

(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 7 月 7 日 (07.07.2022)



(10) 国际公布号
WO 2022/142111 A1

- (51) 国际专利分类号:
G06F 7/58 (2006.01) **G06Q 30/02** (2012.01)
G06N 5/00 (2006.01) **G06Q 40/00** (2012.01)
- (21) 国际申请号: PCT/CN2021/096637
- (22) 国际申请日: 2021 年 5 月 28 日 (28.05.2021)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202011594073.X 2020 年 12 月 29 日 (29.12.2020) 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: 吴贞海 (WU, Zhenhai); 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: 深圳市赛恩倍吉知识产权代理有限公司 (SHENZHEN SCIENBIZIP INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市龙华新区龙观东路 83 号荣群大厦 9 楼, Guangdong 518109 (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, IT,

(54) Title: RANDOM NUMBER GENERATION METHOD AND APPARATUS, ELECTRONIC DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 随机数生成方法、装置、电子设备及存储介质

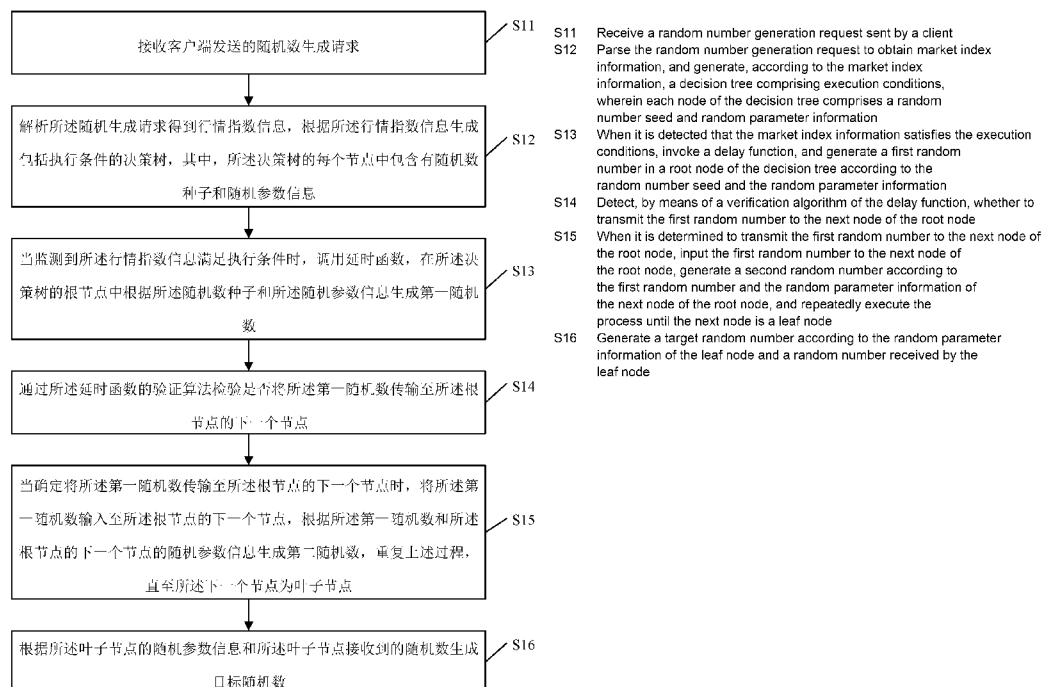


图 1

(57) Abstract: The present application relates to the technical field of artificial intelligence, and provides a random number generation method and apparatus, an electronic device, and a storage medium. The method comprises: parsing a random number generation request to obtain market index information, and generating a decision tree comprising execution conditions; when it is detected that the market index information satisfies the execution conditions, invoking a delay function, and generating a first random number in a root node of the decision tree according to a random number seed and random parameter information; when it is determined to transmit the first

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))。

random number to the next node of the root node, repeatedly executing the process until the next node is a leaf node; and generating a target random number according to the random parameter information of the leaf node and a random number received by the leaf node. According to the present application, a random number, which is obtained by means of calculation, of a previous node is used as the input of a delay subfunction of the next node, and the target random number is obtained by means of calculation in a serial mode, thereby avoiding the phenomenon that the random number seed is modified, and improving the security of the target random number.

(57) 摘要: 本申请涉及人工智能技术领域, 提供一种随机数生成方法、装置、电子设备及存储介质, 所述方法包括: 解析随机生成请求得到行情指数信息, 生成包括执行条件的决策树; 当监测到行情指数信息满足执行条件时, 调用延时函数, 在决策树的根节点中根据随机数种子和随机参数信息生成第一随机数; 当确定将第一随机数传输至根节点的下一个节点时, 重复上述过程, 直至下一个节点为叶子节点; 根据叶子节点的随机参数信息和叶子节点接收到的随机数生成目标随机数。本申请通过将上一个节点的计算得到的随机数作为下一个节点的延时子函数的输入, 通过串行方式计算得到目标随机数, 避免了随机数种子被修改的现象, 提高了目标随机数的安全性。

随机数生成方法、装置、电子设备及存储介质

本申请要求于 2020 年 12 月 29 日提交中国专利局，申请号为 202011594073.X 申请名称为“随机数生成方法、装置、电子设备及存储介质”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

本申请涉及人工智能技术领域，具体涉及一种随机数生成方法、装置、电子设备及存储介质。

背景技术

在计算机安全领域，随机数的生成是否恰当，关系到系统的安全可靠程度，在公平投票领域，随机数本身的随机性需要从可靠的物理随机源产生，现有技术通过从可靠的物理随机源采样多个指数集合加权，但是发明人意识到直接采用或者简单的加权不能完全保证指数作为随机数种子被操作，无法避免随机数种子被更改，导致生成的随机数的安全性及可信度不高。

发明内容

鉴于以上内容，有必要提出一种随机数生成方法、装置、电子设备及存储介质，通过将上一个节点的计算得到的随机数作为下一个节点的延时子函数的输入，通过串行方式计算得到目标随机数，避免了随机数种子被修改的现象，提高了目标随机数的安全性。

本申请的第一方面提供一种随机数生成方法，所述方法包括：

接收客户端发送的随机数生成请求；

解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息；

当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数；

通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点；

当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点；

根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

本申请的第二方面提供一种电子设备，所述电子设备包括存储器及处理器，所述存储器用于存储至少一个计算机可读指令，所述处理器用于执行所述至少一个计算机可读指令以实现以下步骤：

接收客户端发送的随机数生成请求；

解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息；

当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数；

通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点；

当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输

入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点；

根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

本申请的第三方面提供一种计算机可读存储介质，所述计算机可读存储介质存储有至少一个计算机可读指令，所述至少一个计算机可读指令被处理器执行时实现以下步骤：

接收客户端发送的随机数生成请求；

解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息；

当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数；

通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点；

当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点；

根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

本申请的第四方面提供一种随机数生成装置，所述装置包括：

接收模块，用于接收客户端发送的随机数生成请求；

解析模块，用于解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息；

调用模块，用于当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数；

检验模块，用于通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点；

输入模块，用于当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点；

生成模块，用于根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

综上所述，本申请所述的一种随机数生成方法、装置、电子设备及存储介质，一方面，通过解析每个所述随机生成请求获取多个行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，在创建决策树的过程中，通过计算每个随机参数信息之间的时间差，快速的确定出所述决策树中每个节点的执行先后顺序，可以提高随机数生成的效率及行情指数信息的管理效率；另一方面，通过验证所述上一个节点的输出是否为下一个节点的输入，保证计算时串行的，形成计算的先后依赖关系，使得并行的加速设备无法缩短实际的运行时间，从而达到延时的目的，提高了计算过程中的安全性；最后，通过将所述行情指数信息生成包括执行条件的决策树，当满足执行条件时从所述决策树的根节点开始依次遍历所述决策树中的所有子节点，并调用延时函数，在生成目标随机数的流程中设定了一个延时函数计算，将上一个节点的计算得到的随机数作为下一个节点的延时子函数的输入，通过串行方式计算得到目标随机数，避免了当发布者发现行情指数信息生成的随机数不利时随时修改行情指数信息的现象，提高了目标随机数的安全性。

附图说明

图 1 是本申请实施例一提供的随机数生成方法的流程图。

图 2 是本申请实施例二提供的随机数生成装置的结构图。

图 3 是本申请实施例三提供的电子设备的结构示意图。

具体实施方式

为了能够更清楚地理解本申请的上述目的、特征和优点，下面结合附图和具体实施例对本申请进行详细描述。需要说明的是，在不冲突的情况下，本申请的实施例及实施例中的特征可以相互组合。

除非另有定义，本文所使用的所有的技术和科学术语与属于本申请的技术领域的技术人员通常理解的含义相同。本文中在本申请的说明书中所使用的术语只是为了描述具体的实施例的目的，不是旨在于限制本申请。

实施例一

图 1 是本申请实施例一提供的随机数生成方法的流程图。

在本实施例中，所述随机数生成方法可以应用于电子设备中，对于需要进行随机数生成的电子设备，可以直接在电子设备上集成本申请的方法所提供的随机数生成的功能，或者以软件开发工具包（Software Development Kit, SDK）的形式运行在电子设备中。

如图 1 所示，所述随机数生成方法具体包括以下步骤，根据不同的需求，该流程图中步骤的顺序可以改变，某些可以省略。

S11，接收客户端发送的随机数生成请求。

本实施例中，客户端在进行随机数获取时，通过客户端发起随机数生成请求，具体地，所述客户端可以是智能手机、IPAD 或者其他设备，所述服务器可以为随机数生成系统，在进行随机数生成过程中，如所述客户端可以向随机数生成系统发送随机数生成请求，所述随机数生成系统用于接收所述客户端发送的随机数生成请求。

S12，解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息。

本实施例中，在所述服务器接收到不同的客户端发送的多个行情指数信息，针对不同的行情指数信息生成不同的决策树，其中，每个决策树包含有执行条件，具体地，由于每个行情指数信息的发布时间不同，故在确定所述决策树的执行条件可以是到达指点时间。

在其他一些实施例中，所述决策树的执行条件也可以是到达指定状态。

在其他一些实施例中，所述行情指数信息中包括，但不限于随机数种子、多个随机参数信息。

可选地，所述根据所述行情指数信息生成包括执行条件的决策树包括：

随机选取所述行情指数信息中的一个随机参数信息作为所述行情指数信息的决策树的根节点；

计算其余任意一个随机参数信息与所述根节点处的随机参数信息之间的时间差；

判断是否存在与所述时间差相同的子节点；

当判断存在与所述时间差相同的子节点时，将所述子节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点；

当判断不存在与所述时间差相同的子节点时，将所述根节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点，其中，所述父节点处的随机参数信息与对应的所述子节点处的随机参数信息之间的时间差作为所述父节点和所述子节点之间的边的权重。

本实施例中，所述行情指数信息中包含有多个随机参数信息，随机选取一个随机参数信息作为所述行情指数信息的对应的决策树的根节点，然后计算其余任意一个随机参

数信息与所述根节点处的随机参数信息之间的时间差，根据所述时间差可以确定所述决策树中每个节点的执行顺序，当判断存在与所述时间差相同的子节点时，将所述子节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点；当判断不存在与所述时间差相同的子节点时，将所述根节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点。

本实施例中，在根据所述行情指数信息中的多个随机参数信息创建决策树的过程中，通过计算每个随机参数信息之间的时间差，快速的确定出所述决策树中每个节点的执行先后顺序，可以提高随机数生成的效率及行情指数信息的管理效率。

S13，当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数。

本实施例中，根据行情指数信息创建对应的决策树，并且每个决策树的执行条件不同，只有在满足执行条件的才进行对应的决策树的执行，提高了决策树的管理效率。

可选地，所述监测所述行情指数信息是否满足所述执行条件包括：

监测所述行情指数信息对应的时间参数，其中，所述时间参数是根据所述行情指数的发布时间预先设置的；

判断所述时间参数是否达到预设的执行时间阈值；

当所述时间参数达到所述预设的执行时间阈值时，确定监测到所述行情指数信息满足所述执行条件；

当所述时间参数未达到所述预设的执行时间阈值时，确定监测到所述行情指数信息不满足所述执行条件。

示例性的，所述行情指数信息中包括记录所述行情指数的起始时刻，在起始时刻之后经过指定的时间参数，触发所述决策树执行。其中，所述指定的时间参数可以是客户端输入的时间参数，如 60 分钟；则在达到起始时刻后的 60 分钟时，触发所述决策树执行；所述指定的时间参数也可以是系统计算得到的时间参数，如客户端指定 20:00 执行决策树，所述起始时刻为 18:00，则系统计算得到所述指定的时间参数为 120 分钟。当然，在其他一些实施例中，所述指定的时间参数也可以是通过动态计算得到的第一时间参数，这同样属于本公开的保护范围。

本实施例中，通过为每个决策树设置执行条件，避免在服务器接收的随机数生成请求较多时出现执行混乱的现象，提高了行情指数信息的管理效率，进而提高了随机数生成的效率及准确率。

本实施例中，在随机数生成系统中进行随机数生成的过程中，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数。

在其他可选的实施例中，所述在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数包括：

从所述决策树的根节点的随机参数信息中提取所述延时函数的第一延时子函数；

调用所述第一延时子函数对所述随机数种子和所述随机参数信息进行计算得到第一随机数。

本实施例中，所述延时函数中包含有多个延时子函数，并且每个子节点中的延时子函数不同，故在确定执行所述决策树时，首先从所述决策树的根节点的随机参数信息中提取所述延时函数的第一延时子函数对所述随机数种子进行计算得到第一随机数。

S14，通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点。

本实施例中，由于延时函数的每一个延时子函数的计算输出依赖于下一个延时子函数的输入，故在得到第一随机数之后，需要采用延时函数的验证算法检验所述第一随机数是否可以传输至所述根节点的下一个节点。

可选地，所述通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点包括：

对所述第一随机数进行哈希运算，得到第一哈希值；

对所述根节点的下一个节点的随机参数信息中的目标随机参数进行哈希运算，得到第二哈希值；

判断所述第一哈希值与所述第二哈希值是否一致；

当所述第一哈希值与所述第二哈希值一致时，确定将所述第一随机数传输至所述根节点的下一个节点；或者

当所述第一哈希值与所述第二哈希值不一致时，确定不将所述第一随机数传输至所述根节点的下一个节点。

进一步地，所述方法还包括：

当确定不将所述第一随机数传输至所述根节点的下一个节点之后，丢弃所述第一随机数。

本实施例中，通过哈希运算对所述第一随机数进行计算得到第一哈希值，对根节点的下一个节点中的目标随机参数进行计算得到第二哈希值，判断所述第一哈希值与所述第二哈希值是否一致，根据判断结果确定是否可以将所述第一随机数传输至所述根节点的下一个节点，只有所述第一哈希值与所述第二哈希值一致时，确定所述第一随机数可以作为所述根节点的下一个节点的输入。

本实施例中，通过验证所述上一个节点的输出是否为下一个节点的输入，保证计算时串行的，形成计算的先后依赖关系，使得并行的加速设备无法缩短实际的运行时间，从而达到延时的目的，提高了计算过程中的安全性。

S15，当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点。

本实施例中，由于决策树中包含有多个节点，每个节点的输入和输出存在依赖关系，故将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点。

可选地，所述根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数包括：

从所述根节点的下一个节点的随机参数信息中提取所述延时函数的第二延时子函数；

调用所述第二延时子函数对所述第一随机数和所述根节点的下一个节点的随机参数信息进行计算得到第二随机数。

本实施例中，每个随机参数信息中包含有延时子函数，从所述根节点的下一个节点的随机参数信息中提取所述延时函数的第二延时子函数，并调用所述第二延时子函数对所述第一随机数和所述根节点的下一个节点的随机参数信息进行计算得到第二随机数。

S16，根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

本实施例中，所述叶子节点为所述决策树的结束节点，当接收到所述叶子节点的上一个节点传输的目标随机数时，根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数，具体地，所述根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数包括：

从所述叶子节点的随机参数信息中提取所述延时函数的目标延时子函数；

调用所述目标延时子函数对所述叶子节点接收到的随机数和所述叶子节点的随机

参数信息进行计算得到目标随机数。

其中，所述目标随机数是指所述叶子节点的上一个节点根据所述叶子节点的上一个节点的上一个节点传输的随机数和所述叶子节点的上一个节点的随机参数信息生成的，避免了随机数种子被修改的现象，提高了生成的目标随机数的安全性。

本实施例中，通过将所述行情指数信息生成包括执行条件的决策树，当满足执行条件时从所述决策树的根节点开始依次遍历所述决策树中的所有子节点，并调用延时函数，在生成目标随机数的流程中设定了一个延时函数计算，将上一个节点的计算得到的随机数作为下一个节点的延时子函数的输入，通过串行方式计算得到目标随机数，可以保证在经过所述延时函数计算之后，发布者无法立即知道随机数是什么，故无法评判随机数的利弊，只能将随机数种子放入延时函数中进行计算，等待计算结果，当所述计算结果出来时，已经经过了一个延时函数，就算对所述发布者不利，也无法进行更改，避免了当发布者发现行情指数信息生成的随机数不利时随时修改行情指数信息现象，提高了目标随机数的安全性。

进一步地，在根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数之后，所述方法还包括：

检测所述目标随机数对应的叶子节点的地址是否为所述行情指数信息中的计算结果接收地址；

当所述目标随机数对应的叶子节点的地址为所述行情指数信息中的计算结果接收地址，将所述目标随机数反馈至所述计算结果接收地址对应的终端设备；或者

若所述目标随机数对应的叶子节点的地址不为所述行情指数信息中的计算结果接收地址，丢弃所述目标随机数。

在其他一些实施例中，在将所述目标随机数反馈至计算结果接收地址对应的终端设备之后，所述方法包括：

采用多种随机数加密方式加密所述目标随机数，得到密文；

将所述密文反馈至所述目标随机数对应的计算结果接收地址对应的终端设备。

综上所述，本实施例所述的随机数生成的方法，一方面，通过解析每个所述随机生成请求获取多个行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，在创建决策树的过程中，通过计算每个随机参数信息之间的时间差，快速的确定出所述决策树中每个节点的执行先后顺序，可以提高随机数生成的效率及行情指数信息的管理效率；另一方面，通过验证所述上一个节点的输出是否为下一个节点的输入，保证计算时串行的，形成计算的先后依赖关系，使得并行的加速设备无法缩短实际的运行时间，从而达到延时的目的，提高了计算过程中的安全性；最后，通过将所述行情指数信息生成包括执行条件的决策树，当满足执行条件时从所述决策树的根节点开始依次遍历所述决策树中的所有子节点，并调用延时函数，在生成目标随机数的流程中设定了一个延时函数计算，将上一个节点的计算得到的随机数作为下一个节点的延时子函数的输入，通过串行方式计算得到目标随机数，避免了当发布者发现行情指数信息生成的随机数不利时随时修改行情指数信息现象，提高了目标随机数的安全性。

实施例二

图2是本申请实施例二提供的随机数生成装置的结构图。

在一些实施例中，所述随机数生成装置20可以包括多个由程序代码段所组成的功能模块。所述随机数生成装置20中的各个程序段的程序代码可以存储于电子设备的存储器中，并由所述至少一个处理器所执行，以执行（详见图1描述）随机数生成的功能。

本实施例中，所述随机数生成装置20根据其所执行的功能，可以被划分为多个功能模块。所述功能模块可以包括：接收模块201、解析模块202、调用模块203、检验模块204、输入模块205、生成模块206及检测模块207。本申请所称的模块是指一种能够

被至少一个处理器所执行并且能够完成固定功能的一系列计算机可读指令段，其存储在存储器中。在本实施例中，关于各模块的功能将在后续的实施例中详述。

接收模块 201，用于接收客户端发送的随机数生成请求。

本实施例中，客户端在进行随机数获取时，通过客户端发起随机数生成请求，具体地，所述客户端可以是智能手机、IPAD 或者其他设备，所述服务器可以为随机数生成系统，在进行随机数生成过程中，如所述客户端可以向随机数生成系统发送随机数生成请求，所述随机数生成系统用于接收所述客户端发送的随机数生成请求。

解析模块 202，用于解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息。

本实施例中，在所述服务器接收到不同的客户端发送的多个行情指数信息，针对不同的行情指数信息生成不同的决策树，其中，每个决策树包含有执行条件，具体地，由于每个行情指数信息的发布时间不同，故在确定所述决策树的执行条件可以是到达指点时间。

在其他一些实施例中，所述决策树的执行条件也可以是到达指定状态。

在其他一些实施例中，所述行情指数信息中包括，但不限于随机数种子、多个随机参数信息。

可选地，所述解析模块 202 根据所述行情指数信息生成包括执行条件的决策树包括：随机选取所述行情指数信息中的一个随机参数信息作为所述行情指数信息的决策树的根节点；

计算其余任意一个随机参数信息与所述根节点处的随机参数信息之间的时间差；

判断是否存在与所述时间差相同的子节点；

当判断存在与所述时间差相同的子节点时，将所述子节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点；

当判断不存在与所述时间差相同的子节点时，将所述根节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点，其中，所述父节点处的随机参数信息与对应的所述子节点处的随机参数信息之间的时间差作为所述父节点和所述子节点之间的边的权重。

本实施例中，所述行情指数信息中包含有多个随机参数信息，随机选取一个随机参数信息作为所述行情指数信息的对应的决策树的根节点，然后计算其余任意一个随机参数信息与所述根节点处的随机参数信息之间的时间差，根据所述时间差可以确定所述决策树中每个节点的执行顺序，当判断存在与所述时间差相同的子节点时，将所述子节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点；当判断不存在与所述时间差相同的子节点时，将所述根节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点。

本实施例中，在根据所述行情指数信息中的多个随机参数信息创建决策树的过程中，通过计算每个随机参数信息之间的时间差，快速的确定出所述决策树中每个节点的执行先后顺序，可以提高随机数生成的效率及行情指数信息的管理效率。

调用模块 203，用于当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数。

本实施例中，根据行情指数信息创建对应的决策树，并且每个决策树的执行条件不同，只有在满足执行条件的才进行对应的决策树的执行，提高了决策树的管理效率。

可选地，所述调用模块 203 监测所述行情指数信息是否满足所述执行条件包括：

监测所述行情指数信息对应的时间参数，其中，所述时间参数是根据所述行情指数的发布时间预先设置的；

判断所述时间参数是否达到预设的执行时间阈值；

当所述时间参数达到所述预设的执行时间阈值时，确定监测到所述行情指数信息满足所述执行条件；

当所述时间参数未达到所述预设的执行时间阈值时，确定监测到所述行情指数信息不满足所述执行条件。

示例性的，所述行情指数信息中包括记录所述行情指数的起始时刻，在起始时刻之后经过指定的时间参数，触发所述决策树执行。其中，所述指定的时间参数可以是客户端输入的时间参数，如 60 分钟；则在达到起始时刻后的 60 分钟时，触发所述决策树执行；所述指定的时间参数也可以是系统计算得到的时间参数，如客户端指定 20:00 执行决策树，所述起始时刻为 18:00，则系统计算得到所述指定的时间参数为 120 分钟。当然，在其他一些实施例中，所述指定的时间参数也可以是通过动态计算得到的第一时间参数，这同样属于本公开的保护范围。

本实施例中，通过为每个决策树设置执行条件，避免在服务器接收的随机数生成请求较多时出现执行混乱的现象，提高了行情指数信息的管理效率，进而提高了随机数生成的效率及准确率。

本实施例中，在随机数生成系统中进行随机数生成的过程中，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数。

在其他可选的实施例中，所述调用模块 203 在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数包括：

从所述决策树的根节点的随机参数信息中提取所述延时函数的第一延时子函数；

调用所述第一延时子函数对所述随机数种子和所述随机参数信息进行计算得到第一随机数。

本实施例中，所述延时函数中包含有多个延时子函数，并且每个子节点中的延时子函数不同，故在确定执行所述决策树时，首先从所述决策树的根节点的随机参数信息中提取所述延时函数的第一延时子函数对所述随机数种子进行计算得到第一随机数。

检验模块 204，用于通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点。

本实施例中，由于延时函数的每一个延时子函数的计算输出依赖于下一个延时子函数的输入，故在得到第一随机数之后，需要采用延时函数的验证算法检验所述第一随机数是否可以传输至所述根节点的下一个节点。

可选地，所述检验模块 204 通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点包括：

对所述第一随机数进行哈希运算，得到第一哈希值；

对所述根节点的下一个节点的随机参数信息中的目标随机参数进行哈希运算，得到第二哈希值；

判断所述第一哈希值与所述第二哈希值是否一致；

当所述第一哈希值与所述第二哈希值一致时，确定将所述第一随机数传输至所述根节点的下一个节点；或者

当所述第一哈希值与所述第二哈希值不一致时，确定不将所述第一随机数传输至所述根节点的下一个节点。

进一步地，当确定不将所述第一随机数传输至所述根节点的下一个节点之后，丢弃所述第一随机数。

本实施例中，通过哈希运算对所述第一随机数进行计算得到第一哈希值，对根节点的下一个节点中的目标随机参数进行计算得到第二哈希值，判断所述第一哈希值与所述第二哈希值是否一致，根据判断结果确定是否可以将所述第一随机数传输至所述根节点

的下一个节点，只有所述第一哈希值与所述第二哈希值一致时，确定所述第一随机数可以作为所述根节点的下一个节点的输入。

本实施例中，通过验证所述上一个节点的输出是否为下一个节点的输入，保证计算时串行的，形成计算的先后依赖关系，使得并行的加速设备无法缩短实际的运行时间，从而达到延时的目的，提高了计算过程中的安全性。

输入模块 205，用于当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点。

本实施例中，由于决策树中包含有多个节点，每个节点的输入和输出存在依赖关系，故将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点。

可选地，所述输入模块 205 根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数包括：

从所述根节点的下一个节点的随机参数信息中提取所述延时函数的第二延时子函数；

调用所述第二延时子函数对所述第一随机数和所述根节点的下一个节点的随机参数信息进行计算得到第二随机数。

本实施例中，每个随机参数信息中包含有延时子函数，从所述根节点的下一个节点的随机参数信息中提取所述延时函数的第二延时子函数，并调用所述第二延时子函数对所述第一随机数和所述根节点的下一个节点的随机参数信息进行计算得到第二随机数。

生成模块 206，用于根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

本实施例中，所述叶子节点为所述决策树的结束节点，当接收到所述叶子节点的上一个节点传输的目标随机数时，根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数，具体地，所述生成模块 206 根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数包括：

从所述叶子节点的随机参数信息中提取所述延时函数的目标延时子函数；

调用所述目标延时子函数对所述叶子节点接收到的随机数和所述叶子节点的随机参数信息进行计算得到目标随机数。

其中，所述目标随机数是指所述叶子节点的上一个节点根据所述叶子节点的上一个节点的上一个节点传输的随机数和所述叶子节点的上一个节点的随机参数信息生成的，避免了随机数种子被修改的现象，提高了生成的目标随机数的安全性。

本实施例中，通过将所述行情指数信息生成包括执行条件的决策树，当满足执行条件时从所述决策树的根节点开始依次遍历所述决策树中的所有子节点，并调用延时函数，在生成目标随机数的流程中设定了一个延时函数计算，将上一个节点的计算得到的随机数作为下一个节点的延时子函数的输入，通过串行方式计算得到目标随机数，可以保证在经过所述延时函数计算之后，发布者无法立即知道随机数是什么，故无法评判随机数的利弊，只能将随机数种子放入延时函数中进行计算，等待计算结果，当所述计算结果出来时，已经经过了一个延时函数，就算对所述发布者不利，也无法进行更改，避免了当发布者发现行情指数信息生成的随机数不利时随时修改行情指数信息的现象，提高了目标随机数的安全性。

进一步地，在根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数之后，检测模块 207 用于检测所述目标随机数对应的叶子节点的地址是否

为所述行情指数信息中的计算结果接收地址；当所述目标随机数对应的叶子节点的地址为所述行情指数信息中的计算结果接收地址，将所述目标随机数反馈至所述计算结果接收地址对应的终端设备；当所述目标随机数对应的叶子节点的地址不为所述行情指数信息中的计算结果接收地址，丢弃所述目标随机数。

在其他一些实施例中，在将所述目标随机数反馈至计算结果接收地址对应的终端设备之后，采用多种随机数加密方式加密所述目标随机数，得到密文；将所述密文反馈至所述目标随机数对应的计算结果接收地址对应的终端设备。

综上所述，本实施例所述的随机数生成的装置，一方面，通过解析每个所述随机生成请求获取多个行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，在创建决策树的过程中，通过计算每个随机参数信息之间的时间差，快速的确定出所述决策树中每个节点的执行先后顺序，可以提高随机数生成的效率及行情指数信息的管理效率；另一方面，通过验证所述上一个节点的输出是否为下一个节点的输入，保证计算时串行的，形成计算的先后依赖关系，使得并行的加速设备无法缩短实际的运行时间，从而达到延时的目的，提高了计算过程中的安全性；最后，通过将所述行情指数信息生成包括执行条件的决策树，当满足执行条件时从所述决策树的根节点开始依次遍历所述决策树中的所有子节点，并调用延时函数，在生成目标随机数的流程中设定了一个延时函数计算，将上一个节点的计算得到的随机数作为下一个节点的延时子函数的输入，通过串行方式计算得到目标随机数，避免了当发布者发现行情指数信息生成的随机数不利时随时修改行情指数信息现象，提高了目标随机数的安全性。

实施例三

参阅图 3 所示，为本申请实施例三提供的电子设备的结构示意图。在本申请较佳实施例中，所述电子设备 3 包括存储器 31、至少一个处理器 32、至少一条通信总线 33 及收发器 34。

本领域技术人员应该了解，图 3 示出的电子设备的结构并不构成本申请实施例的限定，既可以是总线型结构，也可以是星形结构，所述电子设备 3 还可以包括比图示更多或更少的其他硬件或者软件，或者不同的部件布置。

在一些实施例中，所述电子设备 3 是一种能够按照事先设定或存储的指令，自动进行数值计算和/或信息处理的电子设备，其硬件包括但不限于微处理器、专用集成电路、可编程门阵列、数字处理器及嵌入式设备等。所述电子设备 3 还可包括客户设备，所述客户设备包括但不限于任何一种可与客户通过键盘、鼠标、遥控器、触摸板或声控设备等方式进行人机交互的电子产品，例如，个人计算机、平板电脑、智能手机、数码相机等。

需要说明的是，所述电子设备 3 仅为举例，其他现有的或今后可能出现的电子产品如可适应于本申请，也应包含在本申请的保护范围以内，并以引用方式包含于此。

在一些实施例中，所述存储器 31 用于存储程序代码和各种数据，例如安装在所述电子设备 3 中的随机数生成装置 20，并在电子设备 3 的运行过程中实现高速、自动地完成程序或数据的存取。所述存储器 31 包括只读存储器（Read-Only Memory, ROM）、可编程只读存储器（Programmable Read-Only Memory, PROM）、可擦除可编程只读存储器（Erasable Programmable Read-Only Memory, EPROM）、一次可编程只读存储器（One-time Programmable Read-Only Memory, OTPROM）、电子擦除式可复写只读存储器（Electrically-Erasable Programmable Read-Only Memory, EEPROM）、只读光盘（Compact Disc Read-Only Memory, CD-ROM）或其他光盘存储器、磁盘存储器、磁带存储器、或者能够用于携带或存储数据的计算机可读的任何其他介质。

在一些实施例中，所述至少一个处理器 32 可以由集成电路组成，例如可以由单个封装的集成电路所组成，也可以是由多个相同功能或不同功能封装的集成电路所组成，

包括一个或者多个中央处理器（Central Processing unit, CPU）、微处理器、数字处理芯片、图形处理器及各种控制芯片的组合等。所述至少一个处理器 32 是所述电子设备 3 的控制核心（Control Unit），利用各种接口和线路连接整个电子设备 3 的各个部件，通过运行或执行存储在所述存储器 31 内的程序或者模块，以及调用存储在所述存储器 31 内的数据，以执行电子设备 3 的各种功能和处理数据。

在一些实施例中，所述至少一条通信总线 33 被设置为实现所述存储器 31 以及所述至少一个处理器 32 等之间的连接通信。

尽管未示出，所述电子设备 3 还可以包括给各个部件供电的电源（比如电池），可选的，电源可以通过电源管理装置与所述至少一个处理器 32 逻辑相连，从而通过电源管理装置实现管理充电、放电、以及功耗管理等功能。电源还可以包括一个或一个以上的直流或交流电源、再充电装置、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。所述电子设备 3 还可以包括多种传感器、蓝牙模块、Wi-Fi 模块等，在此不再赘述。

应该了解，所述实施例仅为说明之用，在专利申请范围上并不受此结构的限制。

上述以软件功能模块的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能模块存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，电子设备，或者网络设备等）或处理器（processor）执行本申请各个实施例所述方法的部分。

在进一步的实施例中，结合图 2，所述至少一个处理器 32 可执行所述电子设备 3 的操作装置以及安装的各类应用程序（如所述的随机数生成装置 20）、程序代码等，例如，上述的各个模块。

所述存储器 31 中存储有程序代码，且所述至少一个处理器 32 可调用所述存储器 31 中存储的程序代码以执行相关的功能。例如，图 2 中所述的各个模块是存储在所述存储器 31 中的程序代码，并由所述至少一个处理器 32 所执行，从而实现所述各个模块的功能以达到随机数生成的目的。

示例性的，所述程序代码可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器 31 中，并由所述处理器 32 执行，以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机可读指令段，该指令段用于描述所述程序代码在所述电子设备 3 中的执行过程。例如，所述程序代码可以被分割成接收模块 201、解析模块 202、调用模块 203、检验模块 204、输入模块 205、生成模块 206 及检测模块 207。

在本申请的一个实施例中，所述存储器 31 存储多个计算机可读指令，所述多个计算机可读指令被所述至少一个处理器 32 所执行以实现随机数生成的功能。

具体地，所述至少一个处理器 32 对上述指令的具体实现方法可参考图 1 对应实施例中相关步骤的描述，在此不赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述模块的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式。

进一步地，所述计算机可读存储介质可以是非易失性，也可以是易失性。

所述作为分离部件说明的模块可以是或者也可以不是物理上分开的，作为模块显示的部件可以是或者也可以不是物理单元，既可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能模块的形式实现。

对于本领域技术人员而言，显然本申请不限于上述示范性实施例的细节，而且在不背离本申请的精神或基本特征的情况下，能够以其他的具体形式实现本申请。因此，无论从哪一点来看，均应将实施例看作是示范性的，而且是非限制性的，本申请的范围由所附权利要求而不是上述说明限定，因此旨在将落在权利要求的等同要件的含义和范围内的所有变化涵括在本申请内。不应将权利要求中的任何附图标记视为限制所涉及的权利要求。此外，显然“包括”一词不排除其他单元或，单数不排除复数。本申请中陈述的多个单元或装置也可以由一个单元或装置通过软件或者硬件来实现。第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

最后应说明的是，以上实施例仅用以说明本申请的技术方案而非限制，尽管参照较佳实施例对本申请进行了详细说明，本领域的普通技术人员应当理解，可以对本申请的技术方案进行修改或等同替换，而不脱离本申请技术方案的精神和范围。

权 利 要 求 书

1. 一种随机数生成方法，其中，所述随机数生成方法包括：

接收客户端发送的随机数生成请求；

解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息；

当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数；

通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点；

当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点；

根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

2. 如权利要求 1 所述的随机数生成方法，其中，所述在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数包括：

从所述决策树的根节点的随机参数信息中提取所述延时函数的第一延时子函数；

调用所述第一延时子函数对所述随机数种子和所述随机参数信息进行计算得到第一随机数。

3. 如权利要求 1 所述的随机数生成方法，其中，所述通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点包括：

对所述第一随机数进行哈希运算，得到第一哈希值；

对所述根节点的下一个节点的随机参数信息中的目标随机参数进行哈希运算，得到第二哈希值；

判断所述第一哈希值与所述第二哈希值是否一致；

当所述第一哈希值与所述第二哈希值一致时，确定将所述第一随机数传输至所述根节点的下一个节点；或者

当所述第一哈希值与所述第二哈希值不一致时，确定不将所述第一随机数传输至所述根节点的下一个节点。

4. 如权利要求 1 所述的随机数生成方法，其中，所述根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数包括：

从所述根节点的下一个节点的随机参数信息中提取所述延时函数的第二延时子函数；

调用所述第二延时子函数对所述第一随机数和所述根节点的下一个节点的随机参数信息进行计算得到第二随机数。

5. 如权利要求 1 所述的随机数生成方法，其中，所述在根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数之后，所述方法还包括：

检测所述目标随机数对应的叶子节点的地址是否为所述行情指数信息中的计算结果接收地址；

当所述目标随机数对应的叶子节点的地址为所述行情指数信息中的计算结果接收地址时，将所述目标随机数反馈至所述计算结果接收地址对应的终端设备；或者

当所述目标随机数对应的叶子节点的地址不为每个行情指数信息中的计算结果接收地址时，丢弃所述目标随机数。

6. 如权利要求 1 所述的随机数生成方法，其中，所述监测所述行情指数信息是否满足所述执行条件包括：

监测所述行情指数信息对应的时间参数，其中，所述时间参数是根据所述行情指数的发

布时间预先设置的；

判断所述时间参数是否达到预设的执行时间阈值；

当所述时间参数达到所述预设的执行时间阈值时，确定监测到所述行情指数信息满足所述执行条件；

当所述时间参数未达到所述预设的执行时间阈值时，确定监测到所述行情指数信息不满足所述执行条件。

7. 如权利要求1所述的随机数生成方法，其中，所述根据所述行情指数信息生成包括执行条件的决策树包括：

随机选取所述行情指数信息中的一个随机参数信息作为所述行情指数信息的决策树的根节点；

计算其余任意一个随机参数信息与所述根节点处的随机参数信息之间的时间差；

判断是否存在与所述时间差相同的子节点；

当判断存在与所述时间差相同的子节点时，将所述子节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点；

当判断不存在与所述时间差相同的子节点时，将所述根节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点，其中，所述父节点处的随机参数信息与对应的所述子节点处的随机参数信息之间的时间差作为所述父节点和所述子节点之间的边的权重。

8. 一种电子设备，其中，所述电子设备包括存储器及处理器，所述存储器用于存储至少一个计算机可读指令，所述处理器用于执行所述至少一个计算机可读指令以实现以下步骤：

接收客户端发送的随机数生成请求；

解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息；

当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数；

通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点；

当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点；

根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

9. 如权利要求8所述的电子设备，其中，所述处理器执行所述至少一个计算机可读指令以实现所述在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数时，具体包括：

从所述决策树的根节点的随机参数信息中提取所述延时函数的第一延时子函数；

调用所述第一延时子函数对所述随机数种子和所述随机参数信息进行计算得到第一随机数。

10. 如权利要求8所述的电子设备，其中，所述处理器执行所述至少一个计算机可读指令以实现所述通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点时，具体包括：

对所述第一随机数进行哈希运算，得到第一哈希值；

对所述根节点的下一个节点的随机参数信息中的目标随机参数进行哈希运算，得到第二哈希值；

判断所述第一哈希值与所述第二哈希值是否一致；

当所述第一哈希值与所述第二哈希值一致时，确定将所述第一随机数传输至所述根

节点的下一个节点；或者

当所述第一哈希值与所述第二哈希值不一致时，确定不将所述第一随机数传输至所述根节点的下一个节点。

11. 如权利要求 8 所述的电子设备，其中，所述处理器执行所述至少一个计算机可读指令以实现所述根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数时，具体包括：

从所述根节点的下一个节点的随机参数信息中提取所述延时函数的第二延时子函数；
调用所述第二延时子函数对所述第一随机数和所述根节点的下一个节点的随机参数信息进行计算得到第二随机数。

12. 如权利要求 8 所述的电子设备，其中，所述处理器执行所述至少一个计算机可读指令以实现所述监测所述行情指数信息是否满足所述执行条件时，具体包括：

监测所述行情指数信息对应的时间参数，其中，所述时间参数是根据所述行情指数的发布时间预先设置的；

判断所述时间参数是否达到预设的执行时间阈值；

当所述时间参数达到所述预设的执行时间阈值时，确定监测到所述行情指数信息满足所述执行条件；

当所述时间参数未达到所述预设的执行时间阈值时，确定监测到所述行情指数信息不满足所述执行条件。

13. 如权利要求 8 所述的电子设备，其中，所述处理器执行所述至少一个计算机可读指令以实现所述根据所述行情指数信息生成包括执行条件的决策树时，具体包括：

随机选取所述行情指数信息中的一个随机参数信息作为所述行情指数信息的决策树的根节点；

计算其余任意一个随机参数信息与所述根节点处的随机参数信息之间的时间差；

判断是否存在与所述时间差相同的子节点；

当判断存在与所述时间差相同的子节点时，将所述子节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点；

当判断不存在与所述时间差相同的子节点时，将所述根节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点，其中，所述父节点处的随机参数信息与对应的所述子节点处的随机参数信息之间的时间差作为所述父节点和所述子节点之间的边的权重。

14. 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至少一个计算机可读指令，所述至少一个计算机可读指令被处理器执行时实现以下步骤：

接收客户端发送的随机数生成请求；

解析所述随机生成请求得到行情指数信息，根据所述行情指数信息生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息；

当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数；

通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点；

当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点；

根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

15. 如权利要求 14 所述的存储介质，其中，所述至少一个计算机可读指令被所述处理器执行以实现所述在所述决策树的根节点中根据所述随机数种子和所述随机参数信息

生成第一随机数时，具体包括：

从所述决策树的根节点的随机参数信息中提取所述延时函数的第一延时子函数；

调用所述第一延时子函数对所述随机数种子和所述随机参数信息进行计算得到第一随机数。

16. 如权利要求 14 所述的存储介质，其中，所述至少一个计算机可读指令被所述处理器执行以实现所述通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点时，具体包括：

对所述第一随机数进行哈希运算，得到第一哈希值；

对所述根节点的下一个节点的随机参数信息中的目标随机参数进行哈希运算，得到第二哈希值；

判断所述第一哈希值与所述第二哈希值是否一致；

当所述第一哈希值与所述第二哈希值一致时，确定将所述第一随机数传输至所述根节点的下一个节点；或者

当所述第一哈希值与所述第二哈希值不一致时，确定不将所述第一随机数传输至所述根节点的下一个节点。

17. 如权利要求 14 所述的存储介质，其中，所述至少一个计算机可读指令被所述处理器执行以实现所述根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数时，具体包括：

从所述根节点的下一个节点的随机参数信息中提取所述延时函数的第二延时子函数；

调用所述第二延时子函数对所述第一随机数和所述根节点的下一个节点的随机参数信息进行计算得到第二随机数。

18. 如权利要求 14 所述的存储介质，其中，所述至少一个计算机可读指令被所述处理器执行以实现所述监测所述行情指数信息是否满足所述执行条件时，具体包括：

监测所述行情指数信息对应的时间参数，其中，所述时间参数是根据所述行情指数的发布时间预先设置的；

判断所述时间参数是否达到预设的执行时间阈值；

当所述时间参数达到所述预设的执行时间阈值时，确定监测到所述行情指数信息满足所述执行条件；

当所述时间参数未达到所述预设的执行时间阈值时，确定监测到所述行情指数信息不满足所述执行条件。

19. 如权利要求 14 所述的存储介质，其中，所述至少一个计算机可读指令被所述处理器执行以实现所述根据所述行情指数信息生成包括执行条件的决策树时，具体包括：

随机选取所述行情指数信息中的一个随机参数信息作为所述行情指数信息的决策树的根节点；

计算其余任意一个随机参数信息与所述根节点处的随机参数信息之间的时间差；

判断是否存在与所述时间差相同的子节点；

当判断存在与所述时间差相同的子节点时，将所述子节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点；

当判断不存在与所述时间差相同的子节点时，将所述根节点作为父节点，并将所述其余随机参数信息作为所述父节点的子节点，其中，所述父节点处的随机参数信息与对应的所述子节点处的随机参数信息之间的时间差作为所述父节点和所述子节点之间的边的权重。

20. 一种随机数生成装置，其中，所述随机数生成装置包括：

接收模块，用于接收客户端发送的随机数生成请求；

解析模块，用于解析所述随机生成请求得到行情指数信息，根据所述行情指数信息

生成包括执行条件的决策树，其中，所述决策树的每个节点中包含有随机数种子和随机参数信息；

调用模块，用于当监测到所述行情指数信息满足执行条件时，调用延时函数，在所述决策树的根节点中根据所述随机数种子和所述随机参数信息生成第一随机数；

检验模块，用于通过所述延时函数的验证算法检验是否将所述第一随机数传输至所述根节点的下一个节点；

输入模块，用于当确定将所述第一随机数传输至所述根节点的下一个节点时，将所述第一随机数输入至所述根节点的下一个节点，根据所述第一随机数和所述根节点的下一个节点的随机参数信息生成第二随机数，重复上述过程，直至所述下一个节点为叶子节点；

生成模块，用于根据所述叶子节点的随机参数信息和所述叶子节点接收到的随机数生成目标随机数。

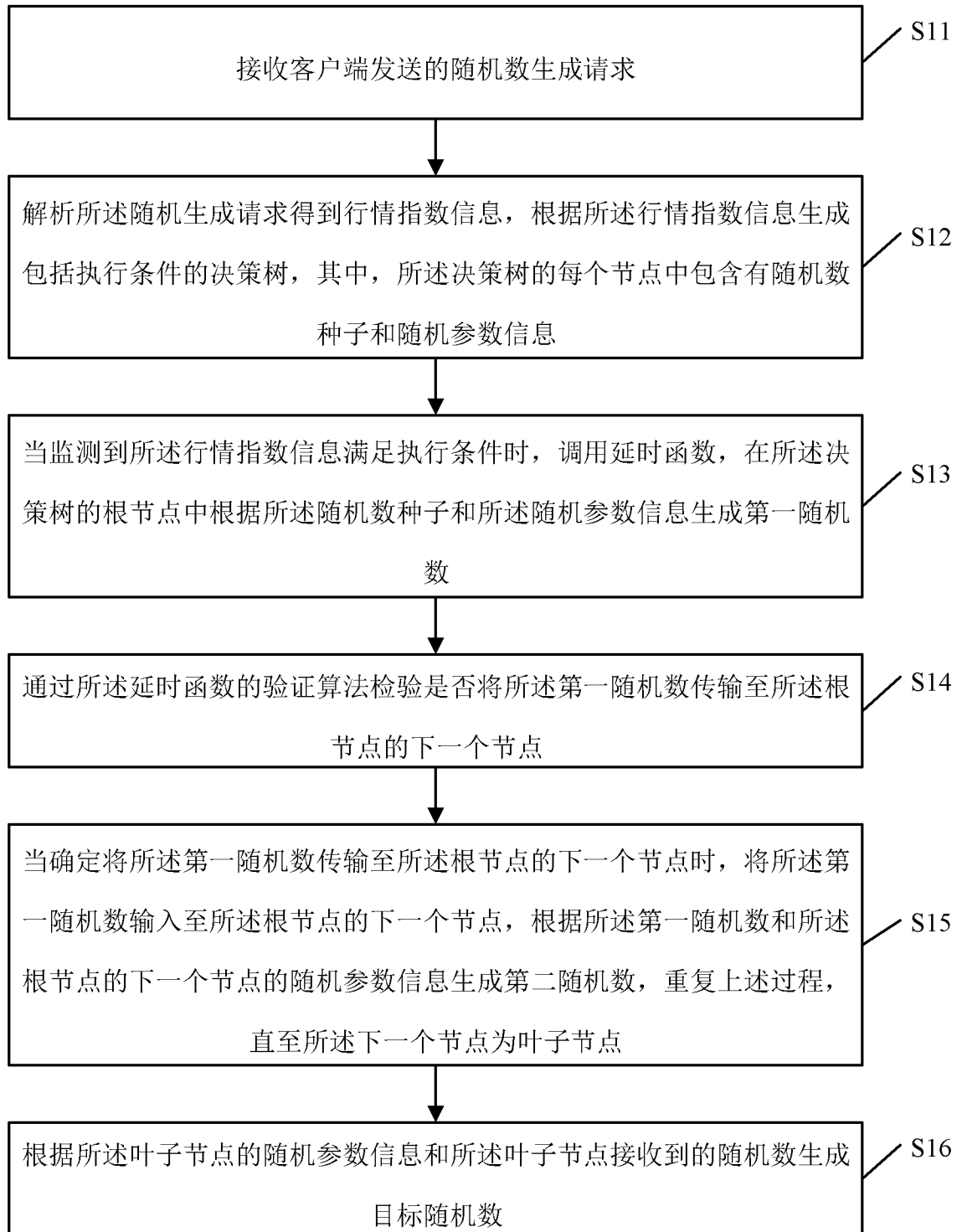


图 1

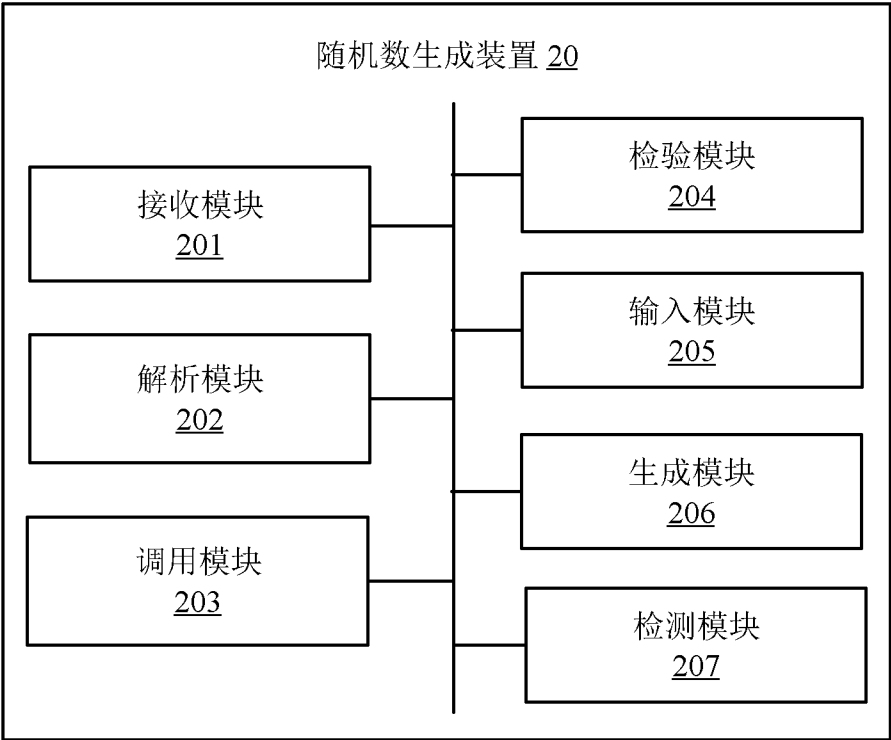


图 2

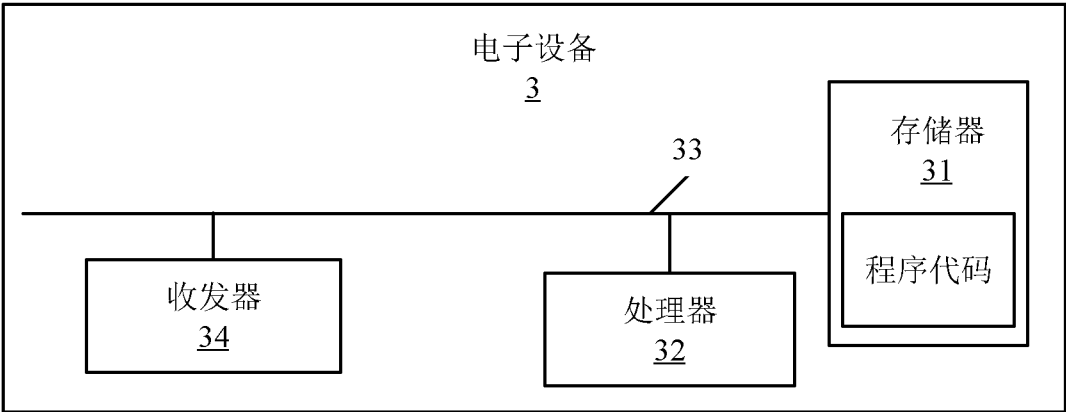


图 3

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/096637

A. CLASSIFICATION OF SUBJECT MATTER

G06F 7/58(2006.01)i; G06N 5/00(2006.01)i; G06Q 30/02(2012.01)i; G06Q 40/00(2012.01)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)

G06F, G06N

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; WOTXT; TWABS; EPTXT; CNKI: 随机数, 生成, 种子, 延时, 决策树, 节点, 叶子, 校验, random number, generate, seed, delay, decision tree, node, leaf, verify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112631551 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 09 April 2021 (2021-04-09) description, paragraphs 3-47	1-20
A	CN 111600709 A (NIUJIN (HAINAN) BLOCKCHAIN RESEARCH INSTITUTE CO., LTD.) 28 August 2020 (2020-08-28) description, paragraphs 5-52	1-20
A	CN 110727414 A (ANHUI QASKY QUANTUM SCIENCE AND TECHNOLOGY CO., LTD.) 24 January 2020 (2020-01-24) description, paragraphs 4-14	1-20
A	CN 109660587 A (PING AN TECHNOLOGY (SHENZHEN) CO., LTD.) 19 April 2019 (2019-04-19) entire document	1-20
A	CN 110083386 A (PING AN PUHUI ENTERPRISE MANAGEMENT CO., LTD.) 02 August 2019 (2019-08-02) entire document	1-20
A	US 2008085005 A1 (SAMSUNG ELECTRONICS CO., LTD.) 10 April 2008 (2008-04-10) 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

06 September 2021

Date of mailing of the international search report

27 September 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088, China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/096637

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	112631551	A	09 April 2021	None			
CN	111600709	A	28 August 2020	None			
CN	110727414	A	24 January 2020	None			
CN	109660587	A	19 April 2019	None			
CN	110083386	A	02 August 2019	None			
US	2008085005	A1	10 April 2008	KR	20080030344	A	04 April 2008

国际检索报告

国际申请号

PCT/CN2021/096637

A. 主题的分类 G06F 7/58(2006.01)i; G06N 5/00(2006.01)i; G06Q 30/02(2012.01)i; G06Q 40/00(2012.01)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) G06F, G06N 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;WOTXT;TWABS;EPTXT;CNKI: 随机数, 生成, 种子, 延时, 决策树, 节点, 叶子, 校验, random number, generate, seed, delay, decision tree, node, leaf, verify		
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 112631551 A (平安科技深圳有限公司) 2021年 4月 9日 (2021 - 04 - 09) 说明书第3-47段	1-20
A	CN 111600709 A (牛津海南区块链研究院有限公司) 2020年 8月 28日 (2020 - 08 - 28) 说明书第5-52段	1-20
A	CN 110727414 A (安徽问天量子科技股份有限公司) 2020年 1月 24日 (2020 - 01 - 24) 说明书第4-14段	1-20
A	CN 109660587 A (平安科技深圳有限公司) 2019年 4月 19日 (2019 - 04 - 19) 全文	1-20
A	CN 110083386 A (平安普惠企业管理有限公司) 2019年 8月 2日 (2019 - 08 - 02) 全文	1-20
A	US 2008085005 A1 (SAMSUNG ELECTRONICS CO LTD) 2008年 4月 10日 (2008 - 04 - 10) 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 2021年 9月 6日		国际检索报告邮寄日期 2021年 9月 27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		授权官员 李艳军 电话号码 86-(20)-28958353

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/096637

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	112631551	A	2021年 4月 9日	无	
CN	111600709	A	2020年 8月 28日	无	
CN	110727414	A	2020年 1月 24日	无	
CN	109660587	A	2019年 4月 19日	无	
CN	110083386	A	2019年 8月 2日	无	
US	2008085005	A1	2008年 4月 10日	KR 20080030344 A	2008年 4月 4日