(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
2019 年 5 月 31 日 (31.05.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/100845 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2018/107501

(22) 国际申请日: 2018 年 9 月 26 日 (26.09.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201711168249.3 2017年11月21日 (21.11.2017) CN

(71) 申请人: 阿里巴巴集团控股有限公司 (**ALIBABA GROUP HOLDING LIMITED**) [—/CN]; 开曼群岛大开曼资本大厦一座四层 847 号邮箱, Grand Cayman (KY)。

(72) 发明人: 杜华兵 (**DU, Huabing**); 中国浙江省杭州市余杭区文一西路 969 号 3 号楼 5 楼阿里巴巴集团法务部, Zhejiang 311121 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (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, 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, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(54) **Title:** KEY MANAGEMENT METHOD AND APPARATUS AND DEVICE

(54) **发明名称**: 一种密钥管理方法、装置及设备

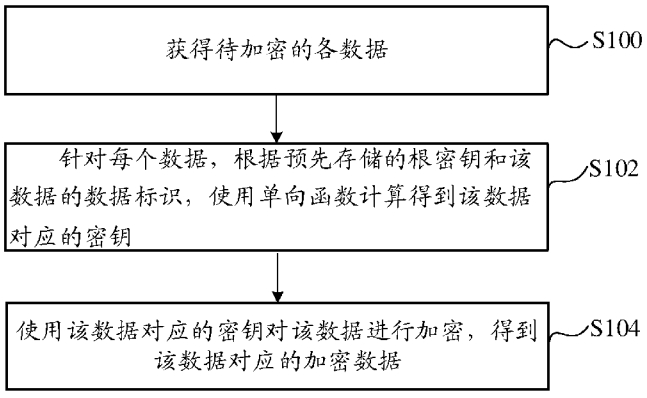

图 1

(57) **Abstract:** Embodiments of the present description disclose a key management method and apparatus and a device. In the embodiments of the present description, a key corresponding to data is calculated according to a data identifier of the data and a pre-stored root key by using a one-way function, and the data is encrypted by using the key corresponding to the data. When it is necessary to authorize a data decryption device to decrypt a certain piece of data, a key corresponding to the data is calculated according to a data identifier of the data and the root key by using the one-way function, and the key corresponding to the data is sent to the data decryption device.

(57) **摘要**: 本说明书实施例公开了一种密钥管理方法、装置及设备。在本说明书实施例中，根据数据的数据标识和预先存储的根密钥，使用单向函数计算数据对应的密钥，并使用数据对应的密钥对数据进行加密。当需要授权数据解密设备解密某个数据时，再次根据该数据的数据标识和根密钥，使用单向函数计算该数据对应的密钥，将该数据对应的密钥发送给数据解密设备。

WO 2019/100845 A1

[见续页]

(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:

— 包括国际检索报告(条约第21条(3))。

一种密钥管理方法、装置及设备

技术领域

[01]本说明书涉及信息技术领域，尤其涉及一种密钥管理方法、装置及设备。

背景技术

[02]目前，数据存储方将存储的数据公开，以供数据获取方使用的模式较为常见。数据获取方可以通过网络访问数据存储方的设备，获取设备上存储的数据。

[03]通常，数据存储方为了对数据获取权限进行管理，会针对每个数据，使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。其中，不同的数据对应的密钥是不同的。数据获取方倘若想要解密某个加密数据，则必须先向数据存储方请求获得该加密数据对应的密钥，随后方能使用获得的密钥解密该加密数据，得到数据原文。

[04]基于现有技术，需要一种成本较低的密钥管理方法。

发明内容

[05]本说明书实施例提供一种密钥管理方法、装置及设备，以解决现有的密钥管理方法成本较高的问题。

[06]为解决上述技术问题，本说明书实施例是这样实现的：

[07]本说明书实施例提供的一种数据加密方法，包括：

[08]获得待加密的各数据；

[09]针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥；

[10]使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

[11]本说明书实施例提供的一种发送密钥的方法，包括：

[12]接收数据解密设备发送的数据解密请求；所述数据解密请求包含数据标识；

[13]根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥；

[14]将计算得到的密钥发送给所述数据解密设备，以使所述数据解密设备根据接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[15]本说明书实施例提供的一种数据解密方法，包括：

[16]向数据加密设备发送数据解密请求；所述数据解密请求包含数据标识；

[17]接收所述数据加密设备返回的密钥，所述密钥是所述数据加密设备根据上述数据加密方法计算得到的；

[18]根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[19]本说明书实施例提供的一种数据加密装置，包括：

[20]获得模块，获得待加密的各数据；

[21]计算模块，针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥；

[22]加密模块，使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

[23]本说明书实施例提供的一种发送密钥的装置，包括：

[24]接收模块，接收数据解密设备发送的数据解密请求；所述数据解密请求包含数据标识；

[25]计算模块，根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥；

[26]发送模块，将计算得到的密钥发送给所述数据解密设备，以使所述数据解密设备根据接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[27]本说明书实施例提供的一种数据解密装置，包括：

[28]发送模块，向数据加密设备发送数据解密请求；所述数据解密请求包含数据标识；

[29]接收模块，接收所述数据加密设备返回的密钥，所述密钥是所述数据加密设备根据上述数据加密方法计算得到的；

[30]解密模块，根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[31]本说明书实施例提供的一种数据加密设备，包括一个或多个处理器及存储器，所述

存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[32]获得待加密的各数据；

[33]针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥；

[34]使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

[35]本说明书实施例提供的一种发送密钥的设备，包括一个或多个处理器及存储器，所述存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[36]接收数据解密设备发送的数据解密请求；所述数据解密请求包含数据标识；

[37]根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥；

[38]将计算得到的密钥发送给所述数据解密设备，以使所述数据解密设备根据接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[39]本说明书实施例提供的一种数据解密设备，包括一个或多个处理器及存储器，所述存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[40]向数据加密设备发送数据解密请求；所述数据解密请求包含数据标识；

[41]接收所述数据加密设备返回的密钥，所述密钥是所述数据加密设备根据上述数据加密方法计算得到的；

[42]根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[43]由以上本说明书实施例提供的技术方案可见，在本说明书实施例中，根据数据的数据标识和预先存储的根密钥，使用单向函数计算数据对应的密钥，并使用数据对应的密钥对数据进行加密。当需要授权数据解密设备解密某个数据时，再次根据该数据的数据标识和根密钥，使用单向函数计算该数据对应的密钥，将该数据对应的密钥发送给数据解密设备。如此一来，数据加密设备无需存储各数据分别对应的密钥，仅存储根密钥即可，数据加密设备可以根据根密钥和各数据的数据标识随时派生出各数据分别对应的密钥，这样，也就降低了数据加密设备的存储成本。

附图说明

[44]为了更清楚地说明本说明书实施例或现有技术中的技术方案，下面将对实施例或现

有技术描述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说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[45]图 1 是本说明书实施例提供的一种数据加密方法流程图；

[46]图 2 是本说明书实施例提供的一种发送密钥的方法流程图；

[47]图 3 是本说明书实施例提供的一种数据解密方法流程图；

[48]图 4 是本说明书实施例提供的树形结构示意图；

[49]图 5 是本说明书实施例提供的一种数据加密装置示意图；

[50]图 6 是本说明书实施例提供的一种发送密钥的装置示意图；

[51]图 7 是本说明书实施例提供的一种数据解密装置示意图；

[52]图 8 是本说明书实施例提供的一种数据加密设备示意图；

[53]图 9 是本说明书实施例提供的一种发送密钥的设备示意图；

[54]图 10 是本说明书实施例提供的一种数据解密设备示意图。

具体实施方式

[55]在现有技术中，数据存储方通常使用不同的密钥对不同的数据进行加密并存储得到的各加密数据以及各加密数据分别对应的密钥。当数据解密设备向数据加密设备请求解密某个加密数据时，数据加密设备将该加密数据对应的密钥发送给数据解密设备，数据解密设备就可以使用接收到的密钥解密加密数据得到数据原文。

[56]但是，这种模式的缺陷在于，随着数据存储方存储的数据越来越多，其需要存储的密钥也会相应地增加，导致数据存储方的存储成本较大。

[57]在本说明书的一个或多个实施例中，数据加密设备加密某个数据所使用密钥是根据该数据的数据标识和预先存储的根密钥，使用单向函数得到的。这意味着：

[58]1、每个数据对应的密钥都是由根密钥派生出来的，数据加密设备仅需存储根密钥即可，每个数据对应的密钥都可以随时由根密钥派生出来，这可以显著降低数据加密设备的存储成本。

[59]2、一方面每个数据的数据标识不同，另一方面对于单向函数而言，输入不同通常导致输出不同。基于此，由于对每个数据进行加密所使用的密钥是根据根密钥和该数据的数据标识，使用单向函数计算得到的，因此解密各加密数据所需的密钥是不同的。

[60]3、由于单向函数具有不可逆性，通常无法根据某个密钥逆推出派生该密钥的根密钥，从而可以有效防止除数据加密设备之外的其他设备未经授权私自生成某个数据对应的密钥的情况发生。

[61]需要说明的是，在本说明书实施例中，数据存储方可以通过自己的设备对数据进行加密后，存储得到的加密数据；也可以是非数据存储方的设备对数据进行加密，得到加密数据，数据存储方获取加密数据并存储。因此，本文将实际加密数据的设备称为“数据加密设备”，其可以是数据存储方的设备，也可以是非数据存储方的设备。

[62]本说明书的各实施例涉及一种密钥管理方法，具体涉及数据加密方法、发送密钥的方法以及数据解密方法。

[63]为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书一个或多个实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。通过本说明书实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都应当属于本说明书保护的范围。

[64]以下结合附图，详细说明本说明书各实施例提供的技术方案。

[65]图 1 是本说明书实施例提供的数据加密方法流程图，包括以下步骤：

[66]S100：数据加密设备获得待加密的各数据。

[67]图 1 所示的方法的执行主体是数据加密设备，例如，可以是数据的拥有者的设备，如文件作者的计算机。数据加密设备可以接收数据作者输入的待加密的数据，也可以从其他途径获取待加密的数据，本说明书对此不作具体限制。

[68]S102：针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥。

[69]在本说明书实施例中，所述根密钥是加密设备需要存储的密钥，对每个数据进行加密所使用的密钥都是由所述根密钥派生出来的。

[70]为了确保根据根密钥和不同的数据的数据标识派生出的密钥不同，以及确保根据派

生出的密钥难以逆推出根密钥，需要利用单向函数的如下特性：其一，若输入到单向函数的数据不同，则通过单向函数计算，输出的数据也往往不同；其二，根据单向函数的输出，难以逆推出单向函数的输入。常见的单向函数均可应用于本说明书实施例中，如MD5（Message Digest Algorithm 5）、SHA（Secure Hash Algorithm）、MAC（Message Authentication Code）等。

[71]S104：使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

[72]此处值得强调，上述步骤S100~S104是对数据进行加密的方法步骤，数据加密设备的主要功能是对待加密的各数据进行加密以及为请求解密数据的数据解密设备派发密钥。数据加密设备不一定会存储得到的各加密数据。

[73]具体来说，数据加密设备可以存储得到的各加密数据，和/或，将得到的各加密数据发送给各区块链节点，由各区块链节点在对各加密数据共识验证通过后，将各加密数据存入区块链。

[74]当各加密数据是由数据加密设备进行存储时，数据解密设备可以向数据加密设备请求获取某个加密数据以及解密该加密数据所需的密钥，随后使用获取的密钥解密获取的加密数据。

[75]当各加密数据被存入区块链时，数据解密设备可以先向数据加密设备请求解密某个加密数据所需的密钥，随后从某个区块链节点处获取该加密数据，并使用数据加密设备派发的该加密数据对应的密钥解密该加密数据，得到数据原文。

[76]图2是本说明书实施例提供的发送密钥的方法流程图，包括：

[77]S200：接收数据解密设备发送的数据解密请求。

[78]图2所示的方法的执行主体是数据加密设备。如前所述，数据加密设备的主要功能除了包括对待加密的各数据进行加密（如图1所示的流程），还包括为请求解密数据的数据解密设备派发密钥（即图2所示的流程）。

[79]数据解密设备是对解密加密数据所需的密钥有需求的设备，其通常是数据获取方的设备。数据解密设备对某个加密数据进行解密前，需要向数据加密设备请求获取该加密数据对应的密钥，相当于请求数据加密设备对其进行解密授权。

[80]在本说明书实施例中，所述数据解密请求可包含数据标识，所述数据标识可对应一个加密数据，也可以对应一批加密数据。数据标识对应的加密数据就是数据解密设备需

要解密的加密数据。

[81]S202：根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥。

[82]在本说明实施例中，为了降低存储成本，数据加密设备不会存储各加密数据分别对应的密钥。因此，在本步骤 S202 中，数据加密设备需要临时生成需要发送的密钥。

[83]类似于步骤 S102，在本步骤 S202 中，数据加密设备根据预先存储的根密钥和数据解密请求中包含的数据标识，使用单向函数计算得到需要发送给数据解密设备的密钥。

[84]S204：将计算得到的密钥发送给所述数据解密设备。

[85]图 3 是本说明书实施例提供的数据解密方法流程图，包括以下步骤：

[86]S300：向数据加密设备发送数据解密请求。

[87]本方法的执行主体是数据解密设备。所述数据解密请求包含数据标识，所述数据标识对应的加密数据就是数据解密设备需要解密的加密数据。数据解密设备可预先获知其所要解密的加密数据对应的数据标识。例如，数据加密设备可以将各加密数据的数据标识组织成列表，并将列表公开，数据解密设备通过查询列表，确定其要解密的加密数据的数据标识。

[88]S302：接收所述数据加密设备返回的密钥。

[89]在本说明书实施例中，所述数据加密设备返回的密钥是所述数据加密设备在图 2 所示的步骤 S202 中计算得到的。

[90]S304：根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[91]如前所述，在本说明书实施例中，由数据加密设备对各加密数据对应的密钥进行管理，而对各加密数据存储于何处不作具体限定。数据加密设备可以存储加密数据，数据加密设备之外的其他设备（甚至包括数据解密设备）也可以存储加密数据。相应地，数据解密设备既可以从数据加密设备获取所述数据标识对应的加密数据，也可以从其他设备（如区块链节点）中获取所述数据标识对应的加密数据，甚至可以预先存储各加密数据。

[92]数据解密设备获得数据加密设备发送的密钥，意味着取得了解密所述数据标识对应的加密数据的权限。

[93]通过图 1~图 3 所示的密钥管理方法，解密不同的加密数据所需要的密钥不同。数据

解密设备无法根据已经获得的某个数据对应的密钥逆推出根密钥，也就无法私自派生其他数据对应的密钥，只能向数据加密设备请求解密权限。管理密钥的数据加密设备无需存储各数据分别对应的密钥，仅存储根密钥即可，数据加密设备可以根据根密钥和各数据的数据标识随时派生出各数据分别对应的密钥，这样，也就降低了数据加密设备的存储成本。

[94]此外，下文对上述的技术方案作进一步扩展。

[95]图 4 是本说明书实施例提供的树形结构示意图。如图 4 所示，在树形结构中，实心点表示根节点，空心点表示中间节点，阴影点表示叶子节点。

[96]在树形结构中，为每个节点分配编号，这样可以方便表示数形结构中任意两个具有上下级关系的节点之间的路径。假设树形结构中任一节点为第一节点，第一节点下的任一节点为第二节点，那么在本说明书中，第二节点相对于第一节点的路径信息实际上是第一节点到第二节点所经过的所有节点的序列。

[97]例如，节点 5 相对于节点 1 的路径信息可以是序列“1-2-5”，节点 15 相对于节点 1 的路径信息可以是序列“1-3-8-15”。

[98]在本说明书实施例中，可以使得上述树形结构的叶子节点与待加密的各数据一一对应，当然，对各数据进行加密后，得到的各加密数据与各叶子节点也是一一对应的。通过这种设置，针对每个数据，可以将该数据对应的叶子节点相对于所述树形结构的根节点的路径信息作为该数据的数据标识。需要说明的是，各加密数据与各叶子节点一一对应，并不意味着各加密数据一定是依照树形结构而被存储的，本说明书对各加密数据的存储形式并不做具体限定。

[99]倘若各数据及其对应的各加密数据与各叶子节点是一一对应的，则可对本技术方案扩展如下:

[100] 在图 1 所示的方法的步骤 S102 中，可以针对每个数据，根据预先存储的根密钥和该数据对应的叶子节点相对于所述根节点的路径信息，使用单向函数计算得到该叶子节点对应的密钥，作为该数据对应的密钥。

[101] 在图 2 所示的发送密钥的方法中，数据解密请求包含的数据标识可以是数据解密设备想要解密的加密数据对应的叶子节点相对于所述树形结构的根节点的路径信息，数据加密设备可以同样采用步骤 S102 中的方法计算出待解密的加密数据对应的密钥，将计算出的密钥发送给数据解密设备。

[102] 在图 3 所示的数据解密方法中，数据解密设备发送的数据解密请求包含的数据标识可以是叶子节点相对于所述根节点的路径信息，数据解密设备可以使用接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[103] 基于图 4 所示的树形结构，本说明书实施例提供了一种根据第一节点对应的密钥和第二节点相对于第一节点的路径信息，使用单向函数计算第二节点对应的密钥的方法（下文称“节点密钥算法”），如下：

[104] 根密钥为根节点对应的密钥；

[105] 将第一节点作为输入节点；

[106] 将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；

[107] 判断所述下一个节点是否是第二节点；

[108] 若是，则将计算得到的密钥作为第二节点对应的密钥；

[109] 否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到第二节点对应的密钥为止。

[110] 以第一节点是节点 3，第二节点是节点 15 为例说明。已知节点 3 对应的密钥，首先将节点 3 作为输入节点，将节点 3 对应的密钥和序列“3-8-15”中节点 3 的下一个节点 8 相对于节点 3 的路径信息“3-8”输入到单向函数，计算得到节点 8 对应的密钥；由于节点 8 不是节点 15，因此，重新将节点 8 作为输入节点，继续计算节点 8 的下一个节点 15 对应的密钥，最终计算出节点 15 对应的密钥。这样，如图 4 所示的树形结构的每个节点（包括根节点、中间节点、叶子节点）都可以有对应的密钥。

[111] 基于上述节点密钥算法，还可以对本技术方案扩展如下：

[112] 在图 1 所示的流程中，已知根节点和某个数据对应的叶子节点相对于根节点的路径信息，可以使用上述节点密钥算法计算出该数据对应的叶子节点对应的密钥，也就是该数据对应的密钥。

[113] 具体地，在步骤 S102 中，针对每个数据，该数据对应的叶子节点相对于所述根节点的路径信息实际上是所述根节点到该叶子节点所经过的所有节点的序列，同时，所述根密钥即是树形结构的根节点对应的密钥。根据预先存储的根密钥和该数据对应的叶子节点相对于所述根节点的路径信息，使用单向函数计算得到该叶子节点对应的密钥，

包括:

[114] 将所述根节点作为输入节点;

[115] 将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥;

[116] 判断所述下一个节点是否是该叶子节点;

[117] 若是，则将计算得到的密钥作为该叶子节点对应的密钥;

[118] 否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到该叶子节点对应的密钥为止。

[119] 在图 2 所示的流程中，数据加密设备接收的数据解密请求中包含的数据标识不一定是某个叶子节点相对于根节点的路径信息，可能是树形结构中的某个中间节点相对于根节点的路径信息。对数据加密设备而言，不论其接收到的数据解密请求中包含的数据标识为何种节点（中间节点或叶子节点）相对于根节点的路径信息，其都可以采用上述的节点密钥算法，根据计算出该节点对应的密钥，并将之发送给数据解密设备。

[120] 具体地，在步骤 S202 中，针对所述树形结构中的任一节点，该节点相对于所述树形结构的根节点的路径信息为所述根节点到该节点所经过的所有节点的序列;所述根密钥为所述根节点对应的密钥;

[121] 根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥的方式可以如下:

[122] 根据所述数据解密请求中包含的路径信息确定序列;

[123] 将所述根节点作为输入节点;

[124] 将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥;

[125] 判断所述下一个节点是否是所述序列中的最后一个节点;

[126] 若是，则将计算得到的密钥作为要发送给所述数据解密设备的密钥;

[127] 否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到所述序列中最后一个节点对应的密钥为止。

[128] 在图 3 所示的流程中，数据解密设备发送给数据加密设备的数据解密请求包含

的数据标识可以是树形结构中某个叶子节点相对于根节点的路径信息，也可以是某个中间节点相对于根节点的路径信息。树形结构是公开可知的，因此数据解密设备可以确定各节点间的路径以及各叶子节点对应的加密数据。

[129] 当数据解密请求包含某个中间节点相对于根节点的路径信息时，相当于数据解密设备请求数据加密设备授予其解密该中间节点下所有叶子节点对应的加密数据的权限。相应地，数据加密设备返回给数据解密设备的密钥就是该中间节点对应的密钥。

[130] 数据解密设备可以根据数据加密设备发送的中间节点对应的密钥采用节点密钥算法，计算得到该中间节点下任一叶子节点对应的密钥，也就可以解密该中间节点下任一叶子节点对应的加密数据。

[131] 具体地，在步骤 S304 中，针对所述中间节点下的任一叶子节点，该叶子节点相对于所述中间节点的路径信息为所述中间节点到该叶子节点所经过的所有节点的序列，数据解密设备可以采用如下方式，根据该叶子节点相对于该中间节点的路径信息和接收到的密钥，使用单向函数计算得到该叶子节点对应的密钥:

[132] 针对所述数据标识对应的中间节点下的每个叶子节点，根据该叶子节点相对于该中间节点的路径信息确定序列;

[133] 将该中间节点作为输入节点;

[134] 将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥;

[135] 判断所述下一个节点是否是所述序列中的最后一个节点;

[136] 若是，则将计算得到的密钥作为该叶子节点对应的密钥;

[137] 否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到所述序列中最后一个节点对应的密钥为止。

[138] 通过对本说明书实施例进行上述扩展，数据加密设备可以较为灵活的授予数据解密设备解密加密数据的权限，即，通过向数据解密设备发送某个中间节点对应的密钥的方式，一次性地授权数据解密设备解密该中间节点下所有叶子节点对应的加密数据。

[139] 基于图 1 所示的数据加密方法，本说明书实施例对应提供了一种数据加密装置，如图 5 所示，包括:

[140] 获得模块 501，获得待加密的各数据;

[141] 计算模块 502，针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥；

[142] 加密模块 503，使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

[143] 各数据与预设的树形结构的各叶子节点一一对应；

[144] 针对每个数据，该数据的数据标识为该数据对应的叶子节点相对于所述树形结构的根节点的路径信息；

[145] 所述计算模块 502，针对每个数据，根据预先存储的根密钥和该数据对应的叶子节点相对于所述根节点的路径信息，使用单向函数计算得到该叶子节点对应的密钥，作为该数据对应的密钥。

[146] 该数据对应的叶子节点相对于所述根节点的路径信息是所述根节点到该叶子节点所经过的所有节点的序列；所述根密钥为所述根节点对应的密钥；

[147] 所述计算模块 502，将所述根节点作为输入节点；将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；判断所述下一个节点是否是该叶子节点；若是，则将计算得到的密钥作为该叶子节点对应的密钥；否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到该叶子节点对应的密钥为止。

[148] 基于图 2 所示的发送密钥的方法，本说明书实施例对应提供了一种发送密钥的装置，如图 6 示，包括：

[149] 接收模块 601，接收数据解密设备发送的数据解密请求；所述数据解密请求包含数据标识；

[150] 计算模块 602，根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥；

[151] 发送模块 603，将计算得到的密钥发送给所述数据解密设备，以使所述数据解密设备根据接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[152] 各加密数据与预设的树形结构的各叶子节点一一对应；

[153] 所述数据解密请求中包含的数据标识为所述树形结构的任一节点相对于所述树形结构的根节点的路径信息。

[154] 针对所述树形结构中的任一节点，该节点相对于所述树形结构的根节点的路径信息为所述根节点到该节点所经过的所有节点的序列；所述根密钥为所述根节点对应的密钥；

[155] 所述计算模块 602，根据所述数据解密请求中包含的路径信息确定序列；将所述根节点作为输入节点；将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；判断所述下一个节点是否是所述序列中的最后一个节点；若是，则将计算得到的密钥作为要发送给所述数据解密设备的密钥；否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到所述序列中最后一个节点对应的密钥为止。

[156] 基于图 3 所示的数据解密方法，本说明书实施例对应提供了一种数据解密装置，如图 7 所示，包括：

[157] 发送模块 701，向数据加密设备发送数据解密请求；所述数据解密请求包含数据标识；

[158] 接收模块 702，接收所述数据加密设备返回的密钥，所述密钥是所述数据加密设备根据如权利要求 4~6 任一项所述的方法计算得到的；

[159] 解密模块 703，根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[160] 各加密数据与预设的树形结构的各叶子节点一一对应；

[161] 所述数据解密请求中包含的数据标识为所述树形结构的任一节点相对于所述树形结构的根节点的路径信息；

[162] 所述解密模块 703，若所述数据标识是叶子节点相对于所述根节点的路径信息，则使用所述密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密；若所述数据标识是中间节点相对于所述根节点的路径信息，则针对该中间节点下的每个叶子节点，根据该叶子节点相对于该中间节点的路径信息和接收到的密钥，使用单向函数计算得到该叶子节点对应的密钥，并使用该叶子节点对应的密钥对该叶子节点对应的加密数据进行解密。

[163] 针对所述中间节点下的任一叶子节点，该叶子节点相对于所述中间节点的路径信息为所述中间节点到该叶子节点所经过的所有节点的序列；

[164] 所述解密模块 703，针对所述数据标识对应的中间节点下的每个叶子节点，根据该叶子节点相对于该中间节点的路径信息确定序列；将该中间节点作为输入节点；将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；判断所述下一个节点是否是所述序列中的最后一个节点；若是，则将计算得到的密钥作为该叶子节点对应的密钥；否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到所述序列中最后一个节点对应的密钥为止。

[165] 图 8 是本说明书实施例提供的一种数据加密设备，包括一个或多个处理器及存储器，所述存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[166] 获得待加密的各数据；

[167] 针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥；

[168] 使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

[169] 图 9 是本说明书实施例提供的一种发送密钥的设备，包括一个或多个处理器及存储器，所述存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[170] 接收数据解密设备发送的数据解密请求；所述数据解密请求包含数据标识；

[171] 根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥；

[172] 将计算得到的密钥发送给所述数据解密设备，以使所述数据解密设备根据接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[173] 图 10 是本说明书实施例提供的一种数据解密设备，包括一个或多个处理器及存储器，所述存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

[174] 向数据加密设备发送数据解密请求；所述数据解密请求包含数据标识；

[175] 接收所述数据加密设备返回的密钥，所述密钥是所述数据加密设备根据上述数据加密方法计算得到的；

[176] 根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

[177] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于图 8、图 9 以及图 10 所示的设备而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[178] 在 20 世纪 90 年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字符系统“集成”在一片 PLD 上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而 HDL 也并非仅有一种，而是有许多种，如 ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是 VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与 Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

[179] 控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步

骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[180] 上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的，计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字符助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[181] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本说明书时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[182] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[183] 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

[184] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

[185] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在

计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

[186] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[187] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[188] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字符多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[189] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[190] 本领域技术人员应明白，本说明书的实施例可提供为方法、系统或计算机程序产品。因此，本说明书可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

[191] 本说明书可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、

对象、组件、数据结构等等。也可以在分布式计算环境中实践本说明书，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[192] 以上所述仅为本说明书的实施例而已，并不用于限制本说明书。对于本领域技术人员来说，本说明书可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本说明书的权利要求范围之内。

权利要求书

1、一种数据加密方法，包括:

获得待加密的各数据;

针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥;

使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

2、根据权利要求 1 所述的方法，各数据与预设的树形结构的各叶子节点一一对应;

针对每个数据，该数据的数据标识为该数据对应的叶子节点相对于所述树形结构的根节点的路径信息;

针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥，具体包括:

针对每个数据，根据预先存储的根密钥和该数据对应的叶子节点相对于所述根节点的路径信息，使用单向函数计算得到该叶子节点对应的密钥，作为该数据对应的密钥。

3、根据权利要求 2 所述的方法，该数据对应的叶子节点相对于所述根节点的路径信息是所述根节点到该叶子节点所经过的所有节点的序列;所述根密钥为所述根节点对应的密钥;

根据预先存储的根密钥和该数据对应的叶子节点相对于所述根节点的路径信息，使用单向函数计算得到该叶子节点对应的密钥，具体包括:

将所述根节点作为输入节点;

将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥;

判断所述下一个节点是否是该叶子节点;

若是，则将计算得到的密钥作为该叶子节点对应的密钥;

否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到该叶子节点对应的密钥为止。

4、一种发送密钥的方法，包括:

接收数据解密设备发送的数据解密请求;所述数据解密请求包含数据标识;

根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥;

将计算得到的密钥发送给所述数据解密设备，以使所述数据解密设备根据接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

5、根据权利要求 4 所述的方法，各加密数据与预设的树形结构的各叶子节点一一

对应；

所述数据解密请求中包含的数据标识为所述树形结构的任一节点相对于所述树形结构的根节点的路径信息。

6、根据权利要求 5 所述的方法，针对所述树形结构中的任一节点，该节点相对于所述树形结构的根节点的路径信息为所述根节点到该节点所经过的所有节点的序列；所述根密钥为所述根节点对应的密钥；

根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥，具体包括：

根据所述数据解密请求中包含的路径信息确定序列；

将所述根节点作为输入节点；

将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；

判断所述下一个节点是否是所述序列中的最后一个节点；

若是，则将计算得到的密钥作为要发送给所述数据解密设备的密钥；

否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到所述序列中最后一个节点对应的密钥为止。

7、一种数据解密方法，包括：

向数据加密设备发送数据解密请求；所述数据解密请求包含数据标识；

接收所述数据加密设备返回的密钥，所述密钥是所述数据加密设备根据如权利要求 4~6 任一项所述的方法计算得到的；

根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

8、根据权利要求 7 所述的方法，各加密数据与预设的树形结构的各叶子节点一一对应；

所述数据解密请求中包含的数据标识为所述树形结构的任一节点相对于所述树形结构的根节点的路径信息；

根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密，具体包括：

若所述数据标识是叶子节点相对于所述根节点的路径信息，则使用所述密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密；

若所述数据标识是中间节点相对于所述根节点的路径信息，则针对该中间节点下的每个叶子节点，根据该叶子节点相对于该中间节点的路径信息和接收到的密钥，使用单向函数计算得到该叶子节点对应的密钥，并使用该叶子节点对应的密钥对该叶子节点对

应的加密数据进行解密。

9、根据权利要求 8 所述的方法，针对所述中间节点下的任一叶子节点，该叶子节点相对于所述中间节点的路径信息为所述中间节点到该叶子节点所经过的所有节点的序列；

针对所述数据标识对应的中间节点下的每个叶子节点，根据该叶子节点相对于该中间节点的路径信息和接收到的密钥，使用单向函数计算得到该叶子节点对应的密钥，具体包括：

针对所述数据标识对应的中间节点下的每个叶子节点，根据该叶子节点相对于该中间节点的路径信息确定序列；

将该中间节点作为输入节点；

将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；

判断所述下一个节点是否是所述序列中的最后一个节点；

若是，则将计算得到的密钥作为该叶子节点对应的密钥；

否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到所述序列中最后一个节点对应的密钥为止。

10、一种数据加密装置，包括：

获得模块，获得待加密的各数据；

计算模块，针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥；

加密模块，使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

11、根据权利要求 10 所述的装置，各数据与预设的树形结构的各叶子节点一一对应；

针对每个数据，该数据的数据标识为该数据对应的叶子节点相对于所述树形结构的根节点的路径信息；

所述计算模块，针对每个数据，根据预先存储的根密钥和该数据对应的叶子节点相对于所述根节点的路径信息，使用单向函数计算得到该叶子节点对应的密钥，作为该数据对应的密钥。

12、根据权利要求 11 所述的装置，该数据对应的叶子节点相对于所述根节点的路径信息是所述根节点到该叶子节点所经过的所有节点的序列；所述根密钥为所述根节点对应的密钥；

所述计算模块，将所述根节点作为输入节点；将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；判断所述下一个节点是否是该叶子节点；若是，则将计算得到的密钥作为该叶子节点对应的密钥；否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到该叶子节点对应的密钥为止。

13、一种发送密钥的装置，包括：

接收模块，接收数据解密设备发送的数据解密请求；所述数据解密请求包含数据标识；

计算模块，根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥；

发送模块，将计算得到的密钥发送给所述数据解密设备，以使所述数据解密设备根据接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

14、根据权利要求 13 所述的装置，各加密数据与预设的树形结构的各叶子节点一一对应；

所述数据解密请求中包含的数据标识为所述树形结构的任一节点相对于所述树形结构的根节点的路径信息。

15、根据权利要求 14 所述的装置，针对所述树形结构中的任一节点，该节点相对于所述树形结构的根节点的路径信息为所述根节点到该节点所经过的所有节点的序列；所述根密钥为所述根节点对应的密钥；

所述计算模块，根据所述数据解密请求中包含的路径信息确定序列；将所述根节点作为输入节点；将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；判断所述下一个节点是否是所述序列中的最后一个节点；若是，则将计算得到的密钥作为要发送给所述数据解密设备的密钥；否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到所述序列中最后一个节点对应的密钥为止。

16、一种数据解密装置，包括：

发送模块，向数据加密设备发送数据解密请求；所述数据解密请求包含数据标识；

接收模块，接收所述数据加密设备返回的密钥，所述密钥是所述数据加密设备根据如权利要求 4~6 任一项所述的方法计算得到的；

解密模块，根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据

进行解密。

17、根据权利要求 16 所述的装置，各加密数据与预设的树形结构的各叶子节点一一对应；

所述数据解密请求中包含的数据标识为所述树形结构的任一节点相对于所述树形结构的根节点的路径信息；

所述解密模块，若所述数据标识是叶子节点相对于所述根节点的路径信息，则使用所述密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密；若所述数据标识是中间节点相对于所述根节点的路径信息，则针对该中间节点下的每个叶子节点，根据该叶子节点相对于该中间节点的路径信息和接收到的密钥，使用单向函数计算得到该叶子节点对应的密钥，并使用该叶子节点对应的密钥对该叶子节点对应的加密数据进行解密。

18、根据权利要求 17 所述的装置，针对所述中间节点下的任一叶子节点，该叶子节点相对于所述中间节点的路径信息为所述中间节点到该叶子节点所经过的所有节点的序列；

所述解密模块，针对所述数据标识对应的中间节点下的每个叶子节点，根据该叶子节点相对于该中间节点的路径信息确定序列；将该中间节点作为输入节点；将所述输入节点对应的密钥和所述序列中所述输入节点的下一个节点相对于所述输入节点的路径信息输入到单向函数，计算得到所述下一个节点对应的密钥；判断所述下一个节点是否是所述序列中的最后一个节点；若是，则将计算得到的密钥作为该叶子节点对应的密钥；否则，将所述下一个节点重新作为输入节点，继续计算所述序列中输入节点的下一个节点对应的密钥，直至得到所述序列中最后一个节点对应的密钥为止。

19、一种数据加密设备，包括一个或多个处理器及存储器，所述存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

获得待加密的各数据；

针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥；

使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据。

20、一种发送密钥的设备，包括一个或多个处理器及存储器，所述存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

接收数据解密设备发送的数据解密请求；所述数据解密请求包含数据标识；

根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥；

将计算得到的密钥发送给所述数据解密设备，以使所述数据解密设备根据接收到的密钥对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

21、一种数据解密设备，包括一个或多个处理器及存储器，所述存储器存储有程序，并且被配置成由所述一个或多个处理器执行以下步骤：

向数据加密设备发送数据解密请求；所述数据解密请求包含数据标识；

接收所述数据加密设备返回的密钥，所述密钥是所述数据加密设备根据如权利要求4~6任一项所述的方法计算得到的；

根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密。

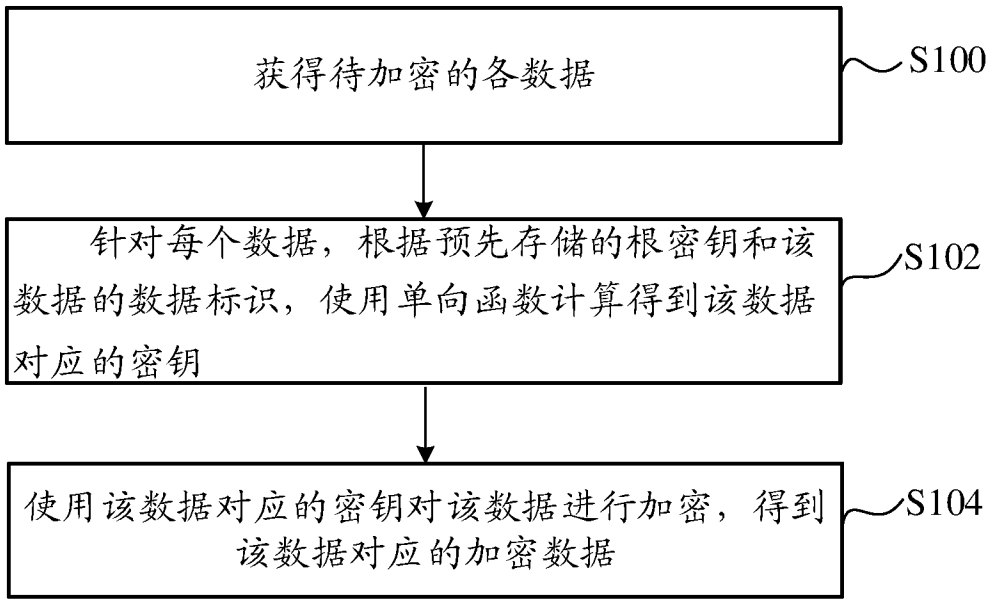
获得待加密的各数据
S100
针对每个数据，根据预先存储的根密钥和该数据的数据标识，使用单向函数计算得到该数据对应的密钥
S102
使用该数据对应的密钥对该数据进行加密，得到该数据对应的加密数据
S104

图 1

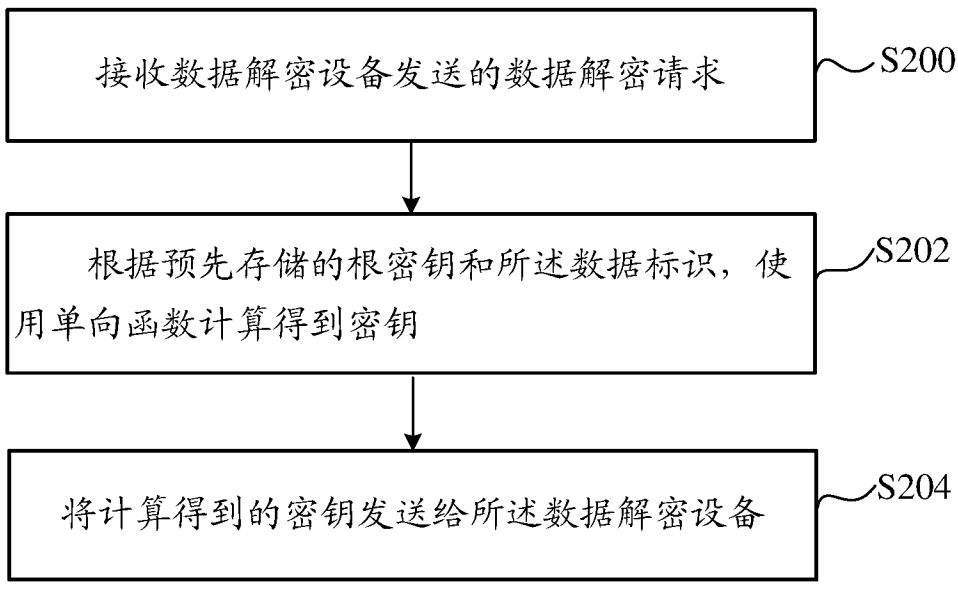
接收数据解密设备发送的数据解密请求
S200
根据预先存储的根密钥和所述数据标识，使用单向函数计算得到密钥
S202
将计算得到的密钥发送给所述数据解密设备
S204

图 2

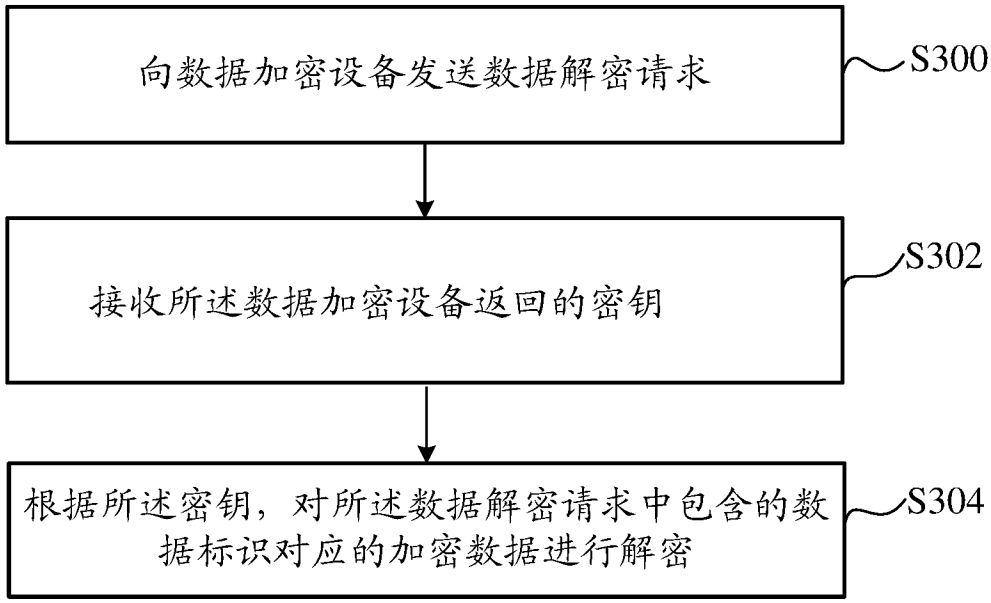
向数据加密设备发送数据解密请求
S300
接收所述数据加密设备返回的密钥
S302
根据所述密钥，对所述数据解密请求中包含的数据标识对应的加密数据进行解密
S304

图 3

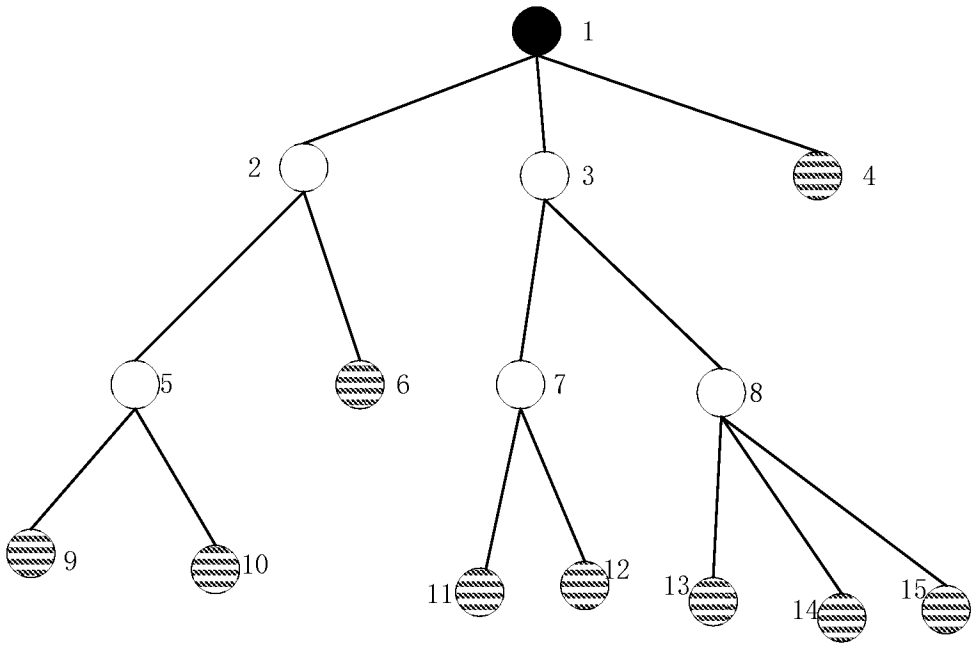
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

图 4

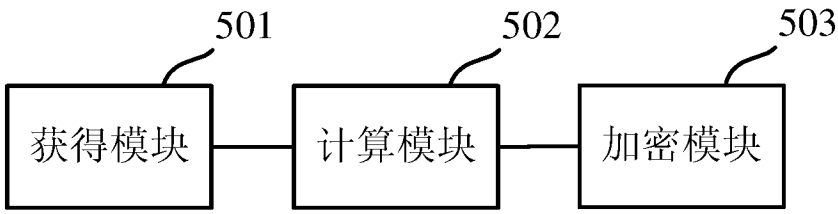
501
502
503
获得模块
计算模块
加密模块

图 5

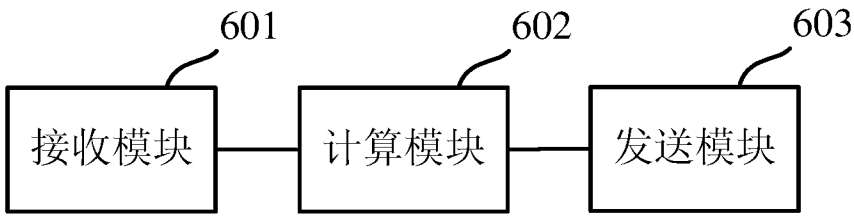
601
602
603
接收模块
计算模块
发送模块

图 6

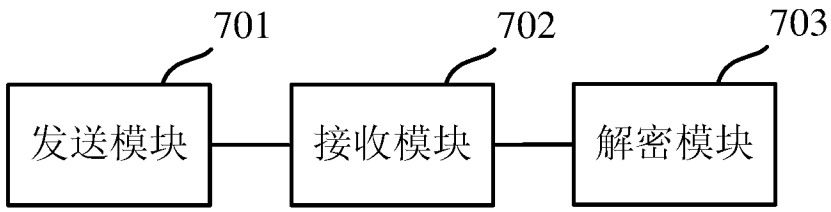
701
702
703
发送模块
接收模块
解密模块

图 7

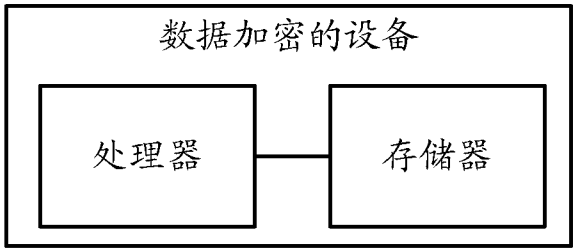

图 8

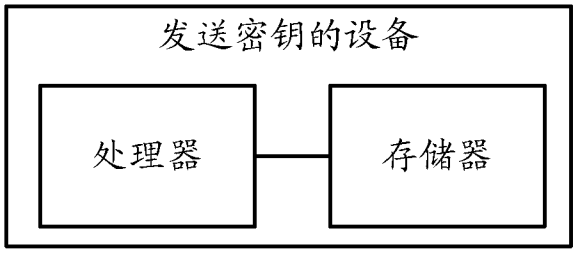

图 9

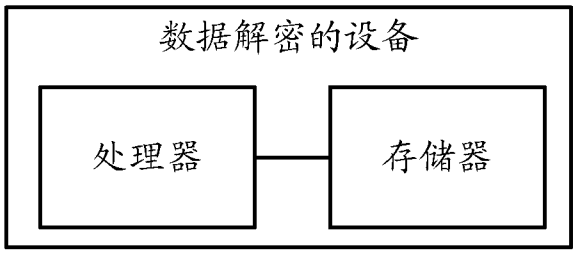

图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/107501

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(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

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)

CNPAT, CNKI, WPI, EPODOC: 加密, 根密钥, 标识, 算法, 函数, 解密, 密钥, encrypt, decrypt, secret key, root key, function, algorithm, identification

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 108063756 A (ALIBABA GROUP HOLDING LIMITED) 22 May 2018 (2018-05-22) claims 1-21	1-21
Y	CN 105825142 A (BEIJING QIDSC TECHNOLOGY CO., LTD.) 03 August 2016 (2016-08-03) abstract, and description, paragraphs [0039]-[0077]	1-21
Y	CN 103905187 A (XIAMEN YAXUN NETWORK CO., LTD.) 02 July 2014 (2014-07-02) abstract, and description, paragraphs [0007]-[0032]	1-21
A	CN 102546151 A (SHANDONG TAIXIN ELECTRONICS CO., LTD.) 04 July 2012 (2012-07-04) entire document	1-21
A	CN 107124271 A (CHENGDU BANGBANG INFORMATION TECHNOLOGY CO., LTD.) 01 September 2017 (2017-09-01) entire document	1-21

☐ 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
29 November 2018	**28 December 2018**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/107501

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	108063756	A	22 May 2018	None	
CN	105825142	A	03 August 2016	None	
CN	103905187	A	02 July 2014	None	
CN	102546151	A	04 July 2012	None	
CN	107124271	A	01 September 2017	None	

国际检索报告

国际申请号
PCT/CN2018/107501

A. 主题的分类

H04L 29/06(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

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））

CNPAT, CNKI, WPI, EPODOC: 加密，根密钥，标识，算法，函数，解密，密钥，encrypt，decrypt，secret key，root key，function，algorithm，identification

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 108063756 A (阿里巴巴集团控股有限公司) 2018年 5月 22日 (2018 - 05 - 22) 权利要求1-21	1-21
Y	CN 105825142 A (北京启迪思创科技有限公司) 2016年 8月 3日 (2016 - 08 - 03) 说明书摘要，说明书[0039]-[0077]段	1-21
Y	CN 103905187 A (厦门雅迅网络股份有限公司) 2014年 7月 2日 (2014 - 07 - 02) 说明书摘要，说明书第[0007]-[0032]段	1-21
A	CN 102546151 A (山东泰信电子有限公司) 2012年 7月 4日 (2012 - 07 - 04) 全文	1-21
A	CN 107124271 A (成都梆梆信息科技有限公司) 2017年 9月 1日 (2017 - 09 - 01) 全文	1-21

☐ 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
2018年 11月 29日	2018年 12月 28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 闫洪波 电话号码 86-(10)-53961740

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/107501

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	108063756	A	2018年 5月 22日	无	
CN	105825142	A	2016年 8月 3日	无	
CN	103905187	A	2014年 7月 2日	无	
CN	102546151	A	2012年 7月 4日	无	
CN	107124271	A	2017年 9月 1日	无	