

(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
2023 年 6 月 29 日 (29.06.2023)



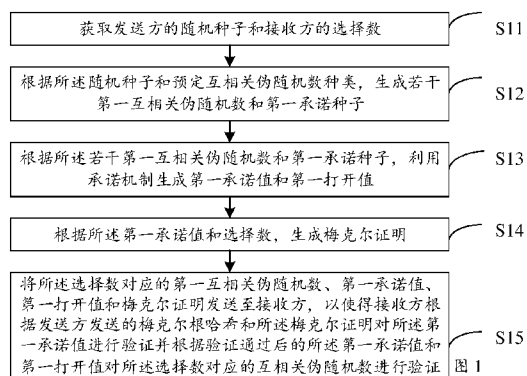
(10) 国际公布号
WO 2023/115602 A1

- (51) 国际专利分类号:
H04L 9/32 (2006.01)
- (21) 国际申请号: PCT/CN2021/141676
- (22) 国际申请日: 2021 年 12 月 27 日 (27.12.2021)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
202111598444.6 2021 年 12 月 24 日 (24.12.2021) CN
- (71) 申请人: 浙江大学(ZHEJIANG UNIVERSITY) [CN/CN]; 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。 浙江大学杭州国际科创中心(ZJU-HANGZHOU GLOBAL SCIENTIFIC AND TECHNOLOGICAL INNOVATION CENTER) [CN/CN]; 中国浙江省杭州市萧山区市心北路 99 号 5 楼, Zhejiang 311215 (CN)。

- (72) 发明人: 张秉晟(ZHANG, Bingsheng); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。 卢益彪(LU, Yibiao); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。 刘巍然(LIU, Weiran); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。 任奎(REN, Kui); 中国浙江省杭州市西湖区余杭塘路 866 号, Zhejiang 310058 (CN)。
- (74) 代理人: 杭州求是专利事务所有限公司(HANGZHOU QIUSHI PATENT OFFICE CO., LTD.); 中国浙江省杭州市西湖区古墩路 701 号 绿城紫金广场 C 座 1506 室 应孔月, Zhejiang 310012 (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:** METHOD AND APPARATUS FOR REMOTELY ACQUIRING CORRELATED RANDOMNESS ON BASIS OF SEMI-TRUSTED HARDWARE

(54) 发明名称: 基于半可信硬件的互相关伪随机数的远程获取方法及装置



- S11 Acquire a random seed of a sender and a choice number of a receiver
- S12 Generate several first correlated randomnesses and first commitment seeds on the basis of the random seed and a predetermined correlated randomness type
- S13 Generate, on the basis of the several first correlated randomnesses and first commitment seeds, a first commitment value and a first open value using a commitment mechanism
- S14 Generate a Merkle proof on the basis of the first commitment value and the choice number
- S15 Send to the receiver the first correlated randomness corresponding to the choice number, and the first commitment value, the first open value and the Merkle proof, such that the receiver verifies the first commitment value on the basis of a Merkle root hash sent by the sender and the Merkle proof, and verifies, on the basis of the first commitment value that has passed verification and the first open value, the correlated randomness corresponding to the choice number

(57) **Abstract:** A method and apparatus for remotely acquiring a correlated randomness on the basis of semi-trusted hardware. The method, when applied to semi-trusted hardware, comprises: acquiring a random seed of a sender and a choice number of a receiver (S11); generating several first correlated randomnesses and first commitment seeds on the basis of the random seed and a predetermined correlated randomness type (S12); on the basis of the several first correlated randomnesses and first commitment seeds, generating a first commitment value and a first open value using a commitment mechanism (S13); generating a Merkle proof on the basis of the first commitment value and the choice number (S14); and sending to the receiver the first correlated randomness corresponding to the choice number, and the first commitment value, the first open value and the Merkle proof, such that the receiver verifies the first commitment value on the basis of a Merkle root hash sent by the sender and the Merkle proof, and verifies, on the basis of the first commitment value that has passed verification and the first open value, the correlated randomness corresponding to the choice number (S15).

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:

— 包括国际检索报告(条约第21条(3))。

(57) 摘要: 一种基于半可信硬件的互相关伪随机数的远程获取方法及装置, 该方法应用于半可信硬件时包括: 获取发送方的随机种子和接收方的选择数(S11); 根据所述随机种子和预定互相关伪随机数种类, 生成若干第一互相关伪随机数和第一承诺种子(S12); 根据所述若干第一互相关伪随机数和第一承诺种子, 利用承诺机制生成第一承诺值和第一打开值(S13); 根据所述第一承诺值和选择数, 生成梅克尔证明(S14); 将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方, 以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证(S15)。

基于半可信硬件的互相关伪随机数的远程获取方法及装置

技术领域

本申请涉及隐私保护数据处理领域，尤其涉及基于半可信硬件的互相关伪随机数的远程获取方法及装置。

背景技术

安全多方计算（Secure Multi-party Computation, MPC）技术可以让多个互不信任的参与方协同计算一个预先商定好的函数，同时不泄露除了函数输出以外的任何信息，如参与方的隐私输入。在安全多方计算协议中，常会使用互相关伪随机数（correlated randomness）作为协议的组成部分。例如，随机不经意传输（Random Oblivious Transfer, ROT）和乘法三元组（Beaver triple）都可以被视为互相关伪随机数。

由于协议的参与方互不信任，且往往都是通过远程信道进行连接，如何生成互相关伪随机数并让参与方获取适当的互相关伪随机数需要经过仔细考虑。目前，一种普遍的做法是让协议的各个参与方运行一个简单的安全多方计算协议，这个协议的作用就是让各个参与方得到相应的互相关伪随机数，而在这个协议中，各个参与方的输入与计算函数时的输入无关，因此这个协议的运行可以在参与方得到函数输入之前，也就是计算的离线阶段（offline phase）。另一种做法是使用半可信硬件，通过向可信硬件输入互相关伪随机数的生成种子和各个参与方需要获取的互相关伪随机数，可以使得半可信硬件直接向各个参与方输出相应的互相关伪随机数。

然而，在实现本发明的过程中，发明人发现现有技术中至少存在如下问题：

对于使用安全多方计算协议生成互相关伪随机数的技术，这一方法需要的通讯量大、通讯轮次多，在实际运行过程中耗时长，导致参与方需要在正式计算前运行协议生成互相关伪随机数，而无法做到在需要进行计算时直接执行用于计算的安全多方计算协议，并且，生成的互相关伪随机数需要在存储介质中长期保存，造成较大的开销；对于使用半可信硬件生成互相关伪随机数的技术，这一方法引入了额外的可信根，依赖于半可信硬件会正确生成互相关伪随机数并输出结果的假设，但如果这一假设不成立，就会影响整体安全多方计算协议

的正确性。总的来说，现有技术或是存在通讯量大、通讯轮次多、耗时长的问题，或是存在获取的互相关伪随机数正确性无法保证的问题，难以兼顾效率和正确性。

发明内容

本申请实施例的目的是提供基于半可信硬件的互相关伪随机数的远程获取方法及装置，以解决相关技术中存在的无法在低通讯量开销下向远程的参与方传输多项式数量级别的互相关伪随机数的技术问题。

根据本申请实施例的第一方面，提供一种基于半可信硬件的互相关伪随机数的远程获取方法，应用于半可信硬件，包括：

获取发送方的随机种子和接收方的选择数；

根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；

根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；

根据所述第一承诺值和选择数，生成梅克尔证明；

将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

进一步地，获取发送方的随机种子和接收方的选择数，包括：

接收发送方的加密随机种子和接收方的随机数；

根据发送方和半可信硬件的对称密钥，对所述加密随机种子进行解密；

对解密得到的结果进行验证；

若验证通过，则获得发送方的随机种子。

进一步地，根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子，包括：

将所述随机种子扩展为第一伪随机种子和第二伪随机种子；

根据所述预定互相关伪随机数种类和第一伪随机种子，生成若干第一互相关伪随机数；

根据所述第二伪随机种子，生成若干第一承诺种子，其中所述第一承诺种

子的数量与所述第一互相关伪随机数的数量相同。

根据本申请实施例的第二方面，提供一种基于半可信硬件的互相关伪随机数的远程获取装置，应用于半可信硬件，包括：

第一获取模块，用于获取发送方的随机种子和接收方的选择数；

第一生成模块，用于根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；

第二生成模块，用于根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；

第三生成模块，用于根据所述第一承诺值和选择数，生成梅克尔证明；

第一发送模块，用于将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

根据本申请实施例的第三方面，提供一种基于半可信硬件的互相关伪随机数的远程获取方法，应用于发送方，包括：

对所述半可信硬件进行验证并得到与所述半可信硬件共享的对称密钥；

根据所述对称密钥，对随机种子进行加密并发送至接收方，以使得接收方将发送方的加密随机种子和接收方的选择数发送至半可信硬件，从而使得所述半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

根据所述随机种子和预定互相关伪随机数种类，生成若干第二互相关伪随机数和第二承诺种子；

根据所述若干第二互相关伪随机数和第二承诺种子，生成第二承诺值；

根据所述第二承诺值，生成梅克尔根哈希；

将所述梅克尔根哈希发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

根据本申请实施例的第四方面，提供一种基于半可信硬件的互相关伪随机数的远程获取装置，应用于发送方，包括：

第一验证模块，用于对所述半可信硬件进行验证并得到与所述半可信硬件共享的对称密钥；

第二发送模块，用于根据所述对称密钥，对随机种子进行加密并发送至接收方，以使得接收方将发送方的加密随机种子和接收方的选择数发送至半可信硬件，从而使得所述半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

第四生成模块，用于根据所述随机种子和预定互相关伪随机数种类，生成若干第二互相关伪随机数和第二承诺种子；

第五生成模块，用于根据所述若干第二互相关伪随机数和第二承诺种子，生成第二承诺值；

第六生成模块，用于根据所述第二承诺值，生成梅克尔根哈希；

第三发送模块，用于将所述梅克尔根哈希发送至接收方，以使得接收方根据所述梅克尔根哈希和梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

根据本申请实施例的第五方面，提供一种基于半可信硬件的互相关伪随机数的远程获取方法，应用于接收方，包括：

接收发送方发送的加密随机种子；

将所述加密随机种子和选择数发送至半可信硬件，以使得半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行

验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

根据本申请实施例的第六方面，提供一种基于半可信硬件的互相关伪随机数的远程获取装置，应用于接收方，包括：

接收模块，用于接收发送方发送的加密随机种子；

第四发送模块，用于将所述加密随机种子和选择数发送至半可信硬件，以使得半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

第二验证模块，用于根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

根据本申请实施例的第七方面，提供一种电子设备，包括：

一个或多个处理器；

存储器，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如第一方面或第三方面或第五方面任一项所述的方法。

根据本申请实施例的第八方面，提供一种计算机可读存储介质，其上存储有计算机指令，其特征在于，该指令被处理器执行时实现如第一方面或第三方面或第五方面中任一项所述方法的步骤。

本申请的实施例提供的技术方案可以包括以下有益效果：

由上述实施例可知，本申请通过使用半可信硬件，降低了远程传输互相关伪随机数的通讯量，允许发送方以常数级别的通讯量向远程的接收方传输多项式级别数量的互相关伪随机数；根据若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值，通过承诺机制保证半可信硬件输出的正确性，同时也防止了接收方从半可信硬件的输出中获取不应该获得的隐私信息；根据所述第一承诺值和选择数，生成梅克尔证明并使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证，通过

梅克尔树技术，在确保信息传输安全性的同时使得发送方只需要常数级别的通讯量就可以向远程的接收方发送验证信息，而接收方只需要对数级别的计算量和存储空间就可以对可信硬件的输出结果进行验证。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并与说明书一起用于解释本申请的原理。

图 1 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取方法（应用于半可信硬件）的流程图。

图 2 是根据一示例性实施例示出的步骤 S11 的流程图。

图 3 是根据一示例性实施例示出的步骤 S12 的流程图。

图 4 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取装置（应用于半可信硬件）的框图。

图 5 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取方法（应用于发送方）的流程图。

图 6 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取装置（应用于发送方）的框图。

图 7 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取方法（应用于接收方）的流程图。

图 8 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取装置（应用于接收方）的框图。

具体实施方式

这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的装置和方法的例子。

在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本

申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

应当理解，尽管在本申请可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本申请范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

首先对半可信硬件进行解释说明：

在现有技术中，可信硬件可以直接得到所有用户的隐私输入，而当硬件制造商并不可信时，它可以通过嵌入后门的方式窃取用户的隐私信息、更改计算流程。例如，硬件制造商可以在可信硬件生成的密码学测度中以电子隐写术的方法嵌入信息，当远程参与方将该密码学测度转发至硬件制造商提供的第三方认证服务器时，硬件制造商就可以从中获取隐私信息；而当用户调用可信硬件进行计算时，硬件制造商可以随意指定其运行结果。在这样的场景下，可信硬件对于协议参与方仍然起到了保护作用：本地参与方无法通过攻击可信硬件的方式得到远程参与方的隐私输入，也无法控制可信硬件的计算流程、篡改可信硬件的计算结果；但是，硬件制造商具备了获取用户向可信硬件发送的隐私输入和更改可信硬件输出结果的能力，因此，我们将这样的硬件称为半可信硬件。

假设用户 B 想要从用户 A 处获取一系列互相关伪随机数中位于特定位置的某个伪随机数。用户 B 持有一个半可信硬件设备，半可信硬件设备的输出需要经过验证。为实现以上要求，用户 A 和用户 B 可以通过下面展示的基于半可信硬件的互相关伪随机数的远程获取方法来获取特定位置的某个互相关伪随机数。用户 A 作为发送方，用户 B 作为接收方。

在本发明的具体实施过程中，所述半可信硬件可以置于接收方内部，也可与接收方建立高速连接。相对于网络传输高延时、低带宽的特性，将半可信硬件置于接收方内部，或是在半可信硬件与接收方之间建立高速连接，可以让半可信硬件与接收方在低延时、高带宽的信道中进行通信、传输数据，进而提升协议的整体性能。

实施例 1：

图 1 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取方法的流程图，如图 1 所示，该方法应用于半可信硬件中，可以包括以下步骤：

步骤 S11：获取发送方的随机种子和接收方的选择数；

步骤 S12：根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；

步骤 S13：根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；

步骤 S14：根据所述第一承诺值和选择数，生成梅克尔证明；

步骤 S15：将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

由上述实施例可知，本申请通过使用半可信硬件，降低了远程传输互相关伪随机数的通讯量，允许发送方以常数级别的通讯量向远程的接收方传输多项式级别数量的互相关伪随机数；根据若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值，通过承诺机制保证半可信硬件输出的正确性，同时也防止了接收方从半可信硬件的输出中获取不应该获得的隐私信息；根据所述第一承诺值和选择数，生成梅克尔证明并使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证，通过梅克尔树技术，在确保信息传输安全性的同时使得发送方只需要常数级别的通讯量就可以向远程的接收方发送验证信息，而接收方只需要对数级别的计算量和存储空间就可以对可信硬件的输出结果进行验证。

在步骤 S11 的具体实施中，获取发送方的随机种子和接收方的选择数；

具体地，如图 2 所示，此步骤包括以下子步骤：

步骤 S21：接收发送方的加密随机种子和接收方的随机数；

具体地，半可信硬件接收由接收方发送的发送方的加密随机种子和接收方的随机数，其中发送方的加密随机种子由发送方发送给接收方，这一步骤的作用是让用户 A 与用户 B 的半可信硬件能够以间接的方式进行通讯，同时防止用户 B 窃取用户 A 的随机种子。

步骤 S22：根据发送方和半可信硬件的对称密钥，对所述加密随机种子进行

解密；

步骤 S23：对解密得到的结果进行验证；

步骤 S24：若验证通过，则获得发送方的随机种子。

在步骤 S22-S24 的具体实施中，半可信硬件以发送方和半可信硬件的对称密钥为解密密钥，以加密随机种子作为密文，调用发送方使用的带有消息验证码的对称加密算法对应的解密算法进行解密，该解密算法会对消息的完整性进行校验，如果校验通过则输出明文的随机种子。这一步骤的作用是让用户 B 的半可信硬件接收用户 A 发送的随机种子，同时防止用户 B 对随机种子进行篡改。

在步骤 S12 的具体实施中，根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；

具体地，如图 3 所示，此步骤包括以下子步骤：

步骤 S31：将所述随机种子扩展为第一伪随机种子和第二伪随机种子；

具体地，以伪随机函数（pseudorandom function, PRF）作为伪随机数生成器。给定安全参数 c ，伪随机函数是定义在 (K, X, Y) 上的能在基于 c 的多项式时间内被计算的确定性函数 $\text{PRF}: K \times X \rightarrow Y$ ，其中 K 为密钥空间，即所有长度为 c 位的字符串组成的空间， X 为输入空间， Y 为输出空间。伪随机函数与真正的随机函数无法区分，具体地，记所有定义在输入空间 X 和输出空间 Y 上的函数构成的函数空间为 F ，对于 K 中任选的一个密钥 k 和 F 中任选的一个函数 f ，伪随机函数 $\text{PRF}(k, \cdot)$ 与 $f(\cdot)$ 无法在多项式时间内被区分。

以随机种子 s 作为密钥，分别以 0 和 1 作为输入调用伪随机函数，得到 $s1 = \text{PRF}(s, 0)$, $s2 = \text{PRF}(s, 1)$ ，分别作为互相关伪随机数的种子和承诺种子的种子，由伪随机函数的定义可知， $s1$ 和 $s2$ 能够快速被计算得到，且在不知道密钥 s 的情况下， $s1$ 和 $s2$ 与真正的随机数无法区分，因此接收方无法得到 $s1$ 和 $s2$ 。

步骤 S32：根据所述预定互相关伪随机数种类和第一伪随机种子，生成若干第一互相关伪随机数；

具体地，根据指定的互相关伪随机数种类，使用第一伪随机种子 $s1$ 生成第一互相关伪随机数，记作 $m_1, \dots, m_n$ 。例如，对随机不经意传输，计算 $\text{PRF}(s1, i||0)$ 和 $\text{PRF}(s1, i||1)$ 作为第 i 组随机不经意传输，其中“||”表示拼接，通过将 i 从 1 递增至预先指定的数量，即可生成所需的随机不经意传输；对混淆电路，则可以根据所需的优化形式，用第一伪随机种子 $s1$ 分别产生线路标签和混淆种子，再利用混淆种子根据电路定义逐个对线路标签进行加密，产生各个门的混

清表。由于第一伪随机种子 s_1 与真正的随机数无法区分，即使接收方知道互相关伪随机数的生成方式，也无法得知生成的互相关伪随机数的任何信息。

步骤 S33：根据所述第二伪随机种子，生成若干第一承诺种子，其中所述第一承诺种子的数量与所述第一互相关伪随机数的数量相同；

具体地，使用第二伪随机种子 s_2 生成与第一互相关伪随机数数量相对应的第一承诺种子，记作 $r_1, \dots, r_n$ ，其中 $r_i = \text{PRF}(s_2, i)$ 。由于第二伪随机种子 s_2 与真正的随机数无法区分， r_i 是以 s_2 为密钥调用 PRF 生成，因此得到的这些承诺种子与真正的随机数无法区分，接收方无法得知承诺种子的任何信息。

在步骤 S13 的具体实施中，根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；

具体地，可以使用多种承诺机制的实现方式，将 i 从 1 到 n 遍历即可生成所有的承诺值和打开值，其中 n 为所述第一互相关伪随机数的数量。

在一实施例中，可以采用具备碰撞抵抗性质的哈希函数 H 来实现承诺机制，第一承诺值为 $c_i = H(m_i || r_i)$ ，第一打开值为 $d_i = m_i || r_i$ 。由于 H 具备碰撞抵抗性质，一旦半可信硬件给出了承诺值，它就无法找到其他的 m_i' 和 r_i' ，使得 $c_i = H(m_i' || r_i')$ ，因此可以保证半可信硬件无法伪造能够通过承诺机制验证的错误互相关伪随机数；由于 H 是单向函数，即使接收方获得了所有互相关伪随机数的承诺值，也无法从承诺值中获取关于互相关伪随机数的任何信息。进一步的，具备碰撞抵抗性质的哈希函数在现实中有着广泛的高效实现，因此这样设计的效率较高。

在另一实施例中，可以采用基于离散对数假设的 Pederson 承诺机制，预先商定阶数为大素数 q 的乘法群 G ， G 有生成元 g, h ，元组 (g, h, q) 都是公开的，第一承诺值为 $c_i = g^{m_i} h^{r_i} \bmod q$ ，第一打开值为 $d_i = r_i$ 。由于 r_i 与真正的随机数无法区分，接收方无法从承诺值中获取关于互相关伪随机数的任何信息，又由于离散对数假设，一旦半可信硬件给出了承诺值，它就无法找到其他的 m_i' 和 r_i' ，使得 $c_i = g^{m_i'} h^{r_i'} \bmod q$ ，因此可以保证半可信硬件无法伪造能够通过承诺机制验证的错误互相关伪随机数。

在步骤 S14 的具体实施中，根据所述第一承诺值和选择数，生成梅克尔证明；

具体地，根据梅克尔树的定义，使用所有的第一承诺值生成一棵梅克尔树，根据所述选择数生成相应的梅克尔证明。为了方便起见，我们假设所述第一互

相关伪随机数的数量为 2^d ，如果数量不为2的指数个，则用空消息填充至2的指数个。对于按生成顺序排列的 2^d 个第一承诺值，将 i 从1到 2^d 进行遍历，对第 i 个承诺值调用哈希函数 H ，得到第一层梅克尔树节点 $t_i^1 = H(c_i)$ 。对 j 从1到 d 进行遍历，对于按生成顺序排列的 2^{d-j+1} 个第 j 层梅克尔树节点，将 i 从1到 2^{d-j} 进行遍历，对第 $2*i-1$ 个和第 $2*i$ 个第一承诺值调用哈希函数 H ，得到第 $j+1$ 层梅克尔树节点 $t_i^{j+1} = H(t_{2*i-1}^j || t_{2*i}^j)$ 。如此形成一棵深度为 d 、层数为 $d+1$ 的二叉树，称为梅克尔树，第 $d+1$ 层的节点 t_1^{d+1} 被称为梅克尔根哈希。梅克尔证明即为，从选择数对应的第一层梅克尔树节点一直到第 $d+1$ 层的梅克尔树根节点这一条路径上，所有兄弟节点的值，例如，如果选择数为1，则相应的梅克尔证明为 $t_2^1, t_2^2, \dots, t_2^d$ 这些节点的值。

在步骤S15的具体实施中，将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

具体地，所述梅克尔根哈希由发送方根据第二承诺值生成，所述第二承诺值由根据若干第二互相关伪随机数和第二承诺种子生成，所述若干第二互相关伪随机数和第二承诺种子由根据所述随机种子和预定互相关伪随机数种类生成，所述第二互相关伪随机数与第一互相关伪随机数相同，所述第二承诺种子与所述第一承诺种子相同，所述第二承诺值与所述第一承诺值相同。

具体地，接收方首先使用所述梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证。接收方对所述第一承诺值调用哈希函数 H ，作为选择数对应的第一层梅克尔树节点，随后接收方逐个读取所述梅克尔证明中的梅克尔树节点，对目前持有的梅克尔树节点和从梅克尔证明中读取得到的梅克尔树节点调用哈希函数 H ，得到下一层的梅克尔树节点，如此得到梅克尔树根节点值，并与所述梅克尔根哈希进行对比，如果相同则验证通过。例如，如果选择数为1，则对所述第一承诺值调用哈希函数，得到的为第一层梅克尔树节点 t_1^1 ，随后对 i 从1到 d 进行遍历，从梅克尔证明中逐个读取 t_2^i ，并与 t_1^i 一起调用哈希函数，得到 t_1^{i+1} ，最后将 t_1^{d+1} 与所述梅克尔根哈希进行对比，相同则验证通过。在梅克尔树验证通过后，接收方使用所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证，具体验证方法需要与前述的承诺实现方式相对应。

对于基于碰撞抵抗的哈希函数 H 的实现方式, 第一打开值中包含所述选择数对应的互相关伪随机数和所述选择数对应的承诺种子, 接收方验证第一打开值中包含的互相关伪随机数与自己收到的互相关伪随机数是否相同, 验证通过后对第一打开值调用哈希函数 H , 并验证输出结果与第一承诺值是否相同, 如果相同则全部验证过程通过; 对于 Pederson 承诺机制, 接收方计算 $c_i = g^{m_i} h^{r_i} \bmod q$, 并验证 c_i 与第一承诺值是否相同, 如果相同则全部验证过程通过。

与前述的基于半可信硬件的互相关伪随机数的远程获取方法的实施例相对应, 本申请还提供了基于半可信硬件的互相关伪随机数的远程获取装置的实施例。

图 4 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取装置框图。参照图 4, 该装置应用于半可信硬件, 包括

第一获取模块 21, 用于获取发送方的随机种子和接收方的选择数;

第一生成模块 22, 用于根据所述随机种子和预定互相关伪随机数种类, 生成若干第一互相关伪随机数和第一承诺种子;

第二生成模块 23, 用于根据所述若干第一互相关伪随机数和第一承诺种子, 利用承诺机制生成第一承诺值和第一打开值;

第三生成模块 24, 用于根据所述第一承诺值和选择数, 生成梅克尔证明;

第一发送模块 25, 用于将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方, 以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

实施例 2:

图 5 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取方法的流程图, 如图 5 所示, 该方法应用于发送方, 可以包括以下步骤:

步骤 S41: 对所述半可信硬件进行验证并得到与所述半可信硬件共享的对称密钥;

具体地, 按照硬件制造商制定的远程认证规则, 用户 A 向用户 B 发起多轮质询挑战请求, 用户 B 将这些质询挑战请求转发给半可信硬件, 由半可信硬件对这些请求做出回应, 用户 B 将这些回应信息转发给用户 A, 用户 A 通过与硬

件制造商提供的第三方可信服务器通讯，对半可信硬件的真实性和可用性进行验证。

步骤 S42：根据所述对称密钥，对随机种子进行加密并发送至接收方，以使得接收方将发送方的加密随机种子和接收方的选择数发送至半可信硬件，从而使得所述半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

具体地，根据所述对称密钥，使用带有消息认证码的对称加密算法对随机种子进行加密，例如 AES-GCM 算法。随后将加密随机种子发送至接收方，以使得接收方将发送方的加密随机种子和接收方的选择数发送至半可信硬件，从而使得半可信硬件执行步骤 S11-S15 的过程。

步骤 S43：根据所述随机种子和预定互相关伪随机数种类，生成若干第二互相关伪随机数和第二承诺种子；

具体地，生成过程与步骤 S12 相同，此处不作赘述。

步骤 S44：根据所述若干第二互相关伪随机数和第二承诺种子，生成第二承诺值；

具体地，所述第二承诺值的生成过程与步骤 S13 中第一承诺值的生成过程相同，此处不作赘述。

步骤 S45：根据所述第二承诺值，生成梅克尔根哈希；

具体地，根据梅克尔树的定义，使用所有的第二承诺值生成一棵梅克尔树，并根据所述梅克尔树生成梅克尔根哈希。

步骤 S46：将所述梅克尔根哈希发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

具体地，接收方进行验证的过程已在步骤 S15 中进行解释说明，此处不作赘述。

与前述的基于半可信硬件的互相关伪随机数的远程获取方法的实施例相对

应，本申请还提供了基于半可信硬件的互相关伪随机数的远程获取装置的实施例。

图 6 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取装置框图。参照图 6，该装置应用于发送方，包括：

第一验证模块 31，用于对所述半可信硬件进行验证并得到与所述半可信硬件共享的对称密钥；

第二发送模块 32，用于根据所述对称密钥，对随机种子进行加密并发送至接收方，以使得接收方将发送方的加密随机种子和接收方的选择数发送至半可信硬件，从而使得所述半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

第四生成模块 33，用于根据所述随机种子和预定互相关伪随机数种类，生成若干第二互相关伪随机数和第二承诺种子；

第五生成模块 34，用于根据所述若干第二互相关伪随机数和第二承诺种子，生成第二承诺值；

第六生成模块 35，用于根据所述第二承诺值，生成梅克尔根哈希；

第三发送模块 36，用于将所述梅克尔根哈希发送至接收方，以使得接收方根据所述梅克尔根哈希和梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

实施例 3：

图 7 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取方法的流程图，如图 7 所示，该方法应用于接收方，可以包括以下步骤：

步骤 S51：接收发送方发送的加密随机种子；

步骤 S52：将所述加密随机种子和选择数发送至半可信硬件，以使得半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若

干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

步骤 S53: 根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

具体地，步骤 S51-S53 的具体实施已在上文中作出解释说明，此处不再赘述。

与前述的基于半可信硬件的互相关伪随机数的远程获取方法的实施例相对应，本申请还提供了基于半可信硬件的互相关伪随机数的远程获取装置的实施例。

图 8 是根据一示例性实施例示出的一种基于半可信硬件的互相关伪随机数的远程获取装置框图。参照图 8，该装置应用于接收方，包括：

接收模块 41，用于接收发送方发送的加密随机种子；

第四发送模块 42，用于将所述加密随机种子和选择数发送至半可信硬件，以使得半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

第二验证模块 43，用于根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

关于上述实施例中的装置，其中各个模块执行操作的具体方式已经在有关该方法的实施例中进行了详细描述，此处将不做详细阐述说明。

对于装置实施例而言，由于其基本对应于方法实施例，所以相关之处参见方法实施例的部分说明即可。以上所描述的装置实施例仅仅是示意性的，其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，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

来实现本申请方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

实施例 4:

相应的，本申请还提供一种电子设备，包括：一个或多个处理器；存储器，用于存储一个或多个程序；当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如上述的基于半可信硬件的互相关伪随机数的远程获取方法。

实施例 5:

相应的，本申请还提供一种计算机可读存储介质，其上存储有计算机指令，其特征在于，该指令被处理器执行时实现如上述的基于半可信硬件的互相关伪随机数的远程获取方法。

本领域技术人员在考虑说明书及实践这里公开的内容后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本申请的真正范围和精神由下面的权利要求指出。

应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

权 利 要 求 书

1. 一种基于半可信硬件的互相关伪随机数的远程获取方法，其特征在于，应用于半可信硬件，包括：

获取发送方的随机种子和接收方的选择数；

根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；

根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；

根据所述第一承诺值和选择数，生成梅克尔证明；

将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

2. 根据权利要求1所述的方法，其特征在于，获取发送方的随机种子和接收方的选择数，包括：

接收发送方的加密随机种子和接收方的随机数；

根据发送方和半可信硬件的对称密钥，对所述加密随机种子进行解密；

对解密得到的结果进行验证；

若验证通过，则获得发送方的随机种子。

3. 根据权利要求1所述的方法，其特征在于，根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子，包括：

将所述随机种子扩展为第一伪随机种子和第二伪随机种子；

根据所述预定互相关伪随机数种类和第一伪随机种子，生成若干第一互相关伪随机数；

根据所述第二伪随机种子，生成若干第一承诺种子，其中所述第一承诺种子的数量与所述第一互相关伪随机数的数量相同。

4. 一种基于半可信硬件的互相关伪随机数的远程获取装置，其特征在于，应用于半可信硬件，包括：

第一获取模块，用于获取发送方的随机种子和接收方的选择数；

第一生成模块，用于根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；

第二生成模块，用于根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；

第三生成模块，用于根据所述第一承诺值和选择数，生成梅克尔证明；

第一发送模块，用于将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

5. 一种基于半可信硬件的互相关伪随机数的远程获取方法，其特征在于，应用于发送方，包括：

对所述半可信硬件进行验证并得到与所述半可信硬件共享的对称密钥；

根据所述对称密钥，对随机种子进行加密并发送至接收方，以使得接收方将发送方的加密随机种子和接收方的选择数发送至半可信硬件，从而使得所述半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

根据所述随机种子和预定互相关伪随机数种类，生成若干第二互相关伪随机数和第二承诺种子；

根据所述若干第二互相关伪随机数和第二承诺种子，生成第二承诺值；

根据所述第二承诺值，生成梅克尔根哈希；

将所述梅克尔根哈希发送至接收方，以使得接收方根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

6. 一种基于半可信硬件的互相关伪随机数的远程获取装置，其特征在于，应用于发送方，包括：

第一验证模块，用于对所述半可信硬件进行验证并得到与所述半可信硬件共享的对称密钥；

第二发送模块，用于根据所述对称密钥，对随机种子进行加密并发送至接

收方，以使得接收方将发送方的加密随机种子和接收方的选择数发送至半可信硬件，从而使得所述半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

第四生成模块，用于根据所述随机种子和预定互相关伪随机数种类，生成若干第二互相关伪随机数和第二承诺种子；

第五生成模块，用于根据所述若干第二互相关伪随机数和第二承诺种子，生成第二承诺值；

第六生成模块，用于根据所述第二承诺值，生成梅克尔根哈希；

第三发送模块，用于将所述梅克尔根哈希发送至接收方，以使得接收方根据所述梅克尔根哈希和梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

7. 一种基于半可信硬件的互相关伪随机数的远程获取方法，其特征在于，应用于接收方，包括：

接收发送方发送的加密随机种子；

将所述加密随机种子和选择数发送至半可信硬件，以使得半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

8. 一种基于半可信硬件的互相关伪随机数的远程获取装置，其特征在于，应用于接收方，包括：

接收模块，用于接收发送方发送的加密随机种子；

第四发送模块，用于将所述加密随机种子和选择数发送至半可信硬件，以使得半可信硬件获取发送方的随机种子和接收方的选择数；根据所述随机种子和预定互相关伪随机数种类，生成若干第一互相关伪随机数和第一承诺种子；根据所述若干第一互相关伪随机数和第一承诺种子，利用承诺机制生成第一承诺值和第一打开值；根据所述第一承诺值和选择数，生成梅克尔证明；将所述选择数对应的第一互相关伪随机数、第一承诺值、第一打开值和梅克尔证明发送至接收方；

第二验证模块，用于根据发送方发送的梅克尔根哈希和所述梅克尔证明对所述第一承诺值进行验证并根据验证通过后的所述第一承诺值和第一打开值对所述选择数对应的互相关伪随机数进行验证。

9. 一种电子设备，其特征在于，包括：

一个或多个处理器；

存储器，用于存储一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求 1-3 或权利要求 5 或权利要求 7 任一项所述的方法。

10. 一种计算机可读存储介质，其上存储有计算机指令，其特征在于，该指令被处理器执行时实现如权利要求 1-3 或权利要求 5 或权利要求 7 中任一项所述方法的步骤。

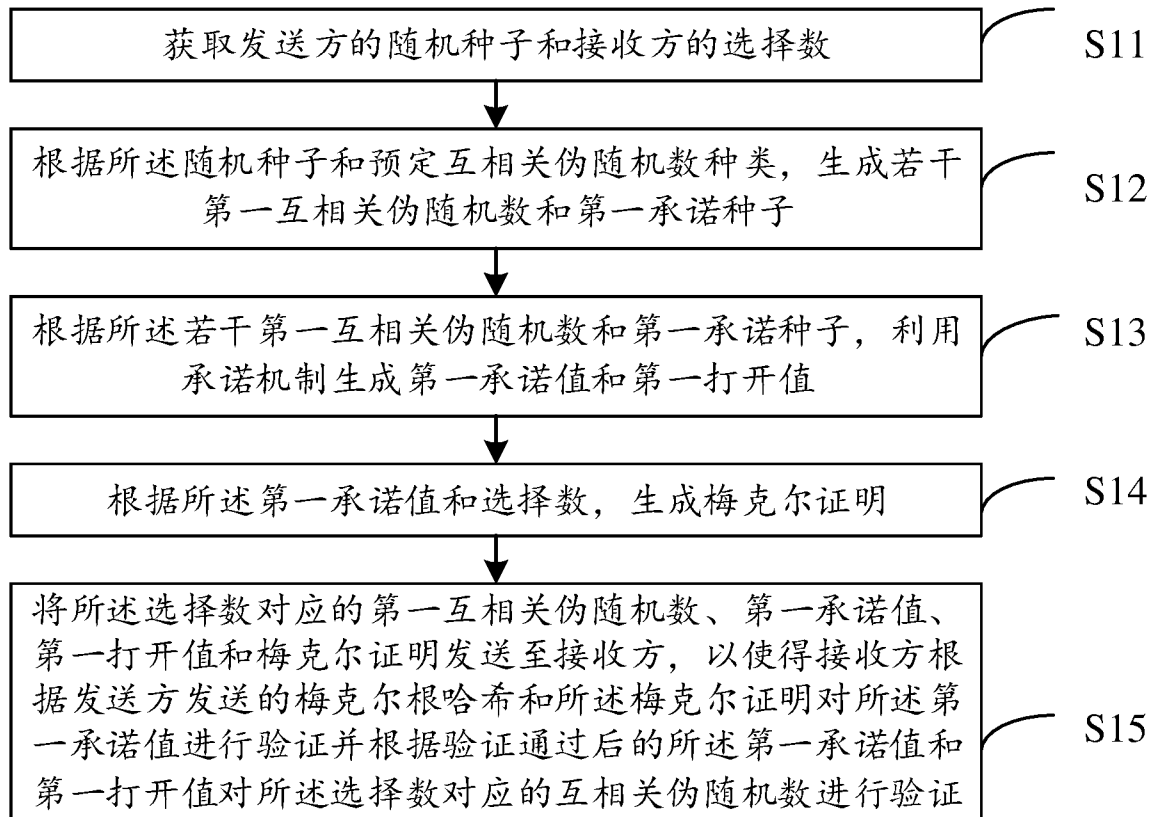


图 1

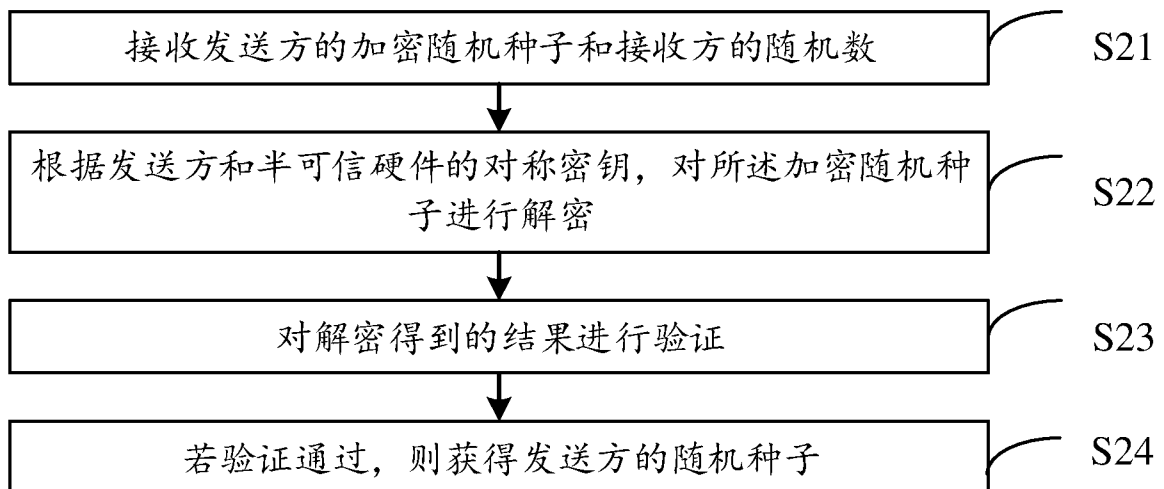


图 2

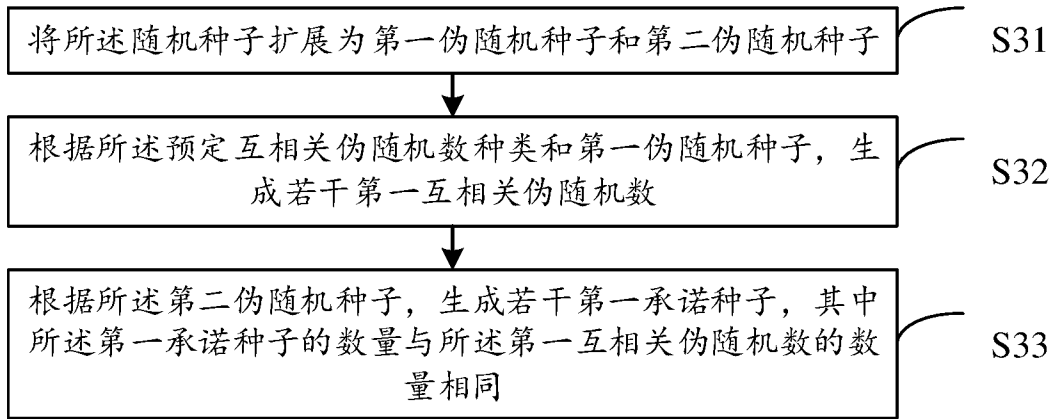


图 3

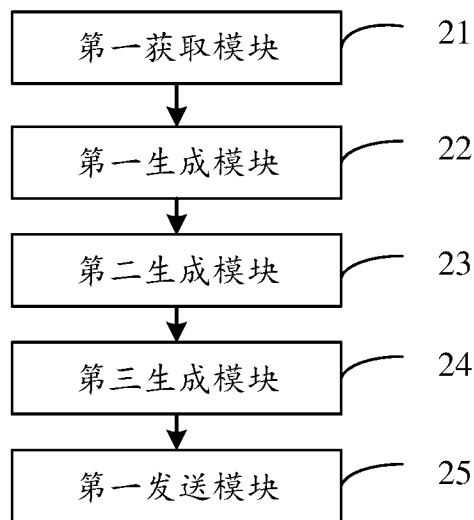


图 4

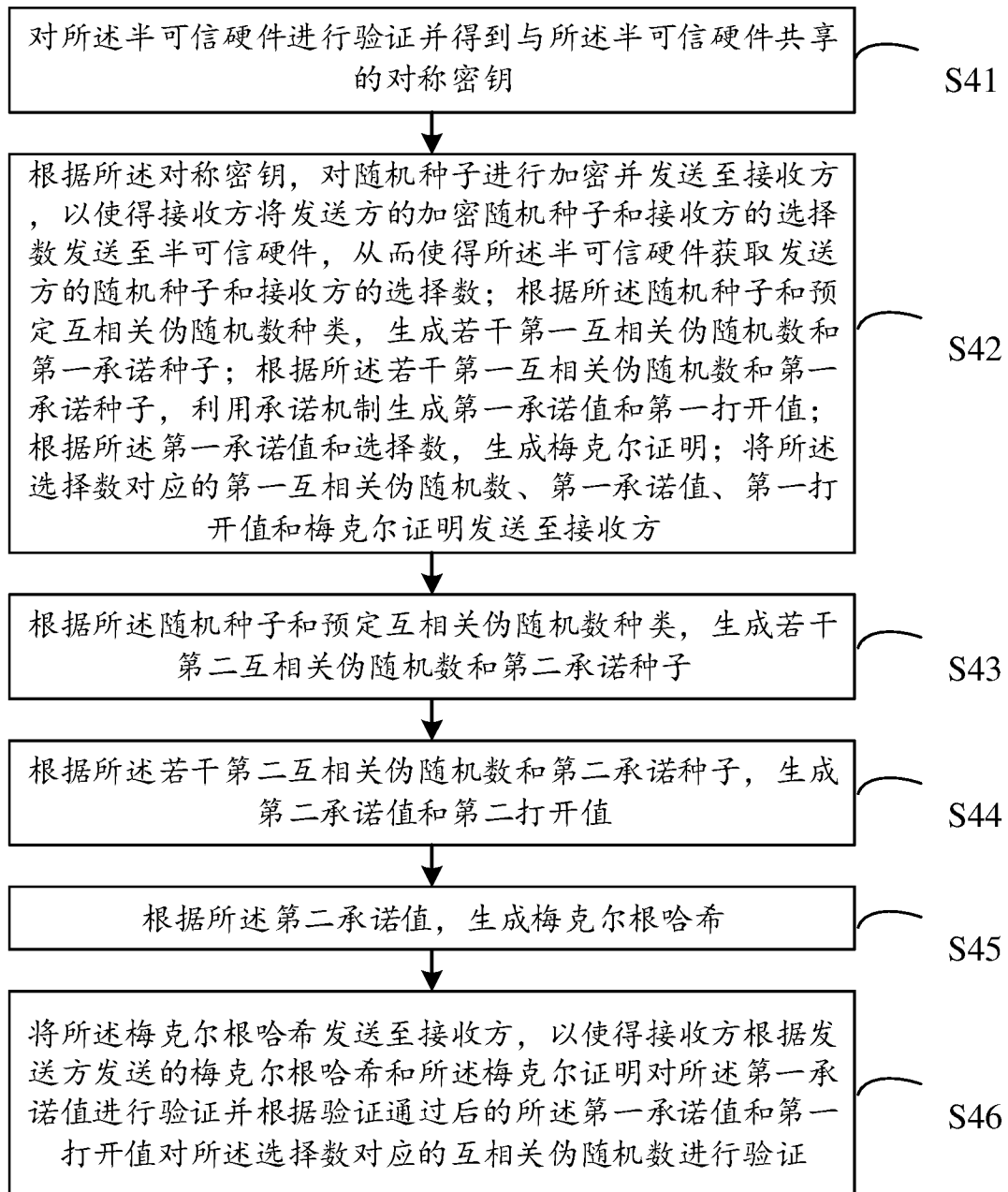


图 5

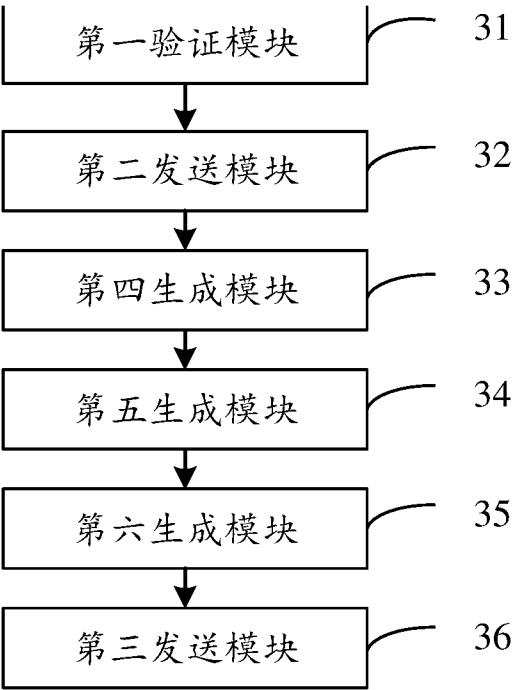


图 6

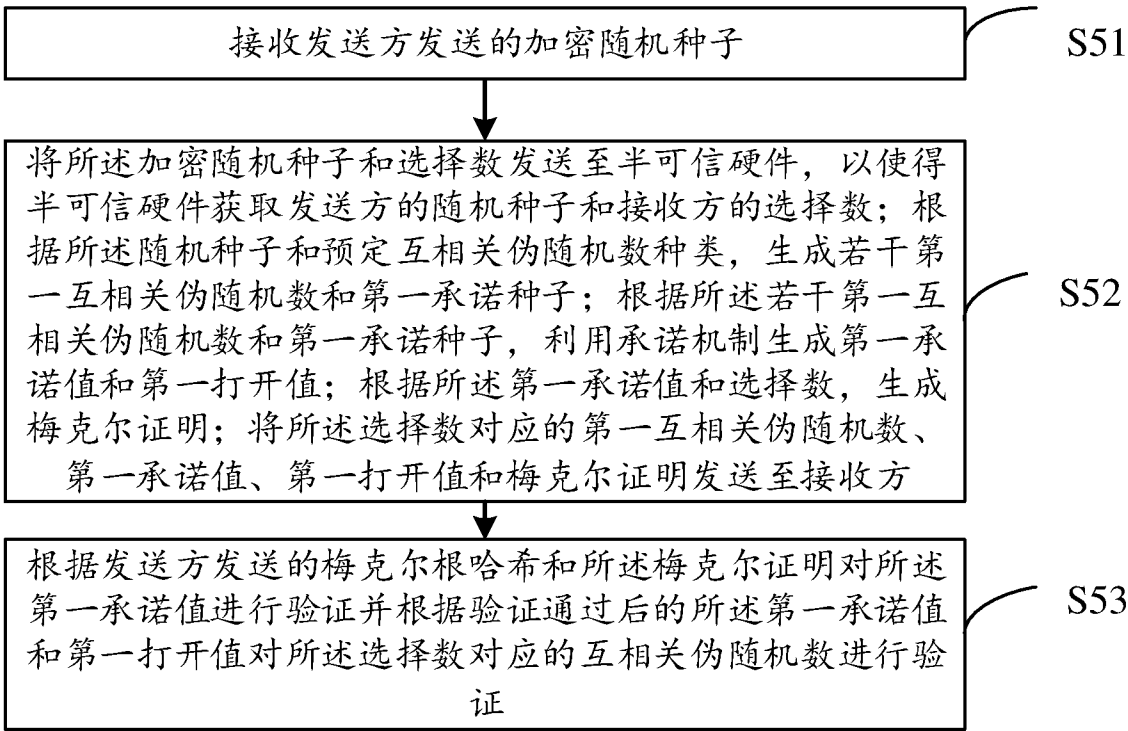


图 7

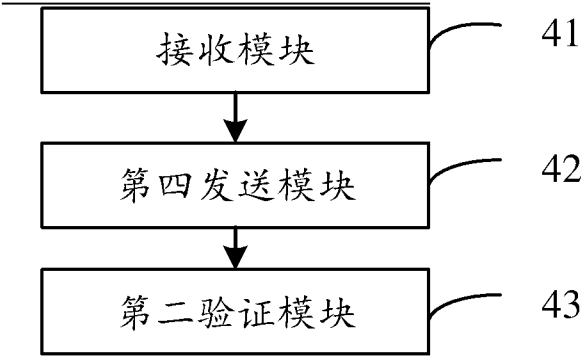


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/141676

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(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)

WPI, EPODOC, CNPAT, CNKI, IEEE: 可信, 硬件, 远程, 随机数, 种子, 承诺, 梅克尔, 默克尔, 验证, trusted, hardware, remote, random number, seed, commit, Merkle, verify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 113489584 A (BEIJING FANRONG TECHNOLOGY CO., LTD.) 08 October 2021 (2021-10-08) description, paragraphs [0004]-[0043] and [0055]-[0085]	1-10
A	US 2021192498 A1 (NCHAIN HOLDINGS LIMITED) 24 June 2021 (2021-06-24) entire document	1-10
A	WO 2016204970 A1 (INTEL CORP.) 22 December 2016 (2016-12-22) entire document	1-10
A	CN 108334553 A (BEIJING ORACLE CHAIN TECHNOLOGY CO., LTD.) 27 July 2018 (2018-07-27) entire document	1-10
A	CN 112631549 A (CHENGZAI (SHANGHAI) INFORMATION TECHNOLOGY CO., LTD.) 09 April 2021 (2021-04-09) entire document	1-10
A	CN 113569294 A (ZHEJIANG UNIVERSITY et al.) 29 October 2021 (2021-10-29) entire document	1-10



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

08 September 2022

Date of mailing of the international search report

21 September 2022

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/CN2021/141676

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	113489584	A	08 October 2021	None			
US	2021192498	A1	24 June 2021	US	2020219097	A1	09 July 2020
				JP	2020532169	A	05 November 2020
				EP	3669315	A1	24 June 2020
				CN	110998630	A	10 April 2020
				JP	2020532170	A	05 November 2020
				WO	2019034984	A1	21 February 2019
				WO	2019034983	A1	21 February 2019
				CN	110998629	A	10 April 2020
				EP	3669314	A1	24 June 2020
WO	2016204970	A1	22 December 2016	EP	3311325	A1	25 April 2018
				US	2016371685	A1	22 December 2016
				CN	107636713	A	26 January 2018
CN	108334553	A	27 July 2018	None			
CN	112631549	A	09 April 2021	None			
CN	113569294	A	29 October 2021	None			

国际检索报告

国际申请号

PCT/CN2021/141676

A. 主题的分类 H04L 9/32 (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)) WPI, EPDOC, CNPAT, CNKI, IEEE: 可信, 硬件, 远程, 随机数, 种子, 承诺, 梅克尔, 默克尔, 验证, trusted, hardware, remote, random number, seed, commit, Merkle, 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
A	CN 113489584 A (北京泛融科技有限公司) 2021年10月8日 (2021 - 10 - 08) 说明书第[0004]-[0043], [0055]-[0085]段	1-10
A	US 2021192498 A1 (NCHAIN HOLDINGS LIMITED) 2021年6月24日 (2021 - 06 - 24) 全文	1-10
A	WO 2016204970 A1 (INTEL CORPORATION) 2016年12月22日 (2016 - 12 - 22) 全文	1-10
A	CN 108334553 A (北京欧链科技有限公司) 2018年7月27日 (2018 - 07 - 27) 全文	1-10
A	CN 112631549 A (橙载上海信息技术有限公司) 2021年4月9日 (2021 - 04 - 09) 全文	1-10
A	CN 113569294 A (浙江大学 等) 2021年10月29日 (2021 - 10 - 29) 全文	1-10
☐ 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 2022年9月8日		国际检索报告邮寄日期 2022年9月21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 郭明华 电话号码 86-(10)-53961414

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/141676

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	113489584	A	2021年10月8日	无	
US	2021192498	A1	2021年6月24日	US	2020219097 A1 2020年7月9日
				JP	2020532169 A 2020年11月5日
				EP	3669315 A1 2020年6月24日
				CN	110998630 A 2020年4月10日
				JP	2020532170 A 2020年11月5日
				WO	2019034984 A1 2019年2月21日
				WO	2019034983 A1 2019年2月21日
				CN	110998629 A 2020年4月10日
				EP	3669314 A1 2020年6月24日
WO	2016204970	A1	2016年12月22日	EP	3311325 A1 2018年4月25日
				US	2016371685 A1 2016年12月22日
				CN	107636713 A 2018年1月26日
CN	108334553	A	2018年7月27日	无	
CN	112631549	A	2021年4月9日	无	
CN	113569294	A	2021年10月29日	无	