(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 7 月 7 日 (07.07.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/141014 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2020/140586

(22) 国际申请日: 2020 年 12 月 29 日 (29.12.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人:深圳大学(**SHENZHEN UNIVERSITY**) [CN/CN]; 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。

(72) 发明人: 张鹏(**ZHANG, Peng**); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。 赵威(**ZHAO, Wei**); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。 孙小强(**SUN, Xiaoqiang**); 中国广东省深圳市南山区南海大道3688号, Guangdong 518000 (CN)。

(74) 代理人: 北京三聚阳光知识产权代理有限公司(**SUNSHINE INTELLECTUAL PROPERTY INTERNATIONAL CO., LTD.**); 中国北京市海淀区海淀南路甲21号中关村知识产权大厦A座5层503, Beijing 100080 (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, 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。

(54) **Title:** SECURITY AVERAGING METHOD BASED ON MULTI-USER DATA

(54) 发明名称: 一种基于多用户数据的安全求均值方法

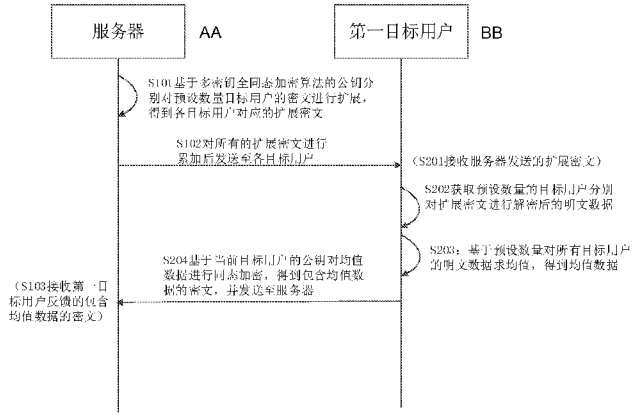

图 1

S101 Respectively expand, on the basis of a multi-key fully homomorphic encryption algorithm, a ciphertext of a preset number of target users by means of a public key to obtain an expanded ciphertext corresponding to each target user
S102 Accumulate all the expanded ciphertexts, and then send same to each target user
S103 Receive a ciphertext fed back by a first target user and comprising average data
S201 Receive the expanded ciphertext sent by a server
S202 Acquire plaintext data after the preset number of target users decrypt the expanded ciphertexts, respectively
S203 Average the plaintext data of all the target users on the basis of the preset number to obtain average data
S204 Perform homomorphic encryption on the average data on the basis of the public key of the current target user to obtain a ciphertext comprising the average data, and send the ciphertext to the server
AA Server
BB First target user

(57) **Abstract:** A security averaging method based on multi-user data, comprising: a server respectively expanding, on the basis of a multi-key fully homomorphic encryption algorithm, a ciphertext of a preset number of target users by means of a public key to obtain an expanded ciphertext corresponding to each target user (S101); accumulating all the expanded ciphertexts, and then sending same to each target user (S102); acquiring, by the current target user, plaintext data after the preset number of target users decrypt the expanded ciphertexts, respectively (S202); averaging the plaintext data of all the target users on the basis of the preset number to obtain average data (S203); and then performing homomorphic encryption on the average data on the basis of the public key of the current target user to obtain a ciphertext comprising the average data, and sending the ciphertext to the server (S204). In this way, the homomorphic encryption algorithm is used, and the server interacts with multiple users, so that the server obtains the ciphertext corresponding to the average while plaintext data information is not leaked, and thus the privacy security of the user is ensured at the server side, and the average ciphertext of the multi-user data is obtained.

WO 2022/141014 A1

[见续页]

(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)。

根据细则4.17的声明：
— 发明人资格(细则4.17(iv))

本国际公布：
— 包括国际检索报告(条约第21条(3))。

(57) 摘要：一种基于多用户数据的安全求均值方法，服务器通过基于多密钥全同态加密算法的公钥分别对预设数量目标用户的密文进行扩展，得到各目标用户对应的扩展密文（S101）；对所有的扩展密文进行累加后发送至各目标用户（S102）；当前目标用户获取预设数量目标用户分别对扩展密文进行解密后的明文数据（S202）；并基于预设数量对所有目标用户的明文数据求均值，得到均值数据（S203）；然后基于当前目标用户的公钥对均值数据进行同态加密，得到包含均值数据的密文，并发送至服务器（S204）。从而利用同态加密算法，通过服务器与多用户之间的交互，在未泄露明文数据信息的前提下，使得服务器得到了均值所对应的密文，在服务器侧既保证了用户隐私安全，又得到了多用户数据的均值密文。

一种基于多用户数据的安全求均值方法

技术领域

本申请涉及计算机网络应用技术领域，具体涉及一种基于多用户数据的安全求均值方法。

背景技术

机器学习的研究是从海量数据中获取隐藏的、有效的、可理解的知识，被广泛应用于人工智能、疾病诊断、基因测序、犯罪预测等领域。与此同时，机器学习给数据隐私保护带来了巨大挑战。如何限定第三方在对用户数据进行机器学习的同时不窥探用户数据隐私成为了热点研究课题。为了实现隐私保护的机器学习，最直接的方式是先加密数据再对数据密文进行机器学习。全同态加密就是这样一种密码技术，允许操作者直接在加密数据上进行运算，运算的结果正确解密后等同于在数据明文上进行同样的运算。

由于求均值运算被广泛应用于机器学习的 k-means 聚类等算法中，因此，服务器端在获取大量用户数据求均值时，存在用户隐私泄露的隐患，而在全同态加密的情况下用户的隐私可以得到保障，但是由于全同态加密仅支持对密文的加法与乘法运算，服务器也无法得到多用户的数据均值对应的密文，因此，在服务器端如何在保护用户数据隐私安全的情况下得到多用户的数据均值，对基于隐私保护机器学习算法的研究非常重要。

发明内容

有鉴于此，本申请实施例提供了一种基于多用户数据的安全求均值方法，以克服现有技术中服务器无法在保护用户数据隐私的情况下实现多用户数据求均值的问题。

本申请实施例提供了一种基于多用户数据的安全求均值方法，包括：

基于多密钥全同态加密算法的公钥分别对预设数量目标用户的密文进行扩展，得到各目标用户对应的扩展密文，所述扩展密文的解密密钥为各目标用户对应的私钥；

对所有的扩展密文进行累加后发送至各目标用户；

接收第一目标用户反馈的包含均值数据的密文，所述均值数据对应的密文为所述第一目标用户基于用户明文数据求均值得到的，所述用户明文数据为各目标用户基于各目标用户对应的私钥对累加后的扩展密文解密得到的，所述第一目标用户为各目标用户中任意一个目标用户。

可选地，所述对所有的扩展密文进行累加后发送至各目标用户，包括：

获取随机扰动数据；

基于所述随机扰动数据，采用所述公钥对所述随机扰动数据进行同态加密得到所述随机扰动数据对应的第一密文；

分别将所述第一密文与各所述扩展密文进行累加，得到第一扩展密文；

对所有第一扩展密文进行累加后发送至各目标用户。

可选地，所述接收第一目标用户反馈的包含均值数据的密文，包括：

获取所述第一目标用户对应的公钥；

基于所述公钥对所述随机扰动数据进行同态加密，得到所述随机扰动数据对应的第二密文；

对第一目标用户反馈的包含均值数据的密文和所述第二密文作差，得到所述均值数据对应的密文。

可选地，在所述基于扩展公钥分别对预设数量的目标用户的密文进行扩展之前，所述方法还包括：

接收所述预设数量的目标用户发送的密文，所述密文为各目标用户采用其对应的公钥对各自用户数据进行同态加密后得到的。

本申请实施例还通过了一种基于多用户数据的安全求均值方法，包括：

接收服务器发送的扩展密文，所述扩展密文为所述服务器基于多密钥全同态加密算法的公钥分别对所有目标用户的密文进行扩展后累加得到的；

获取预设数量的目标用户分别对所述扩展密文进行解密后的明文数据；

基于所述预设数量对所有目标用户的明文数据求均值，得到均值数据；

基于当前目标用户的公钥对所述均值数据进行同态加密，得到包含均值数据的密文，并发送至所述服务器。

可选地，所述扩展密文中包含有随机扰动数据对应的第一密文，所述获取预设数量的目标用户分别对所述扩展密文进行解密后的明文数据包括：

基于当前目标用户的私钥对所述扩展密文进行解密，得到当前明文数据，所述当前明文数据中包含有所述随机扰动数据；

接收其他目标用户发送的明文数据，所述明文数据为其他目标用户基于各自的私钥对所述扩展密文进行解密得到的，所述明文数据中包含有所述随机扰动数据。

可选地，所述基于所述预设数量对所有目标用户的明文数据求均值，得到均值数据，包括：

对当前明文数据及其他目标用户对应的明文数据进行累加，得到总明文数据；

基于所述预设数量对所述总明文数据求均值，得到所述均值数据。

可选地，在所述接收服务器发送的扩展密文之前，所述方法还包括：

基于当前目标用户的公钥对当前目标用户对应的用户数据进行同态加密，得到密文，并将所述密文发送至服务器。

本申请实施例还提供了一种电子设备，包括：存储器和处理器，所述存储器和所述处理器之间互相通信连接，所述存储器中存储有计算机指令，所述处理器通过执行所述计算机指令，从而执行本申请实施例提供的基于多用户数据的安全求均值方法。

本申请实施例还提供了一种计算机可读存储介质，所述计算机可读存储介质存储计算机指令，所述计算机指令用于使所述计算机执行本申请实施例提供的基于多用户数据的安全求均值方法。

本申请技术方案，具有如下优点：

本申请实施例提供了一种基于多用户数据的安全求均值方法，服务器通过基于多密钥全同态加密算法的公钥分别对预设数量目标用户的密文进行扩展，得到各目标用户对应的扩展密文，扩展密文的解密密钥为各目标用户对应的私钥；对所有的扩展密文进行累加后发送至各目标用户；当前目标用户获取预设数量目标用户分别对扩展密文进行解密后的明文数据；并基于预设数量对所有目标用户的明文数据求均值，得到均值数据；然后基于当前目标用户的公钥对均值数据进行同态加密，得到包含均值数据的密文，并发送至服务器。从而利用同态加密算法，通过服务器与多用户之间的交互，在用户端实现多用户数据均值的计算，并通过对均值进行加密后发送至服务器，在未泄露明文数据信息的前提下，使得服务器得到了均值所对应的密文，在服务器侧既保证了用户隐私安全，又得到了多用户数据的均值密文。

附图说明

为了更清楚地说明本申请具体实施方式或现有技术中的技术方案，下面将对具体实施方式或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图是本申请的一些实施方式，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他的附图。

图 1 为本申请实施例中的基于多用户数据的安全求均值的交互过程示意图；

图 2 为本申请实施例中的基于多用户数据的安全求均值的另一交互过程示意图；

图 3 为本申请实施例中的电子设备的结构示意图。

具体实施方式

为使本申请实施例的目的、技术方案和优点更加清楚，下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

下面所描述的本申请不同实施方式中所涉及的技术特征只要彼此之间未构成冲突就可以相互结合。

由于求均值运算被广泛应用于机器学习的 k-means 聚类等算法中，因此，服务器端在获取大量用户数据求均值时，存在用户隐私泄露的隐患，而在全同态加密的情况下用户的隐私可以得到保障，但是由于全同态加密仅支持对密文的加法与乘法运算，服务器也无法得到多用户的数据均值对应的密文，因此，在服务器端如何在保护用户数据隐私安全的情况下得到多用户的数据均值，对基于隐私保护机器学习算法的研究非常重要。

基于上述问题，本申请实施例提供了一种基于多用户数据的安全求均值系统，该系统包括服务器和多个目标用户，其中进行均值计算的第一目标用户为所有目标用户中的任意一个，在本申请实施例中，以服务器和第一目标用户为例，对本申请实施例提供的基于多用户数据的安全求均值方法进行详细的说明，具体如图 1 所示，服务器端用于执行步骤 S101 至步骤 S103，第一目标用户端用于，执行步骤 S201 至步骤 S204。

首先，对本申请实施例所采用的多密钥全同态加密算法进行说明，在本申请实施例中，在现有技术中选择定义为$CZW = \{Setup, KGen, Enc, Dec, CTExt, EVKen\}$的多密钥全同态加密方案，实现对多用户数据的安全求均值协议，具体多用户安全求均值协议背景如下：

运行$CZW.Setup$算法输出系统的公钥等。运行$CZW.KGen$算法输出用户公私钥，特别地定义用户U_i的公私钥对为$\{pk_i, sk_i\}$；运行$CZW.Enc$算法计算明文所对应的密文，假定明文数据$\boldsymbol{m}_i$来自用户U_i，则使用U_i的公钥pk_i加密，得到密文$\boldsymbol{C}_i$。给定数据簇λ中n个数据对象$\{\boldsymbol{m}_1, \boldsymbol{m}_2, \ldots, \boldsymbol{m}_n\}$，分别来自$n$个不同的用户$U_1, U_2, \ldots, U_n$，对应的密文分别记为$\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_n$，数据存储于服务器。安全求平均值协议在云服务器与用户$U_1, U_2, \ldots, U_n$间执行，旨在已知密文而不泄露各用户明文的前提下，计算出给定数据簇内所有数据对象的均值$\overline{\boldsymbol{m}} = \frac{1}{n}\sum_{i=1}^{n} \boldsymbol{m}_i$所对应的密文。需要说明的是，在实际应用中，该多密钥全同态加密算法可以选择现有技术中其他已有的同态加密算法，如 BGV 型多密钥全同态加密方法等，本申请并不以此为限。

具体地，如图 1 所示，该基于多用户数据的安全求均值方法具体包括如下步骤：

步骤 S101：基于多密钥全同态加密算法的公钥分别对预设数量目标用户的密文进行扩展，得到各目标用户对应的扩展密文，扩展密文的解密密钥为各目

标用户对应的私钥。具体地，该密文为各目标用户通过运行上述 $CZW.KGen$算法输出各目标用户对应的公私钥，并利用各自的公钥对目标用户的用户数据进行同态加密后得到的。该公钥为通过运行上述$CZW.Setup$算法得到的公钥。

步骤 S102：对所有的扩展密文进行累加后发送至各目标用户。具体地，服务器运行算法$CZW.CTExt$扩展各用户的密文$\boldsymbol{C}_1, \boldsymbol{C}_2, \ldots, \boldsymbol{C}_n$为$\overline{\boldsymbol{C}}_1, \overline{\boldsymbol{C}}_2, \ldots, \overline{\boldsymbol{C}}_n$，使得$\langle \overline{\boldsymbol{C}}_i, sk_{\overline{U}} \rangle = \langle \boldsymbol{C}_i, sk_i \rangle$，即扩展后密文对应的私钥均为各目标用户对应的私钥，其中$\overline{U} = \{1,2,\ldots,n\}$，$n$表示目标用户的个数。

步骤 S201：接收服务器发送的扩展密文，扩展密文为服务器基于多密钥全同态加密算法的公钥分别对所有目标用户的密文进行扩展后累加得到的。具体地，各目标用户分别接收服务器发送的扩展密文，在本申请实施例中，是以上述第一目标用户接收服务器发送的扩展密文为例进行的说明。

步骤 S202：获取预设数量的目标用户分别对扩展密文进行解密后的明文数据。具体地，各目标用户分别通过上述$CZW.KGen$算法输出用户公私钥后，并利用用户私钥对上述扩展密文进行解密，分别得到一部分明文数据。

步骤 S203：基于预设数量对所有目标用户的明文数据求均值，得到均值数据。具体地，第一目标用户通过将所有目标用户解密得到的明文数据进行累加后求均值，即可得到所有目标用户的明文数据对应的均值数据。

步骤 S204：基于当前目标用户的公钥对均值数据进行同态加密，得到包含均值数据的密文，并发送至服务器。具体地，该当前目标用户即为上述的第一目标用户，其通过运行$CZW.Enc$算法计算均值数据所对应的密文，即上述第一目标用户采用其对应的公钥对均值数据进行加密，得到均值数据对应的密文。

步骤 S103：接收第一目标用户反馈的包含均值数据的密文，均值数据对应的密文为第一目标用户基于用户明文数据求均值得到的，用户明文数据为各目

标用户基于各目标用户对应的私钥对累加后的扩展密文解密得到的，第一目标用户为各目标用户中任意一个目标用户。至此，服务器即可得到所有目标用户的明文数据的均值。

通过执行上述步骤，利用同态加密算法，通过服务器与多用户之间的交互，在用户端实现多用户数据均值的计算，并通过对均值进行加密后发送至服务器，在未泄露明文数据信息的前提下，使得服务器得到了均值所对应的密文，在服务器侧既保证了用户隐私安全，又得到了多用户数据的均值密文。

具体地，在一实施例中，如图 2 所示，上述的步骤 S102，具体包括如下步骤：

步骤 S11：获取随机扰动数据。具体地，在本申请实施例中，该随机扰动数据为服务器选取的一个随机二元向量$\boldsymbol{r}$，在实际应用中，该随机扰动数据也可以是服务器从预先设定的若干扰动数据中随机选择其中一个，本申请并不以此为限。

步骤 S12：基于随机扰动数据，采用公钥对随机扰动数据进行同态加密得到随机扰动数据对应的第一密文。具体地，服务器通过利用上述公钥pk_U对随机扰动数据进行加密得到对应的第一密文$\overline{\boldsymbol{C}}(\boldsymbol{r})$。

步骤 S13：分别将第一密文与各扩展密文进行累加，得到第一扩展密文。具体地，服务器分别为每一个目标用户对应的扩展密文都累加一个随机扰动数据对应的第一密文，得到第一扩展密文，使得每个第一扩展密文中均包含有扰动数据，以增加密文数据的安全性。

步骤 S14：对所有第一扩展密文进行累加后发送至各目标用户。具体地，服务器通过累加所有第一扩展密文，得到$\overline{\boldsymbol{C}}(\boldsymbol{g}) = \sum_{i=1}^{n} \overline{\boldsymbol{C}}_i + n \cdot \overline{\boldsymbol{C}}(\boldsymbol{r})$，并发送$\overline{C}(g)$给各个目标用户。

在本申请实施例中，各个目标用户在接收到上述包含有随机扰动数据对应的第一密文的扩展密文后，各目标用户分别采用自己的私钥对扩展密文进行解密，得到包含有随机扰动数据的明文数据。此时，由于随机扰动数据是服务器设置的，各个目标用户在不知道随机扰动数据的情况下，无法得到真实的明文数据，从而进一步保障了明文数据在目标用户端的隐私，进而也无法得到真实的均值数据的信息，保证了求均值在目标用户端和服务器端的双向安全。

具体地，在一实施例中，如图 2 所示，在上述第一目标用户端接收到上述包含有随机扰动数据对应的第一密文的扩展密文后，上述的步骤 S202，具体包括如下步骤：

步骤 S21：基于当前目标用户的私钥对扩展密文进行解密，得到当前明文数据，当前明文数据中包含有随机扰动数据。

步骤 S22：接收其他目标用户发送的明文数据，该明文数据为其他目标用户基于各自的私钥对扩展密文进行解密得到的，明文数据中包含有随机扰动数据。具体地，通过各个目标用户分别利用自己的私钥对扩展密文进行解密得到对应的明文数据，然后将各自的明文数据发送给参与均值计算的当前目标用户即上述第一目标用户，并由第一目标用户对所有的明文数据进行处理，得到均值数据。

需要说明的是，在本申请实施例中是以扩展密文中包含有随机扰动数据对应的第一密文为例进行的说明，在实际应用中，如果服务器不添加随机扰动数据对应的第一密文，目标用户解密得到的明文数据也不包含随机扰动数据。

具体地，在一实施例中，如图 2 所示，上述的步骤 S203，具体包括如下步骤：

步骤 S23:对当前明文数据及其他目标用户对应的明文数据进行累加，得到

总明文数据。具体地，参与均值计算的上述第一目标用户在接收到其他目标用户发送的明文数据后，对所有目标用户解密得到的明文数据进行累加，得到包含有随机扰动数据的总明文数据，即各目标用户$U_1, U_2, \ldots, U_n$分别运行上述$CZW.Dec$算法利用自身的私钥进行解密，然后将所有解密结果进行累加后得到总明文数据$\boldsymbol{g}$。

步骤 S24:基于预设数量对总明文数据求均值，得到均值数据。具体地，第一目标用户根据所有目标用户的数量计算出含误差项的均值$\overline{\boldsymbol{m}}' = \frac{1}{n}\boldsymbol{g}$。然后通过运行$CZW.Enc$算法加密$\overline{\boldsymbol{m}}'$，得到密文$\boldsymbol{C}_i(\overline{\boldsymbol{m}}')$发送给服务器。

具体地，在一实施例中，如图 2 所示，上述的步骤 S103，具体包括如下步骤：

步骤 S15:获取第一目标用户对应的公钥。具体地，第一目标用户在发送上述密文$\boldsymbol{C}_i(\overline{\boldsymbol{m}}')$时，同时将自己的公钥发送至服务器。

步骤 S16:基于公钥对随机扰动数据进行同态加密，得到随机扰动数据对应的第二密文。服务器通过利用第一目标用户对应的公钥加密上述步骤 S11 选取的随机向量$\mathbf{r}$，得到其对应的密文$\boldsymbol{C}_i(\boldsymbol{r})$。

步骤 S17:对第一目标用户反馈的包含均值数据的密文和第二密文作差，得到均值数据对应的密文。服务器通过计算$\boldsymbol{O}^{(i)} = \boldsymbol{C}_i(\overline{\boldsymbol{m}}) = \boldsymbol{C}_i(\overline{\boldsymbol{m}}') - \boldsymbol{C}_i(\boldsymbol{r})$，亦即数据均值$\overline{\boldsymbol{m}} = \frac{1}{n}\sum_{i=1}^{n}\boldsymbol{m}_i$所对应的密文。

至此，通过云服务器与多用户的交互，完成了对多用户数据的安全求均值计算。一方面，在未泄露明文数据信息的前提下，服务器实现了得到明文数据均值所对应的密文；另一方面，通过服务器增设误差扰动数据，用户也无法直接获取均值信息，从而实现了服务器和用户双向安全求均值，保护了用户隐私不被泄露。

表 1 为本申请实施例采用上述基于多用户数据的安全求均值方法所构建的安全求均值协议的执行流程，其中服务器为云服务器，用户为参与均值计算的上述第一目标用户。在半诚实模型下，上述协议的参与方云服务器、用户诚实地执行协议操作，其中云服务器对属于数据簇λ中的数据对象$\boldsymbol{m}_1,\boldsymbol{m}_2,\ldots,\boldsymbol{m}_n$和$\boldsymbol{O}^{(i)}$所对应的均值$\overline{\boldsymbol{m}}$是好奇的，用户对均值是好奇的。

安全求均值协议
输入：数据簇λ中n个数据对象的密文$\boldsymbol{C}_1,\boldsymbol{C}_2,\ldots,\boldsymbol{C}_n$（公钥$pk_1,pk_2,\ldots,pk_n$下对$\boldsymbol{m}_1,\boldsymbol{m}_2,\ldots,\boldsymbol{m}_n$的加密） 输出：数据簇$\lambda$中所有数据对象的均值$\overline{\boldsymbol{m}}=\frac{1}{n}\sum_{i=1}^{n}\boldsymbol{m}_i$所对应的密文$\boldsymbol{O}^{(i)}$
for 云服务器
1. 令$\overline{U}=\{1,2,\ldots,n\}$，扩展密文$\boldsymbol{C}_1,\boldsymbol{C}_2,\ldots,\boldsymbol{C}_n$为$\overline{\boldsymbol{C}}_1,\overline{\boldsymbol{C}}_2,\ldots,\overline{\boldsymbol{C}}_n$，对应的私钥均为$sk_{\overline{U}}$
2. 选取一个随机二元向量$\boldsymbol{r}$，并用$pk_{\overline{U}}$加密得到密文$\overline{\boldsymbol{C}}(\boldsymbol{r})$
3. 计算$\overline{\boldsymbol{C}}(\boldsymbol{g})=\sum_{i=1}^{n}\overline{\boldsymbol{C}}_i+n\cdot\overline{\boldsymbol{C}}(\boldsymbol{r})$，并发送给用户
for 用户
4. 解密出$\boldsymbol{g}$，并计算$\overline{\boldsymbol{m}}'=\frac{1}{n}\boldsymbol{g}$
5. 用公钥pk_i加密$\overline{\boldsymbol{m}}'$得到密文$\boldsymbol{C}_i(\overline{\boldsymbol{m}}')$
6. 将$\boldsymbol{C}_i(\overline{\boldsymbol{m}}')$发送给云服务器
for 云服务器
7. 用公钥pk_i加密$\boldsymbol{r}$得到密文$\boldsymbol{C}_i(\boldsymbol{r})$
8. 计算$\boldsymbol{O}^{(i)}=\boldsymbol{C}_i(\overline{\boldsymbol{m}})=\boldsymbol{C}_i(\overline{\boldsymbol{m}}')-\boldsymbol{C}_i(\boldsymbol{r})$

由于CZW多密钥全同态加密算法的语义安全性，未拥有私钥$sk_1,sk_2,\ldots,sk_n$的云服务器无法从密文中获得数据对象$\boldsymbol{m}_1,\boldsymbol{m}_2,\ldots,\boldsymbol{m}_n$、含误差项的均值$\overline{\boldsymbol{m}}'$及均值$\overline{\boldsymbol{m}}$的信息。此外，用户在计算$\overline{C}(g)$时引入随机二元向量$\boldsymbol{r}$，使得用户在不确定r的取值的情况下，无法通过含误差项的平均值$\overline{\boldsymbol{m}}'$来推测出均值$\overline{\boldsymbol{m}}$的信息。

综上，上述安全求均值协议在半诚实模型下是安全的，在用户端及服务器端均可保证用户隐私数据的安全。

本申请实施例还提供了一种电子设备，如图 3 所示，该电子设备可以包括处理器 901 和存储器 902，其中处理器 901 和存储器 902 可以通过总线或者其他方式连接，图 3 中以通过总线连接为例。

处理器 901 可以为中央处理器（Central Processing Unit，CPU）。处理器

901 还可以为其他通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现场可编程门阵列（Field-Programmable Gate Array，FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等芯片，或者上述各类芯片的组合。

存储器 902 作为一种非暂态计算机可读存储介质，可用于存储非暂态软件程序、非暂态计算机可执行程序以及模块，如本申请方法实施例中的方法所对应的程序指令/模块。处理器 901 通过运行存储在存储器 902 中的非暂态软件程序、指令以及模块，从而执行处理器的各种功能应用以及数据处理，即实现上述方法实施例中的方法。

存储器 902 可以包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需要的应用程序；存储数据区可存储处理器 901 所创建的数据等。此外，存储器 902 可以包括高速随机存取存储器，还可以包括非暂态存储器，例如至少一个磁盘存储器件、闪存器件、或其他非暂态固态存储器件。在一些实施例中，存储器 902 可选包括相对于处理器 901 远程设置的存储器，这些远程存储器可以通过网络连接至处理器 901。上述网络的实例包括但不限于互联网、企业内部网、局域网、移动通信网及其组合。

一个或者多个模块存储在存储器 902 中，当被处理器 901 执行时，执行上述方法实施例中的方法。

上述电子设备具体细节可以对应参阅上述方法实施例中对应的相关描述和效果进行理解，此处不再赘述。

本领域技术人员可以理解，实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，

存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory，ROM）、随机存储记忆体（Random Access Memory，RAM）、快闪存储器（Flash Memory）、硬盘（Hard Disk Drive，缩写：HDD）或固态硬盘（Solid-State Drive，SSD）等；存储介质还可以包括上述种类的存储器的组合。

虽然结合附图描述了本申请的实施例，但是本领域技术人员可以在不脱离本申请的精神和范围的情况下作出各种修改和变型，这样的修改和变型均落入由所附权利要求所限定的范围之内。

权 利 要 求 书

1. 一种基于多用户数据的安全求均值方法，其特征在于，包括：

基于多密钥全同态加密算法的公钥分别对预设数量目标用户的密文进行扩展，得到各目标用户对应的扩展密文，所述扩展密文的解密密钥为各目标用户对应的私钥；

对所有的扩展密文进行累加后发送至各目标用户；

接收第一目标用户反馈的包含均值数据的密文，所述均值数据对应的密文为所述第一目标用户基于用户明文数据求均值得到的，所述用户明文数据为各目标用户基于各目标用户对应的私钥对累加后的扩展密文解密得到的，所述第一目标用户为各目标用户中任意一个目标用户。

2. 根据权利要求 1 所述的方法，其特征在于，所述对所有的扩展密文进行累加后发送至各目标用户，包括：

获取随机扰动数据；

基于所述随机扰动数据，采用所述公钥对所述随机扰动数据进行同态加密得到所述随机扰动数据对应的第一密文；

分别将所述第一密文与各所述扩展密文进行累加，得到第一扩展密文；

对所有第一扩展密文进行累加后发送至各目标用户。

3. 根据权利要求 2 所述的方法，其特征在于，所述接收第一目标用户反馈的包含均值数据的密文，包括：

获取所述第一目标用户对应的公钥；

基于所述公钥对所述随机扰动数据进行同态加密，得到所述随机扰动数据

对应的第二密文；

对第一目标用户反馈的包含均值数据的密文和所述第二密文作差，得到所述均值数据对应的密文。

4. 根据权利要求 1 所述的方法，其特征在于，在所述基于扩展公钥分别对预设数量的目标用户的密文进行扩展之前，所述方法还包括：

接收所述预设数量的目标用户发送的密文，所述密文为各目标用户采用其对应的公钥对各自用户数据进行同态加密后得到的。

5. 一种基于多用户数据的安全求均值方法，其特征在于，包括：

接收服务器发送的扩展密文，所述扩展密文为所述服务器基于多密钥全同态加密算法的公钥分别对所有目标用户的密文进行扩展后累加得到的；

获取预设数量的目标用户分别对所述扩展密文进行解密后的明文数据；

基于所述预设数量对所有目标用户的明文数据求均值，得到均值数据；

基于当前目标用户的公钥对所述均值数据进行同态加密，得到包含均值数据的密文，并发送至所述服务器。

6. 根据权利要求 5 所述的方法，其特征在于，所述扩展密文中包含有随机扰动数据对应的第一密文，所述获取预设数量的目标用户分别对所述扩展密文进行解密后的明文数据包括：

基于当前目标用户的私钥对所述扩展密文进行解密，得到当前明文数据，所述当前明文数据中包含有所述随机扰动数据；

接收其他目标用户发送的明文数据，所述明文数据为其他目标用户基于各自的私钥对所述扩展密文进行解密得到的，所述明文数据中包含有所述随机扰动数据。

7. 根据权利要求 6 所述的方法，其特征在于，所述基于所述预设数量对所有目标用户的明文数据求均值，得到均值数据，包括：

对当前明文数据及其他目标用户对应的明文数据进行累加，得到总明文数据；

基于所述预设数量对所述总明文数据求均值，得到所述均值数据。

8. 根据权利要求 5 所述的方法，其特征在于，在所述接收服务器发送的扩展密文之前，所述方法还包括：

基于当前目标用户的公钥对当前目标用户对应的用户数据进行同态加密，得到密文，并将所述密文发送至服务器。

9. 一种电子设备，其特征在于，包括：

存储器和处理器，所述存储器和所述处理器之间互相通信连接，所述存储器中存储有计算机指令，所述处理器通过执行所述计算机指令，从而执行权利要求 1-8 任一项所述的方法。

10. 一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有计算机指令，所述计算机指令用于使所述计算机从而执行权利要求 1-8 任一项所述的方法。

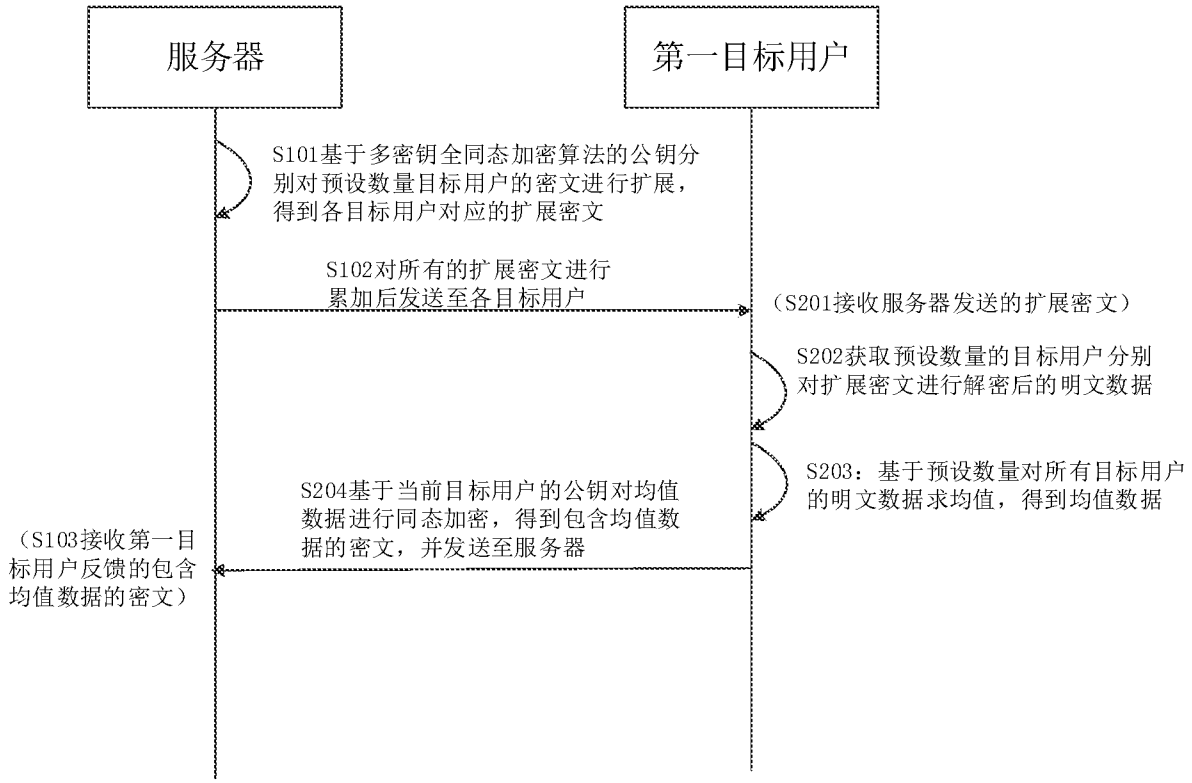
服务器
第一目标用户
S101基于多密钥全同态加密算法的公钥分别对预设数量目标用户的密文进行扩展，得到各目标用户对应的扩展密文
S102对所有的扩展密文进行累加后发送至各目标用户
（S201接收服务器发送的扩展密文）
S202获取预设数量的目标用户分别对扩展密文进行解密后的明文数据
S203：基于预设数量对所有目标用户的明文数据求均值，得到均值数据
S204基于当前目标用户的公钥对均值数据进行同态加密，得到包含均值数据的密文，并发送至服务器
（S103接收第一目标用户反馈的包含均值数据的密文）

图 1

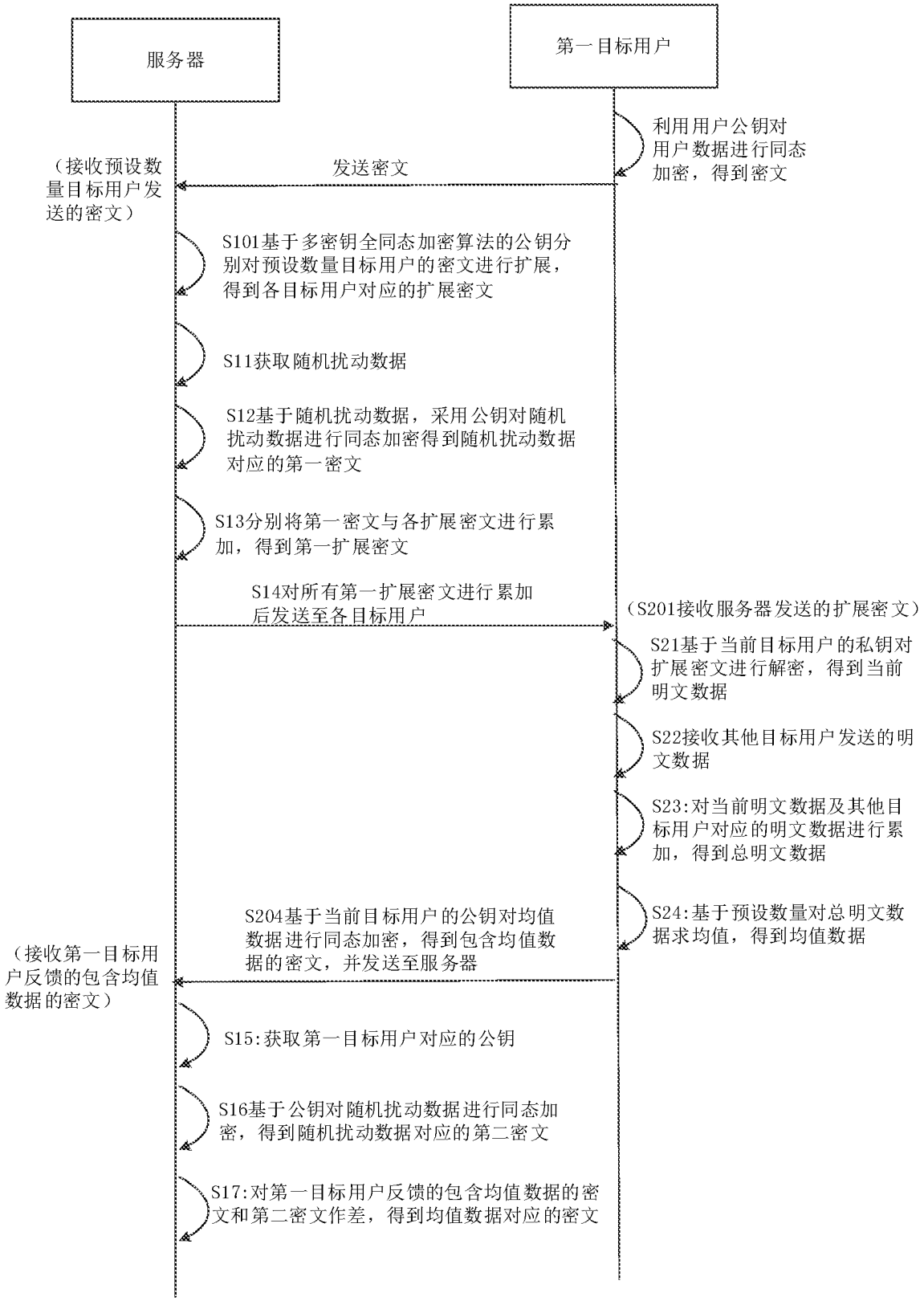
服务器
第一目标用户
利用用户公钥对用户数据进行同态加密，得到密文
（接收预设数量目标用户发送的密文）
发送密文
S101基于多密钥全同态加密算法的公钥分别对预设数量目标用户的密文进行扩展，得到各目标用户对应的扩展密文
S11获取随机扰动数据
S12基于随机扰动数据，采用公钥对随机扰动数据进行同态加密得到随机扰动数据对应的第一密文
S13分别将第一密文与各扩展密文进行累加，得到第一扩展密文
S14对所有第一扩展密文进行累加后发送至各目标用户
（S201接收服务器发送的扩展密文）
S21基于当前目标用户的私钥对扩展密文进行解密，得到当前明文数据
S22接收其他目标用户发送的明文数据
S23:对当前明文数据及其他目标用户对应的明文数据进行累加，得到总明文数据
S24:基于预设数量对总明文数据求均值，得到均值数据
S204基于当前目标用户的公钥对均值数据进行同态加密，得到包含均值数据的密文，并发送至服务器
（接收第一目标用户反馈的包含均值数据的密文）
S15:获取第一目标用户对应的公钥
S16基于公钥对随机扰动数据进行同态加密，得到随机扰动数据对应的第二密文
S17:对第一目标用户反馈的包含均值数据的密文和第二密文作差，得到均值数据对应的密文

图 2

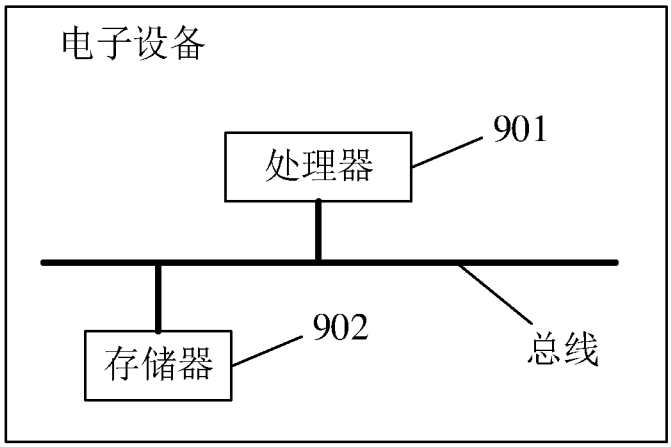

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/140586

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)

CNPAT, WPI, EPODOC, CNKI, IEEE: 均值, 除法, 同态, 加密, 公钥, 私钥, 扩展, 密文, 累加, 解密, 随机, 扰动, mean, public, private, key, encrypt, decrypt, homostasis, random, disturbance

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 109831297 A (ENGINEERING UNIVERSITY OF CAPF) 31 May 2019 (2019-05-31) description, paragraphs [0042]-[0068]	1-10
Y	CN 107145792 A (HARBIN INSTITUTE OF TECHNOLOGY SHENZHEN GRADUATE SCHOOL) 08 September 2017 (2017-09-08) description, paragraphs [0048]-[0058]	1-10
A	CN 105577357 A (SOUTHEAST UNIVERSITY) 11 May 2016 (2016-05-11) entire document	1-10
A	CN 110147681 A (XIDIAN UNIVERSITY) 20 August 2019 (2019-08-20) entire document	1-10
A	US 2015215123 A1 (CISCO TECHNOLOGY, INC.) 30 July 2015 (2015-07-30) 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	Date of mailing of the international search report
28 July 2021	**28 September 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/140586

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109831297 A	31 May 2019	None	
CN 107145792 A	08 September 2017	None	
CN 105577357 A	11 May 2016	None	
CN 110147681 A	20 August 2019	None	
US 2015215123 A1	30 July 2015	WO 2014016795 A2	30 January 2014
		CN 104509024 A	08 April 2015
		EP 2873186 A2	20 May 2015
		US 2016234010 A1	11 August 2016

国际检索报告

国际申请号
PCT/CN2020/140586

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））

CNPAT, WPI, EPODOC, CNKI, IEEE: 均值，除法，同态，加密，公钥，私钥，扩展，密文，累加，解密，随机，扰动，mean, public, private, key, encrypt, decrypt, homostasis, random, disturbance

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
Y	CN 109831297 A (中国人民武装警察部队工程大学) 2019年 5月 31日 (2019-05-31) 说明书第[0042]-[0068]段	1-10
Y	CN 107145792 A (哈尔滨工业大学深圳研究生院) 2017年 9月 8日 (2017-09-08) 说明书第[0048]-[0058]段	1-10
A	CN 105577357 A (东南大学) 2016年 5月 11日 (2016-05-11) 全文	1-10
A	CN 110147681 A (西安电子科技大学) 2019年 8月 20日 (2019-08-20) 全文	1-10
A	US 2015215123 A1 (CISCO TECHNOLOGY, INC.) 2015年 7月 30日 (2015-07-30) 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	国际检索报告邮寄日期
2021年 7月 28日	2021年 9月 28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	周亚楠
传真号 (86-10)62019451	电话号码 86-(10)-53961530

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/140586

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	109831297	A	2019年 5月 31日	无			
CN	107145792	A	2017年 9月 8日	无			
CN	105577357	A	2016年 5月 11日	无			
CN	110147681	A	2019年 8月 20日	无			
US	2015215123	A1	2015年 7月 30日	WO	2014016795	A2	2014年 1月 30日
				CN	104509024	A	2015年 4月 8日
				EP	2873186	A2	2015年 5月 20日
				US	2016234010	A1	2016年 8月 11日