(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
2021 年 3 月 4 日 (04.03.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/036183 A1

(51) 国际专利分类号:
H04L 9/06 (2006.01) *H04L 9/32* (2006.01)
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2020/072112

(22) 国际申请日: 2020 年 1 月 15 日 (15.01.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910808822.5 2019年8月29日 (29.08.2019) CN

(71) 申请人: 创新先进技术有限公司 (ADVANCED NEW TECHNOLOGIES CO., LTD.) [—/CN]; 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心, Grand Cayman KY1-9008 (KY)。

(72) 发明人: 余超凡(YU, Chaofan); 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)。 王磊(WANG, Lei); 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)。 周爱辉(ZHOU, Aihui); 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)。 张宁(ZHANG, Ning); 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)。 田洪亮(TIAN, Hongliang); 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)。 肖俊贤(XIAO, Junxian); 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)。

(54) **Title:** METHOD AND APPARATUS FOR CARRYING OUT SECURE MULTI-PARTY COMPUTATION BY MEANS OF CERTIFICATE ISSUING

(54) **发明名称:** 通过证书签发进行多方安全计算的方法及装置

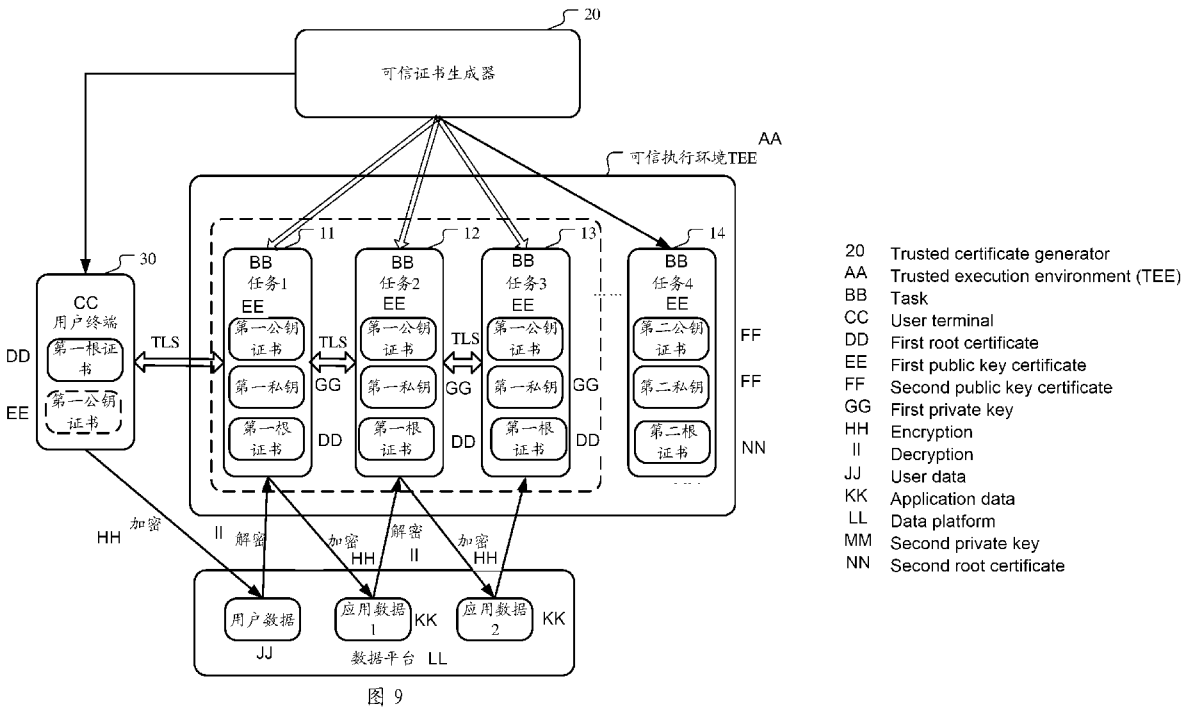

图 9

(57) **Abstract:** Provided in the embodiments of the present description are a method and apparatus for realizing secure multi-party computation by means of certificate distribution. According to the solution, task groups are formed by means of pre-configuration, and group identifiers are allocated. A trusted certificate generator generates a certificate chain and a private key for a group identifier, wherein the certificate chain comprises a root certificate and a corresponding public key certificate, and the public key certificate and a private key match, and constitute a certificate pair. Then, the trusted certificate generator distributes the root certificate and the certificate

WO 2021/036183 A1

[见续页]

(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, 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))。

pair to all trusted computation units which have been authenticated and which operate respective computation tasks corresponding to the group identifier. In addition, the root certificate is also distributed to a user terminal requesting a computation service of the task group. Thus, secure multi-party communication can be carried out between the user terminal with the root certificate and the trusted computation units with the root certificate and the certificate pair by means of a TLS protocol.

(57) 摘要：本说明书实施例提供一种通过分发证书实现多方安全计算的方法和装置。根据该方案，预先配置形成任务分组，并分配组标识。可信证书生成器针对一个组标识生成一套证书链和一个私钥，其中证书链包括根证书和对应的公钥证书，公钥证书与私钥相匹配，构成证书对。然后，可信证书生成器将根证书和证书对分发给经过认证的、运行该组标识对应的各个计算任务的各个可信计算单元。另一方面，还将上述根证书分发给请求该任务分组的计算服务的用户终端。于是，具有根证书的用户终端、具有根证书和证书对的可信计算单元之间，可以通过TLS协议的方式，进行多方安全通信。

通过证书签发进行多方安全计算的方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及分布式计算和安全计算领域，尤其涉及多方安全计算的方法和装置。

背景技术

[02] 为了计算和数据传输的安全，常常使用可信执行环境 TEE（Trusted Execution Environment）中的可信计算单元进行可信计算和数据处理，其中可信计算单元可以保证其中的代码执行是安全的，外界包括操作系统或驱动等都无法获取内部的运行时内存等秘密。例如，可以利用可信计算单元来运行程序代码，执行计算任务，以保证程序代码的执行安全以及与外界的隔离。

[03] 出于可信执行环境的安全需要，在可信计算单元与其他方通信之前，例如与用户终端通信，或与其他可信计算单元通信之前，通常首先通过协商得到一个共同的加密密钥，该密钥除了通信的双方，其他任何人都不可能破解。 双方之间的数据发送均通过该协商得出的密钥来进行加密，如此，我们称为，可信计算单元与其他方建立了可信通道，可以在该可信通道上安全传输保密数据。

[04] 在许多情况下，需要基于多个可信计算单元进行多方安全计算。例如，一些分布式任务需要在多个可信计算单元中执行多个计算任务合作完成，例如需要任务 1，任务 2 和任务 3 共同协作完成。在这样的情况下，用户终端可能需要与运行上述多个计算任务的多个可信计算单元进行通信来获取计算服务，这多个可信计算单元之间也需要彼此通信，以完成计算任务。那么，出于上述安全需要，用户终端与可信计算单元之间，以及多个可信计算单元彼此之间，都需要建立可信通道。如果分别进行密钥协商，分别建立单独的可信通道，那么当可信计算单元数目增多，数量庞大时，多方计算的通信过程会变得复杂繁琐，成本高昂。

[05] 因此，希望能有改进的方案，便于多个参与方进行多方安全计算，提供相应的计算服务。

发明内容

[06] 本说明书一个或多个实施例描述了多方安全计算的方法及装置，其中通过为运行任务分组中各个计算任务的各个可信计算单元和请求该任务分组的计算服务的用户终端分发证书链中的对应证书，确保用户终端与各个可信计算单元之间进行安全的多方通信和计算。

[07] 根据第一方面，提供了一种获取证书以进行多方安全计算的方法，通过运行第一计算任务的第一计算单元执行，所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括至少一个其他计算任务；所述方法包括：

[08] 向可信证书生成器发送第一证书请求，所述第一证书请求包括所述第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对第一计算单元进行可信认证，并包括所述第一计算任务的第一代码哈希；

[09] 从所述可信证书生成器接收第一证书报告，所述第一证书报告包括针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书以及对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对；

[10] 以所述第一计算单元作为提供所述第一计算任务的计算服务的 TLS 服务端，将所述第一证书对设置为所述 TLS 服务端的证书对，并且以所述第一计算单元作为与所述至少一个其他计算任务连接的 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信根证书。

[11] 在第一方面的一个实施例中，所述第一计算单元实现为可信围圈 Enclave。

[12] 根据第一方面的一个实施例，在向可信证书生成器发送第一认证请求之前，方法还包括：

[13] 生成第一计算单元的单元报告文件，所述单元报告文件包括所述第一代码哈希，以及所述第一计算单元的签名信息；

[14] 将所述单元报告文件发送至第三方认证机构，以获得认证结果文件，所述认证结果文件包含所述第三方认证机构的签名信息；

[15] 将所述认证结果文件作为所述第一认证信息包含在所述第一证书请求中。

[16] 根据第一方面的另一实施例，在向可信证书生成器发送第一认证请求之前，方法还包括：

[17] 生成第一计算单元的单元报告文件，所述单元报告文件包括所述第一代码哈希，所述第一计算单元的签名信息；

[18] 将所述单元报告文件作为所述第一认证信息包含在所述第一证书请求中。

[19] 根据一种实施方式，在向可信证书生成器发送第一认证请求之前，第一计算单元与所述可信证书生成器进行密钥协商，建立可信通道，所述可信通道用于发送所述第一证书请求，以及接收所述第一证书报告。

[20] 根据第二方面，提供了一种为计算单元分发证书的方法，通过可信证书生成器执行，所述方法包括：

[21] 从运行第一计算任务的第一计算单元接收第一证书请求，所述第一证书请求包括第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对所述第一计算单元进行认证，且包括所述第一计算任务的第一代码哈希；

[22] 根据所述第一认证信息对所述第一计算单元进行认证；

[23] 在认证通过的情况下，根据所述第一代码哈希判断所述第一计算任务是否属于所述第一任务分组；

[24] 在确认所述第一计算任务属于所述第一任务分组的情况下，获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对；

[25] 向所述第一计算单元发送第一证书报告，所述第一证书报告包括所述第一根证书和所述第一证书对，使得所述第一计算单元以自身为提供计算服务的 TLS 服务端和与其他计算任务连接的 TLS 客户端，将所述第一证书对设置为 TLS 服务端的证书对，将所述第一根证书设置为 TLS 客户端的可信根证书。

[26] 根据第二方面的一个实施例，所述第一认证信息为经过第三方认证机构认证的认证结果文件，该认证结果文件包含该第三方认证机构的签名信息；在这样的情况下，对所述第一计算单元进行认证包括：

[27] 校验所述签名信息，在校验成功的情况下，确定所述第一计算单元认证通过。

[28] 根据第二方面的另一实施例，所述第一认证信息为所述第一计算单元生成的单元报告文件，所述单元报告文件包括所述第一代码哈希，以及所述第一计算单元的签名信息；在这样的情况下，对所述第一计算单元进行认证包括：

[29] 将所述单元报告文件发送至第三方认证机构，以获得认证结果文件，所述认证结果文件包含所述第三方认证机构的签名信息；

[30] 校验所述签名信息，在校验成功的情况下，确定所述第一计算单元认证通过。

[31] 根据第二方面的一种实施方式，在从运行第一计算任务的第一计算单元接收第一证书请求之前，所述可信证书管理器从配置管理器接收第一生成命令，所述第一生成命令包括，所述第一组标识，以及与所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；针对所述第一组标识，生成所述第一证书链和第一私钥。

[32] 根据第二方面的一个实施例，通过以下方式判断所述第一计算任务是否属于所述第一任务分组：

[33] 获取预先配置的、与所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；

[34] 判断所述第一代码哈希是否位于所述第一哈希列表中，如果是，则确认所述第一计算任务属于所述第一任务分组。

[35] 根据第二方面的一个具体实施例，所述第一公钥证书包括针对所述第一组标识生成的第一公钥，以及所述可信证书生成器签名的第一签名信息，其中所述第一公钥和所述第一私钥构成密钥对；所述第一根证书中包括针对所述第一组标识生成的第二公钥，以及所述可信证书生成器自签名的第二签名信息；所述第二公钥用于对所述第一签名信息和第二签名信息进行校验。

[36] 根据第二方面的另一具体实施例，所述第一公钥证书包括针对所述第一组标识生成的第一公钥，以及所述可信证书生成器签名的第一签名信息，其中所述第一公钥和所述第一私钥构成密钥对；所述第一根证书包括所述第一公钥，以及所述可信证书生成器自签名的第二签名信息；所述第一公钥用于对所述第一签名信息和第二签名信息进行校验。

[37] 根据第二方面的一种实施方式，在从运行第一计算任务的第一计算单元接收第一证书请求之前，可信证书生成器与所述第一计算单元进行密钥协商，建立可信通道，所述可信通道用于接收所述第一证书请求，以及发送所述第一证书报告。

[38] 根据第三方面，提供了一种获取证书以进行多方安全计算的方法，通过用户终端执行，所述方法包括：

[39] 向可信证书生成器发送第二证书请求，所述第二证书请求中包括，期望连接的第一任务分组的第一组标识；

[40] 从所述可信证书生成器接收第二证书报告，所述第二证书报告至少包括针对所述第一组标识生成的第一证书链中的第一根证书，所述第一证书链还包括与所述第一根证书对应的第一公钥证书；所述第一公钥证书和匹配的第一私钥构成第一证书对，被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元；

[41] 以所述用户终端为 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

[42] 根据第三方面的一种实施方式，在向可信证书生成器发送第二证书请求之前，还包括：

[43] 获取所述可信证书生成器的第二认证信息；

[44] 根据所述第二认证信息，对所述可信证书生成器进行认证。

[45] 根据一个进一步的实施例，所述第二认证信息为经过第三方认证机构认证的认证结果文件，该认证结果文件包含该第三方认证机构的签名信息；

[46] 所述根据所述第二认证信息，对所述可信证书生成器进行认证包括：

[47] 校验所述签名信息，在校验成功的情况下，确定所述可信证书生成器认证通过。

[48] 根据另一个进一步的实施例，所述第二认证信息为所述可信证书生成器生成的报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息；

[49] 所述根据所述第二认证信息，对所述可信证书生成器进行认证包括：

[50] 将所述报告文件发送至第三方认证机构，以获得认证结果文件，所述认证结果文件包含所述第三方认证机构的签名信息；

[51] 校验所述签名信息，在校验成功的情况下，确定所述证书生成器认证通过。

[52] 根据第三方面的一种实施方式，所述第二证书报告还包括，所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；

[53] 在将所述第一根证书设置为所述 TLS 客户端的可信根证书之前，所述方法还包括，

判断所述第一哈希列表是否符合预期。

[54] 根据第三方面的一个实施例，在将所述第一根证书设置为所述 TLS 客户端的可信根证书之后，还包括，

[55] 与所述至少一个计算单元进行 TLS 握手，建立 TLS 可信通道；

[56] 通过 TLS 可信通道，从所述至少一个计算单元获取所述第一任务分组的计算服务。

[57] 根据第三方面的一个实施例，所述第二证书报告还包括，所述第一公钥证书，所述方法还包括：利用所述第一公钥证书加密所述用户终端的用户数据，并将加密的用户数据存入数据平台，以供所述至少一个计算单元利用所述第一证书对进行解密获取。

[58] 根据第四方面，提供了一种为用户终端分发证书的方法，通过可信证书生成器执行，所述方法包括：

[59] 接收用户终端发送的第二证书请求，所述第二证书请求中包括，所述用户终端期望连接的第一任务分组的第一组标识；

[60] 获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和与其对应的第一公钥证书，所述第一公钥证书与所述第一私钥匹配，构成第一证书对；至少所述第一证书对被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元；

[61] 向所述用户终端发送第二证书报告，所述第二证书报告至少包括所述第一根证书，以使得所述用户终端以自身为 TLS 客户端，将所述第一根证书作为 TLS 客户端的可信根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

[62] 根据第四方面的一种实施方式，在接收用户终端发送的第二证书请求之前，还包括：

[63] 响应于所述用户终端的认证请求，向所述用户终端提供第二认证信息，以供所述用户终端进行认证。

[64] 根据一个进一步的实施例，向所述用户终端提供第二认证信息包括：

[65] 生成报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息；

[66] 将所述报告文件发送至第三方认证机构，以获得认证结果文件，所述认证结果文

件包含所述第三方认证机构的签名信息;

[67] 将所述认证结果文件作为所述第二认证信息提供给所述用户终端。

[68] 根据另一个进一步的实施例，向所述用户终端提供第二认证信息包括:

[69] 生成报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息;

[70] 将所述报告文件作为所述第二认证信息提供给所述用户终端。

[71] 根据第四方面的一个实施例，所述第二证书报告还包括，所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希。

[72] 根据第四方面的一个实施例，所述第二证书报告还包括所述第一公钥证书，以使得所述用户终端利用所述第一公钥证书加密用户数据。

[73] 根据第五方面，提供了一种通过数字证书进行多方安全计算的方法，通过运行第一计算任务的第一计算单元执行，其中:

[74] 所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括第二计算单元所运行的第二计算任务;

[75] 所述第一计算单元预先被分发有针对所述第一任务分组生成的第一证书对和第一根证书，所述第一证书对包括第一公钥证书和匹配的第一私钥，所述第一公钥证书和第一根证书构成第一证书链;

[76] 并且,所述第一计算单元被配置作为提供所述第一计算任务的计算服务的第一 TLS 服务端，该第一 TLS 服务端以所述第一证书对作为其证书对; 所述第一计算单元还被配置作为至少与所述第二计算单元连接的第一 TLS 客户端，所述第一 TLS 客户端以所述第一根证书作为其可信根证书;

[77] 所述方法包括:

[78] 利用所述第一 TLS 服务端与作用为第二 TLS 客户端的用户终端进行 TLS 握手，建立第一 TLS 可信通道;其中所述第二 TLS 客户端将所述第一根证书作为其可信根证书;

[79] 通过所述第一 TLS 可信通道接收第一用户数据;

[80] 对所述第一用户数据进行第一处理，得到第一应用数据;

[81] 利用所述第一 TLS 客户端与作用为第二 TLS 服务端的第二计算单元进行 TLS 握手，

建立第二 TLS 可信通道；其中所述第二 TLS 服务端将所述第一证书对作为其证书对；

[82] 通过所述第二 TLS 可信通道将所述第一应用数据传送给所述第二计算单元。

[83] 在第五方面的一个实施例中，所述方法还包括，从数据平台读取第二用户数据，所述第二用户数据由所述用户终端使用所述第一公钥证书加密产生；

[84] 使用所述第一私钥解密所述第二用户数据。

[85] 在第五方面的一种实施方式中，所述方法还包括：

[86] 生成第二应用数据；

[87] 使用所述第一公钥证书加密所述第二应用数据，得到第二加密应用数据；

[88] 将所述第二加密应用数据存入数据平台，以供所述第二计算单元利用所述第一证书对进行解密获取。

[89] 根据第六方面，提供了一种获取证书以进行多方安全计算的装置，部署在运行第一计算任务的第一计算单元中，所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括至少一个其他计算任务；所述装置包括：

[90] 第一证书请求模块，配置为向可信证书生成器发送第一证书请求，所述第一证书请求包括所述第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对第一计算单元进行可信认证，并包括所述第一计算任务的第一代码哈希；

[91] 第一报告接收模块，配置为从所述可信证书生成器接收第一证书报告，所述第一证书报告包括针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书以及对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对；

[92] 第一设置模块，配置为以所述第一计算单元作为提供所述第一计算任务的计算服务的 TLS 服务端，将所述第一证书对设置为所述 TLS 服务端的证书对；并且以所述第一计算单元作为与所述至少一个其他计算任务连接的 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信根证书。

[93] 根据第七方面，提供了一种为计算单元分发证书的装置，部署在可信证书生成器中，所述装置包括：

[94] 第一请求接收模块，配置为从运行第一计算任务的第一计算单元接收第一证书请求，所述第一证书请求包括第一任务分组的第一组标识，以及第一认证信息，所述第一

认证信息用于对所述第一计算单元进行认证，且包括所述第一计算任务的第一代码哈希；

[95] 单元认证模块，配置为根据所述第一认证信息对所述第一计算单元进行认证；

[96] 分组判断模块，配置为在认证通过的情况下，根据所述第一代码哈希判断所述第一计算任务是否属于所述第一任务分组；

[97] 证书获取模块，配置为在确认所述第一计算任务属于所述第一任务分组的情况下，获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对；

[98] 第一报告发送模块，配置为向所述第一计算单元发送第一证书报告，所述第一证书报告包括所述第一根证书和所述第一证书对，使得所述第一计算单元以自身为提供计算服务的 TLS 服务端和与其他计算任务连接的 TLS 客户端，将所述第一证书对设置为 TLS 服务端的证书对，将所述第一根证书设置为 TLS 客户端的可信根证书。

[99] 根据第八方面，提供了一种获取证书以进行多方安全计算的装置，部署在用户终端中，所述装置包括：

[100] 第二请求发送模块，配置为向可信证书生成器发送第二证书请求，所述第二证书请求中包括，期望连接的第一任务分组的第一组标识；

[101] 第二报告接收模块，配置为从所述可信证书生成器接收第二证书报告，所述第二证书报告至少包括针对所述第一组标识生成的第一证书链中的第一根证书，所述第一证书链还包括与所述第一根证书对应的第一公钥证书；所述第一公钥证书和匹配的第一私钥构成第一证书对，被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元；

[102] 第二配置模块，配置为以所述用户终端为 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

[103] 根据第九方面，提供了一种为用户终端分发证书的装置，部署在可信证书生成器中，所述装置包括：

[104] 第二请求接收模块，配置为接收用户终端发送的第二证书请求，所述第二证书请求中包括，所述用户终端期望连接的第一任务分组的第一组标识；

[105] 证书获取模块，配置为获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和与其对应的第一公钥证书，所述第一公钥证书与所述第一私钥匹配，构成第一证书对；至少所述第一证书对被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元；

[106] 第二报告发送模块，配置为向所述用户终端发送第二证书报告，所述第二证书报告至少包括所述第一根证书，以使得所述用户终端以自身为 TLS 客户端，将所述第一根证书作为 TLS 客户端的可信根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

[107] 根据第十方面，提供了一种通过数字证书进行多方安全计算的装置，部署在运行第一计算任务的第一计算单元中，其中：

[108] 所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括第二计算单元所运行的第二计算任务；

[109] 所述第一计算单元预先被分发有针对所述第一任务分组生成的第一证书对和第一根证书，所述第一证书对包括第一公钥证书和匹配的第一私钥，所述第一公钥证书和第一根证书构成第一证书链；

[110] 并且，所述第一计算单元被配置作为提供所述第一计算任务的计算服务的第一 TLS 服务端，该第一 TLS 服务端以所述第一证书对作为其证书对；所述第一计算单元还被配置作为至少与所述第二计算单元连接的第一 TLS 客户端，所述第一 TLS 客户端以所述第一根证书作为其可信根证书；

[111] 所述装置包括：

[112] 第一握手模块，配置为利用所述第一 TLS 服务端与作用为第二 TLS 客户端的用户终端进行 TLS 握手，建立第一 TLS 可信通道；其中所述第二 TLS 客户端将所述第一根证书作为其可信根证书；

[113] 数据接收模块，配置为通过所述第一 TLS 可信通道接收第一用户数据；

[114] 数据处理模块，配置为对所述第一用户数据进行第一处理，得到第一应用数据；

[115] 第二握手模块，配置为利用所述第一 TLS 客户端与作用为第二 TLS 服务端的第二计算单元进行 TLS 握手，建立第二 TLS 可信通道；其中所述第二 TLS 服务端将所述第一证书对作为其证书对；

[116] 数据发送模块，配置为通过所述第二 TLS 可信通道将所述第一应用数据传送给所述第二计算单元。

[117] 根据第十一方面，提供了一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行第一方面到第五方面的方法。

[118] 根据第十二方面，提供了一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现第一方面到第五方面的方法。

[119] 根据本说明书实施例提供的方法和装置，通过可信证书生成器生成并分发证书，实现安全认证和校验，便于用户终端与可信计算单元之间进行多方安全通信和计算。具体的，预先将计算任务进行分组，形成任务分组。可信证书生成器通过组标识区分不同任务分组，针对一个组标识生成一套证书链和一个私钥，其中证书链中包括根证书和对应的公钥证书，公钥证书与私钥相匹配，构成一个证书对。然后，可信证书生成器将该上述根证书和证书对分发给经过认证的、运行该组标识对应的各个计算任务的各个可信计算单元。于是，运行同一任务分组中各个计算任务的多个可信计算单元会获得同样的根证书和证书对。另一方面，可信证书生成器将上述根证书分发给请求该任务分组的计算服务的用户终端。于是，具有根证书的用户终端、具有根证书和证书对的可信计算单元之间，可以通过 TLS 协议的方式，进行多方安全通信。

附图说明

[120] 为了更清楚地说明本发明实施例的技术方案，下面将对实施例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发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其它的附图。

[121] 图 1 为本说明书披露的一个实施例的实施场景示意图；

[122] 图 2 示出根据一个实施例通过配置管理器进行分组配置的过程示意图；

[123] 图 3 示出一个示例中的数字证书的证书链和证书对；

[124] 图 4 示出根据一个实施例为计算单元签发证书的过程示意图；

[125] 图 5 示出在一个实施例中的第一证书链；

[126] 图 6 示出在另一实施例中的第一证书链;

[127] 图 7 示出在执行图 4 所示的过程之后各个计算单元的状态;

[128] 图 8 示出根据一个实施例为用户终端分发证书的过程示意图;

[129] 图 9 示出在执行图 4 和图 8 所示的过程之后系统的状态;

[130] 图 10 示出在一个实施例中进行多方安全计算的方法流程图;

[131] 图 11 示出在一个实施例中部署在第一计算单元中的获取证书的装置的示意性框图;

[132] 图 12 示出在一个实施例中为计算单元分发证书的装置的示意性框图;

[133] 图 13 示出在一个实施例中部署在用户终端中的获取证书的装置的示意性框图;

[134] 图 14 示出在一个实施例中为用户终端分发证书的装置的示意性框图;

[135] 图 15 示出在一个实施例中部署在第一计算单元中的进行多方计算的装置的示意性框图。

具体实施方式

[136] 下面结合附图，对本说明书提供的方案进行描述。

[137] 图 1 为本说明书披露的一个实施例的实施场景示意图。如图所示，可以通过可信执行环境 TEE 中的可信计算单元执行所需的计算任务。可信计算单元可以是具有一定隔离能力从而保证计算安全性的计算模块或计算设备，例如是可信的计算围圈 Enclave，比如采用 SGX 或 Trust Zone 等技术而实现。例如，根据 SGX 技术，通过提供一系列 CPU 指令码，允许用户代码创建具有高访问权限的私有内存区域而形成计算围圈 Enclave。其他应用程序，包括操作系统 OS，BIOS 系统，虚拟机系统等，均不能访问围圈 Enclave 中的数据，也就不能窥探和篡改其中应用程序的状态和数据。因此，通过例如围圈 Enclave 的可信计算单元执行计算任务，可以保证任务代码与外界的隔离，确保任务程序的运行安全。

[138] 在图 1 的示例中，各个可信计算单元（例如各个围圈 Enclave）分别执行各自的计算任务，例如，可信计算单元 11,12,13,14 分别执行不同的计算任务，任务 1，任务 2，任务 3 和任务 4。可以理解，这仅仅是一个示例。还可以存在其他可信计算单元执行其他任务，也可以存在多个可信计算单元执行同一任务的多个副本。

[139] 在分布式任务的情况下，会需要运行多个计算任务的多个可信计算单元共同协作，

进行多方计算。例如，在一个例子中，假定需要任务 1，任务 2 和任务 3 协同计算，共同提供一套计算服务。

[140] 如前所述，由于可信执行环境的安全需要，这就要求在用户终端与各个可信计算单元，以及各个可信计算单元之间，均建立可信通道才能进行数据的传输和交换。

[141] 为了便于在分布式任务的场景下进行多方安全计算，根据本说明书的一个实施例，预先为各个计算任务进行分组，将执行同一分布式任务的计算任务划分到同一分组。然后，采用可信证书生成器 20 基于任务分组来生成数字证书并管理数字证书，通过证书的生成和分发管理，促使用户终端和多个可信计算单元进行多方安全计算。

[142] 具体地，可信证书生成器 20 根据组标识区分各个任务分组。针对某一任务分组，例如称为第一任务分组，可信证书生成器为其生成一套证书链和一个私钥，其中证书链中包括公钥证书和对应的根证书，公钥证书与上述私钥相匹配，构成一个证书对。然后，可信证书生成器将该根证书和证书对分发给经过认证的、运行该第一任务分组中各个计算任务的各个可信计算单元。于是，运行同一任务分组中各个计算任务的多个可信计算单元会获得同样的证书对和根证书。另一方面，可信证书生成器将上述证书链中的根证书分发给请求该第一任务分组的计算服务的用户终端 30。

[143] 接下来，对于运行第一任务分组中某个计算任务的某个可信计算单元，可以将其作为提供计算服务的传输层安全协议 TLS 服务端，将上述证书对设置为该 TLS 服务端的证书对，还可以将该可信计算单元作为与同一任务分组中其他计算单元连接的 TLS 客户端，将上述根证书设置为 TLS 客户端的可信根证书。

[144] 对于请求该第一任务分组的计算服务的用户终端，可以将其作为 TLS 客户端，将分发给用户终端的根证书设置为 TLS 客户端的可信根证书。

[145] 由于上述证书对和根证书构成一套证书链，而 TLS 客户端只会与拥有同一证书链中对应证书对的 TLS 服务端握手，于是保证了，请求第一任务分组的用户终端，只会与运行第一任务分组中各计算任务的可信计算单元进行握手，且运行第一任务分组中各计算任务的各个可信计算单元之间彼此可以进行握手，建立可信通道，从而实现多方安全计算。

[146] 下面描述以上构思的具体实现方式。

[147] 首先，在配置阶段，为各个计算任务设置分组，使得执行同一分布式任务的多个计算任务构成一个任务分组。对于形成的任务分组，为其分配组标识。于是，每个任务

分组对应具有一个组标识。之后，使得各个计算任务获知其所属的任务分组的组标识，此外，还使得可信证书生成器获知分组信息，以便针对各个分组生成证书链。

[148] 在一个实施例中，通过配置管理器进行上述任务分组配置，并由配置管理器将分组配置信息通知可信证书生成器以及各个计算任务。

[149] 图 2 示出根据一个实施例通过配置管理器进行分组配置的过程示意图。如图所示，在步骤 201，配置管理器可以接收配置人员进行的分组配置请求或配置操作，其中指示将多个计算任务划归为一个任务分组，简单起见称为第一任务分组。上述配置人员可以是配置管理器的管理员，分布式计算系统的管理员，甚至可以是请求计算服务的用户。在接收到上述配置请求或配置操作后，配置管理器为划归形成的第一任务分组分配组标识，称为第一组标识，并建立该第一组标识与第一任务分组中包含的上述多个计算任务的对应关系。

[150] 具体的，在一个例子中，假定图 1 中的三个计算任务，任务 1，任务 2 和任务 3 用于执行同一分布式任务，那么配置人员可以在配置管理器中设定，将该三个计算任务划归为一个任务分组。于是，配置管理器为该任务分组分配组标识 GID1，并建立组标识 GID1 与任务 1，任务 2 和任务 3 的对应关系。

[151] 接着，在步骤 202，配置管理器将上述第一组标识通知给第一任务分组中包含的多个计算任务。例如，将组标识 GID1 分别通知给任务 1，任务 2 和任务 3。

[152] 另一方面，在步骤 203，配置管理器向可信证书生成器发出配置通知，该通知中包括，第一组标识，以及与第一组标识对应的第一哈希列表，该第一哈希列表包括属于第一任务分组的所有计算任务的代码哈希。

[153] 延续上例，对于任务 1，任务 2 和任务 3 形成的任务分组 GID1，配置管理器可以形成与组标识 GID1 对应的哈希列表 1，其中包括，上述三个计算任务，任务 1，任务 2 和任务 3 各自的代码哈希 H1，H2 和 H3。于是，配置管理器可以向可信证书生成器发出针对上述任务分组的配置通知，其中包括组标识 GID1，以及对应的哈希列表 1:{ H1，H2，H3}。

[154] 可以理解，步骤 202 和 203 可以以任意顺序执行。

[155] 在一个实施例中，可信证书生成器在接收到上述配置通知后，记录其中第一组标识和第一哈希列表的对应关系，以用于后续验证，并在后续证书签发阶段生成对应的证书。

[156] 更优选的，在另一实施例中，可信证书生成器将上述配置通知作为证书生成请求，相应地生成证书。具体的，在步骤 204，可信证书生成器判断是否存在与第一组标识对应的证书链；如果存在，则拒绝生成请求，不再生成；如果没有，则针对该第一组标识，生成第一证书链和第一私钥，其中第一证书链包括第一根证书和对应的第一公钥证书，第一公钥证书与第一私钥相匹配，构成第一证书对。

[157] 下面对证书链和证书对进行简单的介绍。

[158] 数字证书是由证书认证机构 CA（Certificate Authority）签发的、用来认证持有者身份合法性的电子文档，以防止第三方的冒充行为。一般地，数字证书中包括，持有者信息，持有者公钥，签发者信息，以及签发者的签名。由于数字证书中包含为持有者生成的公钥，因此也将这样的数字证书称为公钥证书。相应的，签发机构还会生成一个与持有者公钥对应匹配的私钥，该公钥和私钥构成非对称加密的密钥对。此时，公钥证书与私钥构成一个证书对。

[159] 图 3 示出一个示例中的数字证书的证书链和证书对。假定其中的数字证书 33 是签发机构 CA1 颁发给持有者 U1 的公钥证书，那么证书 33 中包括，持有者 U1 信息，持有者 U1 公钥 K1，签发者 CA1 信息，以及签发者 CA1 的签名。 签发者 CA1 还会生成与公钥 K1 对应的私钥 k1，于是证书 33 和私钥 k1 构成证书对。

[160] 当验证者想要验证该证书 33 时，可以利用签发者 CA1 的公钥进行验证。然而，如果验证者对于签发者 CA1 不够信任的话，那么就需要向上追溯，获取 CA1 的证书，来验证 CA1 是否合法可信。于是，可以向上追溯到证书 32，该证书 32 是签发机构 CA2 颁发给 CA1 的证书，其中包括，CA1 信息（此时 CA1 是证书持有者），CA1 公钥，签发者 CA2 信息，签发者 CA2 的签名。验证者可以利用证书 32 中的 CA1 公钥，验证证书 33 中的 CA1 签名。然而，如果验证者对于签发机构 CA2 仍然不够信任的话，就需要继续向上追溯，直到最终的根证书 30。

[161] 根证书是根 CA 自己给自己颁发的证书，其中根 CA 一般是最高权威的 CA 中心，必须给予信任。如图所示，根证书 30 包括，根 CA 信息（此时根 CA 既是持有者，也是签发者），根 CA 公钥，以及根 CA 自己给自己的签名信息。

[162] 如此，根证书 30 和各个公钥证书构成一个证书链或信任链，其中根证书由根 CA 签发给自己，后续的各个公钥证书由根 CA 以及根 CA 逐级授权的各级 CA 签发产生。根证书是证书链的起点，证书链的层级数根据实际情况而定。

[163] 回到图 2，与上述证书链类似的，在步骤 204，证书生成器针对当前请求的第一任务分组生成第一证书链，该证书链中包括针对第一组标识生成的第一公钥证书，以及可信证书生成器作为根 CA 自签名的第一根证书，第一根证书和第一公钥证书形成证书链。可信证书生成器还生成第一私钥，该第一私钥与第一公钥证书中的公钥相匹配，构成第一证书对。这样的第一证书链和第一私钥，用于后续分发给用户终端和运行第一任务分组中各计算任务的可信计算单元。

[164] 可以理解，图 2 示出了通过配置管理器进行任务分组配置的过程。然而，任务分组配置还可以通过其他方式实现。例如，可以由配置人员直接对可信证书生成器和各个计算任务进行配置。

[165] 具体地，在一个实施例中，可信证书生成器具有配置接口，配置人员可以通过该配置接口，直接向可信证书生成器输入计算任务的分组信息，包括任务分组的组标识和对应的哈希列表，以使得可信证书生成器记录上述分组信息，并可选地针对各个组标识生成相应的证书链。配置人员还可以通过配置计算任务的启动项或可信计算单元的启动项，在其中设置各个计算任务所属的任务分组的组标识。如此，将任务分组信息配置到各个计算任务和可信证书生成器。

[166] 在进行任务分组配置之后，可信证书生成器可以分别为可信计算单元和用户终端签发证书，以实现其间的多方安全计算。

[167] 图 4 示出根据一个实施例为计算单元签发证书的过程示意图。通过图 4 的过程，可信证书生成器向运行第一计算任务的第一计算单元分发数字证书，便于其后续参与与计算服务相关的多方计算。可以理解，第一计算任务可以是任何计算任务，第一计算单元可以是执行该任务的任意可信计算单元。并且，在分组配置阶段该第一计算任务预先被配置为属于某个任务分组，在此称为第一任务分组。可以理解，该第一任务分组还可以包括至少一个其他计算任务。

[168] 例如，延续之前的例子，假定图 1 中所示的任务 1，任务 2，任务 3 被配置为形成一个任务分组。那么，图 4 中的第一计算任务可以是任务 1，任务 2，任务 3 中的任一个，相应的，第一计算单元可以是可信计算单元 11,12,13 中的任一个。更具体的，可以假定第一计算任务为任务 1，第一计算单元为可信计算单元 11。

[169] 下面描述签发证书的过程。

[170] 在步骤 401，当第一计算任务在第一计算单元中启动时，生成第一认证信息，用于

其他方对第一计算单元进行可信认证。该可信认证一般是通过远程认证 RA（Remote Attestation）实现，因此，又将生成的认证信息称为 RA 信息或 RA 报告。

[171] 在一个实施例中，第一计算单元生成本计算单元的单元报告文件作为上述第一认证信息，其中单元报告文件用于描述第一计算单元自身配置状况和运行状况。具体的，该单元报告文件至少包括，其中运行的第一计算任务的代码哈希，称为第一代码哈希。可以理解，第一代码哈希可以唯一地标识出所运行的第一计算任务。可选的，该单元报告中还可以包括其中运行的第一计算任务的其他描述信息，例如名称、版本、属性信息等等。

[172] 上述单元报告文件还包括该第一计算单元的签名信息，以此保证单元报告文件的真实可靠，防止伪造和篡改。签名信息可以通过各种签名方式得到，例如哈希算法，加密算法等。在一个具体实施例中，签名信息依赖于对应第一计算单元的硬件密钥，该硬件密钥唯一对应于实体硬件，如此确保单元报告文件中的签名信息确实是由基于该硬件的可信计算单元产生。

[173] 在一个实施例中，上述单元报告文件还包括第一计算单元的硬件信息，例如 CPU 主频，内存容量等等。在一个实施例中，上述单元报告文件还包括第一计算单元的运行时环境信息，从而更全面地描述当前的运行状况。在又一实施例中，单元报告文件还可以包括其他用户自定义的数据，以根据需要描述和定义可信计算单元的其他信息。

[174] 如此，上述生成的单元报告文件可以作为第一认证信息，用于其他方对第一计算单元进行可信认证。

[175] 在一个实施例中，第一计算单元在生成上述单元报告文件后，将该单元报告文件发送至第三方认证机构进行认证，以获得认证结果文件，从而将认证结果文件作为第一认证信息。

[176] 可以理解，上述第三方认证机构是可信的、具有认证能力的权威认证机构。通常，假定各个可信计算单元在投入使用之前，会向该第三方认证机构进行注册，因此，该第三方认证结构登记有各个可信计算单元的配置状况，从而后续可以对其进行认证。

[177] 例如，在上述第一计算单元是通过 Intel SGX 实现的可信围圈 Enclave 的情况下，该第三方认证机构即为 Intel 认证服务器（Attestation Service）。在第一计算单元通过其他方式实现的情况下，该第三方认证机构可以是生产、部署对应计算单元的机构或其关联机构。

[178] 在接收到第一计算单元的单元报告文件后，第三方认证机构可以基于该单元报告，对第一计算单元的安全性和可信性进行认证。具体地，第三方认证机构首先根据单元报告文件中的签名信息，认证该单元报告文件是否真实无篡改，并根据维护的各个可信计算单元预先注册的信息，判断第一计算单元是否确实可信。此外，第三方认证机构还根据单元报告文件中的第一计算任务的相关信息，验证第一计算任务的程序代码是否运行在可信执行环境中，并验证第一代码哈希是否符合预期。

[179] 在对上述单元报告文件进行验证且验证通过的情况下，第三方机构可以在该单元报告文件上添加自身的签名，生成认证结果文件。也就是说，该认证结果文件中包含第三方认证机构的签名信息。

[180] 在获取到第三方认证机构返回的认证结果文件后，第一计算单元可以将该认证结果文件作为第一认证信息，作为可信计算单元的证明。

[181] 此外，在步骤 402，第一计算单元与可信证书生成器进行密钥协商，建立可信通道，又称为 RA 通道。

[182] 具体地，第一计算单元与可信证书生成器可以采用各种密钥协商方式，确定出共同的密钥或密钥对。例如，采用 DH(Diffie-Hellman)密钥交换方法，或者采用基于椭圆曲线的 ECDH 密钥交换方式，等等。利用协商得到的密钥或密钥对，可以建立可信通道，确保通过该可信通道传输的数据只有双方可以获取。

[183] 需要理解，步骤 401 和步骤 402 可以不限于图 4 所示的顺序，两者可以交换顺序执行，也可以并行执行。

[184] 接着，在步骤 403，利用上述 RA 通道，第一计算单元向可信证书生成器发送获取证书的请求，以下称为第一证书请求。该第一证书请求中包括，第一计算任务所属的第一任务分组的组标识，称为第一组标识，以及步骤 401 中得到的第一认证信息，其中包含有第一计算任务的第一代码哈希。其中，第一组标识在如前所述的任务分组配置阶段，已经通知或配置给第一计算任务，因此，在第一计算单元中启动第一计算任务时，可以直接获取到之前配置的第一组标识，将其包含在第一证书请求中。

[185] 在接收到第一证书请求后，在步骤 404，可信证书生成器首先基于上述第一认证信息，对第一计算单元进行认证。

[186] 如前所述，在一个实施例中，上述第一认证信息可以是第一计算单元生成的单元报告文件。在这样的情况下，可信证书生成器将该单元报告文件发送至上述第三方认证

机构，由该第三方认证机构进行验证。在验证通过的情况下，返回认证结果文件，其中包含有该第三方认证机构的签名信息。于是，可信证书生成器进一步验证该签名信息，验证通过，则认为第一计算单元认证通过。

[187] 在另一实施例中，上述第一认证信息也可以是第一计算单元从第三方认证机构收到的认证结果文件。在这样的情况下，可信证书生成器只需要验证该认证结果文件中的签名信息。验证通过，则认为第一计算单元认证通过。

[188] 如果对第一计算单元的认证通过，那么在步骤 405，可信证书生成器根据第一代码哈希判断第一计算任务是否属于第一任务分组。

[189] 如前所述，在任务分组配置阶段，可信证书生成器会通过配置管理器或通过配置接口，获取到各个任务分组对应的哈希列表，其中包括属于对应任务分组的所有计算任务的代码哈希。于是，在步骤 405，可信证书生成器可以读取预先配置的、与第一组标识对应的第一哈希列表，该第一哈希列表包括属于第一任务分组的所有计算任务的代码哈希。然后，判断第一认证信息中包含的第一代码哈希是否位于第一哈希列表中，如果是，则确认该第一计算任务属于第一任务分组。

[190] 例如，假定步骤 403 中的第一证书请求中包含第一组标识 GID1，第一认证信息中包含第一代码哈希 H1。那么在步骤 405，可信证书生成器可以根据该组标识 GID1 读取到配置阶段获得的对应的哈希列表 1:{ H1，H2，H3}。然后判断第一代码哈希 H1 是否包含在哈希列表 1 中，据此判断第一计算任务是否属于第一任务分组。

[191] 如果第一计算任务不属于第一任务分组，那么拒绝该证书请求，返回错误信息。如果确认第一计算任务属于第一任务分组，那么继续执行后续步骤。

[192] 接下来，在步骤 406，可信证书生成器获取针对第一组标识生成的第一证书链和第一私钥。

[193] 在一个实施例中，在前述的分组配置阶段，可信证书生成器已经针对各个任务分组各自的组标识，生成对应的证书链。在这样的情况下，在步骤 406，可信证书生成器读取预先针对第一组标识生成的第一证书链和第一私钥。

[194] 在另一实施例中，在分组配置阶段，可信证书生成器只是记录各个任务分组的组标识和对应的哈希列表。在证书分发阶段，可信证书生成器针对各个组标识生成证书链。相应的，在步骤 406，可信证书生成器判断是否存在与第一组标识对应的证书链，如果存在（例如运行同一任务分组中其他计算任务的其他计算单元先于第一计算单元发出了

证书请求），则读取该已经生成的证书链作为第一证书链。如果不存在，那么可信证书生成器针对该第一组标识生成第一证书链和第一私钥。

[195] 如前所述，第一证书链包括第一根证书和对应的第一公钥证书，第一根证书是可信证书生成器作为根 CA 自签名的证书，第一公钥证书是第一根证书的下游公钥证书，并与第一私钥相匹配，构成第一证书对。

[196] 在不同实施例中，第一公钥证书和第一根证书可以采用多种格式，例如，采用密码学中公钥证书的标准格式 X.509 证书。

[197] 此外，需要理解的是，可信证书生成器会针对不同任务分组，也就是不同组标识，生成不同证书链，一个证书链中的根证书和公钥证书具有对应关系，不同证书链中的根证书彼此不同。

[198] 相应地，对于第一证书链来说，第一根证书是信任链起点，与第一公钥证书相对应。在不同实施例中，第一公钥证书与第一根证书以不同的方式相对应。

[199] 图 5 示出在一个实施例中的第一证书链。在图 5 中，证书 51 为第一公钥证书，其中包括，作为证书持有者的第一任务分组（例如记为 GID1）信息，第一公钥 K1（为组标识 GID1 生成的公钥），作为签发者的证书生成器的信息，以及证书生成器签名的第一签名信息。第一私钥 k1 与第一公钥 K1 相匹配。证书 50 为第一根证书，其中包括证书生成器的信息（既作为证书持有者又作为签发者），第二公钥 K2（证书生成器对外的签名公钥），以及证书生成器自签名的第二签名信息。其中，第一公钥证书 51 中的第一签名信息和第一根证书 50 中的第二签名信息，均使用第二公钥 K2 进行校验。并且，该第二公钥 K2 是针对第一任务分组的第一组标识生成的，如此，第一根证书 50 和第一公钥证书 51 均唯一地对应于第一组标识。

[200] 图 6 示出在另一实施例中的第一证书链。在图 6 中，证书 61 为第一公钥证书，其中包括，作为证书持有者的第一任务分组（例如记为 GID1）信息，第一公钥 K1（为组标识 GID1 生成的公钥），作为签发者的证书生成器的信息，以及证书生成器签名的第一签名信息。证书 60 为第一根证书，其中包括证书生成器的信息（既作为证书持有者又作为签发者），第一公钥 K1，以及证书生成器自签名的第二签名信息。

[201] 可以看到，图 6 不同于图 5 之处在于，在图 6 的第一根证书 60 中，同样使用为组标识 GID1 生成的第一公钥 K1 作为证书生成器对外的签名公钥。于是，第一公钥证书 61 中的第一签名信息和第一根证书 60 中的第二签名信息，均使用第一公钥 K1 进行校

验。如此，简化了证书链的公钥生成。并且，由于第一公钥 K1 针对 GID1 而生成，第一根证书 60 和第一公钥证书 61 均唯一地对应于第一组标识。

[202] 在其他例子中，第一公钥证书和第一根证书还可以相隔更多层级（如图 3 中的证书 33 和 30）而互相对应。

[203] 如此，可信证书生成器获取针对第一组标识生成的第一根证书，第一公钥证书和第一私钥。

[204] 接着，在步骤 407，可信证书生成器通过之前建立的可信通道，即 RA 通道，向第一计算单元发送证书报告，称为第一证书报告。该第一证书报告中包括，第一根证书，以及第一公钥证书和第一私钥构成的第一证书对。通过 RA 通道，第一证书报告的内容不会被其他计算单元获得。

[205] 在第一计算单元获取到第一证书报告后，在步骤 408，使用其中的证书以 TLS 安全协议的方式来加固在线服务接口，从而为后续进行与计算服务相关的多方计算提供基础。

[206] 传输层安全协议 TLS（Transport Layer Security）是与上层应用层解耦合的安全协议，用于在两个通信应用程序之间提供保密性和数据完整性。应用层协议，例如 HTTP/RPC 协议等，能透明地运行在 TLS 协议之上，由 TLS 协议进行创建加密通道需要的协商和认证。应用层协议传送的数据在通过 TLS 协议时都会被加密，从而保证通信的私密性。

[207] 具体的，TLS 安全协议支持客户端和服务端通信方式，其中 TLS 客户端和 TLS 服务端利用证书进行握手，建立加密通道，以此加固上层的网络服务，例如 HTTP/RPC 网络服务。

[208] 相应的，在步骤 408，第一计算单元可以以自身作为提供第一计算任务的计算服务的 TLS 服务端，将接收到的第一证书对设置为 TLS 服务端的证书对。此外，为了与同一任务分组中其他计算任务协作，第一计算单元还将自身作为与其他计算任务连接的 TLS 客户端，并将第一根证书设置为 TLS 客户端的可信根证书。于是，第一计算单元后续可以作为 TLS 服务端，向具有对应的第一根证书的其他 TLS 客户端提供第一计算任务的计算服务，还可以作为 TLS 客户端，与具有第一证书对的其他 TLS 服务端通信，与其进行协同计算。这将在后续进行详细描述。

[209] 如此，通过图 4 的过程，运行第一计算任务的第一计算单元从可信证书生成器获

得针对第一任务分组生成的证书和私钥。可以理解，其他各个计算单元均可以执行图 4 所示的过程，分别获得与运行的计算任务所属任务分组所对应的证书。

[210] 图 7 示出在执行图 4 所示的过程之后各个计算单元的状态。如图 7 所示，由于可信计算单元 11、12、13 分别执行任务 1、任务 2 和任务 3，假定任务 1、任务 2 和任务 3 同属于第一任务分组，那么，可信计算单元 11、12、13 均可以获取到针对第一任务分组的组标识 GID1 生成的第一根证书、第一公钥证书和第一私钥。可信计算单元 14 运行任务 4，假定任务 4 属于第二任务分组，因此可信计算单元 14 可以获得针对第二任务分组生成的第二根证书、第二公钥证书和第二私钥。如此，各个计算单元可以获得与其运行的计算任务对应的证书和私钥。

[211] 在此基础上，可信证书生成器还响应于用户终端的请求，为用户终端分发对应的证书，以便于用户终端和可信计算单元进行通信。

[212] 图 8 示出根据一个实施例为用户终端分发证书的过程示意图。

[213] 首先，在步骤 801，用户终端向可信证书生成器发出认证请求，请求对可信证书生成器进行 RA 认证。

[214] 于是，在步骤 802，可信证书生成器向用户终端提供自身的 RA 信息，称为第二认证信息，以供用户终端进行认证。

[215] 相应的，在步骤 803，用户终端基于该第二认证信息，对可信证书生成器进行认证。

[216] 与可信计算单元的认证类似的，在一个实施例中，可信证书生成器生成自身的报告文件，该报告文件包括可信证书生成器自身的代码哈希和签名信息。可选的，该报告文件还包括可信证书生成器的其他配置描述信息。于是，在步骤 802，可信证书生成器将该报告文件作为上述第二认证信息，发送给用户终端。

[217] 在步骤 803，用户终端将上述报告文件发送给第三方认证机构。与前述类似的，第三方认证机构基于该报告文件的签名信息和代码哈希进行验证，在验证通过后，在报告文件上添加上签名，作为认证结果文件。因此，该认证结果文件包含第三方认证机构的签名信息。于是，用户终端可以对该签名信息进行验证，据此对可信证书生成器进行认证。

[218] 或者，在另一实施例中，可信证书生成器在生成上述报告文件后，将该报告文件发送至第三方认证机构，并从该第三方认证机构获得认证结果文件。在步骤 802，可信证书生成器将该认证结果文件作为第二认证信息，提供给用户终端。相应的，在步骤 803，

用户终端仅需要对认证结果文件中的签名信息进行验证，据此实现对可信证书生成器的认证。

[219] 在对可信证书生成器认证通过后，在步骤 804，用户终端向可信证书生成器发送证书请求，称为第二证书请求，该第二证书请求中包括，用户终端期望连接的第一任务分组的第一组标识。在一个具体例子中，用户终端可以向配置管理器查询期望连接的任务分组的组标识，将其包含在第二证书请求中。

[220] 例如，在图 1 的示意图中，用户终端想要连接到任务 1、任务 2 和任务 3 所形成的第一任务分组，则在上述证书请求中包含该任务分组的组标识，例如 GID1。

[221] 可信证书生成器在接收到上述第二证书请求后，在步骤 805，获取预先针对该第一组标识生成的第一证书链和第一私钥，其中第一证书链包括第一根证书和与其对应的第一公钥证书，第一公钥证书与第一私钥构成第一证书对。并且，如图 4 所示，可信证书生成器已经预先将第一证书对分发给经过认证的、运行第一任务分组中各个计算任务的至少一个计算单元。

[222] 然后，在步骤 806，可信证书生成器向用户终端返回证书报告，称为第二证书报告，其中至少包括上述第一证书链中的第一根证书。

[223] 可选的，在一个实施例中，第二证书报告中还包括，第一组标识对应的第一哈希列表，该第一哈希列表包括属于第一任务分组的所有计算任务的代码哈希。

[224] 在这样的情况下，在步骤 807，用户终端判断所述第一哈希列表是否符合预期。具体地，用户终端判断第一哈希列表中包括的每个代码哈希是否符合预期，也就是，每个代码哈希是否是期望连接的任务分组中计算任务的代码哈希。据此，用户终端判断可信证书生成器中的任务分组信息是否符合预期，该任务分组中的任务程序代码行为是否符合预期。

[225] 如果第一哈希列表中包含任何一个非预期的代码哈希，那么用户终端会认为，任务分组信息不一致，拒绝信任可信证书生成器发送的证书。

[226] 如果第一哈希列表符合预期，那么接着在步骤 808，用户终端将自身作为 TLS 客户端，将接收到的第一根证书设置为 TLS 客户端的可信根证书。

[227] 而另一方面，如图 4 中步骤 408 所示以及如图 7 所示，运行第一任务分组中各个计算任务的各个计算单元在通过认证之后，会获得第一根证书和第一证书对，并进行相应的 TLS 设置，也就是以自身为 TLS 客户端和 TLS 服务端，将第一根证书作为 TLS 客

户端信任的根证书，将第一证书对作为 TLS 服务端证书对。在用户终端和各个计算单元均进行相应 TLS 设置之后，用户终端与运行第一任务分组的各个计算单元之间，以及该各个计算单元彼此之间，就可以使用 TLS 安全协议进行安全的多方计算。

[228] 如前所述，TLS 安全协议支持客户端和服务端通信方式。具体来说，在第一根证书与第一公钥证书形成证书链的情况下，将第一根证书作为唯一可信根证书的 TLS 客户端就可以，并且仅可以，与具有第一证书对的 TLS 服务端进行握手，进而建立 TLS 可信通道。具有第一根证书的 TLS 客户端与具有第一证书对的 TLS 服务端可以通过以下方式实现 TLS 握手。

[229] 首先，TLS 客户端发起握手请求，TLS 服务端将第一公钥证书和生成的随机数 N1 返回给 TLS 客户端。

[230] 由于 TLS 客户端已经将第一根证书设置为唯一可信根证书，而第一公钥证书为该第一根证书信任链中的证书，因此，TLS 客户端会认为第一公钥证书可信。于是 TLS 客户端生成另一随机数 N2，并使用第一公钥证书中的第一公钥加密该随机数 N2，发送给 TLS 服务端。

[231] TLS 服务端利用第一证书对中的第一私钥解密出随机数 N2，并根据之前的随机数 N1，N2 和约定的加密算法，生成用于加密后续传输数据的会话密钥。TLS 客户端在确认该会话密钥后，双方就握手成功，利用该会话密钥建立了 TLS 可信通道。在握手成功后，TLS 客户端就可以与 TLS 服务端通过 TLS 可信通道交换数据。

[232] 利用以上的 TLS 客户端和服务端的通信机制，用户终端以及运行第一任务分组的计算单元之间就可以进行多方安全计算。具体的，由于用户终端作为 TLS 客户端，将第一根证书设置为可信根证书，而运行第一任务分组中各个计算任务的各个计算单元均可以作为 TLS 服务端，且将第一证书对作为服务端证书对，因此，请求第一任务分组的计算服务的用户终端，可以与运行第一任务分组中各个计算任务的各个计算单元建立 TLS 可信通道，进行安全通信。此外，各个计算单元本身又可以作为 TLS 客户端，且也将第一根证书设置为可信根证书，因此，作为 TLS 客户端的一个计算单元可以与作为 TLS 服务端的另一计算单元建立 TLS 可信通道，并且，该另一计算单元必然是运行同一任务分组中计算任务的计算单元。如此，在用户终端和多个计算单元之间实现安全的多方计算。

[233] 可以看到，在图 8 的过程中，用户终端只是对可信证书生成器进行了 RA 认证，而

没有对各个计算单元进行RA认证。但是应理解，根据图4的过程，可信证书生成器在分发证书前，会首先对计算单元进行RA认证，认证通过的情况下，才为计算单元分发证书。因此，用户终端对可信证书生成器进行RA认证，就意味着，对可信计算单元间接地进行了RA认证。并且，综合图4和图8的过程，证书链中证书的各自分发相当于同时实现了RA认证和TLS校验，简化了安全认证的过程。

[234]在一个实施例中，第一任务分组的计算服务不仅需要在多方之间进行数据交换，还需要存储和读取持久化的数据。在这样的情况下，在图8的步骤806中，可信证书生成器可以在返回给用户终端的第二证书报告中进一步包括第一公钥证书。于是，用户终端可以利用该第一公钥证书加密用户数据，并将加密的用户数据持久化存入数据平台。而如前所述，运行第一任务分组中各个计算任务的各个计算单元均获取有第一证书对，其中包含第一私钥。因此，上述各个计算单元可以利用第一证书对中的第一私钥解密获取上述用户数据。此外，各个计算单元也可以利用第一证书对中的第一公钥加密产生的中间数据，存入数据平台，其他计算单元可以利用第一私钥解密获得该中间数据。如此，确保需要持久化存储的数据仅可以由同一任务分组中的计算单元获得。

[235]图9示出在执行图4和图8所示的过程之后系统的状态。如图9所示，运行同一任务分组中各个计算任务的各个计算单元，均获得该任务分组对应的根证书和证书对。例如，任务1、任务2、任务3同属于第一任务分组，那么分别运行这3个计算任务的可信计算单元11、12、13均获取到针对第一任务分组生成的第一根证书和第一证书对。而运行另一任务分组中计算任务4的可信计算单元14则获得到不同的第二根证书和第二证书对。另一方面，请求第一任务分组的计算服务的用户终端也从可信证书生成器获取到第一根证书，其中第一根证书与第一证书对中的第一公钥证书相对应，构成证书链。可选的，用户终端也可以获取到第一公钥证书，用于加密持久化数据。

[236]基于图9所示的系统状态，用户终端和多个计算单元之间可以利用TLS协议进行安全计算。下面结合图9，描述运行第一任务分组中某个计算任务的计算单元，仍称为第一计算单元，进行多方计算的过程。

[237]图10示出在一个实施例中进行多方安全计算的方法流程图。需要说明的是，图10的方法由运行第一任务分组中第一计算任务的第一计算单元执行，且运行第一任务分组中各个计算任务的各个计算单元，以及用户终端，已经进行了相应的TLS设置，如图9所示。

[238]在这样的情况下，在步骤101，第一计算单元作为TLS服务端，与作用为TLS客

户端的用户终端进行 TLS 握手，建立第一 TLS 可信通道。握手的过程如前所述，不复赘述。

[239] 在步骤 102，第一计算单元通过第一 TLS 可信通道，从用户终端接收第一用户数据。

[240] 在步骤 103，第一计算单元运行的第一计算任务对第一用户数据进行第一处理，得到第一应用数据。

[241] 在步骤 104，第一计算单元作为 TLS 客户端，与作用为 TLS 服务端的第二计算单元进行 TLS 握手，建立第二 TLS 可信通道；其中第二计算单元是运行第一任务分组中另一计算任务，即第二计算任务，的计算单元。

[242] 在步骤 105，第一计算单元通过第二 TLS 可信通道，将上述第一应用数据传送给第二计算单元。

[243] 通过以上过程，利用 TLS 可信通道，第一计算单元从用户终端接收用户数据，对其处理之后，传输给运行同一任务分组中计算任务的第二计算单元，从而至少在用户终端、第一计算单元和第二计算单元之间实现多方安全传输和计算。

[244] 进一步的，在一个实施例中，第一任务分组的计算服务需要存储持久化数据。在这样的情况下，在一个例子中，图 10 的方法还包括，第一计算单元从数据平台读取第二用户数据，该第二用户数据由用户终端使用第一公钥证书加密产生。于是，第一计算单元可以使用第一私钥解密该第二用户数据，从而得到对应的数据明文。

[245] 在另一实施例中，第一计算单元自身会产生中间数据，并将其持久化进行存储，同一任务分组中的其他计算单元可以读取该持久化数据。具体的，在一个例子中，图 10 的方法还包括以下步骤。第一计算单元生成第二应用数据，然后使用第一公钥证书加密该第二应用数据，得到第二加密应用数据。第一计算单元于是将该第二加密应用数据存入数据平台，以供其他计算单元，例如第二计算单元利用第一证书对进行解密获取。

[246] 通过以上过程，第一计算单元可以与用户终端，以及与同一任务分组中的其他计算单元进行多方安全计算。

[247] 基于图 9 回顾整个过程，在本说明书的一个实施例中，通过可信证书生成器生成并分发证书，实现安全认证和校验，便于用户终端与可信计算单元之间进行多方安全通信和计算。具体的，预先将计算任务进行分组，形成任务分组。可信证书生成器通过组标识区分不同任务分组，针对一个组标识生成一套证书链和一个私钥，其中证书链中包

括根证书和对应的公钥证书，公钥证书与私钥相匹配，构成一个证书对。然后，可信证书生成器将该上述根证书和证书对分发给经过认证的、运行该组标识对应的各个计算任务的各个可信计算单元。于是，运行同一任务分组中各个计算任务的多个可信计算单元会获得同样的根证书和证书对。另一方面，可信证书生成器将上述根证书分发给请求该任务分组的计算服务的用户终端。于是，具有根证书的用户终端、具有根证书和证书对的可信计算单元之间，可以通过 TLS 协议的方式，进行多方安全通信。

[248] 根据另一方面的实施例，提供了一种获取证书以进行多方安全计算的装置，该装置部署在运行第一计算任务的第一计算单元中。所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括至少一个其他计算任务。图 11 示出在一个实施例中部署在第一计算单元中的获取证书的装置的示意性框图。如图 11 所示，该装置 110 包括:

[249] 第一证书请求模块 111，配置为向可信证书生成器发送第一证书请求，所述第一证书请求包括所述第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对第一计算单元进行可信认证，并包括所述第一计算任务的第一代码哈希;

[250] 第一报告接收模块 113，配置为从所述可信证书生成器接收第一证书报告，所述第一证书报告包括针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书以及对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对;

[251] 第一设置模块 115，配置为以所述第一计算单元作为提供所述第一计算任务的计算服务的 TLS 服务端，将所述第一证书对设置为所述 TLS 服务端的证书对；并且以所述第一计算单元作为与所述至少一个其他计算任务连接的 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信根证书。

[252] 在一个具体实施例中，所述第一计算单元实现为可信围圈 Enclave。

[253] 根据一个实施例，上述装置 110 还包括认证信息生成模块（未示出），用于生成上述第一认证信息。

[254] 在一个具体的实施例中，所述认证信息生成模块配置为:

[255] 生成第一计算单元的单元报告文件，所述单元报告文件包括所述第一代码哈希，所述第一计算单元的签名信息;

[256] 将所述单元报告文件发送至第三方认证机构，以获得认证结果文件，所述认证结

果文件包含所述第三方认证机构的签名信息;

[257] 将所述认证结果文件作为所述第一认证信息包含在所述第一证书请求中。

[258] 在另一具体的实施例中，所述认证信息生成模块配置为:

[259] 生成第一计算单元的单元报告文件，所述单元报告文件包括所述第一代码哈希，所述第一计算单元的签名信息;

[260] 将所述单元报告文件作为所述第一认证信息包含在所述第一证书请求中。

[261] 根据一种实施方式，该装置 110 还包括密钥协商模块，配置为在向可信证书生成器发送第一认证请求之前，与所述可信证书生成器进行密钥协商，建立可信通道，所述可信通道用于发送所述第一证书请求，以及接收所述第一证书报告。

[262] 根据另一方面的实施例，提供了一种为计算单元分发证书的装置，部署在可信证书生成器中。该可信证书生成器可以通过任何具有计算、处理能力的设备、平台或设备集群实现。图 12 示出在一个实施例中为计算单元分发证书的装置的示意性框图。如图 12 所示，该装置 120 包括:

[263] 第一请求接收模块 121，配置为从运行第一计算任务的第一计算单元接收第一证书请求，所述第一证书请求包括第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对所述第一计算单元进行认证，且包括所述第一计算任务的第一代码哈希;

[264] 单元认证模块 123，配置为根据所述第一认证信息对所述第一计算单元进行认证;

[265] 分组判断模块 125，配置为在认证通过的情况下，根据所述第一代码哈希判断所述第一计算任务是否属于所述第一任务分组;

[266] 证书获取模块 127，配置为在确认所述第一计算任务属于所述第一任务分组的情况下，获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对;

[267] 第一报告发送模块 129，配置为向所述第一计算单元发送第一证书报告，所述第一证书报告包括所述第一根证书和所述第一证书对，使得所述第一计算单元以自身为提供计算服务的 TLS 服务端和与其他计算任务连接的 TLS 客户端，将所述第一证书对设置为 TLS 服务端的证书对，将所述第一根证书设置为 TLS 客户端的可信根证书。

[268] 在一个实施例中，第一请求接收模块 121 接收的第一认证信息为经过第三方认证机构认证的认证结果文件，该认证结果文件包含该第三方认证机构的签名信息；在这样的情况下，所述单元认证模块 123 配置为：

[269] 校验所述签名信息，在校验成功的情况下，确定所述第一计算单元认证通过。

[270] 在另一实施例中，第一请求接收模块 121 接收的第一认证信息为所述第一计算单元生成的单元报告文件，所述单元报告文件包括所述第一代码哈希，以及所述第一计算单元的签名信息；在这样的情况下，所述单元认证模块 123 配置为：

[271] 将所述单元报告文件发送至第三方认证机构，以获得认证结果文件，所述认证结果文件包含所述第三方认证机构的签名信息；

[272] 校验所述签名信息，在校验成功的情况下，确定所述第一计算单元认证通过。

[273] 根据一种实施方式，装置 120 还包括证书生成模块（未示出），配置为：

[274] 从配置管理器接收第一生成命令，所述第一生成命令包括，所述第一组标识，以及与所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；

[275] 针对所述第一组标识，生成所述第一证书链和第一私钥。

[276] 根据一个实施例，所述分组判断模块 125 配置为，获取预先配置的、与所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；

[277] 判断所述第一代码哈希是否位于所述第一哈希列表中，如果是，则确认所述第一计算任务属于所述第一任务分组。

[278] 根据一个具体实施例，所述第一公钥证书包括针对所述第一组标识生成的第一公钥，以及所述可信证书生成器签名的第一签名信息，其中所述第一公钥和所述第一私钥构成密钥对；所述第一根证书中包括针对所述第一组标识生成的第二公钥，以及所述可信证书生成器自签名的第二签名信息；所述第二公钥用于对所述第一签名信息和第二签名信息进行校验。

[279] 根据另一具体实施例，所述第一公钥证书包括针对所述第一组标识生成的第一公钥，以及所述可信证书生成器签名的第一签名信息，其中所述第一公钥和所述第一私钥构成密钥对；所述第一根证书包括所述第一公钥，以及所述可信证书生成器自签名的第

二签名信息；所述第一公钥用于对所述第一签名信息和第二签名信息进行校验。

[280]根据一种实施方式，装置 120 还包括密钥协商模块（未示出），用于在接收第一证书请求之前，与所述第一计算单元进行密钥协商，建立可信通道，所述可信通道用于接收所述第一证书请求，以及发送所述第一证书报告。

[281]根据又一方面的实施例，提供了一种获取证书以进行多方安全计算的装置，部署在用户终端中。该用户终端可以通过任何具有计算、处理能力的设备实现。图 13 示出在一个实施例中部署在用户终端中的获取证书的装置的示意性框图。如图 13 所示，该装置 130 包括:

[282]第二请求发送模块 131，配置为向可信证书生成器发送第二证书请求，所述第二证书请求中包括，期望连接的第一任务分组的第一组标识;

[283]第二报告接收模块 133，配置为从所述可信证书生成器接收第二证书报告，所述第二证书报告至少包括针对所述第一组标识生成的第一证书链中的第一根证书，所述第一证书链还包括与所述第一根证书对应的第一公钥证书；所述第一公钥证书和匹配的第一私钥构成第一证书对，被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元;

[284]第二设置模块 135，配置为以所述用户终端为 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

[285]根据一种实施方式，上述装置 130 还包括认证模块（未示出），配置为:

[286]获取所述可信证书生成器的第二认证信息;

[287]根据所述第二认证信息，对所述可信证书生成器进行认证。

[288]进一步的，根据一个实施例，上述第二认证信息为经过第三方认证机构认证的认证结果文件，该认证结果文件包含该第三方认证机构的签名信息；相应的，认证模块配置为：校验所述签名信息，在校验成功的情况下，确定所述可信证书生成器认证通过。

[289]根据另一实施例，所述第二认证信息为所述可信证书生成器生成的报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息；相应的，认证模块配置为:

[290]将所述报告文件发送至第三方认证机构，以获得认证结果文件，所述认证结果文

件包含所述第三方认证机构的签名信息；

[291] 校验所述签名信息，在校验成功的情况下，确定所述证书生成器认证通过。

[292] 根据一种实施方式，第二证书报告还包括，所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；相应的，装置130还包括哈希确认模块（未示出），配置为，在所述第二配置模块135将所述第一根证书设置为所述TLS客户端的可信根证书之前，判断所述第一哈希列表是否符合预期。

[293] 根据一种实施方式，上述装置130还包括通信模块（未示出），在第二配置模块135将所述第一根证书设置为所述TLS客户端的可信根证书之后，所述通信模块用于与所述至少一个计算单元进行TLS握手，建立TLS可信通道；通过TLS可信通道，从所述至少一个计算单元获取所述第一任务分组的计算服务。

[294] 根据一个实施例，第二证书报告还包括第一公钥证书；相应的，装置130还包括加密模块，配置为，利用所述第一公钥证书加密所述用户终端的用户数据，并将加密的用户数据存入数据平台，以供所述至少一个计算单元利用所述第一证书对进行解密获取。

[295] 根据另一方面的实施例，还提供了一种为用户终端分发证书的装置，部署在可信证书生成器中。该可信证书生成器可以通过任何具有计算、处理能力的设备、平台或设备集群实现。图14示出在一个实施例中为用户终端分发证书的装置的示意性框图。如图14所示，该装置140包括：

[296] 第二请求接收模块141，配置为接收用户终端发送的第二证书请求，所述第二证书请求中包括，所述用户终端期望连接的第一任务分组的第一组标识；

[297] 证书获取模块143，配置为获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和与其对应的第一公钥证书，所述第一公钥证书与所述第一私钥匹配，构成第一证书对；至少所述第一证书对被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元；

[298] 第二报告发送模块145，配置为向所述用户终端发送第二证书报告，所述第二证书报告至少包括所述第一根证书，以使得所述用户终端以自身为TLS客户端，将所述第一根证书作为TLS客户端的可信根证书，从而与具有所述第一证书对、且作用为TLS服务端的所述至少一个计算单元通信。

[299] 根据一种实施方式，上述装置140还包括认证信息提供模块（未示出），在第二请求接收模块141接收用户终端发送的第二证书请求之前，该认证信息提供模块响应于

所述用户终端的认证请求，向所述用户终端提供第二认证信息，以供所述用户终端进行认证。

[300] 在一个进一步的实施例中，所述认证信息提供模块配置为：

[301] 生成报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息；

[302] 将所述报告文件发送至第三方认证机构，以获得认证结果文件，所述认证结果文件包含所述第三方认证机构的签名信息；

[303] 将所述认证结果文件作为所述第二认证信息提供给所述用户终端。

[304] 在另一个进一步的实施例中，所述认证信息提供模块配置为：

[305] 生成报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息；

[306] 将所述报告文件作为所述第二认证信息提供给所述用户终端。

[307] 在一个实施例中，第二报告发送模块 145 发送的第二证书报告还包括，所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希。

[308] 在一种实施方案中，第二报告发送模块 145 发送的第二证书报告还包括所述第一公钥证书，以使得所述用户终端利用所述第一公钥证书加密用户数据。

[309] 根据另一方面的实施例，提供了一种通过数字证书进行多方安全计算的装置，该装置部署在运行第一计算任务的第一计算单元中。图 15 示出在一个实施例中部署在第一计算单元中的进行多方计算的装置的示意性框图，其中：

[310] 第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括第二计算单元所运行的第二计算任务；

[311] 所述第一计算单元预先被分发有针对所述第一任务分组生成的第一证书对和第一根证书，所述第一证书对包括第一公钥证书和匹配的第一私钥，所述第一公钥证书和第一根证书构成第一证书链；

[312] 并且，所述第一计算单元被配置作为提供所述第一计算任务的计算服务的第一 TLS 服务端，该第一 TLS 服务端以所述第一证书对作为其证书对；所述第一计算单元还被配置作为至少与所述第二计算单元连接的第一 TLS 客户端，所述第一 TLS 客户端以所述

第一根证书作为其可信根证书。

[313] 如图 15 所示，该装置 150 包括:

[314] 第一握手模块 151，配置为利用所述第一 TLS 服务端与作用为第二 TLS 客户端的用户终端进行 TLS 握手，建立第一 TLS 可信通道；其中所述第二 TLS 客户端将所述第一根证书作为其可信根证书;

[315] 数据接收模块 153，配置为通过所述第一 TLS 可信通道接收第一用户数据;

[316] 数据处理模块 155，配置为对所述第一用户数据进行第一处理，得到第一应用数据;

[317] 第二握手模块 157，配置为利用所述第一 TLS 客户端与作用为第二 TLS 服务端的第二计算单元进行 TLS 握手，建立第二 TLS 可信通道；其中所述第二 TLS 服务端将所述第一证书对作为其证书对;

[318] 数据发送模块 159，配置为通过所述第二 TLS 可信通道将所述第一应用数据传送给所述第二计算单元。

[319] 在一个实施例中，上述装置 150 还包括数据获取模块（未示出），配置为：从数据平台读取第二用户数据，所述第二用户数据由所述用户终端使用所述第一公钥证书加密产生；使用所述第一私钥解密所述第二用户数据。

[320] 在一种实施方式中，上述装置 150 还包括，数据加密存储模块（未示出），配置为：生成第二应用数据；使用所述第一公钥证书加密所述第二应用数据，得到第二加密应用数据；将所述第二加密应用数据存入数据平台，以供所述第二计算单元利用所述第一证书对进行解密获取。

[321] 根据另一方面的实施例，还提供一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行结合图 4、图 8 和图 10 所描述的方法。

[322] 根据再一方面的实施例，还提供一种计算设备，包括存储器和处理器，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现结合图 4、图 8 和图 10 所述的方法。

[323] 本领域技术人员应该可以意识到，在上述一个或多个示例中，本发明所描述的功能可以用硬件、软件、固件或它们的任意组合来实现。当使用软件实现时，可以将这些功能存储在计算机可读介质中或者作为计算机可读介质上的一个或多个指令或代码进

行传输。

[324] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的技术方案的基础之上，所做的任何修改、等同替换、改进等，均应包括在本发明的保护范围之内。

权利要求书

1. 一种获取证书以进行多方安全计算的方法，通过运行第一计算任务的第一计算单元执行，所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括至少一个其他计算任务；所述方法包括：

向可信证书生成器发送第一证书请求，所述第一证书请求包括所述第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对第一计算单元进行可信认证，并包括所述第一计算任务的第一代码哈希；

从所述可信证书生成器接收第一证书报告，所述第一证书报告包括针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书以及对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对；

以所述第一计算单元作为提供所述第一计算任务的TLS服务端，将所述第一证书对设置为所述TLS服务端的证书对，并且以所述第一计算单元作为与所述至少一个其他计算任务连接的TLS客户端，将所述第一根证书设置为所述TLS客户端的可信根证书。

2. 根据权利要求1所述的方法，其中，所述第一计算单元实现为可信围圈Enclave。

3. 根据权利要求1所述的方法，还包括，在向可信证书生成器发送第一认证请求之前：

生成第一计算单元的单元报告文件，所述单元报告文件包括所述第一代码哈希，以及所述第一计算单元的签名信息；

将所述单元报告文件发送至第三方认证机构，以获得针对第一计算单元的第一认证结果文件，所述第一认证结果文件包含所述第三方认证机构的签名信息；

将所述第一认证结果文件作为所述第一认证信息包含在所述第一证书请求中。

4. 根据权利要求1所述的方法，还包括，在向可信证书生成器发送第一认证请求之前：

生成第一计算单元的单元报告文件，所述单元报告文件包括所述第一代码哈希，所述第一计算单元的签名信息；

将所述单元报告文件作为所述第一认证信息包含在所述第一证书请求中。

5. 根据权利要求1所述的方法，还包括，在向可信证书生成器发送第一认证请求之前：

与所述可信证书生成器进行密钥协商，建立可信通道，所述可信通道用于发送所述第一证书请求，以及接收所述第一证书报告。

6. 一种为计算单元分发证书的方法，通过可信证书生成器执行，所述方法包括：

从运行第一计算任务的第一计算单元接收第一证书请求，所述第一证书请求包括第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对所述第一计算单元进行认证，且包括所述第一计算任务的第一代码哈希；

根据所述第一认证信息对所述第一计算单元进行认证；

在认证通过的情况下，根据所述第一代码哈希判断所述第一计算任务是否属于所述第一任务分组；

在确认所述第一计算任务属于所述第一任务分组的情况下，获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对；

向所述第一计算单元发送第一证书报告，所述第一证书报告包括所述第一根证书和所述第一证书对，使得所述第一计算单元以自身为提供计算服务的 TLS 服务端和与其他计算任务连接的 TLS 客户端，将所述第一证书对设置为 TLS 服务端的证书对，将所述第一根证书设置为 TLS 客户端的可信根证书。

7. 根据权利要求 6 所述的方法，其中，所述第一认证信息为第三方认证机构针对所述第一计算单元认证的第一认证结果文件，该第一认证结果文件包含该第三方认证机构的签名信息；

所述根据所述第一认证信息对所述第一计算单元进行认证包括：

校验所述第三方认证机构的签名信息，在校验成功的情况下，确定所述第一计算单元认证通过。

8. 根据权利要求 6 所述的方法，其中，所述第一认证信息为所述第一计算单元生成的单元报告文件，所述单元报告文件包括所述第一代码哈希，以及所述第一计算单元的签名信息；

所述根据所述第一认证信息对所述第一计算单元进行认证包括：

将所述单元报告文件发送至第三方认证机构，以获得针对第一计算单元的第一认证结果文件，所述第一认证结果文件包含所述第三方认证机构的签名信息；

校验所述第三方认证机构的签名信息，在校验成功的情况下，确定所述第一计算单元认证通过。

9. 根据权利要求 6 所述的方法，其中，从运行第一计算任务的第一计算单元接收第一证书请求之前，还包括：

从配置管理器接收第一生成命令，所述第一生成命令包括，所述第一组标识，以及

与所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；

针对所述第一组标识，生成所述第一证书链和第一私钥。

10. 根据权利要求 6 所述的方法，其中，根据所述第一代码哈希判断所述第一计算任务是否属于所述第一任务分组，包括：

获取预先配置的、与所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；

判断所述第一代码哈希是否位于所述第一哈希列表中，如果是，则确认所述第一计算任务属于所述第一任务分组。

11. 根据权利要求 6 所述的方法，其中，所述第一公钥证书包括针对所述第一组标识生成的第一公钥，以及所述可信证书生成器签名的第一签名信息，其中所述第一公钥和所述第一私钥构成密钥对；所述第一根证书中包括针对所述第一组标识生成的第二公钥，以及所述可信证书生成器自签名的第二签名信息；所述第二公钥用于对所述第一签名信息和第二签名信息进行校验。

12. 根据权利要求 6 所述的方法，其中，所述第一公钥证书包括针对所述第一组标识生成的第一公钥，以及所述可信证书生成器签名的第一签名信息，其中所述第一公钥和所述第一私钥构成密钥对；所述第一根证书包括所述第一公钥，以及所述可信证书生成器自签名的第二签名信息；所述第一公钥用于对所述第一签名信息和第二签名信息进行校验。

13. 根据权利要求 6 所述的方法，其中，在从运行第一计算任务的第一计算单元接收第一证书请求之前，还包括：

与所述第一计算单元进行密钥协商，建立可信通道，所述可信通道用于接收所述第一证书请求，以及发送所述第一证书报告。

14.一种获取证书以进行多方安全计算的方法，通过用户终端执行，所述方法包括：

向可信证书生成器发送第二证书请求，所述第二证书请求中包括，期望连接的第一任务分组的第一组标识；

从所述可信证书生成器接收第二证书报告，所述第二证书报告至少包括针对所述第一组标识生成的第一证书链中的第一根证书，所述第一证书链还包括与所述第一根证书对应的第一公钥证书；所述第一公钥证书和匹配的第一私钥构成第一证书对，被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元；

以所述用户终端为 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信

根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

15. 根据权利要求 14 所述的方法，其中，在向可信证书生成器发送第二证书请求之前，还包括：

获取所述可信证书生成器的第二认证信息；

根据所述第二认证信息，对所述可信证书生成器进行认证。

16. 根据权利要求 15 所述的方法，其中，所述第二认证信息为第三方认证机构针对所述可信证书生成器认证的第二认证结果文件，该第二认证结果文件包含该第三方认证机构的签名信息；

所述根据所述第二认证信息，对所述可信证书生成器进行认证包括：

校验所述第三方认证机构的签名信息，在校验成功的情况下，确定所述可信证书生成器认证通过。

17. 根据权利要求 15 所述的方法，其中，所述第二认证信息为所述可信证书生成器生成的报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息；

所述根据所述第二认证信息，对所述可信证书生成器进行认证包括：

将所述报告文件发送至第三方认证机构，以获得针对所述可信证书生成器的第二认证结果文件，所述第二认证结果文件包含所述第三方认证机构的签名信息；

校验所述第三方认证机构的签名信息，在校验成功的情况下，确定所述证书生成器认证通过。

18. 根据权利要求 14 所述的方法，其中，所述第二证书报告还包括，所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希；

在将所述第一根证书设置为所述 TLS 客户端的可信根证书之前，所述方法还包括，判断所述第一哈希列表是否符合预期。

19. 根据权利要求 14 所述的方法，其中，在将所述第一根证书设置为所述 TLS 客户端的可信根证书之后，还包括，

与所述至少一个计算单元进行 TLS 握手，建立 TLS 可信通道；

通过 TLS 可信通道，从所述至少一个计算单元获取所述第一任务分组的计算服务。

20. 根据权利要求 14 所述的方法，其中，所述第二证书报告还包括，所述第一公钥证书，所述方法还包括：

利用所述第一公钥证书加密所述用户终端的用户数据，并将加密的用户数据存入数

据平台，以供所述至少一个计算单元利用所述第一证书对进行解密获取。

21. 一种为用户终端分发证书的方法，通过可信证书生成器执行，所述方法包括：

接收用户终端发送的第二证书请求，所述第二证书请求中包括，所述用户终端期望连接的第一任务分组的第一组标识；

获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和与其对应的第一公钥证书，所述第一公钥证书与所述第一私钥匹配，构成第一证书对；至少所述第一证书对被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元；

向所述用户终端发送第二证书报告，所述第二证书报告至少包括所述第一根证书，以使得所述用户终端以自身为 TLS 客户端，将所述第一根证书作为 TLS 客户端的可信根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

22. 根据权利要求 21 的方法，其中，在接收用户终端发送的第二证书请求之前，还包括：

响应于所述用户终端的认证请求，向所述用户终端提供第二认证信息，以供所述用户终端进行认证。

23. 根据权利要求 22 所述的方法，其中，向所述用户终端提供第二认证信息包括：

生成报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息；

将所述报告文件发送至第三方认证机构，以获得针对所述可信证书生成器的第二认证结果文件，所述第二认证结果文件包含所述第三方认证机构的签名信息；

将所述第二认证结果文件作为所述第二认证信息提供给所述用户终端。

24. 根据权利要求 22 所述的方法，其中，向所述用户终端提供第二认证信息包括：

生成报告文件，所述报告文件包括所述可信证书生成器自身的代码哈希和签名信息；

将所述报告文件作为所述第二认证信息提供给所述用户终端。

25. 根据权利要求 22 所述的方法，其中，所述第二证书报告还包括，所述第一组标识对应的第一哈希列表，该第一哈希列表包括属于所述第一任务分组的所有计算任务的代码哈希。

26. 根据权利要求 22 所述的方法，其中，所述第二证书报告还包括所述第一公钥证书，以使得所述用户终端利用所述第一公钥证书加密用户数据。

27. 一种通过数字证书进行多方安全计算的方法，通过运行第一计算任务的第一计算单元执行，其中：

所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括第二计算单元所运行的第二计算任务；

所述第一计算单元预先被分发有针对所述第一任务分组生成的第一证书对和第一根证书，所述第一证书对包括第一公钥证书和匹配的第一私钥，所述第一公钥证书和第一根证书构成第一证书链；

并且，所述第一计算单元被配置作为提供所述第一计算任务的计算服务的第一 TLS 服务端，该第一 TLS 服务端以所述第一证书对作为其证书对；所述第一计算单元还被配置作为至少与所述第二计算单元连接的第一 TLS 客户端，所述第一 TLS 客户端以所述第一根证书作为其可信根证书；

所述方法包括：

利用所述第一 TLS 服务端与作用为第二 TLS 客户端的用户终端进行 TLS 握手，建立第一 TLS 可信通道；其中所述第二 TLS 客户端将所述第一根证书作为其可信根证书；

通过所述第一 TLS 可信通道接收第一用户数据；

对所述第一用户数据进行第一处理，得到第一应用数据；

利用所述第一 TLS 客户端与作用为第二 TLS 服务端的第二计算单元进行 TLS 握手，建立第二 TLS 可信通道；其中所述第二 TLS 服务端将所述第一证书对作为其证书对；

通过所述第二 TLS 可信通道将所述第一应用数据传送给所述第二计算单元。

28. 根据权利要求 27 所述的方法，还包括：

从数据平台读取第二用户数据，所述第二用户数据由所述用户终端使用所述第一公钥证书加密产生；

使用所述第一私钥解密所述第二用户数据。

29. 根据权利要求 27 所述的方法，还包括：

生成第二应用数据；

使用所述第一公钥证书加密所述第二应用数据，得到第二加密应用数据；

将所述第二加密应用数据存入数据平台，以供所述第二计算单元利用所述第一证书对进行解密获取。

30. 一种获取证书以进行多方安全计算的装置，部署在运行第一计算任务的第一计算单元中，所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括至少一个其他计算任务；所述装置包括：

第一证书请求模块，配置为向可信证书生成器发送第一证书请求，所述第一证书请求包括所述第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对

第一计算单元进行可信认证，并包括所述第一计算任务的第一代码哈希；

第一报告接收模块，配置为从所述可信证书生成器接收第一证书报告，所述第一证书报告包括针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书以及对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对；

第一设置模块，配置为以所述第一计算单元作为提供所述第一计算任务的计算服务的 TLS 服务端，将所述第一证书对设置为所述 TLS 服务端的证书对；并且以所述第一计算单元作为与所述至少一个其他计算任务连接的 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信根证书。

31. 一种为计算单元分发证书的装置，部署在可信证书生成器中，所述装置包括：

第一请求接收模块，配置为从运行第一计算任务的第一计算单元接收第一证书请求，所述第一证书请求包括第一任务分组的第一组标识，以及第一认证信息，所述第一认证信息用于对所述第一计算单元进行认证，且包括所述第一计算任务的第一代码哈希；

单元认证模块，配置为根据所述第一认证信息对所述第一计算单元进行认证；

分组判断模块，配置为在认证通过的情况下，根据所述第一代码哈希判断所述第一计算任务是否属于所述第一任务分组；

证书获取模块，配置为在确认所述第一计算任务属于所述第一任务分组的情况下，获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和对应的第一公钥证书，所述第一公钥证书与所述第一私钥相匹配，构成第一证书对；

第一报告发送模块，配置为向所述第一计算单元发送第一证书报告，所述第一证书报告包括所述第一根证书和所述第一证书对，使得所述第一计算单元以自身为提供计算服务的 TLS 服务端和与其他计算任务连接的 TLS 客户端，将所述第一证书对设置为 TLS 服务端的证书对，将所述第一根证书设置为 TLS 客户端的可信根证书。

32. 一种获取证书以进行多方安全计算的装置，部署在用户终端中，所述装置包括：

第二请求发送模块，配置为向可信证书生成器发送第二证书请求，所述第二证书请求中包括，期望连接的第一任务分组的第一组标识；

第二报告接收模块，配置为从所述可信证书生成器接收第二证书报告，所述第二证书报告至少包括针对所述第一组标识生成的第一证书链中的第一根证书，所述第一证书链还包括与所述第一根证书对应的第一公钥证书；所述第一公钥证书和匹配的第一私钥构成第一证书对，被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的

至少一个计算单元;

第二设置模块，配置为以所述用户终端为 TLS 客户端，将所述第一根证书设置为所述 TLS 客户端的可信根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

33. 一种为用户终端分发证书的装置，部署在可信证书生成器中，所述装置包括:

第二请求接收模块，配置为接收用户终端发送的第二证书请求，所述第二证书请求中包括，所述用户终端期望连接的第一任务分组的第一组标识;

证书获取模块，配置为获取预先针对所述第一组标识生成的第一证书链和第一私钥，所述第一证书链包括第一根证书和与其对应的第一公钥证书，所述第一公钥证书与所述第一私钥匹配，构成第一证书对; 至少所述第一证书对被预先分发给经过认证的、运行所述第一任务分组中各个计算任务的至少一个计算单元;

第二报告发送模块，配置为向所述用户终端发送第二证书报告，所述第二证书报告至少包括所述第一根证书，以使得所述用户终端以自身为 TLS 客户端，将所述第一根证书作为 TLS 客户端的可信根证书，从而与具有所述第一证书对、且作用为 TLS 服务端的所述至少一个计算单元通信。

34. 一种通过数字证书进行多方安全计算的装置，部署在运行第一计算任务的第一计算单元中，其中:

所述第一计算任务预先被配置为属于第一任务分组，所述第一任务分组还包括第二计算单元所运行的第二计算任务;

所述第一计算单元预先被分发有针对所述第一任务分组生成的第一证书对和第一根证书，所述第一证书对包括第一公钥证书和匹配的第一私钥，所述第一公钥证书和第一根证书构成第一证书链;

并且，所述第一计算单元被配置作为提供所述第一计算任务的计算服务的第一 TLS 服务端，该第一 TLS 服务端以所述第一证书对作为其证书对; 所述第一计算单元还被配置作为至少与所述第二计算单元连接的第一 TLS 客户端，所述第一 TLS 客户端以所述第一根证书作为其可信根证书;

所述装置包括:

第一握手模块，配置为利用所述第一 TLS 服务端与作用为第二 TLS 客户端的用户终端进行 TLS 握手，建立第一 TLS 可信通道; 其中所述第二 TLS 客户端将所述第一根证书作为其可信根证书;

数据接收模块，配置为通过所述第一 TLS 可信通道接收第一用户数据;

数据处理模块，配置为对所述第一用户数据进行第一处理，得到第一应用数据；

第二握手模块，配置为利用所述第一 TLS 客户端与作用为第二 TLS 服务端的第二计算单元进行 TLS 握手，建立第二 TLS 可信通道；其中所述第二 TLS 服务端将所述第一证书对作为其证书对；

数据发送模块，配置为通过所述第二 TLS 可信通道将所述第一应用数据传送给所述第二计算单元。

35.一种计算机可读存储介质，其上存储有计算机程序，当所述计算机程序在计算机中执行时，令计算机执行权利要求 1-29 中任一项的所述的方法。

36. 一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-29 中任一项所述的方法。

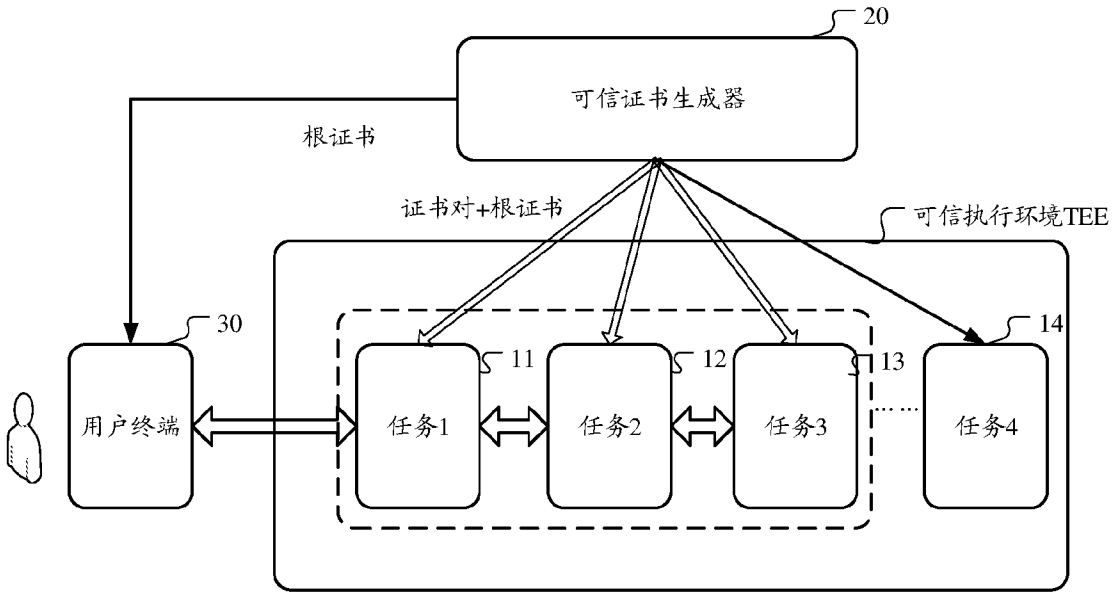
20
可信证书生成器
根证书
证书对+根证书
可信执行环境TEE
30
14
11
12
13
用户终端
任务1
任务2
任务3
任务4

图 1

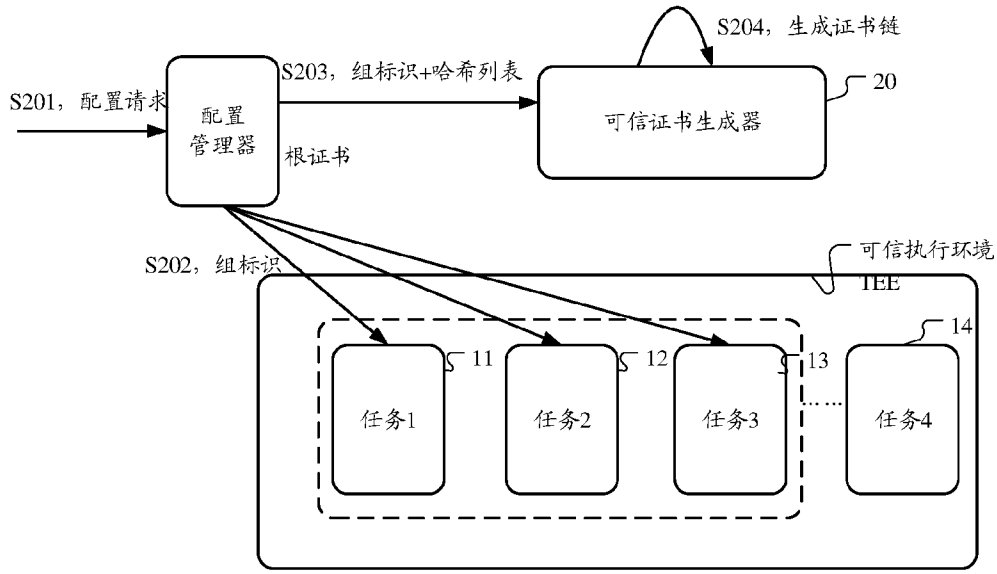
S204，生成证书链
S203，组标识+哈希列表
S201，配置请求
配置
管理器
根证书
20
可信证书生成器
S202，组标识
可信执行环境
TEE
14
11
12
13
任务1
任务2
任务3
任务4

图 2

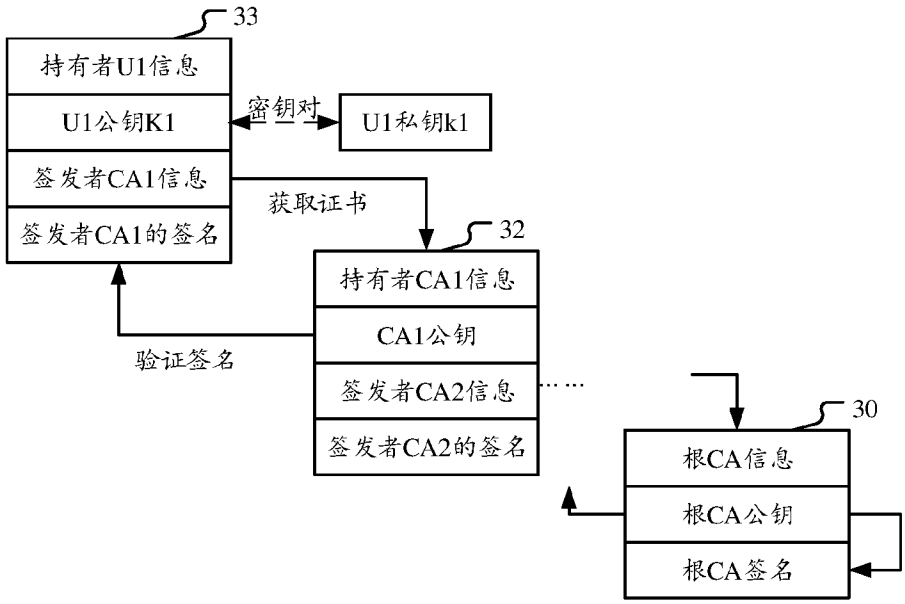
33
持有者U1信息
U1公钥K1
密钥对
U1私钥k1
签发者CA1信息
签发者CA1的签名
获取证书
32
持有者CA1信息
CA1公钥
验证签名
签发者CA2信息
签发者CA2的签名
30
根CA信息
根CA公钥
根CA签名

图 3

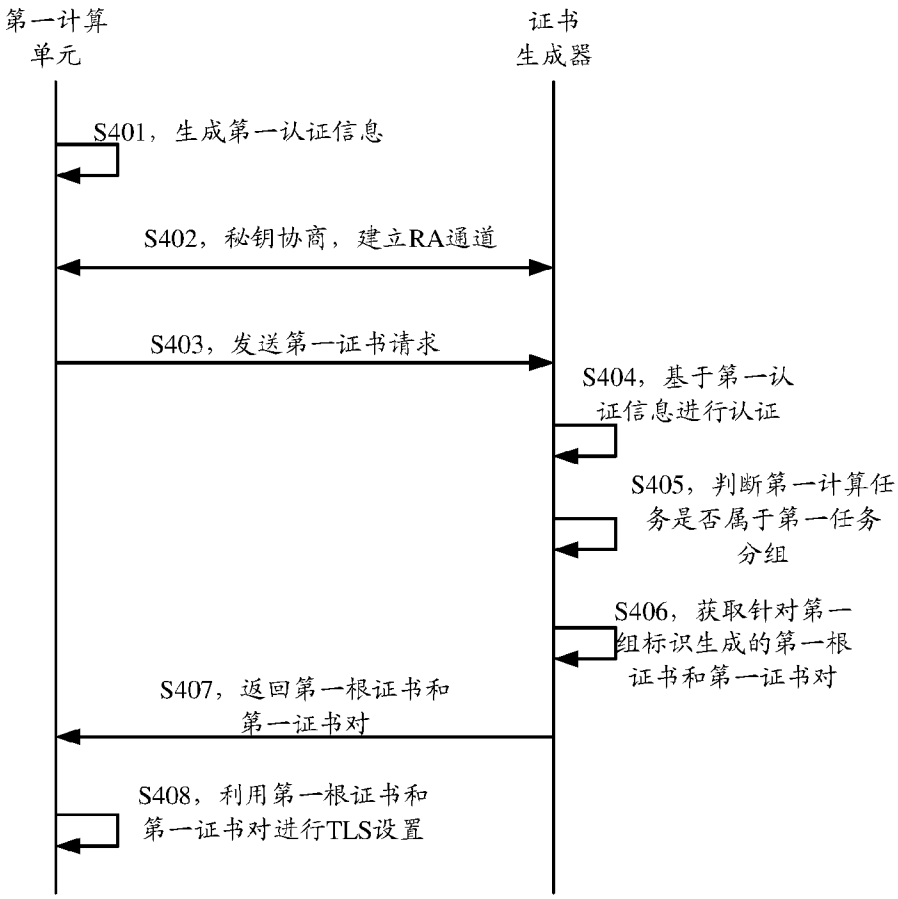
第一计算单元
证书生成器
S401，生成第一认证信息
S402，秘钥协商，建立RA通道
S403，发送第一证书请求
S404，基于第一认证信息进行认证
S405，判断第一计算任务是否属于第一任务分组
S406，获取针对第一组标识生成的第一根证书和第一证书对
S407，返回第一根证书和第一证书对
S408，利用第一根证书和第一证书对进行TLS设置

图 4

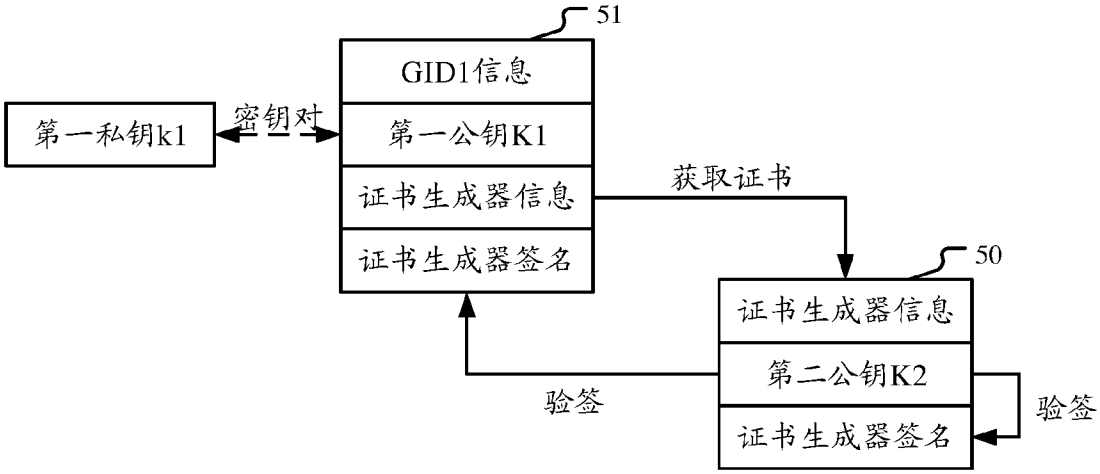
51
GID1信息
第一私钥k1
密钥对
第一公钥K1
证书生成器信息
证书生成器签名
获取证书
50
证书生成器信息
第二公钥K2
证书生成器签名
验签
验签

图 5

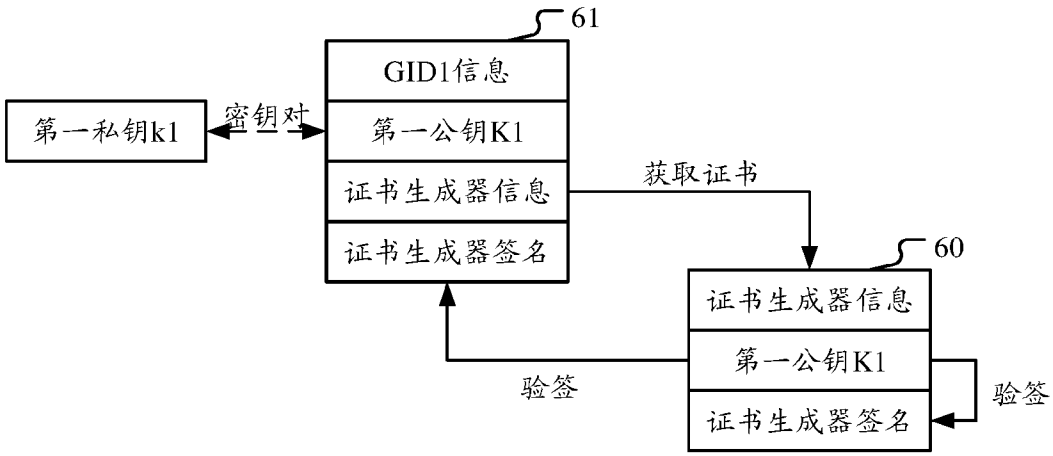
61
GID1信息
第一私钥k1
密钥对
第一公钥K1
证书生成器信息
证书生成器签名
获取证书
60
证书生成器信息
第一公钥K1
证书生成器签名
验签
验签

图 6

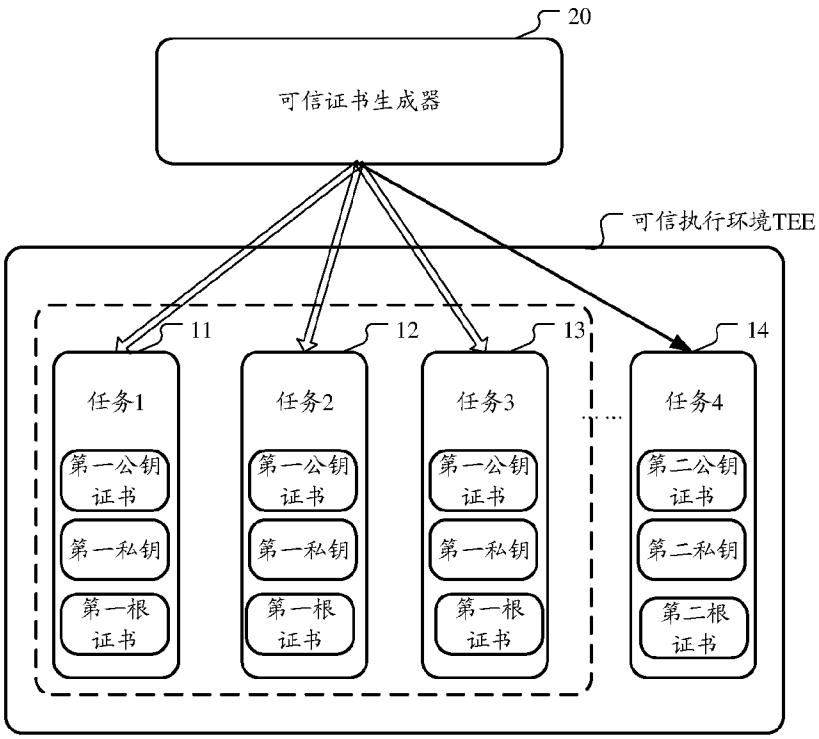
20
可信证书生成器
可信执行环境TEE
11
12
13
14
任务1
任务2
任务3
任务4
第一公钥证书
第一私钥
第一根证书
第一公钥证书
第一私钥
第一根证书
第一公钥证书
第一私钥
第一根证书
第二公钥证书
第二私钥
第二根证书

图 7

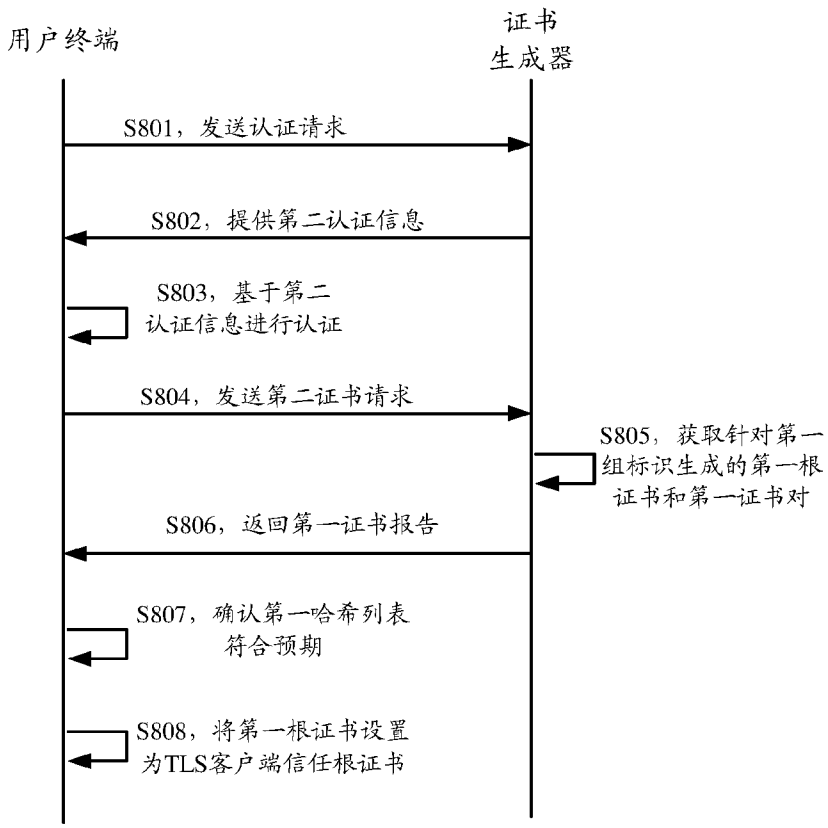
用户终端
证书生成器
S801，发送认证请求
S802，提供第二认证信息
S803，基于第二认证信息进行认证
S804，发送第二证书请求
S805，获取针对第一组标识生成的第一根证书和第一证书对
S806，返回第一证书报告
S807，确认第一哈希列表符合预期
S808，将第一根证书设置为TLS客户端信任根证书

图 8

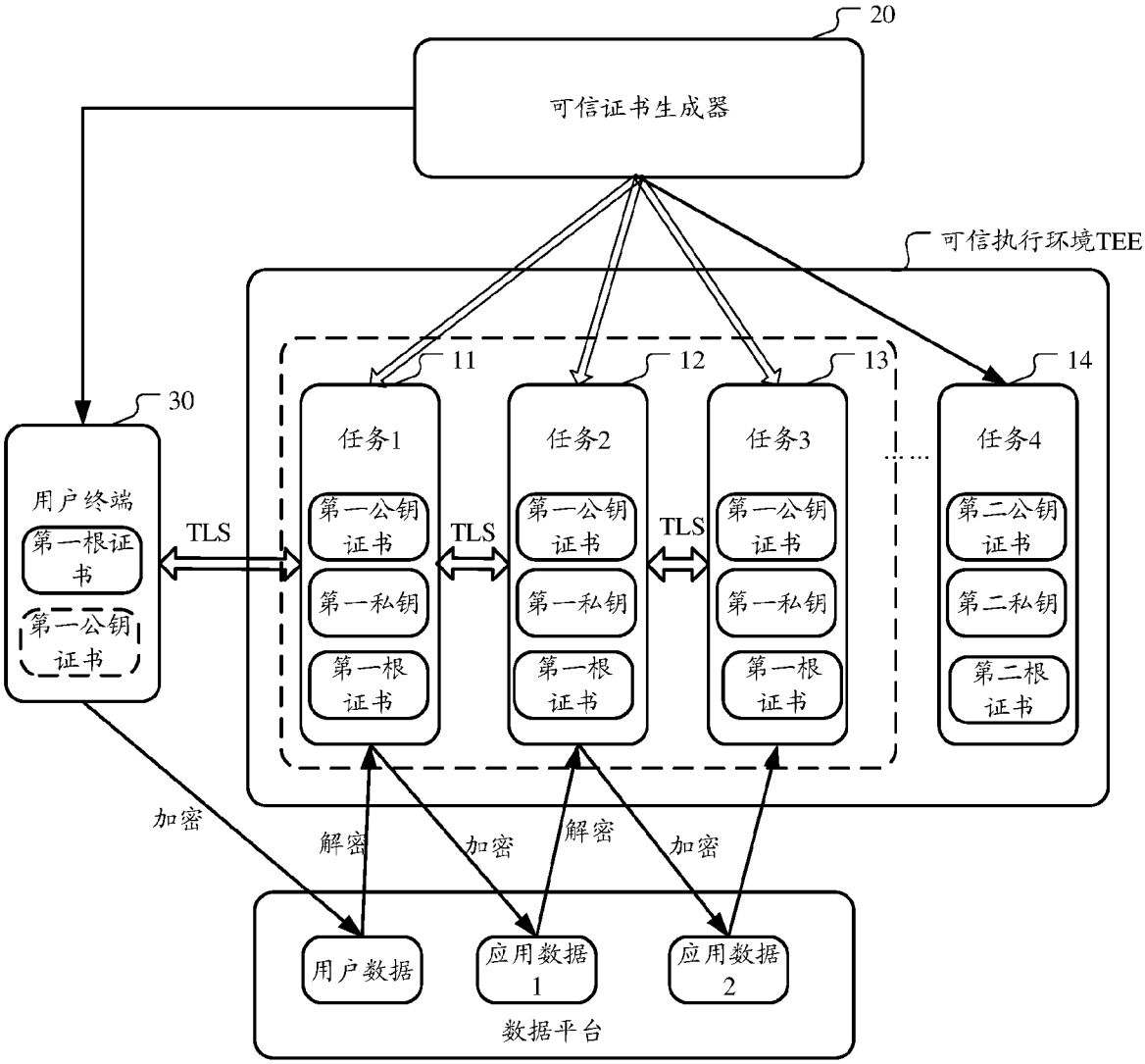
20
可信证书生成器
可信执行环境TEE
11
12
13
14
30
任务1
任务2
任务3
任务4
用户终端
第一根证书
第一公钥证书
TLS
TLS
TLS
第一公钥证书
第一私钥
第一根证书
第一公钥证书
第一私钥
第一根证书
第一公钥证书
第一私钥
第一根证书
第二公钥证书
第二私钥
第二根证书
加密
解密
加密
解密
加密
用户数据
应用数据1
应用数据2
数据平台

图 9

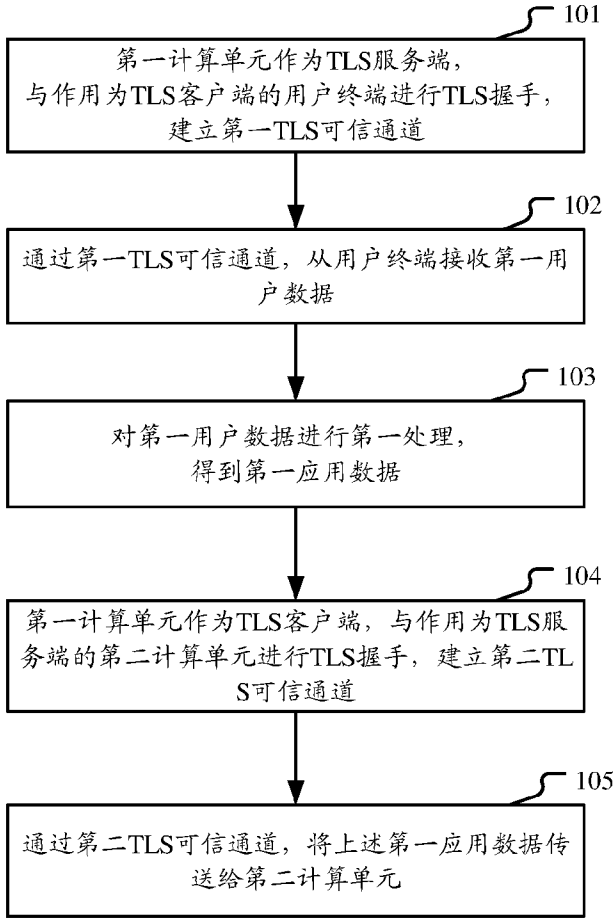
101
第一计算单元作为TLS服务端，
与作用为TLS客户端的用户终端进行TLS握手，
建立第一TLS可信通道
102
通过第一TLS可信通道，从用户终端接收第一用户数据
103
对第一用户数据进行第一处理，
得到第一应用数据
104
第一计算单元作为TLS客户端，与作用为TLS服务端的第二计算单元进行TLS握手，建立第二TLS可信通道
105
通过第二TLS可信通道，将上述第一应用数据传送给第二计算单元

图 10

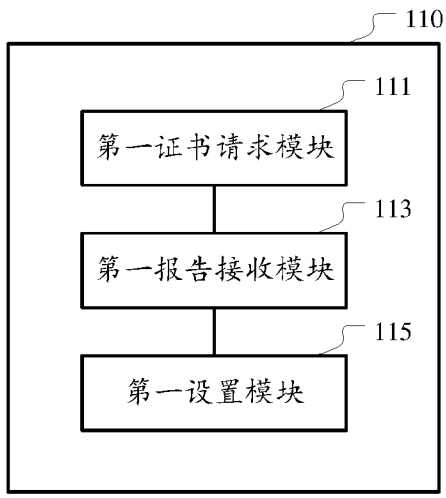
110
111
第一证书请求模块
113
第一报告接收模块
115
第一设置模块

图 11

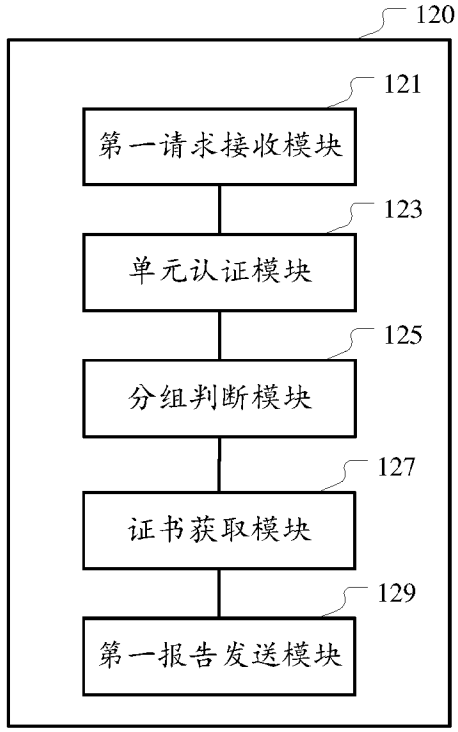
120
121
第一请求接收模块
123
单元认证模块
125
分组判断模块
127
证书获取模块
129
第一报告发送模块

图 12

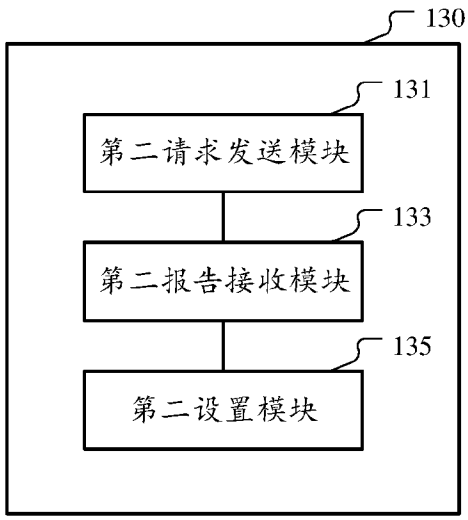
130
131
第二请求发送模块
133
第二报告接收模块
135
第二设置模块

图 13

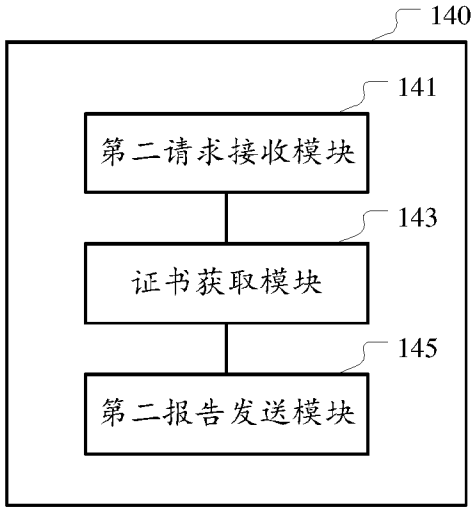
140
141
第二请求接收模块
143
证书获取模块
145
第二报告发送模块

图 14

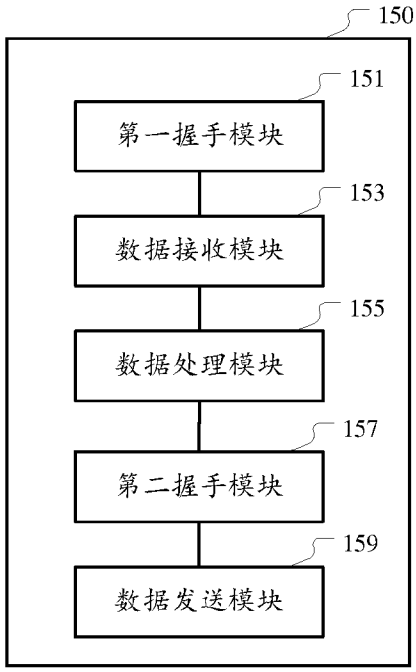
150
151
第一握手模块
153
数据接收模块
155
数据处理模块
157
第二握手模块
159
数据发送模块

图 15

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/072112

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/06(2006.01)i; H04L 9/08(2006.01)i; 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

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; CNKI; WOTXT; EPTXT; USTXT: 可信计算, 证书, 集群, 群, 组, 标识, 私钥, 公钥, 证书链, 认证, 终端, 用户, TEE, certificate, group, cluster, ID, private key, public key, PK, chain, authentication, terminal, user

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110535628 A (ALIBABA GROUP HOLDING LIMITED) 03 December 2019 (2019-12-03) claims 1-36, description, paragraphs [0006]-[0325]	1-36
PX	CN 110677240 A (ALIBABA GROUP HOLDING LIMITED) 10 January 2020 (2020-01-10) claims 1-28, description, paragraphs [0006]-[0237]	1-36
A	CN 108881252 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD. et al.) 23 November 2018 (2018-11-23) description, paragraphs [0046]-[0136]	1-36
A	US 2006036850 A1 (ENOKIDA TOMOAKI) 16 February 2006 (2006-02-16) description, paragraphs [0136]-[0566]	1-36

☐ 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
01 May 2020	**02 June 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/CN2020/072112

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110535628 A	03 December 2019	None	
CN 110677240 A	10 January 2020	None	
CN 108881252 A	23 November 2018	CN 110493273 A	22 November 2019
US 2006036850 A1	16 February 2006	US 2005033957 A1	10 February 2005
		JP 2005039790 A	10 February 2005
		EP 1492305 B1	19 March 2008
		DE 602004012485 T2	05 March 2009
		JP 4504099 B2	14 July 2010
		EP 1492305 A2	29 December 2004
		US 7489783 B2	10 February 2009
		DE 602004012485 D1	30 April 2008
		EP 1492305 A3	30 August 2006
		US 6981139 B2	27 December 2005

国际检索报告

国际申请号
PCT/CN2020/072112

A. 主题的分类

H04L 9/06(2006.01)i; H04L 9/08(2006.01)i; 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

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;CNKI;WOTXT;EPTXT;USTXT:可信计算，证书，集群，群，组，标识，私钥，公钥，证书链，认证，终端，用户，TEE，certificate，group，cluster，ID，private key，public key，PK，chain，authentication，terminal，user

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 110535628 A (阿里巴巴集团控股有限公司) 2019年 12月 3日 (2019-12-03) 权利要求1-36，说明书[0006]-[0325]段	1-36
PX	CN 110677240 A (阿里巴巴集团控股有限公司) 2020年 1月 10日 (2020-01-10) 权利要求1-28，说明书[0006]-[0237]段	1-36
A	CN 108881252 A (腾讯科技深圳有限公司 等) 2018年 11月 23日 (2018-11-23) 说明书[0046]-[0136]段	1-36
A	US 2006036850 A1 (ENOKIDA TOMOAKI) 2006年 2月 16日 (2006-02-16) 说明书[0136]-[0566]段	1-36

☐ 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
2020年 5月 1日	2020年 6月 2日

ISA/CN的名称和邮寄地址	受权官员
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	薛乐梅
传真号 (86-10)62019451	电话号码 86-(20)-28950448

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/072112

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	110535628	A	2019年 12月 3日	无			
CN	110677240	A	2020年 1月 10日	无			
CN	108881252	A	2018年 11月 23日	CN	110493273	A	2019年 11月 22日
US	2006036850	A1	2006年 2月 16日	US	2005033957	A1	2005年 2月 10日
				JP	2005039790	A	2005年 2月 10日
				EP	1492305	B1	2008年 3月 19日
				DE	602004012485	T2	2009年 3月 5日
				JP	4504099	B2	2010年 7月 14日
				EP	1492305	A2	2004年 12月 29日
				US	7489783	B2	2009年 2月 10日
				DE	602004012485	D1	2008年 4月 30日
				EP	1492305	A3	2006年 8月 30日
				US	6981139	B2	2005年 12月 27日