

(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
2020 年 12 月 30 日 (30.12.2020)



(10) 国际公布号
WO 2020/258567 A1

(51) 国际专利分类号:
G06F 9/50 (2006.01) **G06Q 40/04** (2012.01)

(21) 国际申请号: PCT/CN2019/108917

(22) 国际申请日: 2019 年 9 月 29 日 (29.09.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910575768.4 2019年6月28日 (28.06.2019) CN

(71) 申请人: 苏州浪潮智能科技有限公司 (INSPUR SUZHOU INTELLIGENT TECHNOLOGY CO., LTD) [CN/CN]; 中国江苏省苏州市官浦路 1 号 9 幢, Jiangsu 215000 (CN)。

(72) 发明人: 李雪雷 (LI, Xuelei); 中国江苏省苏州市官浦路 1 号 9 幢, Jiangsu 215000 (CN)。赵雅倩 (ZHAO, Yaqian); 中国江苏省苏州市官浦路 1 号 9 幢, Jiangsu 215000 (CN)。李仁刚 (LI, Rengang); 中国江苏省苏州市官浦路 1 号 9 幢, Jiangsu 215000 (CN)。

(74) 代理人: 北京集佳知识产权代理有限公司 (UNITALEN ATTORNEYS AT LAW); 中国北京市朝阳区建国门外大街 22 号赛特广场 7 层, Beijing 100004 (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,

(54) Title: BLOCKCHAIN DIGITAL SIGNING METHOD AND SYSTEM

(54) 发明名称: 区块链数字签名方法与系统

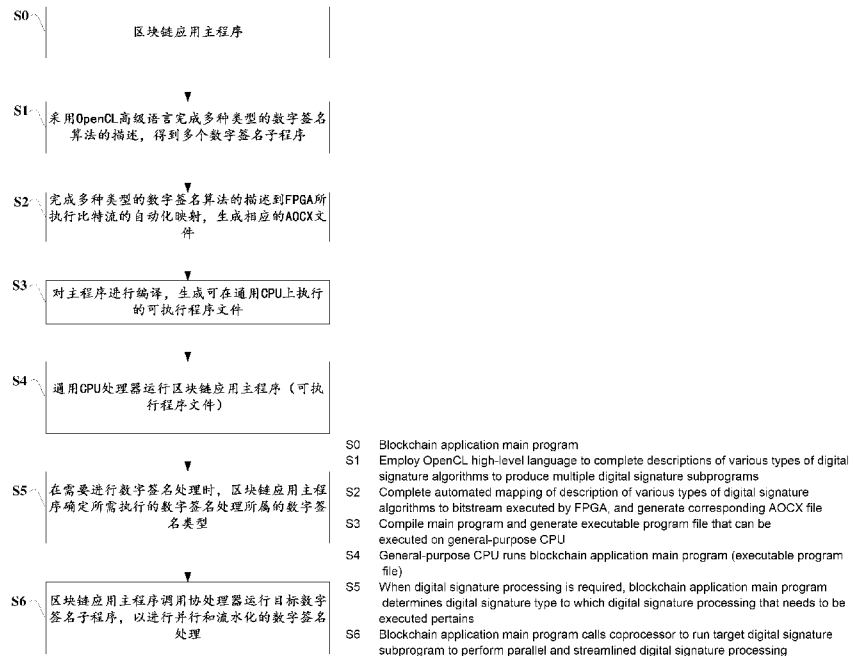


图 4

(57) Abstract: A blockchain digital signing method and system. The blockchain digital signing system comprises a main processor (1) and a coprocessor (2). The main processor (1) is at least used for running a blockchain application main program (3). The coprocessor (2) serves as a hardware acceleration unit and is used for running multiple digital signature subprograms (4). The multiple digital signature subprograms (4) correspond to different digital signature types. The method comprises: when digital signature processing is required, the blockchain application main program (3) determines the digital signature type to which the digital signature processing

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。

(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))。

that needs to be executed pertains; the determined digital signature type serves as a target digital signature type; the digital signature subprogram corresponding to the target digital signature type serves as a digital signature subprogram (4); the blockchain application main program (3) calls the coprocessor (2) to run the target digital signature subprogram to perform parallel and streamlined digital signature processing.

(57) 摘要: 一种区块链数字签名方法与系统, 该区块链数字签名系统包括主处理器(1)和协处理器(2); 主处理器(1)至少用于运行区块链应用主程序(3); 协处理器(2)作为硬件加速单元, 用于运行多个数字签名子程序(4); 多个数字签名子程序(4)对应不同的数字签名类型; 上述方法包括: 在需要进行数字签名处理时, 区块链应用主程序(3)确定所需执行的数字签名处理所属的数字签名类型; 确定出的数字签名类型为目标数字签名类型; 目标数字签名类型对应的数字签名子程序为数字签名子程序(4); 区块链应用主程序(3)调用协处理器(2)运行目标数字签名子程序, 以进行并行和流水化的数字签名处理。

区块链数字签名方法与系统

本申请要求于 2019 年 6 月 28 日提交中国专利局、申请号为 201910575768 .4、发明名称为“区块链数字签名方法与系统”的国内申请的优先权，其全部内容通过引用结合在本申请中。

5 技术领域

本发明涉及可重构计算技术领域，特别涉及区块链数字签名方法与系统。

背景技术

由于信息时代数据量的暴增，信息和数据的隐私安全成为各商业领域内最有价值的资产，尤其在区块链应用中更加注重数据的隐私和安全。

10 区块链应用中利用数字签名（包括但不限于：群签名、环签名、标准数字签名算法、盲签名等）实现消息的准确性和不可否认性。数字签名作为区块链应用的基础技术和核心算法，发挥着极其重要的安全作用，在数据处理速度上直接影响区块链应用的响应时间、吞吐量和可扩展性。

发明内容

15 有鉴于此，本发明实施例提供区块链数字签名方法与系统，以提高数字签名的数据处理速度。

为实现上述目的，本发明实施例提供如下技术方案：

一种区块链数字签名方法，基于区块链数字签名系统，所述区块链数字签名系统包括主处理器和协处理器；所述主处理器至少用于运行区块链应用主程序；所述协处理器作为硬件加速单元，用于运行多个数字签名子程序；
20 所述多个数字签名子程序对应不同的数字签名类型；

所述方法包括：

所述主处理器运行所述区块链应用主程序；

25 在进行数字签名处理时，所述区块链应用主程序确定所需执行的数字签名处理所属的数字签名类型；确定出的数字签名类型为目标数字签名类型；所述目标数字签名类型对应的数字签名子程序为数字签名子程序；

所述区块链应用主程序调用所述协处理器运行所述目标数字签名子程序，以进行并行和流水化的数字签名处理。

30 可选的，所述主处理器为通用 CPU；所述协处理器为现场可编程门阵列 FPGA。

可选的，在所述调用协处理器运行所述目标数字签名子程序之前，所述区块链应用主程序还用于执行如下操作：

准备待处理数据集；

创建主机端与 FPGA 端进行数据通信的缓存；

5 将辅助数据集传输到所述缓存；

将准备好的待处理数据集传输到所述缓存；

设置 FPGA 端运行所需的参数信息；

在所述调用协处理器运行所述目标数字签名子程序之后，所述区块链应用主程序还用于执行如下操作：

10 在所述 FPGA 端返回完成信号之后，读取 FPGA 端的执行结果。

可选的，所述协处理器运行所述目标数字签名子程序，以进行并行和流水化的数字签名处理包括：

从所述缓存处读取所述辅助数据集和所述待处理数据集；

15 依据所述辅助数据集，对所述待处理数据集中的数据进行并行和流水化的计算操作；

将计算操作所得数据写入所述缓存；

在对所述待处理数据集中的数据的计算结束后，向主机端返回完成信号。

可选的，所述参数信息包括：缓存大小、数据的写入和读出配置信息、所述目标数字签名子程序的执行配置信息以及 FPGA 平台信息。

20 可选的，在所述主处理器运行所述区块链应用主程序之前，所述方法还包括：采用高级语言完成多种类型的数字签名算法的描述，得到所述多个数字签名子程序；通过映射工具完成所述多种类型的数字签名算法的描述到 FPGA 所执行比特流的自动化映射，生成相应的 AOCX 文件；对所述主程序进行编译，生成可在所述通用 CPU 上执行的可执行程序文件。

25 可选的，所述主处理器运行所述区块链应用主程序包括：所述通用 CPU 运行所述可执行程序文件；所述协处理器运行所述目标数字签名子程序包括：所述 FPGA 运行所述目标数字签名子程序对应的 AOCX 文件。

一种区块链数字签名系统，包括主处理器和作为硬件加速单元的协处理器；其中，所述协处理器用于运行多个数字签名子程序；所述多个数字签名

子程序对应不同的数字签名类型；

所述主处理器用于：

运行区块链应用主程序；

5 在进行数字签名处理时，确定所需执行的数字签名处理所属的数字签名类型；确定出的数字签名类型为目标数字签名类型；所述目标数字签名类型对应的数字签名子程序为数字签名子程序；

调用所述协处理器运行所述目标数字签名子程序，以进行并行和流水化的数字签名处理。

可选的，所述主处理器为 CPU；所述协处理器为现场可编程门阵列 FPGA。

10 可见，在本发明实施例中，主处理器与协作处理器合作提供区块链应用服务，其中主处理器负责在进行数字签名处理时，从多种数字签名类型中确定出所需的目标数字签名类型，并调用协作处理器执行运行目标数字签名类型所对应的目标数字签名子程序，协作处理器的并行流水化方式可提高数字签名算法的并行度和数据处理速度，进而改善数字签名算法执行时的数
15 据处理速度，提高区块链应用的响应时间、吞吐量和可扩展性。

附图说明

图1为本发明实施例提供的区块链数字签名系统应用场景示意图；

图2为本发明实施例提供的区块链数字签名系统示例性结构图；

图3为本发明实施例提供的区块链数字签名系统另一示例性结构图；

20 图4为本发明实施例提供的区块链数字签名方法示例性流程图；

图5为本发明实施例提供的文件生成示例图；

图6为本发明实施例提供的区块链数字签名方法的另一示例性流程图。

具体实施方式

为了引用和清楚起见，下文中使用的技术名词、简写或缩写总结如下：

25 区块链：Blockchain。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链是比特币的一个重要概念，它本质上是一个去中心化的数据库，同时作为比特币的底层技术，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比特币网络交易的信息，用于验证其信息的有效性（防伪）和生成下一个区块；

30 OpenCL: Open Computing Language，开放式计算语言；

DDR: Dual Data Rate, 双倍速率同步动态随机存储器;

FPGA: Field-Programmable Gate Array, 现场可编程门阵列;

DSA: Digital Signature Algorithm, 标准数字签名算法;

GPU: Graphics Processing Unit, 图形处理器;

5 PCI: Peripheral Component Interconnect, 外设部件互连标准;

PCI-E: PCI Express, PCI-E 接口是主板上比较通用的一种接口标准, 目前主要提供给需要直接与 CPU 进行通讯的设备使用, 通常是为了扩展主板上没有支持的功能;

DDRSDRAM: Double Data RateSDRAM, 双倍速率同步动态随机存储器;

10 DDR3: 一种计算机内存规格。属于 SDRAM 家族的内存产品, 提供了相较于 DDR2 SDRAM 更高的运行效能与更低的电压, 是 DDR2 SDRAM (同步动态动态随机存取内存) 的后继者 (增加至八倍), 也是现时流行的内存产品规格;

EXE File: executable program, 可执行程序。可执行程序是可在操作系统存储空间中浮动定位的二进制可执行程序。它可以加载到内存中, 由操作系统加载并执行;

OpenCL: Open Computing Language, 开放运算语言。OpenCL 是第一个面向异构系统通用目的并行编程的开放式、免费标准, 也是一个统一的编程环境, 便于软件开发人员为高性能计算服务器、桌面计算系统、手持设备编写高效轻便的代码, 而且广泛适用于多核心处理器 (CPU)、图形处理器 (GPU)、Cell 类型架构以及数字信号处理器 (DSP) 等其他并行处理器, 在游戏、娱乐、科研、医疗等各种领域都有广阔的发展前景;

GCC: GNU Compiler Collection, GNU 编译器套件, 包括 C、C++、Objective-C、Fortran、Java、Ada 和 Go 语言的前端, 也包括了这些语言的库 (如 libstdc++、libgcj 等等)。GCC 原本作为 GNU 操作系统的官方编译器, 现已被大多数类 Unix 操作系统 (如 Linux、BSD、Mac OS X 等) 采纳为标准的编译器;

MAC: MessageAuthenticationCode, 消息认证码。

区块链技术可应用于商品溯源、个人征信等领域, 数字签名是区块链应

用的基础技术和核心算法。

数字签名算法是应用较早、技术成熟的一些算法。在数字签名算法中，签名者利用自己的密钥对消息进行处理，生成数字签名（签章）。收到消息的为验证者，利用系统公开（可验证）的公钥对数字签名进行验证，用来确认消息来源及其准确性。

数字签名处理过程需要一定的计算资源。在数据暴增、响应时间有限的条件下，能够以最快的速度满足用户对数据的存取响应成为一项严峻的挑战。

为解决上述问题，本发明实施例提供了区块链数字签名方法与系统。

请参见图 1，上述区块链数字签名系统具体可为后端服务器 102（例如应用服务器、平台服务器、数字签名服务器），其应用场景示例性如下：用户向 web 服务器 101 提交数字签名处理请求（生成消息签名请求或验证请求），web 服务器 101 与后端服务器 102 通讯，由后端服务器 102 进行数字签名处理。

请参见图 2，上述区块链数字签名系统可包括主处理器 1 和协处理器 2；其中，主处理器 1 至少用于运行区块链应用主程序 3；而协处理器 2 作为硬件加速单元，用于运行多个数字签名子程序 4。

在需要进行数字签名处理时，区块链应用主程序会调用协处理器 2 运行数字签名子程序，以进行并行和流水化的数字签名处理。协作处理器的并行流水化方式可提高数字签名算法的并行度和数据处理速度，进而改善数字签名算法执行时的吞吐率性能。

在一个示例中，请参见图 3，区块链数字签名系统为异构加速平台：主处理器 1 为通用 CPU1'，而协处理器 2 为 FPGA 2'。通用 CPU1' 与 FPGA2' 之间采用 PCI-E 接口进行数据通信，并采用 FPGA 开发板上的 DDR3 内存作为数据缓存（Buffer）。

在另一示例中，协处理器也可为 GPU。

数字签名算法非常适合于并行、流水化的加速处理，与 FPGA、GPU 的计算特点相当吻合。因此，采用 FPGA 或 GPU 作为数字签名处理的硬件加速单元（或称为硬件电路），其并行流水化处理方式可提高数字签名算法的并行度和数据处理速度，进而改善数字签名算法执行时的吞吐率性能。

此外，FPGA 可以很容易实现细粒化并行，相当于 CPU 起多个线程。但 CPU 起多个线程需要价格昂贵的服务器或集群进行支持，而 FPGA 则不需要，

因此，采用本发明实施例所提供的方案可以降低硬件成本。

下面将以主处理器为通用 CPU、协处理器为 FPGA 的区块链数字签名系统为例，对本发明所提供的技术方案进行具体的介绍。

图 4 和图 5 示出了由区块链数字签名系统所执行的区块链数字签名方法的一种示例性流程，包括：

S0：生成区块链应用主程序；

在一个示例中，区块链应用主程序可采用 C 语言编写。区块链应用主程序可执行除数字签名处理之外或之前的处理操作，例如，调度、准备待处理数据、数据回收等。

10 S1：采用OpenCL高级语言完成多种类型的数字签名算法的描述，得到多个数字签名子程序。

数字签名算法种类示例性得可包括：标准数字签名算法、代理签名算法、盲签名算法、群签名算法和环签名算法等。不同算法应用在不同领域以实现其特定的功能，但是签名算法的根本不会发生改变：确保消息的来源及其可
15 靠性。

具体的，对于linux操作系统而言，每一数字签名子程序可为面向FPGA平台的Kernel程序文件。

需要说明的是，数字签名处理算法包括签名和验证两部分，则在一个示例中，与一数字签名处理算法对应的 Kernel 程序文件具体可包含用于签名的
20 Kernel 程序文件，以及用于验证的 Kernel 程序文件。

需要说明的是，由于FPGA目前仅支持OpenCL高级语言，因此，本实施例采用OpenCL高级语言完成数字签名算法的描述。但未来并不排除FPGA可支持其他高级语言的可能。此外，若协处理器为GPU，则也可使用其他高级语言完成数字签名算法的描述。

25 S2：通过映射工具完成多种类型的数字签名算法的描述到 FPGA 所执行比特流的自动化映射，生成相应的、可在 FPGA 上运行的 AOCX 文件（比特流）。

具体的，可采用 AOC（Altera SDK for OpenCL）高层次综合工具对 Kernel 程序文件进行编译综合（即自动化映射），生成 AOCX 文件。

30 在一个示例中，若与一数字签名算法对应的 Kernel 程序文件包含用于签

名的 Kernel 程序文件, 以及用于验证的 Kernel 程序文件, 则 AOCX 文件相应包括用于签名的 AOCX 文件, 以及用于验证的 AOCX 文件。

具体的, AOCX 文件在 FPGA 上的数字签名核心算法硬件电路上执行计算。

- 5 S3: 对区块链应用主程序进行编译, 生成可在通用 CPU 上执行的可执行程序文件。

具体的, 可采用 GCC 编译器对主机端程序进行编译, 生成 EXE File。

S4: 主处理器运行区块链应用主程序。

具体的, 是在通用 CPU 上运行上述可执行程序文件。

- 10 通用 CPU 可将可执行程序文件加载至内存运行。

S5: 在需要进行数字签名处理时, 区块链应用主程序确定所需执行的数字签名处理所属的数字签名类型。

当然, 实际上是通用 CPU 运行可执行程序文件来确定所需执行的数字签名处理所属的数字签名类型。

- 15 每一数字签名类型可对应唯一标识, 可通过类型标识来确定数字签名类型。类型标识可在应用请求中携带。

需要说明的是, 应用请求是触发区块链应用主程序进行数字签名处理的请求。

- 20 为后续称呼方便, 可将确定出的数字签名类型称为目标数字签名类型, 而将目标数字签名类型对应的数字签名子程序称为数字签名子程序。

S6: 区块链应用主程序调用协处理器运行目标数字签名子程序, 以进行并行和流水化的数字签名处理。

当然, FPGA 底层真正执行的是 AOCX 文件。

- 25 可见, 在本发明实施例中, 主处理器与协作处理器合作提供区块链应用服务, 其中主处理器负责在需要进行数字签名处理时, 从多种数字签名类型中确定出所需的目标数字签名类型, 并调用协作处理器执行运行目标数字签名类型所对应的目标数字签名子程序, 协作处理器的并行流水化方式可提高数字签名算法的并行度和数据处理速度, 进而改善数字签名算法执行时的数据处理速度, 提高区块链应用的响应时间、吞吐量和可扩展性。

使用FPGA作为协处理器，能够有效的提升数字签名核心算法的执行性能，上述自动化映射方式能够有效缩短将数字签名算法部署到基于FPGA的异构加速平台时的时间，提高产品研发周期。

下面介绍通用CPU运行可执行程序文件所执行的具体操作，以及FPGA运行AOCX文件所执行的具体操作。

请参见图6，通用CPU运行可执行程序文件所执行的具体操作可包括：

S601：准备待处理数据集。

前述提及了，数字签名处理包括签名和验证，对于签名过程，待处理数据集可包括待签名数据；而对于验证过程，待处理数据集可包括待验证数据（已签名数据）。

S602：创建主机端与FPGA端进行数据通信的缓存。

该缓存位于在FPGA开发板的DDR内存上。

S603：将辅助数据集传输到上述缓存。

辅助数据集参与数字签名处理的运算。以签名过程为例，辅助数据集可包括：将待签名数据的分块信息（指示将待签名数据以多大分块）、用户私钥以及签名过程中所使用的函数（例如哈希函数）何时调用等信息。

在验证时，辅助数据集包括签名系统参数（模数、数域等）和公钥。

S604：将准备好的待处理数据集传输到上述缓存。

需要说明的是，辅助数据集要先于待处理数据集传输。

S605：设置FPGA端运行所需的参数信息。

其中，参数信息可包括：缓存大小、数据的写入和读出配置信息（例如何时写入，何时读出、一次写入的数据量、一次读取的数据量等）、kernel文件的执行配置信息（例如，何时调用）以及FPGA平台信息（例如FPGA板卡型号）。

S606：确定所需执行的数字签名处理所属的数字签名类型，调用FPGA端运行目标数字签名子程序。

具体的，可先向FPGA发送启动信号，再调用FPGA端运行目标数字签名子程序。

FPGA运行AOCX文件所执行的具体操作则可包括：

S607：读取上述辅助数据集和待处理数据集。

前述提及，可使用 FPGA 的 DDR 作为缓存，则在本步骤中，可从 FPGA 的 DDR 批量读取辅助数据集和待处理数据集至 FPGA 的片上缓存。

S608：依据辅助数据集，对待处理数据集中的数据进行并行和流水化的计算操作。

5 S609：将计算操作所得数据写入上述缓存；

S610：对待处理数据集中的数据的计算结束后，向主机端返回完成信号。

在签名或验证步骤执行完毕后，可向主机端返回完成信号。由主机端读取缓存中的数据。

则通用CPU运行可执行程序文件所执行的具体操作还包括：

10 S611：在接收到FPGA端返回完成信号后，从缓存中读取数字签名处理得到的数据；

S612：完成数字签名过程并输出相应的签名信息或者验证结果。

专业人员还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及模型步骤，能够以电子硬件、计算机软件或者二者的结合来实现，
15 为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本发明的范围。

20 结合本文中所公开的实施例描述的方法或模型的步骤可以直接用硬件、处理器执行的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器（RAM）、内存、只读存储器（ROM）、电可编程 ROM、电可擦除可编程 ROM、寄存器、硬盘、可移动磁盘、WD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

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

权利要求书

1、一种区块链数字签名方法，其特征在于，基于区块链数字签名系统，所述区块链数字签名系统包括主处理器和协处理器；所述主处理器至少用于运行区块链应用主程序；所述协处理器作为硬件加速单元，用于运行多个数字签名子程序；所述多个数字签名子程序对应不同的数字签名类型；

所述方法包括：

所述主处理器运行所述区块链应用主程序；

在需要进行数字签名处理时，所述区块链应用主程序确定所需执行的数字签名处理所属的数字签名类型；确定出的数字签名类型为目标数字签名类型；所述目标数字签名类型对应的数字签名子程序为数字签名子程序；

所述区块链应用主程序调用所述协处理器运行所述目标数字签名子程序，以进行并行和流水化的数字签名处理。

2、如权利要求1所述的方法，其特征在于，所述主处理器为通用CPU；所述协处理器为现场可编程门阵列FPGA。

3、如权利要求2所述的方法，其特征在于，在所述调用协处理器运行所述目标数字签名子程序之前，所述区块链应用主程序还用于执行如下操作：

准备待处理数据集；

创建主机端与FPGA端进行数据通信的缓存；

将辅助数据集传输到所述缓存；

将准备好的待处理数据集传输到所述缓存；

设置FPGA端运行所需的参数信息；

在所述调用协处理器运行所述目标数字签名子程序之后，所述区块链应用主程序还用于执行如下操作：

在所述FPGA端返回完成信号之后，读取FPGA端的执行结果。

4、如权利要求3所述的方法，其特征在于，所述协处理器运行所述目标数字签名子程序，以进行并行和流水化的数字签名处理包括：

从所述缓存处读取所述辅助数据集和所述待处理数据集；

依据所述辅助数据集，对所述待处理数据集中的数据进行并行和流水化的计算操作；

将计算操作所得数据写入所述缓存；

在对所述待处理数据集中的数据的计算结束后，向主机端返回完成信号。

5、如权利要求3所述的方法，其特征在于，所述参数信息包括：

缓存大小、数据的写入和读出配置信息、所述目标数字签名子程序的执行配置信息以及FPGA平台信息。

6、如权利要求2-5任一项所述的方法，其特征在于，

在所述主处理器运行所述区块链应用主程序之前，所述方法还包括：

采用高级语言完成多种类型的数字签名算法的描述，得到所述多个数字签名子程序；

10 通过映射工具完成所述多种类型的数字签名算法的描述到FPGA所执行比特流的自动化映射，生成相应的AOCX文件；

对所述主程序进行编译，生成可在所述通用CPU上执行的可执行程序文件。

7、如权利要求6所述的方法，其特征在于，

15 所述主处理器运行所述区块链应用主程序包括：所述通用CPU运行所述可执行程序文件；

所述协处理器运行所述目标数字签名子程序包括：所述FPGA运行所述目标数字签名子程序对应的AOCX文件。

8、一种区块链数字签名系统，其特征在于，包括主处理器和作为硬件加速单元的协处理器；其中，所述协处理器用于运行多个数字签名子程序；所述多个数字签名子程序对应不同的数字签名类型；

所述主处理器用于：

运行区块链应用主程序；

25 在进行数字签名处理时，确定所需执行的数字签名处理所属的数字签名类型；确定出的数字签名类型为所述目标数字签名类型；所述目标数字签名类型对应的数字签名子程序为数字签名子程序；

调用所述协处理器运行所述目标数字签名子程序，以进行并行和流水化的数字签名处理。

9、如权利要求8所述的系统，其特征在于，所述主处理器为CPU；所述协处理器为现场可编程门阵列FPGA。

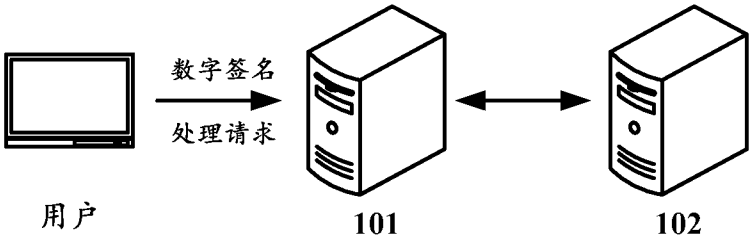


图 1

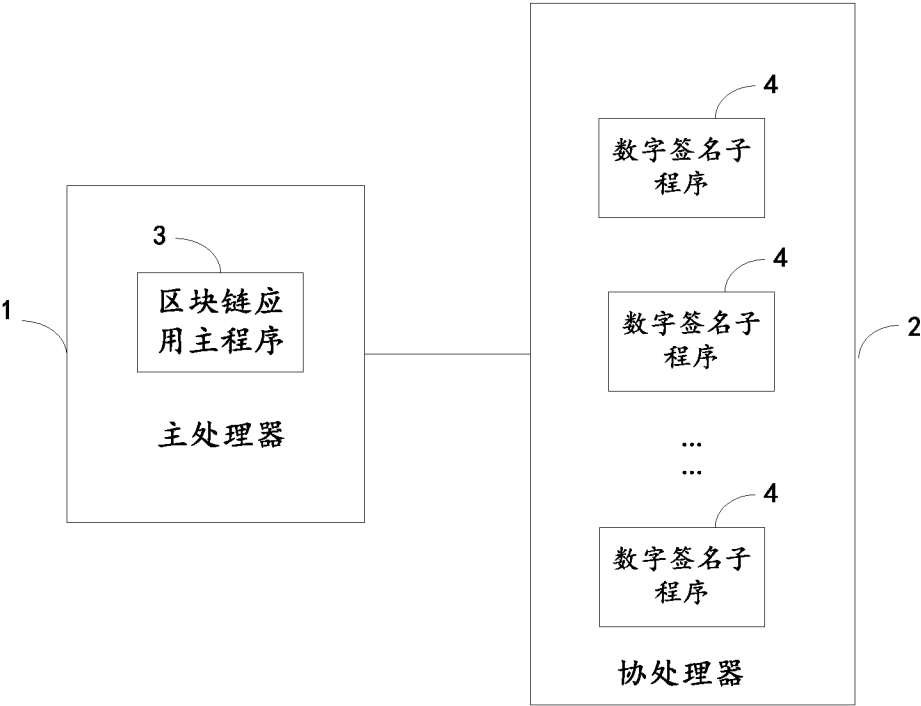


图 2

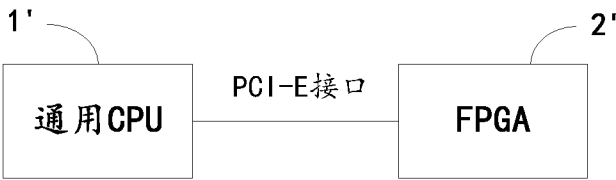


图 3

- 2/4 -

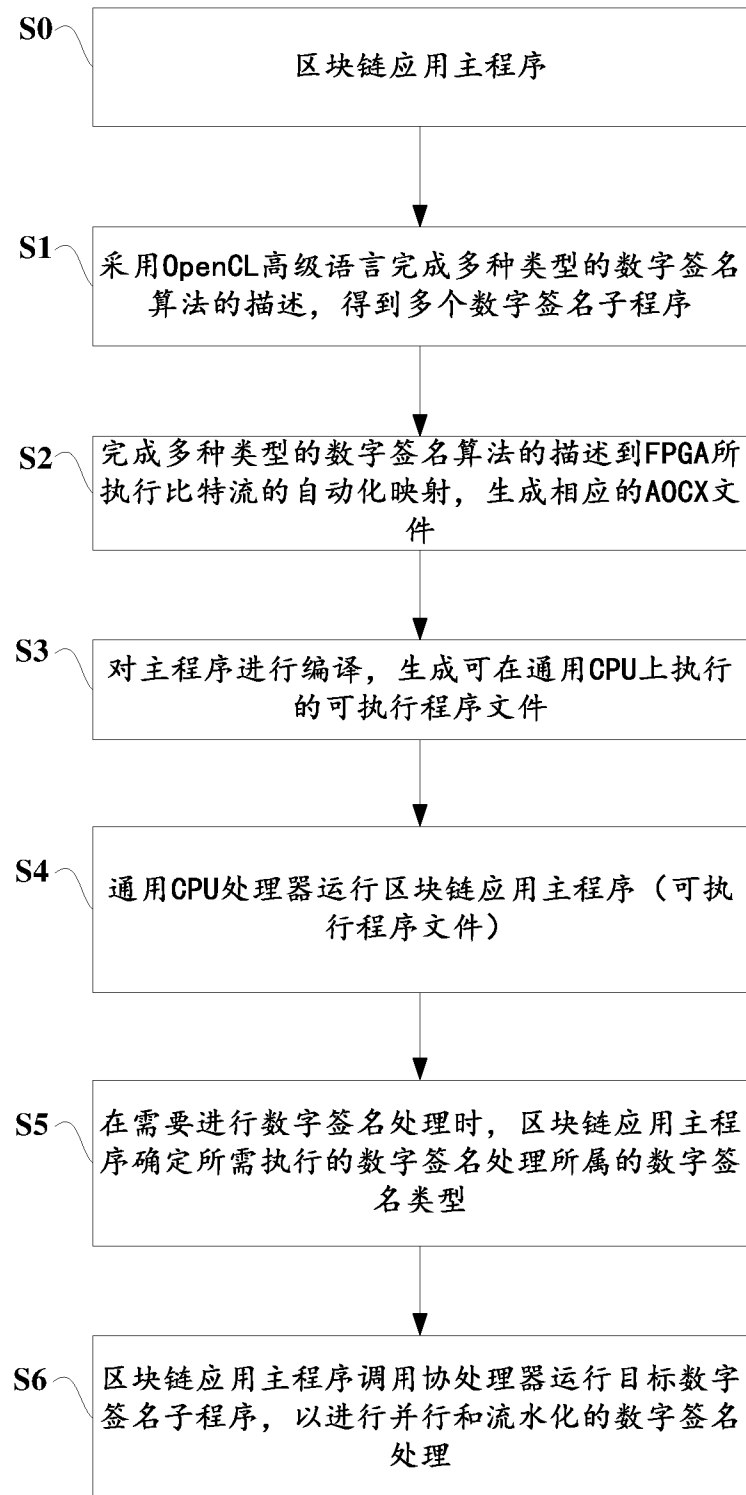


图 4

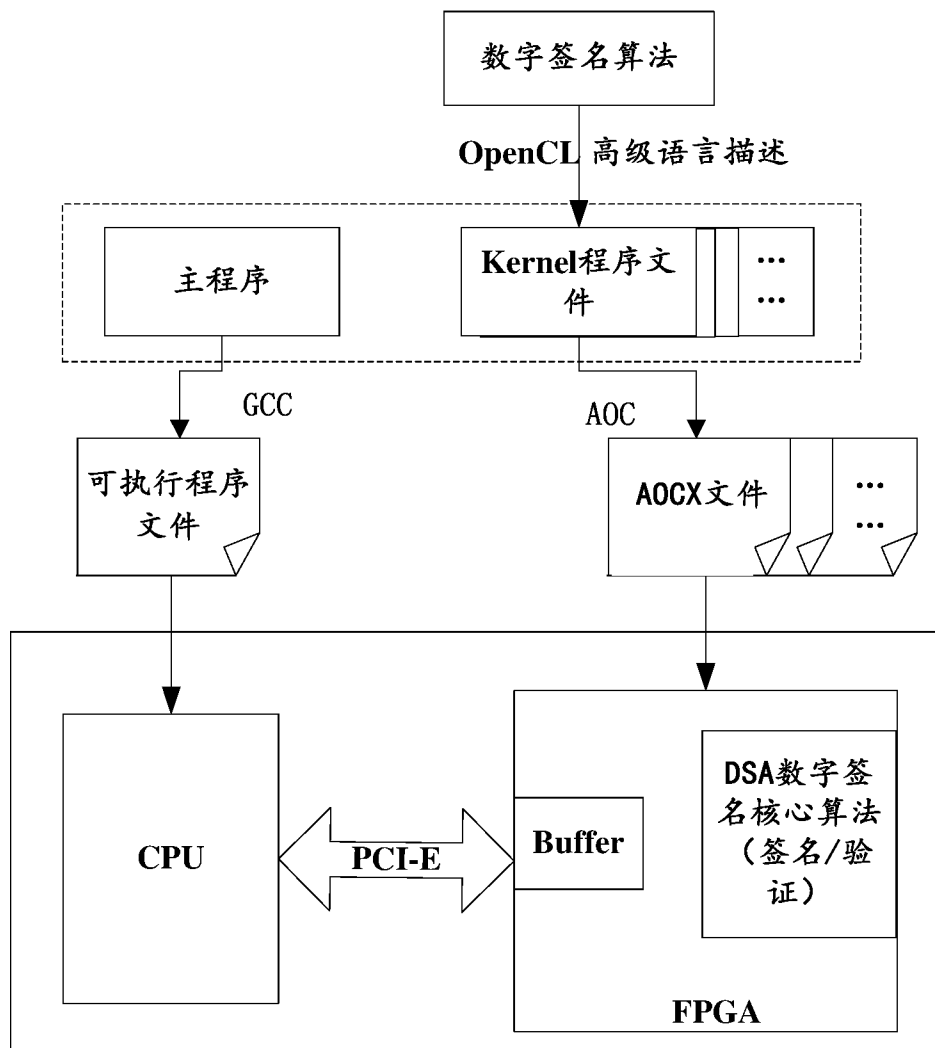


图 5

— 4/4 —

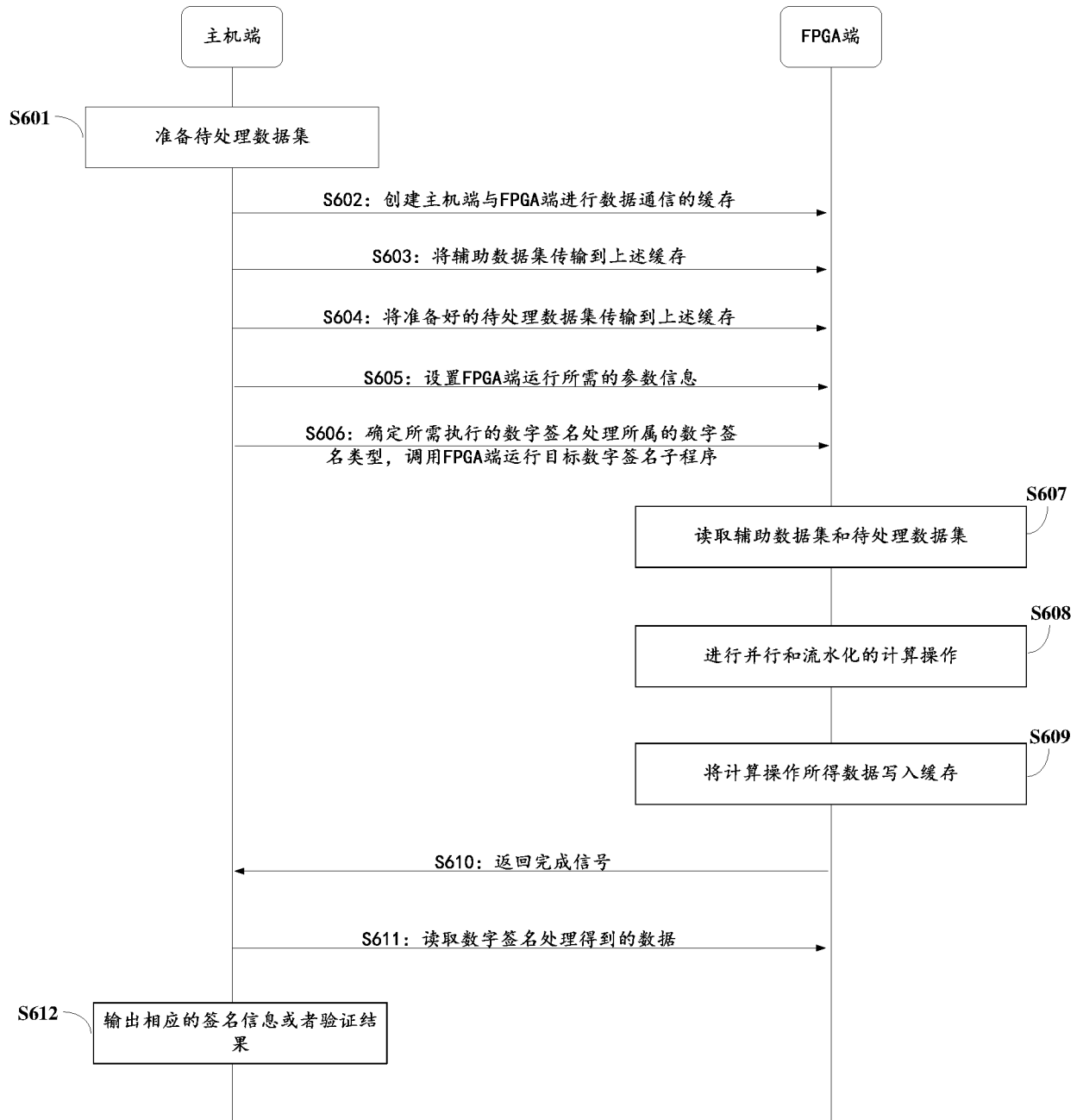


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/108917

A. CLASSIFICATION OF SUBJECT MATTER

G06F 9/50(2006.01)i; G06Q 40/04(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; G06Q

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, EPODOC, WPI: 区块链, 签名, 并行, 类型, 主, 协处理器, 从处理器, blockchain, signature, parallel, type, main, coprocessor

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110400141 A (SUZHOU LANGCHAO INTELLIGENT TECHNOLOGY CO., LTD.) 01 November 2019 (2019-11-01) claims 1-9	1-9
X	CN 109284185 A (INTEL CORPORATION) 29 January 2019 (2019-01-29) description, paragraphs 39-86	1-2, 8-9
Y	CN 109284185 A (INTEL CORPORATION) 29 January 2019 (2019-01-29) description, paragraphs 39-86	3-7
Y	CN 107491317 A (ZHENGZHOU YUNHAI INFORMATION TECHNOLOGY CO., LTD.) 19 December 2017 (2017-12-19) description, paragraphs 53-70	3-7
A	CN 108063758 A (ZHONGAN INFORMATION TECHNOLOGY SERVICE CO., LTD.) 22 May 2018 (2018-05-22) entire document	1-9
A	US 2018352033 A1 (VERIZON PATENT AND LICENSING INC.) 06 December 2018 (2018-12-06) entire document	1-9



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

18 March 2020

Date of mailing of the international search report

31 March 2020

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/CN2019/108917

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110400141	A	01 November 2019	None			
CN	109284185	A	29 January 2019	EP	3432146	A1	23 January 2019
				US	2019026146	A1	24 January 2019
CN	107491317	A	19 December 2017	None			
CN	108063758	A	22 May 2018	None			
US	2018352033	A1	06 December 2018	None			

国际检索报告

国际申请号

PCT/CN2019/108917

A. 主题的分类

G06F 9/50(2006.01)i; G06Q 40/04(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; G06Q

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, EPDOC, WPI:区块链, 签名, 并行, 类型, 主, 协处理器, 从处理器, blockchain, signature, parallel, type, main, coprocessor

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 110400141 A (苏州浪潮智能科技有限公司) 2019年 11月 1日 (2019 - 11 - 01) 权利要求1-9	1-9
X	CN 109284185 A (英特尔公司) 2019年 1月 29日 (2019 - 01 - 29) 说明书第39-86段	1-2, 8-9
Y	CN 109284185 A (英特尔公司) 2019年 1月 29日 (2019 - 01 - 29) 说明书第39-86段	3-7
Y	CN 107491317 A (郑州云海信息技术有限公司) 2017年 12月 19日 (2017 - 12 - 19) 说明书第53-70段	3-7
A	CN 108063758 A (众安信息技术服务有限公司) 2018年 5月 22日 (2018 - 05 - 22) 全文	1-9
A	US 2018352033 A1 (VERIZON PATENT AND LICENSING INC.) 2018年 12月 6日 (2018 - 12 - 06) 全文	1-9

☐ 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

2020年 3月 18日

国际检索报告邮寄日期

2020年 3月 31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

吴黄飞

电话号码 86-(10)-53961430

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/108917

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	110400141	A	2019年 11月 1日	无			
CN	109284185	A	2019年 1月 29日	EP	3432146	A1	2019年 1月 23日
				US	2019026146	A1	2019年 1月 24日
CN	107491317	A	2017年 12月 19日	无			
CN	108063758	A	2018年 5月 22日	无			
US	2018352033	A1	2018年 12月 6日	无			