(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 10 月 21 日 (21.10.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/208906 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2021/086900

(22) 国际申请日: 2021 年 4 月 13 日 (13.04.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010307601.2 2020年4月17日 (17.04.2020) CN

(71) 申请人: 支付宝（杭州）信息技术有限公司 (**ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.**) [CN/CN]; 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(72) 发明人: 王磊 (**WANG, Lei**); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。 余超凡 (**YU, Chaofan**); 中国浙江省杭州市西湖区西溪路 556 号 8 层 B 段 801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街 9 号嘉华大厦 B 座 409, Beijing 100085 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK,

(54) **Title:** DATA TRANSMISSION, PROCESSING, AND AUTHORIZATION

(54) 发明名称: 数据传输、处理、授权

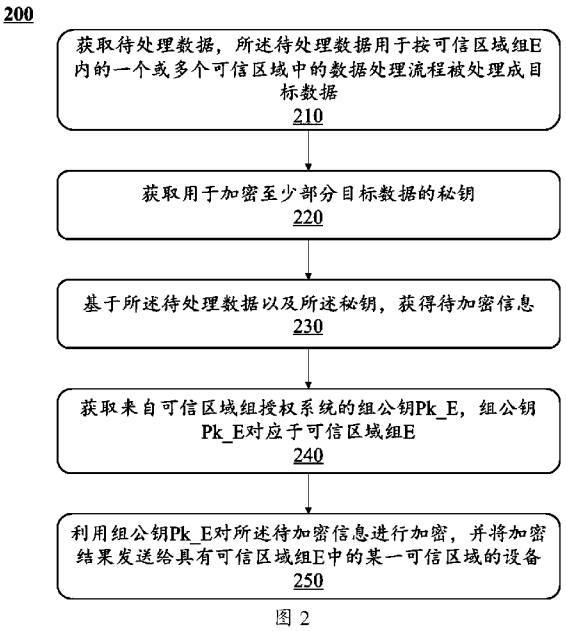

图 2

219 Acquire data to be processed, said data being used for being processed into target data according to a data processing process in one or more trusted zones of a trusted zone group E

220 Acquire key used for encrypting at least some of the target data

230 Acquire, on the basis of said data and of the key, information to be encrypted

240 Acquire group public key Pk_E from a trusted zone group authorization system, group public key Pk_E corresponding to trusted zone group E

250 Encrypt said information by utilizing group public key Pk_E and transmit an encryption result to a device of a trusted zone in the trusted zone group E

(57) **Abstract:** Provided in the embodiments of the present description are a method for data transmission, processing, and authorization and a system thereof. Private data of different parties can be processed into target data according to a data processing process in one or more trusted zones of a trusted zone group, data to be processed or result data always carries a key from a specified party before being securely transmitted to the trusted zones, the two are encrypted together, when a trusted zone of the trusted zone group acquires the target data and the decrypted key from the specified party, at least some of the target data is encrypted using the key, and the at least some of the target data encrypted using the key is then outputted. As such, data privacy of the different parties is effectively safeguarded.

WO 2021/208906 A1

[见续页]

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：本说明书中的实施例提供了数据传输、处理、授权方法及其系统。各方的私密数据可按可信区域组内的一个或多个可信区域内的数据处理流程被处理成目标数据，待处理数据或结果数据在安全传输至可信区域前始终携来自指定方的秘钥，两者被一并加密，可信区域组内的某一可信区域获得目标数据以及解密出的来自指定方的秘钥后，使用该秘钥加密至少部分目标数据，再将使用该秘钥加密后的至少部分目标数据输出。如此，可以有效保护各方数据隐私。

数据传输、处理、授权

技术领域

[01]本说明书实施例涉及信息技术领域，特别涉及数据传输、处理、授权。

背景技术

[02]在可信执行环境（Trusted Execution Environment，TEE）中联合多方的私密数据进行数据处理时，除了需要对数据的处理代码进行限制，以避免数据滥用和隐私泄漏，还有一种需求，就是希望在 TEE 中进行数据处理后输出的结果（如，模型、预测结果、统计信息等）只能由指定方使用，以避免数据滥用。目前，希望提供一种可避免在 TEE 中进行数据处理后输出的结果被滥用的方案。

发明内容

[03]本说明书实施例之一提供一种数据传输方法，其中，所述方法由数据提供方的设备执行，其包括：获取待处理数据，所述待处理数据用于按可信区域组内的一个或多个可信区域中的数据处理流程被处理成目标数据；获取用于加密至少部分目标数据的秘钥；基于所述待处理数据以及所述秘钥，获得待加密信息；获取来自可信区域组授权系统的组公钥，所述组公钥对应于所述可信区域组；使用所述组公钥加密所述待加密信息，并将加密结果发送给具有所述可信区域内某一可信区域的设备。

[04]本说明书实施例之一提供一种数据传输系统，其中，包括：待处理数据获取模块，用于获取待处理数据，所述待处理数据用于按可信区域组内的一个或多个可信区域中的数据处理流程被处理成目标数据；秘钥获取模块，用于获取用于加密至少部分目标数据的秘钥；第一待加密信息获得模块，用于基于所述待处理数据以及所述秘钥，获得待加密信息；组公钥获取模块，获取来自可信区域组授权系统的组公钥，所述组公钥对应于所述可信区域组；第一加密模块，用于使用所述组公钥加密所述待加密信息，并将加密结果发送给具有所述可信区域组内的某一可信区域的设备。

[05]本说明书实施例之一提供一种数据传输装置，其中，包括处理器和存储设备，所述存储设备用于存储指令，当所述处理器执行指令时，实现如本说明书任一实施例所述的数据传输方法。

[06]本说明书实施例之一提供一种数据处理方法，其中，所述方法在可信区域组内的某一可信区域中执行，其包括：接收密文；获取来自可信区域组授权系统的组公钥和组私钥，所述组公钥和组私钥与所述可信区域组对应；使用所述组私钥解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥；对所述待处理数据执行数据处理流程，以得到结果数据；基于所述结果数据以及所述秘钥，获得待加密信息；使用所述组私钥加密所述待加密信息，并将加密结果发送给所述可信区域组内的其他可信区域。

[07]本说明书实施例之一提供一种数据处理系统，其中，所述系统在可信区域组内的某一可信区域中实现，其包括：第一接收模块，用于接收密文；组公私钥获取模块，用于获取来自可信区域组授权系统的组公钥和组私钥，所述组公钥和组私钥与所述可信区域组对应；第一解密模块，用于使用所述组私钥解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥；数据处理模块，用于对所述待处理数据执行数据处理流程，以得到结果数据；第二待加密信息获得模块，用于基于所述结果数据以及所述秘钥，获得待加密信息；第二加密模块，用于使用所述组私钥加密所述待加密信息，并将加密结果发送给所述可信区域组内的其他可信区域。

[08]本说明书实施例之一提供一种数据处理装置，其中，包括处理器和存储设备，所述存储设备用于存储指令，当所述处理器执行指令时，实现如本说明书任一实施例所述的数据处理方法。

[09]本说明书实施例之一提供一种数据授权方法，其中，所述方法在可信区域组内的某一可信区域中执行，其包括：接收密文；获取来自可信区域组授权系统的组私钥，所述组私钥与所述可信区域组对应；使用所述组私钥解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥；基于所述待处理数据获得目标数据；利用所述秘钥加密至少部分目标数据；输出经过加密的至少部分目标数据。

[10]本说明书实施例之一提供一种数据授权系统，其中，所述系统在可信区域组内的某一可信区域中实现，其包括：第二接收模块，用于接收密文；组私钥获取模块，用于获取来自可信区域组授权系统的组私钥，所述组私钥与所述可信区域组对应；第二解密模块，用于使用所述组私钥解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥；目标数据获得模块，用于基于所述待处理数据获得目标数据；第三加密模块，用于利用所述秘钥加密至少部分目标数据；输出模块，用于输出经过加密的至少部分目标数据。

[11]本说明书实施例之一提供一种数据授权装置，其中，包括处理器和存储设备，所述

存储设备用于存储指令，当所述处理器执行指令时，实现如本说明书任一实施例所述的数据授权方法。

附图说明

[12]本说明书将以示例性实施例的方式进一步说明，这些示例性实施例将通过附图进行详细描述。这些实施例并非限制性的，在这些实施例中，相同的编号表示相同的结构。

[13]图 1 是根据本说明书一些实施例所示的数据共享系统的应用场景示意图;

[14]图 2 是根据本说明书一些实施例所示的数据传输方法的示例性流程图;

[15]图 3 是根据本说明书一些实施例所示的数据处理方法的示例性流程图;

[16]图 4 是根据本说明书一些实施例所示的数据在可信区域组内安全传输的示意图;

[17]图 5 是根据本说明书一些实施例所示的数据授权方法的示例性流程图;

[18]图 6 是根据本说明书一些实施例所示的数据传输系统的示例性框图;

[19]图 7 是根据本说明书一些实施例所示的数据处理系统的示例性框图;

[20]图 8 是根据本说明书一些实施例所示的数据授权系统的示例性框图。

具体实施方式

[21]为了更清楚地说明本说明书实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单的介绍。显而易见地，下面描述中的附图仅仅是本说明书的一些示例或实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图将本说明书应用于其它类似情景。除非从语言环境中显而易见或另做说明，图中相同标号代表相同结构或操作。

[22]应当理解，本文使用的“系统”、“装置”、“单元”和/或“模组”是用于区分不同级别的不同组件、元件、部件、部分或装配的一种方法。然而，如果其他词语可实现相同的目的，则可通过其他表达来替换所述词语。

[23]如本说明书和权利要求书中所示，除非上下文明确提示例外情形，“一”、“一个”、“一种”和/或“该”等词并非特指单数，也可包括复数。一般说来，术语“包括”与“包含”仅提示包括已明确标识的步骤和元素，而这些步骤和元素不构成一个排它性的罗列，方法或者设备也可能包含其它的步骤或元素。

[24]本说明书中使用了流程图用来说明根据本说明书的实施例的系统所执行的操作。应当理解的是，前面或后面操作不一定按照顺序来精确地执行。相反，可以按照倒序或同时处理各个步骤。同时，也可以将其他操作添加到这些过程中，或从这些过程移除某一步或数步操作。

[25]在一些场景下，需要联合多方的私密数据进行数据处理。例如，数据提供方 A 持有特征数据，数据提供方 B 持有私密的标签数据，需要联合两方各自持有的特征数据和标签数据进行模型训练。又如，多个数据提供方持有私密且不同的特征数据，联合多方的特征数据进行模型训练可以提高模型的精度，或者需要联合多方的特征数据进行模型预测。需要说明的是，虽然本说明书中主要以机器学习为例进行了说明，但是本说明书中的原理同样可以应用到其他需要联合多方的私密数据进行数据处理的场景，例如，联合多方的私密数据进行数据统计、数据分析等等。

[26]为了避免各方私密数据被泄露和滥用，各方可以将数据加密后上传至具有可信区域的设备（也可称为具备 TEE 的设备，或简称为 TEE 设备），TEE 设备在可信区域内解密出各方的私密数据，并对各方的私密数据进行数据处理。可信区域内存储有数据处理代码，该代码在可信区域内运行且实现相应的数据处理流程。外界（如，设备的操作系统）无法访问可信区域内的数据和代码，因此，在可信区域内联合各方的私密数据进行数据处理，可以避免各方私密数据被泄露滥用。在一些实施例中，本说明书中提及的可信区域可以包括 SGX（Software Guard eXtensions，软件保护拓展）可信执行环境中的 Enclave（飞地）。

[27]然后，当在可信区域内处理各方的私密数据得到目标数据后，有时还需要对目标数据的使用权加以限制，以避免目标数据被滥用。换言之，希望目标数据只能由一个或多个指定方使用。例如，目标数据包括模型时，指定方可以包括模型迁移任务中以该模型为初始模型的模型训练方。又如，目标数据包括预测结果时，指定方可以包括预测请求的发起方。又如，目标数据包括可拆分的模型时，可以在可信区域内将该模型拆分成与多个特征方一一对应的多个子模型，其中，每个特征方可作为一个子模型的指定方。进而，多个特征方可使用各自得到的子模型进行联合预测。

[28]本说明书中的实施例提供了数据传输、处理、授权方法及其系统。各方的私密数据可按一个或多个可信区域内的数据处理流程被处理成目标数据，待处理数据或结果数据在传输至可信区域前始终携来自指定方的秘钥，两者被一并加密，某一可信区域获得目标数据以及解密出的来自指定方的秘钥后，使用该秘钥加密至少部分目标数据，再将使

用该秘钥加密后的至少部分目标数据输出。如此，只有指定方可以解密出所述至少部分目标数据进行使用，可避免目标数据被滥用。

[29]图 1 是根据本说明书一些实施例所示的数据共享系统的应用场景示意图。如图 1 所示，数据共享系统 100 可以包括两个以上数据提供方的设备 110、具有可信区域的设备 120 以及网络 150。

[30]数据提供方的设备 110 可以将待处理的私密数据携用于加密至少部分目标数据的秘钥一并加密后，将加密结果上传至具有可信区域的设备 120。在一些实施例中，各方的私密数据按一个或多个可信区域内的数据处理流程被处理成目标数据后，数据提供方的设备 110 可以获取经过加密的至少目标数据，若数据提供方的设备 110 持有用于解密该至少部分目标数据的秘钥，即可解密出该至少部分目标数据进行使用。

[31]数据提供方的设备 110 可以包括各类具有信息接收和/或发送功能的设备。在一些实施例中，数据提供方的设备 110 可以包括智能电话、平板计算机、膝上型计算机、台式计算机、服务器等中的一种或其任意组合。

[32]在一些实施例中，本说明书中提及的服务器可以是独立的服务器或者服务器组，该服务器组可以是集中式的或者分布式的。在一些实施例中，服务器可以是区域的或者远程的。在一些实施例中，服务器可在云平台上执行。例如，该云平台可包括私有云、公共云、混合云、社区云、分散式云、内部云等中的一种或其任意组合。

[33]具有可信区域的设备 120 可以包括各类计算设备，如服务器。数据共享系统 100 可以包括一个或多个具有可信区域的设备。在一些实施例中，具有可信区域的设备 120 可以获取来自多个数据提供方的密文，在可信区域内解密出来自各方的私密数据（以及用于加密至少部分目标数据的秘钥）并联合各方的私密数据进行数据处理，得到中间结果数据或目标数据。

[34]在一些实施例中，各方的私密数据可以按多个可信区域内的数据处理流程被处理为目标数据，获得私密数据的可信区域经数据处理得到中间结果数据后，可以将中间结果数据携解密出的用于加密至少部分目标数据的秘钥一并加密，并将加密结果传输至下一可信区域。每个负责数据处理的可信区域都可按上述流程加密传输数据，直至有可信区域获得目标数据。

[35]在一些实施例中，负责数据处理的可信区域经数据处理得到目标数据后，可用解密出的秘钥加密至少部分目标数据，并输出经过加密的至少部分目标数据。在一些实施例

中，负责数据处理的可信区域经数据处理得到目标数据后，可以将目标数据携用于加密至少部分目标数据的秘钥一并加密后，将加密结果发送给负责数据授权的可信区域。负责数据授权的可信区域解密出目标数据以及用于加密至少部分目标数据的秘钥后，可用解密出的秘钥加密至少部分目标数据，并输出经过加密的至少部分目标数据。

[36]值得说明的是，同一设备上可以创建一个可信区域，也可以创建多个可信区域。例如，可以在设备 120 上同时创建可信区域 E1、可信区域 E2 和可信区域 E3。换句话说，多个可信区域可以位于同一设备上，也可以分别部署于不同的设备上。

[37]在一些实施例中，数据共享系统 100 还可以包括第三方设备 130。第三方设备 130 可以获取经过加密的至少部分目标数据，若第三方设备 130 持有用于解密该至少部分目标数据的秘钥，即可解密出该至少部分目标数据进行使用。例如，第三方设备 130 可以获取用第三方设备 130 的公钥加密的模型，进而可用第三方设备 130 本地的私钥解密出模型进行使用，具体地，可以将解密出的模型作为初始模型继续进行模型训练。

[38]第三方设备130可以包括各类具有信息接收和/或发送功能的设备。在一些实施例中，数据提供方的设备 110 可以包括智能电话、平板计算机、膝上型计算机、台式计算机、服务器等中的一种或其任意组合。

[39]在一些实施例中，数据共享系统 100 还可以包括可信区域组授权系统 140。当基于多方私密数据的数据处理及数据授权的任务（以下简称数据共享任务）由多个可信区域（逻辑上组成一个可信区域组）共同负责时，可信区域组授权系统 140 可以为同组的可信区域提供统一的用于数据加密/解密的秘钥，如包括组公钥和组私钥的公私钥对，以便数据在可信区域组内的安全传输。

[40]具体地，可信区域组授权系统 140 可以获取待组网的多个可信区域的标识信息（也可称为签名信息），为所述多个可信区域组成的可信区域组生成公私钥对，将所述多个可信区域的签名信息以及所述公私钥对保存为所述可信区域组的组别信息。可信区域组授权系统 140 可以保存多个可信区域组的组别信息，不同的可信区域组可以负责不同的数据共享任务。相应地，准备启动同一数据共享任务的各数据提供方的设备 110 可以向可信区域组授权系统 140 获取该数据共享任务对应的组别信息，需要注意的是，数据提供方的设备 110 获取的组别信息是缺少组私钥的。进而，各数据提供方的设备 110 可以用该组别信息中的公钥加密待加密信息，并将加密结果上传至具有该组别信息中某一签名信息对应的可信区域的设备 120。

[41]在一些实施例中，可信区域的标识信息可以包括预期在该可信区域内运行的代码的哈希值。可信区域组内的各可信区域在执行数据共享任务（运行代码）之前，具有组内可信区域的设备可以向可信区域组授权系统 140 发起远程认证，远程认证通过后再执行数据共享任务。远程认证过程中，具有组内可信区域的设备可以向可信区域组授权系统 140 提交可信区域中运行的代码的哈希值，可信区域组授权系统 140 获取预先保存的组别信息中该可信区域的代码的哈希值，比对两个哈希值可验证该可信区域中是否会运行预期的代码，若哈希值不一致，则远程认证不通过。可信区域组授权系统 140 可以在远程认证通过后再将组别信息中的公私钥对发送给对应的可信区域组内的各可信区域。

[42]网络 150 连接系统 100 的各组成部分，使得各部分之间可以进行通讯。在系统 100 中各部分之间的网络 150 可以包括有线网络和/或无线网络。例如，网络 150 可以包括电缆网络、有线网络、光纤网络、电信网络、内部网络、互联网、局域网络（LAN）、广域网络（WAN）、无线局域网络（WLAN）、城域网（MAN）、公共交换电话网络（PSTN）、蓝牙网络、紫蜂网络（ZigBee）、近场通信（NFC）、设备内总线、设备内线路、线缆连接等中的一种或其任意组合。每两个部分之间的网络连接可以是采用上述一种方式，也可以是采取多种方式。

[43]图 2 是根据本说明书一些实施例所示的数据传输方法的示例性流程图。流程 200 可以由数据提供方的设备 110 执行。如图 2 所示，流程 200 可以包括:

[44]步骤 210，获取待处理数据，所述待处理数据用于按可信区域组（记为 E）内的一个或多个可信区域中的数据处理流程被处理成目标数据。在一些实施例中，步骤 210 可以由待处理数据获取模块 610 实现。

[45]步骤 210 中，待处理数据即数据提供方的私密数据。例如，在有关模型训练的数据共享任务中，所述待处理数据可以包括数据提供方持有的私密的特征数据和/或标签数据，相应地，目标数据可以包括经样本数据（包括各方的特征数据和/或标签数据）训练得到的模型和/或模型信息，其中，模型信息可以包括与模型相关的信息，如模型性能参数、梯度信息等。

[46]步骤 220，获取用于加密至少部分目标数据的秘钥。在一些实施例中，步骤 220 可以由秘钥获取模块 620 实现。

[47]所述秘钥用于加密至少部分目标数据，以防止该至少部分目标数据被滥用，相应地，解密秘钥的持有者可以解密出该至少部分目标数据进行使用。在一些实施例中，所述秘

钥可以包括来自数据提供方的公钥和/或来自第三方设备 130 的公钥。

[48] 例如，加密至少部分目标数据的秘钥可以是某一数据提供方的公钥或者来自第三方设备 130 的公钥。如此，只有该数据提供方的设备 110 或第三方设备 130 可以用本地的私钥解密出该至少部分目标数据进行使用。另外，当至少部分目标数据只能由一个指定方使用，而同一数据共享任务中各数据提供方又没有提供相同的用于加密所述至少部分目标数据的秘钥时，具有可信区域的设备 120 可以拒绝执行数据共享任务，且可以向数据提供方反馈任务执行失败。当参与同一数据共享任务的多个数据提供方中仅部分数据提供方提供了相同的用于加密至少部分目标数据的秘钥，而所述多个数据提供方中的剩余数据提供方未提供用于加密所述至少部分目标数据的秘钥时，具有可信区域的设备 120 可以基于接收到的用于加密所述至少部分目标数据的秘钥继续执行数据共享任务。

[49] 又如，目标数据可以被拆分成多个部分，每部分指定一方可以使用。相应地，所述秘钥可以包括来自多方的公钥，且来自任一方的公钥对应部分目标数据，具有可信区域的设备 120 可以将目标数据拆分成多个部分，并用来自多方的公钥分别加密目标数据中对应的部分。进而，任一方可用本地的私钥解密出部分目标数据进行使用。具体地，在有关模型训练的数据共享任务中，具有可信区域的设备 120 可以将模型拆分成多个子模型，并用来自各特征方的公钥分别加密各子模型，其中，各特征方持有的特征数据不同。进而，任一特征方可用本地的私钥解密出子模型进行使用，即，各特征方可以基于各自解密出的子模型进行多方联合预测。

[50] 步骤 230，基于所述待处理数据以及所述秘钥，获得待加密信息。在一些实施例中，步骤 230 可以由第一待加密信息获得模块 630 实现。

[51] 在一些实施例中，第一待加密信息获得模块 630 可以对所述待处理数据以及所述秘钥进行数据打包，得到待加密信息。

[52] 步骤 240，获取来自可信区域组授权系统 140 的组公钥（记为 Pk_E），组公钥 Pk_E 对应于可信区域组 E。在一些实施例中，步骤 240 可以由组公钥获取模块 640 实现。

[53] 关于组公钥的获取细节，可以参考图 1 披露的可信区域组授权系统 140 的相关描述。

[54] 步骤 250，利用组公钥 Pk_E 对所述待加密信息进行加密，并将加密结果发送给具有可信区域组 E 中的某一可信区域的设备 120。在一些实施例中，步骤 250 可以由第一加密模块 650 实现。

[55] 关于数据在可信区域组内的安全传输，可以参考图 3、图 4 及其相关描述。

[56]图 3 是根据本说明书一些实施例所示的数据处理方法的示例性流程图。流程 300 在可信区域组（记为 E）内的某一可信区域中执行，为了避免混淆，此处的某一可信区域可记为当前可信区域。如图 3 所示，流程 300 可以包括:

[57]步骤 310，接收密文。在一些实施例中，步骤 310 可以由第一接收模块 710 实现。

[58]步骤 320，获取来自可信区域组授权系统 140 的组公钥（记为 Pk_E）和组私钥（记为 Pr_E），组公钥 Pk_E 和组私钥 Pr_E 与可信区域组 E 对应。在一些实施例中，步骤 320 可以由组公私钥获取模块 720 实现。

[59]关于组公钥和组私钥的获取细节，可以参考图 1 披露的可信区域组授权系统 140 的相关描述。

[60]步骤 330，利用组私钥 Pr_E 解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥。在一些实施例中，步骤 320 可以由第一解密模块 730 实现。

[61]在一些实施例中，所述密文可以来自数据提供方的设备 110，其对应的明文包括来自数据提供方的待处理数据（即私密数据）和用于加密至少部分目标数据的秘钥。在一些实施例中，所述密文可以来自可信区域组 E 内的其他可信区域，如上一个负责数据处理的可信区域。

[62]在一些实施例中，所述秘钥可以包括来自数据提供方的公钥和/或来自第三方设备 130 的公钥。

[63]步骤 340，对所述待处理数据执行数据处理流程，以得到结果数据。在一些实施例中，步骤 340 可以由数据处理模块 740 实现。

[64]在一些实施例中，结果数据可以指在获得目标数据之前由某一可信区域中的数据处流程获得的处理结果（以下简称中间结果数据），也可以指由某一可信区域中的数据处流程获得的作为目标数据的处理结果。

[65]在一些实施例中，任一可信区域中的数据处理流程可以包括数据融合流程，数据融合流程可用于将来自多个数据提供方的待处理数据进行融合。例如，在有监督学习中，数据融合流程可用于融合各方的特征数据和标签数据。又如，在无监督学习中，数据融合流程可用于融合各方的特征数据。在一些实施例中，任一可信区域中的数据处理流程可以包括模型训练流程，模型训练流程可用于利用样本数据对模型进行训练。模型训练流程可以采用各类模型训练算法，例如，线性回归算法、逻辑回归算法、XGBoost(eXtreme Gradient Boosting，极端梯度提升）算法、梯度下降算法等中的一种或其任意组合。数

据处理流程还可以是其他与机器学习模型无关的处理过程，本说明书对此不做任何限定。

[66]步骤 350，基于所述结果数据以及所述秘钥，获得待加密信息。在一些实施例中，步骤 350 可以由第二待加密信息获得模块 750 实现。

[67]在一些实施例中，第二待加密信息获得模块 750 可以对所述结果数据以及所述秘钥进行数据打包，得到所述待加密信息。

[68]步骤 360，利用组公钥 Pk_E 加密所述待加密信息，并将加密结果发送给可信区域组 E 内的其他可信区域。在一些实施例中，步骤 360 可以由第二加密模块 760 实现。

[69]在一些实施例中，结果数据为中间结果数据，第二加密模块 760 可以将加密结果从当前可信区域向可信区域组 E 内下一个负责数据处理的可信区域发送。在一些实施例中，结果数据为目标数据，第二加密模块 760 可以将加密结果从当前可信区域向可信区域组 E 内负责数据授权的可信区域发送。

[70]仅作为示例，如图 4 所示，负责数据共享任务的可信区域组 E 包含三个可信区域（可信区域 E1、可信区域 E2 和可信区域 E3），来自数据提供方 A 的待处理数据 data_A 和来自数据提供方 B 的待处理数据 data_B 按可信区域 E1 和可信区域 E2 中的数据处理流程被处理，得到目标数据 S，可信区域 E3 可负责目标数据的发布，用于加密目标数据 S 的秘钥为来自第三方设备 130 的公钥 PubKey_S，可信区域组 E 对应的组公钥和组私钥分别为 PubKey_E 和 PriKey_E。基于此，数据在可信区域组 E 内的安全传输过程可包括：1.在可信区域 E1 中，接收来自数据提供方 A 的密文 M1，密文 M1 对应的明文包括来自数据提供方 A 的待处理数据 data_A 以及来自第三方设备 130 的公钥 PubKey_S，接收来自数据提供方 B 的密文 M2，密文 M2 对应的明文包含来自数据提供方 B 的待处理数据 data_B 以及来自第三方设备 130 的公钥 PubKey_S，其中，密文 M1 和密文 M2 都是用组公钥 PubKey_E 加密的，所以用组私钥 PriKey_E 解密密文 M1 和密文 M2 可得到待处理数据 data_A、待处理数据 data_B 以及公钥 PubKey_S，待处理数据 data_A 和待处理数据 data_B 经处理后得到中间结果数据 data_M，用组公钥 PubKey_E 加密包含中间结果数据 data_M 以及公钥 PubKey_S 在内的明文后，得到密文 M3 并将 M3 发送给可信区域 E2；2.在可信区域 E2 中，接收密文 M3，用组私钥 PriKey_E 解密密文 M3 可得到中间结果数据 data_M 以及公钥 PubKey_S，中间结果数据 data_M 经处理后得到目标数据 data_S，用组公钥 PubKey_E 加密包含目标数据 data_S 以及公钥 PubKey_S 在内的明文后，得到密文 M4 并将 M4 发送给可信区域 E3；在可信区域 E3 中，接收密文 M4，解密密文 M4 可得到目标数据 data_S 以及公钥 PubKey_S，用公钥 PubKey_S 加密目标数

据 data_S 得到密文 M5，输出密文 M5。由于密文 M5 是用来自第三方设备 130 的公钥 PubKey_S 加密的，第三方设备 130 可用本地保存的与公钥 PubKey_S 匹配的私钥解密密文 M5，得到目标数据 data_S 进行使用。

[71]图 5 是根据本说明书一些实施例所示的数据授权方法的示例性流程图。流程 500 在可信区域组（记为 E）内的某一可信区域中执行，为了避免混淆，此处的某一可信区域可称为目标可信区域。如图 5 所示，流程 500 可以包括:

[72]步骤 510，接收密文。在一些实施例中，步骤 510 可以由第二接收模块 810 实现。

[73]步骤 520，获取来自可信区域组授权系统 140 的组私钥（记为 Pr_E），组私钥 Pr_E 与可信区域组 E 对应。在一些实施例中，步骤 520 可以由组私钥获取模块 820 实现。

[74]关于组私钥的获取细节，可以参考图 1 披露的可信区域组授权系统 140 的相关描述。

[75]步骤 530，利用组私钥 Pr_E 解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥。在一些实施例中，步骤 530 可以由第二解密模块 830 实现。

[76]当数据共享任务由包含目标可信区域的可信区域组 E 执行时，所述密文可来自可信区域组 E 内的其他可信区域，其对应的明文包括来自所述其他可信区域的待处理数据（即结果数据）以及用于加密至少部分目标数据的秘钥。所述密文是用可信区域组 E 对应的组公钥 Pk_E 加密所述明文得到的，因此，第二解密模块 830 可以用可信区域组 E 对应的组私钥 Pr_E 解密所述密文，得到所述待处理数据以及用所述秘钥。

[77]步骤 540，基于所述待处理数据获得目标数据。在一些实施例中，步骤 540 可以由目标数据获得模块 840 实现。

[78]在一些实施例中，目标可信区域中解密出的待处理数据可以是目标数据，例如，如图 4 所示，在负责数据授权的可信区域 E3 中可解密出目标数据 data_S。即，目标数据获得模块 830 可以直接将所述待处理数据确定为目标数据。

[79]在一些实施例中，目标可信区域中解密出的待处理数据可以是中间结果数据，目标数据获得模块 830 可以对所述待处理数据执行数据处理流程，以获得目标数据。

[80]在一些实施例中，所述目标数据可包括经样本数据训练得到的模型和/或模型信息，其中，所述样本数据可以通过融合来自各数据提供方的特征数据和/或标签数据得到，模型信息可以包括与模型相关的信息，如模型性能参数、梯度信息等。

[81]步骤 550，利用所述秘钥加密至少部分目标数据。在一些实施例中，步骤 550 可以

由第三加密模块 850 实现。

[82]步骤 560，输出经过加密的至少部分目标数据。在一些实施例中，步骤 560 可以由输出模块 860 实现。

[83]所述秘钥用于加密至少部分目标数据，即，能够使用所述至少部分目标数据的一方应持有相应的解密秘钥才可解密出所述至少部分目标数据。

[84]在一些实施例中，所述秘钥可以包括来自数据提供方的公钥和/或来自第三方设备 130 的公钥。

[85]在一些实施例中，所述秘钥可以包括来自多方的公钥。第三加密模块 850 可以将所述目标数据拆分为多个部分，并分别用来自多方的公钥分别加密目标数据中对应的部分。以目标数据为可拆分的模型为例，第三加密模块 850 可以将完整模型拆分为多个子模型，每个子模型可对应一个特征方（各特征方持有不同的特征数据）。针对每个子模型，第三加密模块 850 可以用来自该特征方的公钥加密该特征方对应的子模型。如此，每个特征方获得经过加密的子模型后，可以用本地的私钥解密出自身对应的子模型进行使用。

[86]应当注意的是，上述有关流程的描述仅仅是为了示例和说明，而不限定本说明书的适用范围。对于本领域技术人员来说，在本说明书的指导下可以对流程进行各种修正和改变。然而，这些修正和改变仍在本说明书的范围之内。

[87]图 6 是根据本说明书一些实施例所示的数据传输系统的示例性框图。系统 600 可以在数据提供方的设备 110 上实现。如图 6 所示，系统 600 可以包括待处理数据获取模块 610、秘钥获取模块 620、第一待加密信息获得模块 630、组公钥获取模块 640 和第一加密模块 650。

[88]在一些实施例中，待处理数据获取模块 610 可以用于获取待处理数据，所述待处理数据用于按可信区域组（记为 E）内的一个或多个可信区域中的数据处理流程被处理成目标数据。

[89]在一些实施例中，秘钥获取模块 620 可用于获取用于加密至少部分目标数据的秘钥。

[90]在一些实施例中，第一待加密信息获得模块 630 可以用于基于所述待处理数据以及所述秘钥，获得待加密信息。

[91]在一些实施例中，组公钥获取模块 640 可以用于获取来自可信区域组授权系统 140 的组公钥（记为 Pk_E），组公钥 Pk_E 对应于可信区域组 E。

[92]在一些实施例中，第一加密模块 650 可以用于使用组公钥 Pk_E 加密所述待加密信息，并将加密结果发送给具有可信区域组 E 内的某一可信区域的设备 120。

[93]关于系统 600 及其模块的更多细节，可以参考图 2 及其相关描述。

[94]图 7 是根据本说明书一些实施例所示的数据处理系统的示例性框图。系统 700 可在可信区域组（记为 E）内的某一可信区域中实现。如图 7 所示，系统 700 可以包括第一接收模块 710、组公私钥获取模块 720、第一解密模块 730、数据处理模块 740、第二待加密信息获得模块 750 和第二加密模块 760。

[95]在一些实施例中，第一接收模块 710 可以用于接收密文。

[96]在一些实施例中，组公私钥获取模块 720 可以用于获取来自可信区域组授权系统 140 的组公钥（记为 Pk_E）和组私钥（记为 Pr_E），组公钥 Pk_E 和组私钥 Pr_E 与可信区域组 E 对应。

[97]在一些实施例中，第一解密模块 730 可以用于利用组私钥 Pr_E 解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥。

[98]在一些实施例中，数据处理模块 740 可以用于对所述待处理数据执行数据处理流程，以得到结果数据。

[99]在一些实施例中，第二待加密信息获得模块 750 可以用于基于所述结果数据以及所述秘钥，获得待加密信息。

[100] 在一些实施例中，第二加密模块 760 可以用于利用组公钥 Pk_E 加密所述待加密信息，并将加密结果发送给可信区域组 E 内的其他可信区域。

[101] 关于系统 700 及其模块的更多细节，可以参考图 3 及其相关描述。

[102] 图 8 是根据本说明书一些实施例所示的数据授权系统的示例性框图。系统 800 可在可信区域组（记为 E）内的某一可信区域中实现。如图 8 所示，系统 800 可以包括第二接收模块 810、组私钥获取模块 820、第二解密模块 830、目标数据获得模块 840、第三加密模块 850 和输出模块 860。

[103] 在一些实施例中，第二接收模块 810 可以用于接收密文。

[104] 在一些实施例中，组私钥获取模块 820 可以用于获取来自可信区域组授权系统 140 的组私钥（记为 Pr_E），组私钥 Pr_E 与可信区域组 E 对应。

[105] 在一些实施例中，第二解密模块 830 可以用于利用组私钥 Pr_E 解密所述密文，

以获得待处理数据以及用于加密至少部分目标数据的秘钥。

[106] 在一些实施例中，目标数据获得模块840可基于所述待处理数据获得目标数据。

[107] 在一些实施例中，第三加密模块850可利用所述秘钥加密至少部分目标数据。

[108] 在一些实施例中，输出模块860可以用于输出经过加密的至少部分目标数据。

[109] 关于系统800及其模块的更多细节，可以参考图5及其相关描述。

[110] 应当理解，本说明书中的系统（如，系统100、系统140、系统600、系统700、系统800等）及其组成部分可以利用各种方式来实现。例如，在一些实施例中，系统及其组成部分可以通过硬件、软件或者软件和硬件的结合来实现。其中，硬件可以利用专用逻辑来实现；软件则可以存储在存储器中，由适当的指令执行系统，例如微处理器或者专用设计硬件来执行。本领域技术人员可以理解上述的方法和系统可以使用计算机可执行指令和/或包含在处理器控制代码中来实现，例如在诸如磁盘、CD或DVD-ROM的载体介质、诸如只读存储器（固件）的可编程的存储器或者诸如光学或电子信号载体的数据载体上提供了这样的代码。本说明书的系统及其组成部分不仅可以有诸如超大规模集成电路或门阵列、诸如逻辑芯片、晶体管等的半导体、或者诸如现场可编程门阵列、可编程逻辑设备等的可编程硬件设备的硬件电路实现，也可以用例如由各种类型的处理器所执行的软件实现，还可以由上述硬件电路和软件的结合（例如，固件）来实现。

[111] 需要注意的是，以上对于系统及其模块的描述，仅为描述方便，并不能把本说明书限制在所举实施例范围之内。可以理解，对于本领域的技术人员来说，在了解系统的原理后，可能在不背离这一原理的情况下，对各个模块进行任意组合，或者构成子系统与其他模块连接。例如，图6中披露的第一待加密信息获得模块630和第一加密模块650可以两个模块，也可以合并为一个模块。又如，在可信区域中实现的任一系统内的加密模块和解密模块以两个模块，也可以合并为一个模块。具体地，可以将在可信区域中实现的任一系统内的加密模块和解密模块封装成易于使用的SDK（Software Development Kit，软件开发工具包）。诸如此类的变形，均在本说明书的保护范围之内。

[112] 本说明书实施例可能带来的有益效果包括但不限于：（1）待处理数据或结果数据在安全传输至可信区域组内的可信区域前始终携来自指定方的秘钥，两者被一并加密，该秘钥用于加密至少部分目标数据，这样只有指定方可以解密出所述至少部分目标数据进行使用，可避免目标数据被滥用；（2）将在可信区域中实现的任一系统内的加密模

块和解密模块封装成 SDK，SDK 更易于编写代码的用户使用。需要说明的是，不同实施例可能产生的有益效果不同，在不同的实施例里，可能产生的有益效果可以是以上任意一种或几种的组合，也可以是其他任何可能获得的有益效果。

[113] 上文已对基本概念做了描述，显然，对于本领域技术人员来说，上述详细披露仅仅作为示例，而并不构成对本说明书实施例的限定。虽然此处并没有明确说明，本领域技术人员可能会对本说明书实施例进行各种修改、改进和修正。该类修改、改进和修正在本说明书实施例中被建议，所以该类修改、改进、修正仍属于本说明书示范实施例的精神和范围。

[114] 同时，本说明书使用了特定词语来描述本说明书的实施例。如“一个实施例”、“一实施例”、和/或“一些实施例”意指与本说明书至少一个实施例相关的某一特征、结构或特点。因此，应强调并注意的是，本说明书中在不同位置两次或多次提及的“一实施例”或“一个实施例”或“一个替代性实施例”并不一定是指同一实施例。此外，本说明书的一个或多个实施例中的某些特征、结构或特点可以进行适当的组合。

[115] 此外，本领域技术人员可以理解，本说明书实施例的各方面可以通过若干具有可专利性的种类或情况进行说明和描述，包括任何新的和有用的工序、机器、产品或物质的组合，或对他们的任何新的和有用的改进。相应地，本说明书实施例的各个方面可以完全由硬件执行、可以完全由软件（包括固件、常驻软件、微码等）执行、也可以由硬件和软件组合执行。以上硬件或软件均可被称为“数据块”、“模块”、“引擎”、“单元”、“组件”或“系统”。此外，本说明书实施例的各方面可能表现为位于一个或多个计算机可读介质中的计算机产品，该产品包括计算机可读程序编码。

[116] 计算机存储介质可能包含一个内含有计算机程序编码的传播数据信号，例如在基带上或作为载波的一部分。该传播信号可能有多种表现形式，包括电磁形式、光形式等，或合适的组合形式。计算机存储介质可以是除计算机可读存储介质之外的任何计算机可读介质，该介质可以通过连接至一个指令执行系统、装置或设备以实现通讯、传播或传输供使用的程序。位于计算机存储介质上的程序编码可以通过任何合适的介质进行传播，包括无线电、电缆、光纤电缆、RF、或类似介质，或任何上述介质的组合。

[117] 本说明书实施例各部分操作所需的计算机程序编码可以用任意一种或多种程序语言编写，包括面向对象编程语言如 Java、Scala、Smalltalk、Eiffel、JADE、Emerald、C++、C#、VB.NET、Python 等，常规程序化编程语言如 C 语言、VisualBasic、Fortran2003、Perl、COBOL2002、PHP、ABAP，动态编程语言如 Python、Ruby 和 Groovy，或其他

编程语言等。该程序编码可以完全在用户计算机上运行、或作为独立的软件包在用户计算机上运行、或部分在用户计算机上运行部分在远程计算机运行、或完全在远程计算机或处理设备上运行。在后种情况下，远程计算机可以通过任何网络形式与用户计算机连接，比如局域网（LAN）或广域网（WAN），或连接至外部计算机（例如通过因特网），或在云计算环境中，或作为服务使用如软件即服务（SaaS）。

[118] 此外，除非权利要求中明确说明，本说明书实施例所述处理元素和序列的顺序、数字字母的使用、或其他名称的使用，并非用于限定本说明书实施例流程和方法的顺序。尽管上述披露中通过各种示例讨论了一些目前认为有用的发明实施例，但应当理解的是，该类细节仅起到说明的目的，附加的权利要求并不仅限于披露的实施例，相反，权利要求旨在覆盖所有符合本说明书实施例实质和范围的修正和等价组合。例如，虽然以上所描述的系统组件可以通过硬件设备实现，但是也可以只通过软件的解决方案得以实现，如在现有的处理设备或移动设备上安装所描述的系统。

[119] 同理，应当注意的是，为了简化本说明书实施例披露的表述，从而帮助对一个或多个发明实施例的理解，前文对本说明书实施例的描述中，有时会将多种特征归并至一个实施例、附图或对其的描述中。但是，这种披露方法并不意味着本说明书实施例对象所需要的特征比权利要求中提及的特征多。实际上，实施例的特征要少于上述披露的单个实施例的全部特征。

[120] 针对本说明书引用的每个专利、专利申请、专利申请公开物和其他材料，如文章、书籍、说明书、出版物、文档等，特此将其全部内容并入本说明书作为参考。与本说明书内容不一致或产生冲突的申请历史文件除外，对本申请权利要求最广范围有限制的文件（当前或之后附加于本说明书中的）也除外。需要说明的是，如果本说明书附属材料中的描述、定义、和/或术语的使用与本说明书所述内容有不一致或冲突的地方，以本说明书的描述、定义和/或术语的使用为准。

[121] 最后，应当理解的是，本说明书中所述实施例仅用以说明本说明书实施例的原则。其他的变形也可能属于本说明书实施例的范围。因此，作为示例而非限制，本说明书实施例的替代配置可视为与本说明书的教导一致。相应地，本说明书的实施例不仅限于本说明书明确介绍和描述的实施例。

权利要求书

1、一种数据传输方法，所述方法由数据提供方的设备执行，其包括:

获取待处理数据，所述待处理数据用于按可信区域组内的一个或多个可信区域中的数据处理流程被处理成目标数据;

获取用于加密至少部分目标数据的秘钥;

基于所述待处理数据以及所述秘钥，获得待加密信息;

获取来自可信区域组授权系统的组公钥，所述组公钥对应于所述可信区域组;

使用所述组公钥加密所述待加密信息，并将加密结果发送给具有所述可信区域内某一可信区域的设备。

2、如权利要求 1 所述的方法，其中，所述待处理数据包括用于进行模型训练的样本数据，所述目标数据包括经过样本数据训练得到的模型和/或模型信息。

3、如权利要求 1 所述的方法，其中，所述秘钥包括数据提供方的公钥和/或来自第三方设备的公钥。

4、如权利要求 1 所述的方法，其中，所述可信区域包括 SGX 可信执行环境中的 Enclave。

5、一种数据传输系统，包括:

待处理数据获取模块，用于获取待处理数据，所述待处理数据用于按可信区域组内的一个或多个可信区域中的数据处理流程被处理成目标数据;

秘钥获取模块，用于获取用于加密至少部分目标数据的秘钥;

第一待加密信息获得模块，用于基于所述待处理数据以及所述秘钥，获得待加密信息;

组公钥获取模块，获取来自可信区域组授权系统的组公钥，所述组公钥对应于所述可信区域组;

第一加密模块，用于使用所述组公钥加密所述待加密信息，并将加密结果发送给具有所述可信区域组内的某一可信区域的设备。

6、一种数据传输装置，包括处理器和存储设备，

所述存储设备用于存储指令，

当所述处理器执行所述指令时，实现如权利要求 1~4 中任一项所述的方法。

7、一种数据处理方法，所述方法在可信区域组内的某一可信区域中执行，其包括:

接收密文;

获取来自可信区域组授权系统的组公钥和组私钥，所述组公钥和组私钥与所述可信

区域组对应；

使用所述组私钥解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥；

对所述待处理数据执行数据处理流程，以得到结果数据；

基于所述结果数据以及所述秘钥，获得待加密信息；

使用所述组私钥加密所述待加密信息，并将加密结果发送给所述可信区域组内的其他可信区域。

8、如权利要求 7 所述的方法，其中，所述秘钥包括来自数据提供方的公钥和/或来自第三方设备的公钥。

9、如权利要求 7 所述的方法，其中，所述数据处理流程为：

数据融合流程，用于将来自多个数据提供方的待处理数据进行融合；或者，

模型训练流程，用于利用样本数据对模型进行训练。

10、如权利要求 7 所述的方法，其中，所述可信区域包括 SGX 可信执行环境中的 Enclave。

11、一种数据处理系统，所述系统在可信区域组内的某一可信区域中实现，其包括：

第一接收模块，用于接收密文；

组公私钥获取模块，用于获取来自可信区域组授权系统的组公钥和组私钥，所述组公钥和组私钥与所述可信区域组对应；

第一解密模块，用于使用所述组私钥解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥；

数据处理模块，用于对所述待处理数据执行数据处理流程，以得到结果数据；

第二待加密信息获得模块，用于基于所述结果数据以及所述秘钥，获得待加密信息；

第二加密模块，用于使用所述组私钥加密所述待加密信息，并将加密结果发送给所述可信区域组内的其他可信区域。

12、一种数据处理装置，包括处理器和存储设备，

所述存储设备用于存储指令，

当所述处理器执行所述指令时，实现如权利要求 7~10 中任一项所述的方法。

13、一种数据授权方法，所述方法在可信区域组内的某一可信区域中执行，其包括：

接收密文；

获取来自可信区域组授权系统的组私钥，所述组私钥与所述可信区域组对应；

使用所述组私钥解密所述密文，以获得待处理数据以及用于加密至少部分目标数据

的秘钥;

基于所述待处理数据获得目标数据;

利用所述秘钥加密至少部分目标数据;

输出经过加密的至少部分目标数据。

14、如权利要求 13 所述的方法，其中，所述基于待处理数据获得目标数据，包括:

将所述待处理数据确定为目标数据；或者，

对所述待处理数据执行数据处理流程，以获得目标数据。

15、如权利要求 13 所述的方法，其中，所述秘钥包括来自数据提供方的公钥和/或来自第三方设备的公钥。

16、如权利要求 13 所述的方法，其中，所述秘钥包括来自多方的公钥，且来自任一方的公钥对应部分目标数据;

所述利用所述秘钥加密至少部分目标数据，包括:

将所述目标数据拆分为多个部分;

用来自多方的公钥分别加密目标数据中对应的部分。

17、如权利要求 13 或 16 所述的方法，其中，所述目标数据包括经过样本数据训练的模型和/或模型信息。

18、如权利要求 13 所述的方法，其中，所述可信区域包括 SGX 可信执行环境中的 Enclave。

19、一种数据授权系统，所述系统在可信区域组内的某一可信区域中实现，其包括:

第二接收模块，用于接收密文;

组私钥获取模块，用于获取来自可信区域组授权系统的组私钥，所述组私钥与所述可信区域组对应;

第二解密模块，用于使用所述组私钥解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥;

目标数据获得模块，用于基于所述待处理数据获得目标数据;

第三加密模块，用于利用所述秘钥加密至少部分目标数据;

输出模块，用于输出经过加密的至少部分目标数据。

20、一种数据授权装置，包括处理器和存储设备，

所述存储设备用于存储指令，

当所述处理器执行所述指令时，实现如权利要求 13~18 中任一项所述的方法。

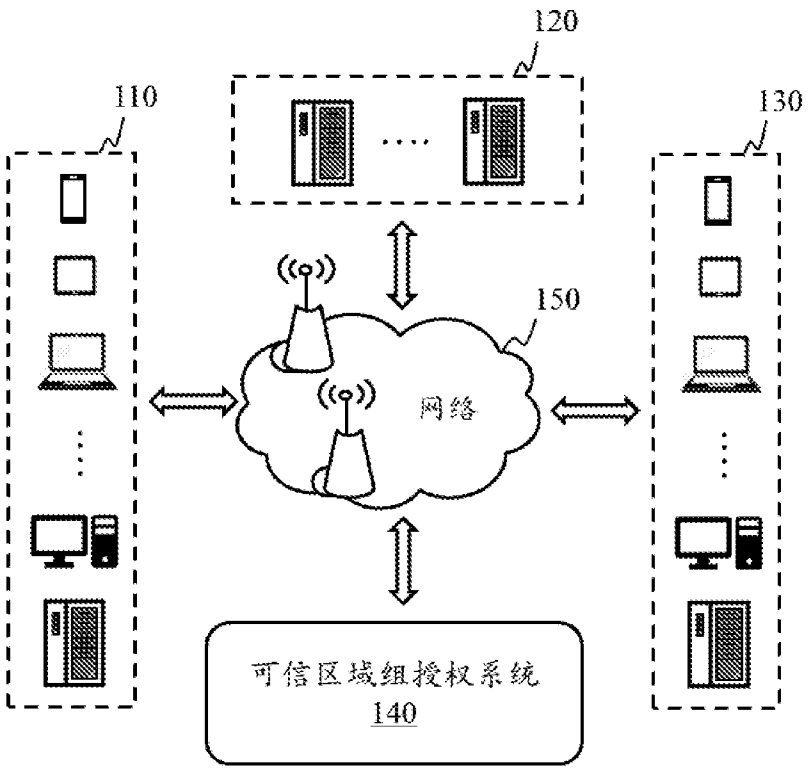
100
120
110
130
150
网络
可信区域组授权系统
140

图 1

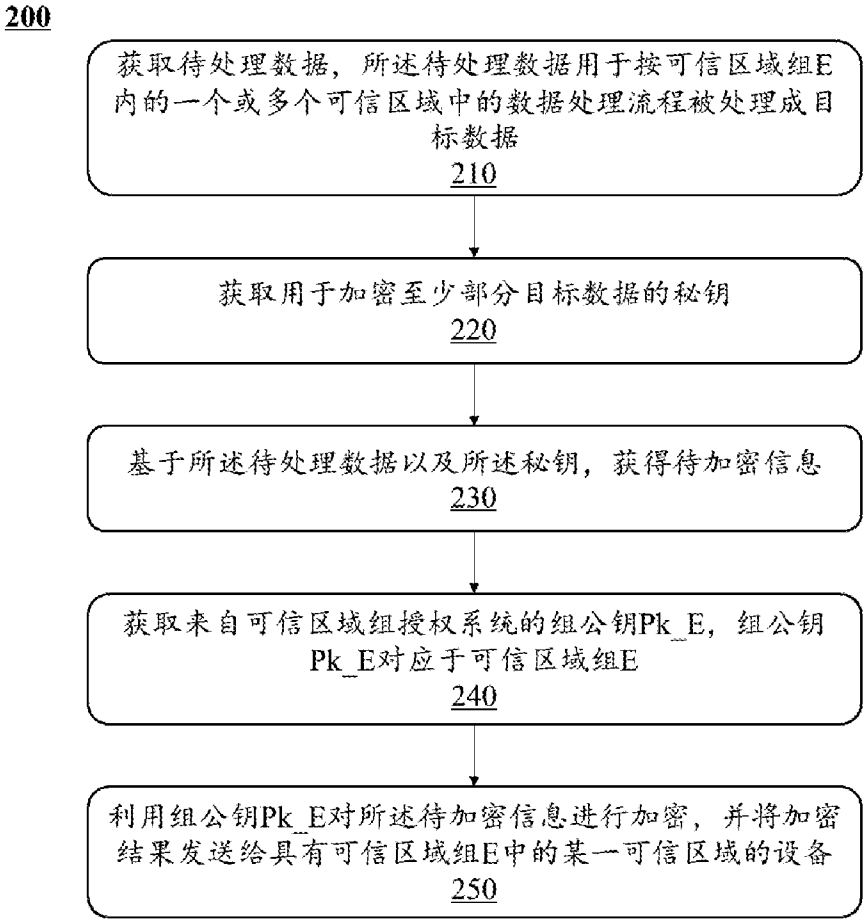
200
获取待处理数据，所述待处理数据用于按可信区域组E内的一个或多个可信区域中的数据处理流程被处理成目标数据
210
获取用于加密至少部分目标数据的秘钥
220
基于所述待处理数据以及所述秘钥，获得待加密信息
230
获取来自可信区域组授权系统的组公钥Pk_E，组公钥Pk_E对应于可信区域组E
240
利用组公钥Pk_E对所述待加密信息进行加密，并将加密结果发送给具有可信区域组E中的某一可信区域的设备
250

图 2

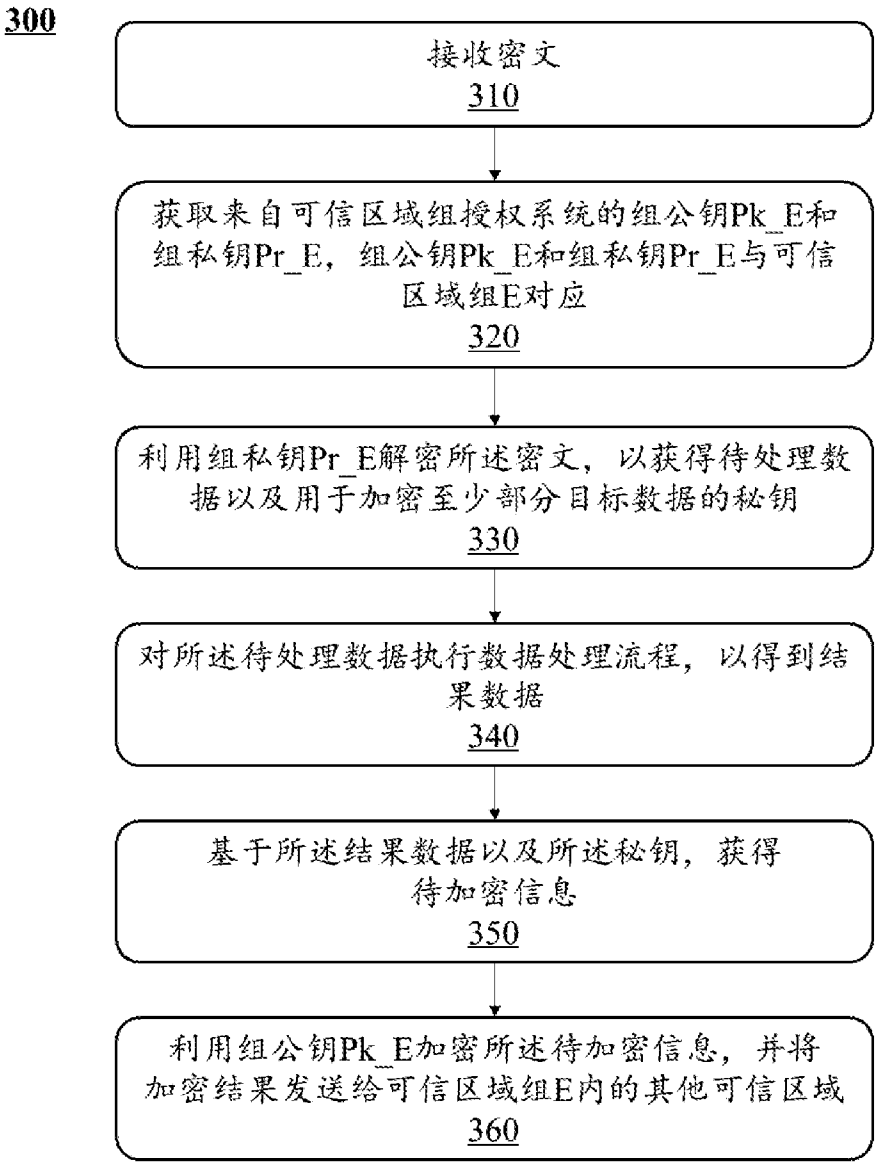
300
接收密文
310
获取来自可信区域组授权系统的组公钥Pk_E和组私钥Pr_E，组公钥Pk_E和组私钥Pr_E与可信区域组E对应
320
利用组私钥Pr_E解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥
330
对所述待处理数据执行数据处理流程，以得到结果数据
340
基于所述结果数据以及所述秘钥，获得待加密信息
350
利用组公钥Pk_E加密所述待加密信息，并将加密结果发送给可信区域组E内的其他可信区域
360

图 3

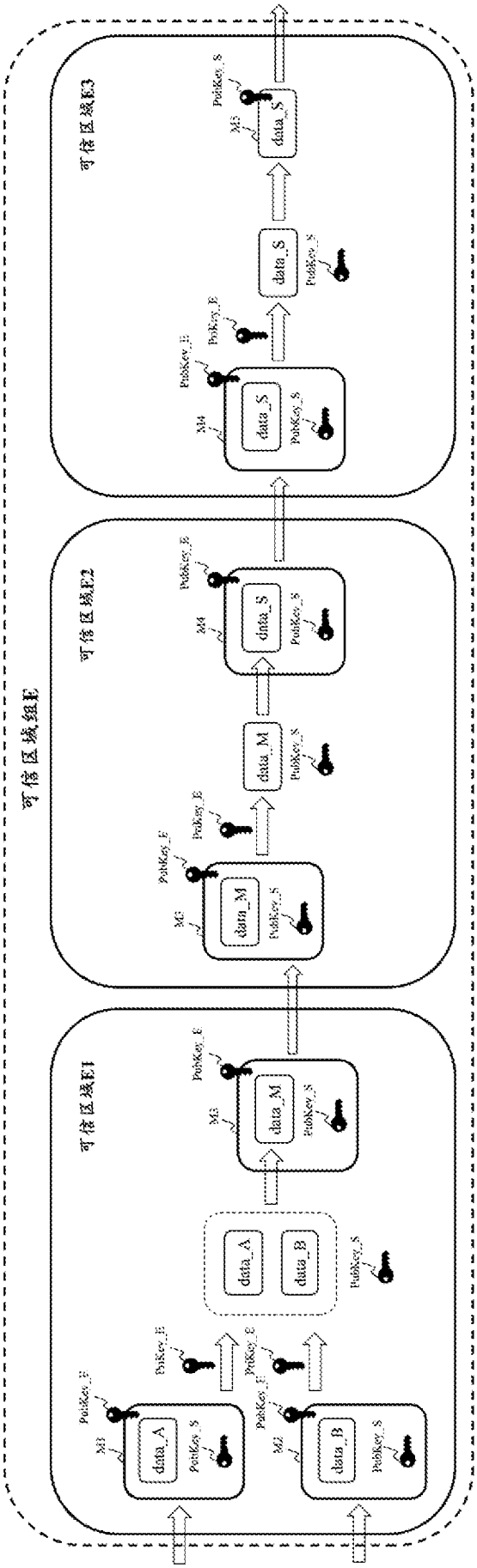
可信区域组E
可信区域E1
可信区域E2
可信区域E3
data_A
data_B
data_M
data_S
PubKey_E
PubKey_S
M1
M2
M3
M4

图 4

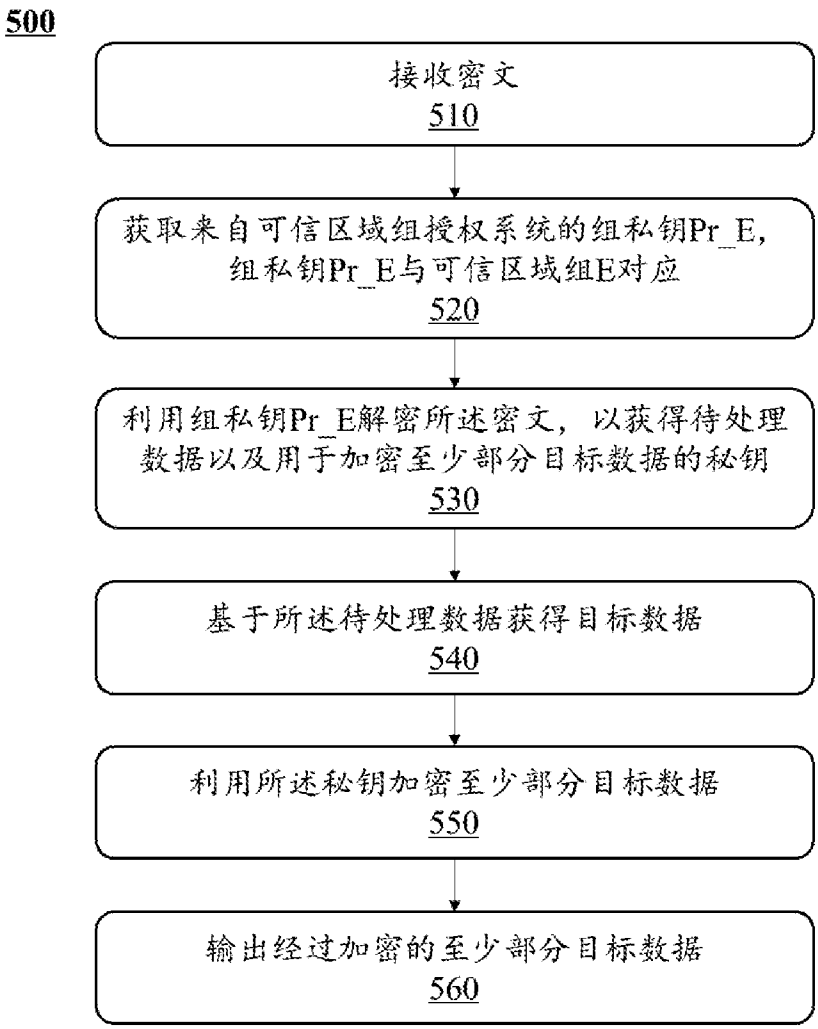
500
接收密文
510
获取来自可信区域组授权系统的组私钥Pr_E，组私钥Pr_E与可信区域组E对应
520
利用组私钥Pr_E解密所述密文，以获得待处理数据以及用于加密至少部分目标数据的秘钥
530
基于所述待处理数据获得目标数据
540
利用所述秘钥加密至少部分目标数据
550
输出经过加密的至少部分目标数据
560

图 5

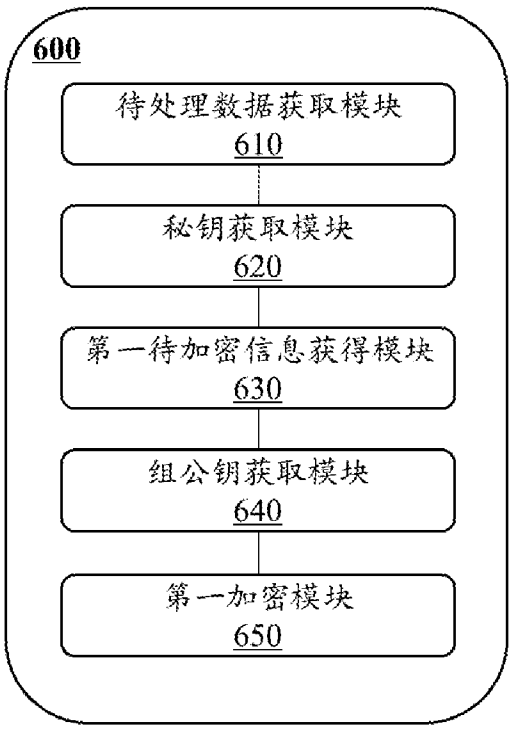
600
待处理数据获取模块
610
秘钥获取模块
620
第一待加密信息获得模块
630
组公钥获取模块
640
第一加密模块
650

图 6

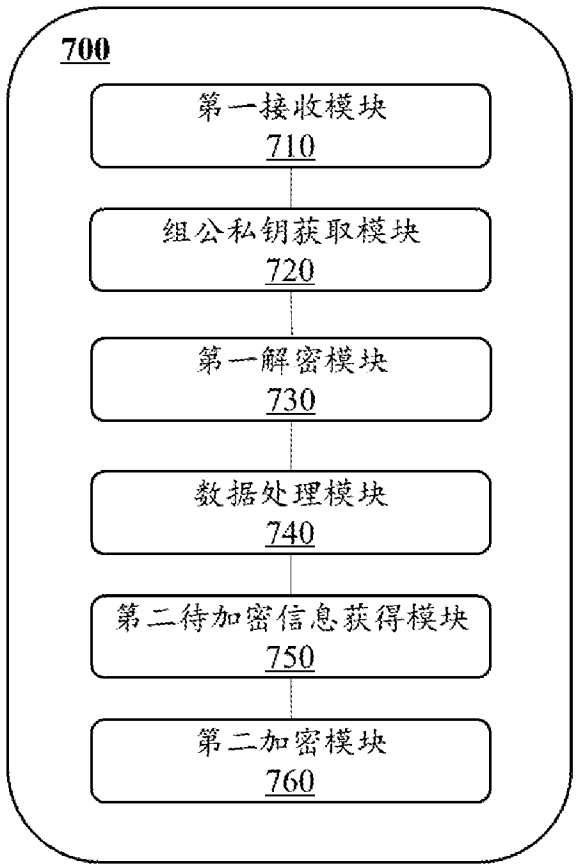
700
第一接收模块
710
组公私钥获取模块
720
第一解密模块
730
数据处理模块
740
第二待加密信息获得模块
750
第二加密模块
760

图 7

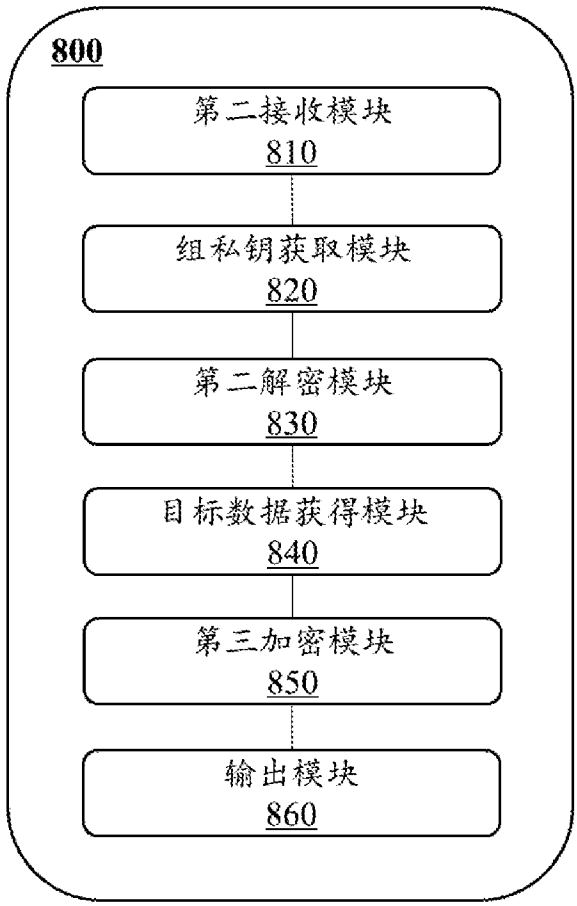
800
第二接收模块
810
组私钥获取模块
820
第二解密模块
830
目标数据获得模块
840
第三加密模块
850
输出模块
860

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/086900

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT ; CNKI; VEN; WOTXT; EPTXT; USTXT: 可信区域, 可信执行环境, 可信环境, 秘钥, 密钥, 组, 加密, 公钥, 私钥, 模型, Trusted Execution Environment, TEE, group, key, encrypt, public, private, model

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111628966 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 04 September 2020 (2020-09-04) claims 1-20	1-20
X	CN 110968743 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD.) 07 April 2020 (2020-04-07) description, paragraphs [0126]-[0151]	1-20
A	CN 109657479 A (XIAMEN YAXON NETWORKS CO., LTD.) 19 April 2019 (2019-04-19) entire document	1-20
A	CN 106851351 A (ACADEMY OF BROADCASTING SCIENCE, SAPPRFT et al.) 13 June 2017 (2017-06-13) entire document	1-20
A	US 9722775 B2 (VERIZON PATENT AND LICENSING INC.) 01 August 2017 (2017-08-01) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 May 2021	**28 May 2021**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/086900

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 111628966 A	04 September 2020	None	
CN 110968743 A	07 April 2020	None	
CN 109657479 A	19 April 2019	None	
CN 106851351 A	13 June 2017	WO 2017092687 A1	08 June 2017
		CN 106851351 B	27 February 2018
		US 2018367829 A1	20 December 2018
US 9722775 B2	01 August 2017	US 2016254904 A1	01 September 2016

国际检索报告

国际申请号
PCT/CN2021/086900

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT ;CNKI;VEN; WOTXT;EPTXT; USTXT：可信区域，可信执行环境，可信环境，秘钥，密钥，组，加密，公钥，私钥，模型，Trusted Execution Environment, TEE, group, key, encrypt, public, private, model

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 111628966 A (支付宝杭州信息技术有限公司) 2020年 9月 4日 (2020-09-04) 权利要求1-20	1-20
X	CN 110968743 A (支付宝杭州信息技术有限公司) 2020年 4月 7日 (2020-04-07) 说明书第[0126]-[0151]段	1-20
A	CN 109657479 A (厦门雅迅网络股份有限公司) 2019年 4月 19日 (2019-04-19) 全文	1-20
A	CN 106851351 A (国家新闻出版广电总局广播科学研究院等) 2017年 6月 13日 (2017-06-13) 全文	1-20
A	US 9722775 B2 (VERIZON PATENT & LICENSING INC) 2017年 8月 1日 (2017-08-01) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 5月 20日	2021年 5月 28日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 曹玉华 电话号码 86-(010)-62412272

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/086900

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	111628966	A	2020年 9月 4日	无			
CN	110968743	A	2020年 4月 7日	无			
CN	109657479	A	2019年 4月 19日	无			
CN	106851351	A	2017年 6月 13日	WO	2017092687	A1	2017年 6月 8日
				CN	106851351	B	2018年 2月 27日
				US	2018367829	A1	2018年 12月 20日
US	9722775	B2	2017年 8月 1日	US	2016254904	A1	2016年 9月 1日