到所述每条子信息对应的坐标信息的密文。

15、一种计算机可读存储介质，其中，所述计算机可读存储介质存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行以下方法：

获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息，所述目标信息包括至少两条子信息，所述每条子信息的属性信息包括所述每条子信息所属的机构、所述每条子信息的生成地址以及所述每条子信息的数据类型中的至少一种；

根据所述每条子信息的属性信息生成所述每条子信息对应的密钥；

获取所述每条子信息对应的第一随机数，根据所述第一随机数对所述每条子信息进行调整，得到调整后的每条子信息；

根据所述目标函数以及所述调整后的每条子信息，获取所述至少两条子信息中每条子信息对应的坐标信息；

采用所述每条子信息对应的密钥，对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文；

将所述每条子信息对应的坐标信息的密文确定为所述目标信息的密文，将所述目标信息的密文存储至区块链网络中。

16、根据权利要求 15 所述的计算机可读存储介质，其中，所述每条子信息的属性信息包括所述每条子信息所属的机构；执行所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

获取所述每条子信息所属的机构向所述区块链网络中写入信息的时间以及写入信息的条数；

根据所述写入信息的时间以及所述写入信息的条数确定所述每条子信息所属的机构的活跃度；

分别对所述每条子信息所属的机构的活跃度进行哈希运算，得到所述每条子信息对应的密钥。

17、根据权利要求 15 所述的计算机可读存储介质，其中，所述每条子信息的属性信息包括所述每条子信息的生成地址；执行所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

对所述每条子信息的生成地址进行编码，得到所述每条信息对应的第二随机数；

分别对所述每条信息对应的第二随机数进行哈希运算，得到所述每条子信息对应的密钥。

18、根据权利要求 15 所述的计算机可读存储介质，其中，所述每条子信息的属性信息包括所述每条子信息的数据类型；执行所述根据所述每条子信息的属性信息生成所述每条子信息对应的密钥，包括：

根据所述每条子信息的数据类型，确定处理所述每条子信息的实时性等级；

根据所述每条子信息的实时性等级生成所述每条子信息对应的第三随机数；

分别对所述每条信息对应的第三随机数进行哈希运算，得到所述每条子信息对应的密钥。

19、根据权利要求 15 所述的计算机可读存储介质，其中，执行所述对所述至少两条子信息中的对应子信息的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文，包括：

获取所述目标信息所属的终端的私钥，以及所述每条子信息对应的密钥；

根据所述终端的私钥以及所述每条子信息对应的密钥，对所述至少两条子信息中每条子信息对应的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文。

20、根据权利要求 19 所述的计算机可读存储介质，其中，执行所述根据所述私钥以及所述每条子信息对应的密钥，对所述至少两条子信息中每条子信息对应的坐标信息进行加密，得到所述每条子信息对应的坐标信息的密文，包括：

获取所述目标函数的曲线的基点坐标；

获取所述基点坐标与所述终端的私钥的乘积，得到候选坐标；

根据所述每条子信息对应的密钥对所述候选坐标进行加密，得到所述候选坐标的密文；

对所述每条子信息对应的坐标信息与对应的候选坐标的密文进行融合，得到所述每条子信息对应的坐标信息的密文。

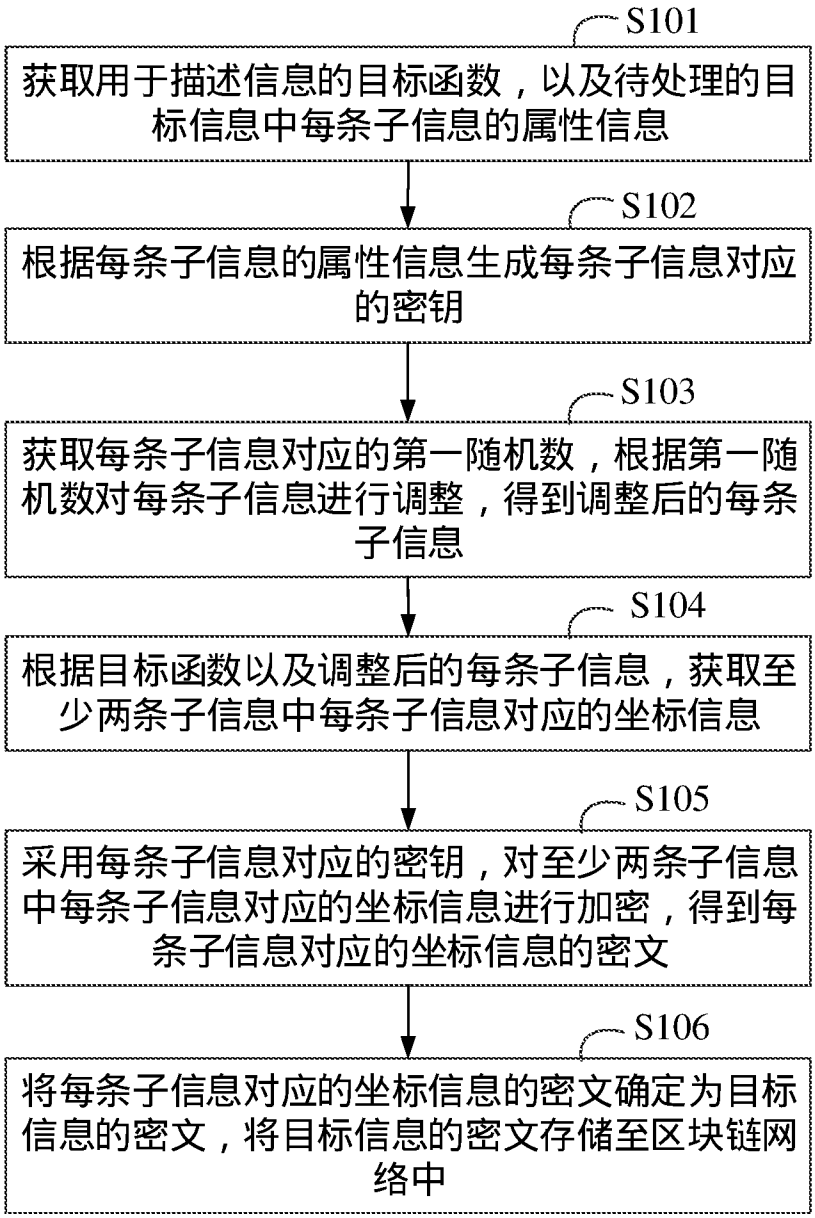

S101
获取用于描述信息的目标函数，以及待处理的目标信息中每条子信息的属性信息
S102
根据每条子信息的属性信息生成每条子信息对应的密钥
S103
获取每条子信息对应的第一随机数，根据第一随机数对每条子信息进行调整，得到调整后的每条子信息
S104
根据目标函数以及调整后的每条子信息，获取至少两条子信息中每条子信息对应的坐标信息
S105
采用每条子信息对应的密钥，对至少两条子信息中每条子信息对应的坐标信息进行加密，得到每条子信息对应的坐标信息的密文
S106
将每条子信息对应的坐标信息的密文确定为目标信息的密文，将目标信息的密文存储至区块链网络中

图 1

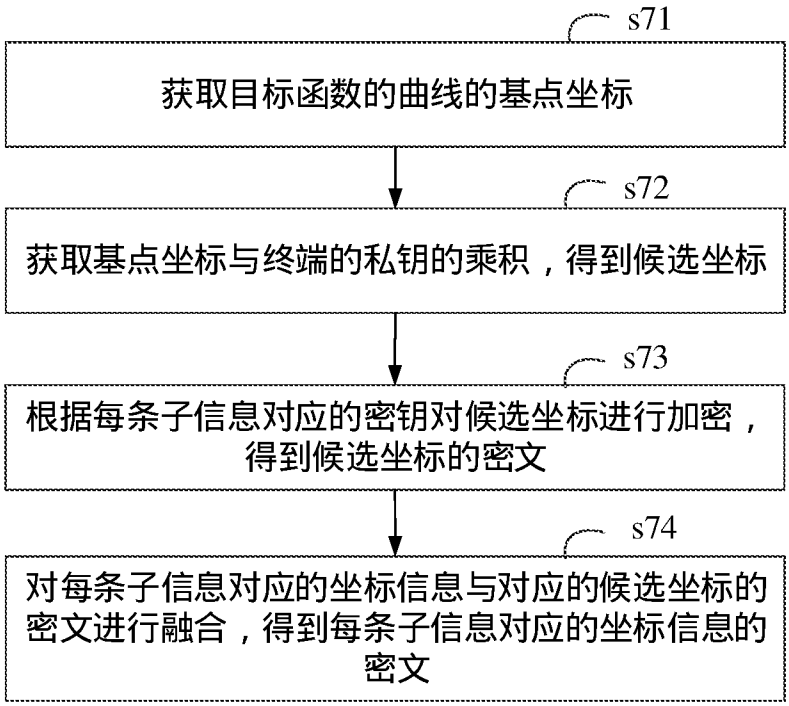

s71
获取目标函数的曲线的基点坐标
s72
获取基点坐标与终端的私钥的乘积，得到候选坐标
s73
根据每条子信息对应的密钥对候选坐标进行加密，得到候选坐标的密文
s74
对每条子信息对应的坐标信息与对应的候选坐标的密文进行融合，得到每条子信息对应的坐标信息的密文

图 2

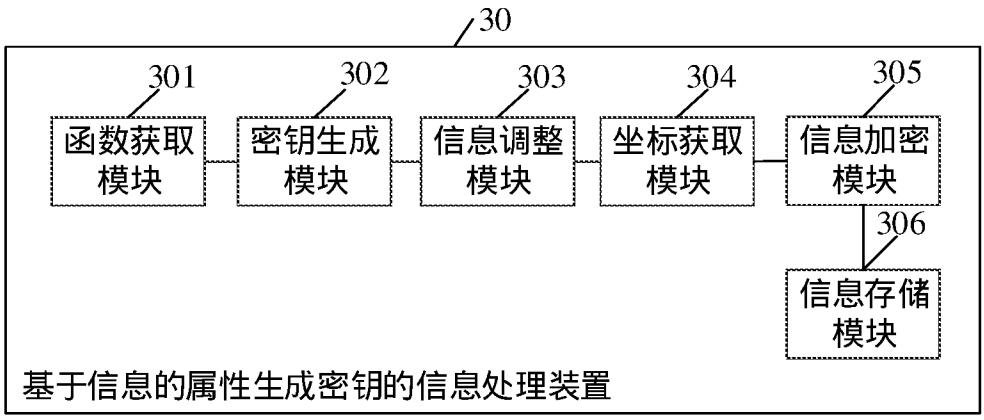

30
301
函数获取模块
302
密钥生成模块
303
信息调整模块
304
坐标获取模块
305
信息加密模块
306
信息存储模块
基于信息的属性生成密钥的信息处理装置

图 3

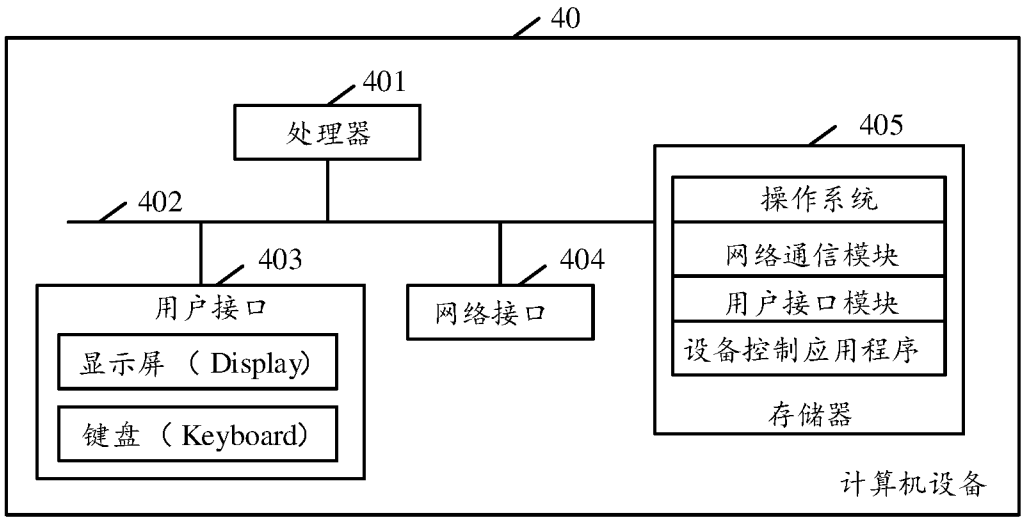

40
401
处理器
402
403
用户接口
显示屏（Display）
键盘（Keyboard）
404
网络接口
405
操作系统
网络通信模块
用户接口模块
设备控制应用程序
存储器
计算机设备

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/097120

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; USTXT; EPTXT; WOTXT; CNKI; IEEE; ISI: 加密, 密钥, 属性, 机构, 地址, 类型, 信息, 文件, 数据, 曲线, 函数, 坐标, 随机数, 随机值, 区块链, encrypt, key, attribute, property, institute, orgnization, address, category, type, information, file, data, curve, function, coordinate, random, nonce, blockchain, block chain

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112202554 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 08 January 2021 (2021-01-08) description paragraphs 42-146	1-20
PX	CN 112199697 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 08 January 2021 (2021-01-08) description paragraphs 41-157	1-20
A	CN 110839026 A (SHENZHEN WANGXIN TECHNOLOGY CO., LTD.) 25 February 2020 (2020-02-25) description paragraphs 70-149	1-20
A	CN 102571790 A (SHANGHAI SYNACAST MEDIA TECHNOLOGY CO., LTD.) 11 July 2012 (2012-07-11) entire document	1-20
A	CN 1890916 A (MATSUSHITA ELECTRIC INDUSTRY CO., LTD.) 03 January 2007 (2007-01-03) entire document	1-20

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 July 2021	**05 August 2021**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/097120

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 102624522 A (HUAZHONG UNIVERSITY OF SCIENCE AND TECHNOLOGY) 01 August 2012 (2012-08-01) entire document	1-20
A	US 2010111296 A1 (CERTICOM CORPORATION) 06 May 2010 (2010-05-06) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/097120

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112202554	A	08 January 2021	None			
CN	112199697	A	08 January 2021	None			
CN	110839026	A	25 February 2020	None			
CN	102571790	A	11 July 2012	CN	102571790	B	25 November 2015
CN	1890916	A	03 January 2007	JP	2007507742	A	29 March 2007
				JP	4611305	B2	12 January 2011
				EP	1668818	A2	14 June 2006
				WO	2005034421	A3	16 June 2005
				WO	2005034421	A2	14 April 2005
				US	7936874	B2	03 May 2011
				US	2007121933	A1	31 May 2007
CN	102624522	A	01 August 2012	CN	102624522	B	19 August 2015
US	2010111296	A1	06 May 2010	US	8891756	B2	18 November 2014

国际检索报告

国际申请号
PCT/CN2021/097120

A. 主题的分类

H04L 9/08(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;VEN;USTXT;EPTXT;WOTXT;CNKI;IEEE;ISI:加密,密钥,属性,机构,地址,类型,信息,文件,数据,曲线,函数,坐标,随机数,随机值,区块链,encrypt,key,attribute, property,institute,orgnization,address,category,type,information,file,data, curve,function,coordinate,random,nonce,blockchain,block chain

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 112202554 A (平安科技深圳有限公司) 2021年 1月 8日 (2021-01-08) 说明书第42-146段	1-20
PX	CN 112199697 A (深圳壹账通智能科技有限公司) 2021年 1月 8日 (2021-01-08) 说明书第41-157段	1-20
A	CN 110839026 A (深圳市网心科技有限公司) 2020年 2月 25日 (2020-02-25) 说明书第70-149段	1-20
A	CN 102571790 A (上海聚力传媒技术有限公司) 2012年 7月 11日 (2012-07-11) 全文	1-20
A	CN 1890916 A (松下电器产业株式会社) 2007年 1月 3日 (2007-01-03) 全文	1-20
A	CN 102624522 A (华中科技大学) 2012年 8月 1日 (2012-08-01) 全文	1-20
A	US 2010111296 A1 (CERTICOM CORP) 2010年 5月 6日 (2010-05-06) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 7月 14日	2021年 8月 5日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 马超 电话号码 (86-27) 59182733

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/097120

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	112202554	A	2021年 1月 8日	无			
CN	112199697	A	2021年 1月 8日	无			
CN	110839026	A	2020年 2月 25日	无			
CN	102571790	A	2012年 7月 11日	CN	102571790	B	2015年 11月 25日
CN	1890916	A	2007年 1月 3日	JP	2007507742	A	2007年 3月 29日
				JP	4611305	B2	2011年 1月 12日
				EP	1668818	A2	2006年 6月 14日
				WO	2005034421	A3	2005年 6月 16日
				WO	2005034421	A2	2005年 4月 14日
				US	7936874	B2	2011年 5月 3日
				US	2007121933	A1	2007年 5月 31日
CN	102624522	A	2012年 8月 1日	CN	102624522	B	2015年 8月 19日
US	2010111296	A1	2010年 5月 6日	US	8891756	B2	2014年 11月 18日