(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 11 月 19 日 (19.11.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/228304 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2019/123141

(22) 国际申请日: 2019 年 12 月 5 日 (05.12.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910390295.0 2019年5月10日 (10.05.2019) CN

(71) 申请人: 深圳壹账通智能科技有限公司(ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。

(72) 发明人: 冯承勇(FENG, Chengyong); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。

(74) 代理人: 深圳中一联合知识产权代理有限公司(SHENZHEN ZHONGYI UNION INTELLECTUAL PROPERTY AGENCY CO., LTD.); 中国广东省深圳市福田区园岭街道深南中路1014号报春大厦9楼（5号信箱）, Guangdong 518028 (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,

(54) **Title:** INFORMATION INTERACTION METHOD AND APPARATUS, AND COMPUTER DEVICE AND READABLE STORAGE MEDIUM

(54) **发明名称**: 信息交互方法、装置、计算机设备及可读存储介质

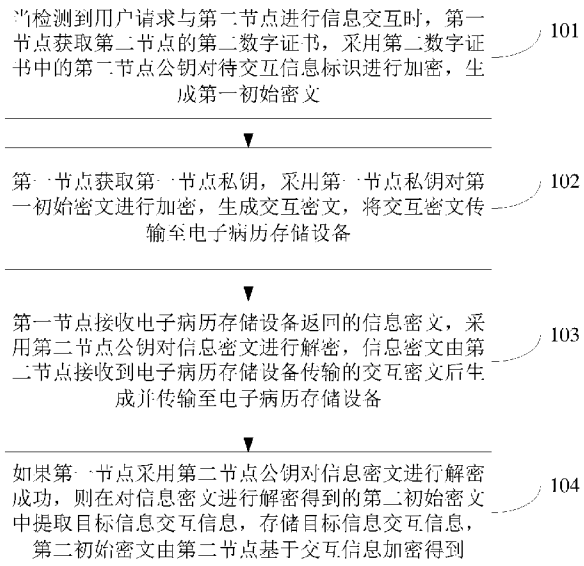

图 1A

101 When it is detected that a user makes a request for information interaction with a second node, a first node acquires a second digital certificate of the second node, and uses a second node public key in the second digital certificate to encrypt an identifier of information to be interacted with to generate a first initial ciphertext

102 The first node acquires a first node private key, uses the first node private key to encrypt the first initial ciphertext to generate an interaction ciphertext, and transmits the interaction ciphertext to an electronic medical record storage device

103 The first node receives an information ciphertext returned by the electronic medical record storage device, and uses the second node public key to decrypt the information ciphertext, wherein the information ciphertext is generated by the second node after receiving the interaction ciphertext transmitted by the electronic medical record storage device, and is transmitted to the electronic medical record storage device

104 If the first node uses the second node public key to decrypt the information ciphertext successfully, then target information interaction information from a second initial ciphertext obtained by means of decrypting the information ciphertext is extracted, and the target information interaction information is stored, wherein the second initial ciphertext is obtained by means of the second node performing encryption on the basis of the interaction information

(57) **Abstract:** The implementation of the present application is applicable to the technical field of data transmission. Provided are an information interaction method and apparatus, and a computer device and a readable storage medium. The method comprises: when it is detected that a user makes a request for information interaction, acquiring a second digital certificate of a second node, and using a second node public key in the second digital certificate to encrypt an identifier of information to be interacted with to generate a first initial ciphertext; acquiring a first node private key to encrypt the first initial ciphertext to generate an interaction ciphertext, and transmitting the interaction ciphertext to an electronic medical record storage device; receiving an information ciphertext, and using the second node public key to decrypt the information ciphertext; and if the decryption is successful, extracting interaction information

WO 2020/228304 A1

[见续页]

PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

from a second initial ciphertext obtained by means of decrypting the information ciphertext, and storing the interaction information. By means of using a multi-layer encryption form to ensure the security of interaction information during a transmission process, the privacy during an information interaction process is improved, information will not easily be leaked, and the security of information is better.

(57) 摘要：本申请实施适用于数据传输技术领域，提供了一种信息交互方法、装置、计算机设备及可读存储介质，所述方法包括：当检测到用户请求进行信息交互时，获取第二节点的第二数字证书，采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文；获取第一节点私钥，对第一初始密文进行加密，生成交互密文，将交互密文传输至电子病历存储设备；接收信息密文，采用第二节点公钥对信息密文进行解密；如果解密成功，则在对信息密文进行解密得到的第二初始密文中提取交互信息，存储交互信息。通过采用多层加密的形式保证交互信息在传输过程中的安全，提高信息交互过程中的私密性，信息不容易泄露，信息的安全性较好。

信息交互方法、装置、计算机设备及可读存储介质

[0001] 本申请申明享有2019年05月10日递交的申请号为201910390295.0、名称为“信息交互方法、装置、计算机设备及可读存储介质”中国专利申请的优先权，该中国专利申请的整体内容以参考的方式结合在本申请中。

技术领域

[0002] 本申请属于数据传输技术领域，特别是涉及一种信息交互方法、装置、计算机设备及可读存储介质。

背景技术

[0003] 随着互联网技术的飞速发展，卫生与健康现代医疗卫生体系的建设规划也越来越成熟，预计到2020年，将建成全面的健康信息平台，实现所在地区各大医院之间信息的相互交互。健康信息平台中采用电子病历的形式存储患者的所有数据并实时更新数据，目前已经建立的健康信息平台通常依赖中心化的信息系统所搭载，并基于该中心化的信息系统实现电子病历的存储及更新。

[0004] 相关技术中，每个医院均建立了中心化的信息系统，对于每个医院来说，该医院的信息系统存储了该医院中涉及到的全部信息，例如，工作人员信息、病人治疗信息、医院运营信息等，为了使各大医院之间的信息实现互联互通，通常来说，医院之间都会进行信息交互。目前，医院在进行信息交互时，需要将待交互的信息从信息系统中提取出来，采用纸质或者电子版的形式将待交互的信息传输给其他医院。

[0005] 在实现本申请的过程中，发明人发现相关技术至少存在以下问题：每个医院的信息系统中存储的信息仅是在本医院的相关信息，若采用纸质或者电子版的形式将待交互的信息传输给其他医院，会导致信息交互过程的私密性不好，信息容易泄露，信息的安全性较差。

发明概述

技术问题

[0006] 有鉴于此，本申请提供了一种信息交互方法、装置、计算机设备及可读存储介

质，主要目的在于解决目前采用纸质或者电子版的形式将待交互的信息传输给其他医院，会导致信息交互过程的私密性不好，信息容易泄露，信息的安全性较差的问题。

问题的解决方案

技术解决方案

[0007] 为解决上述技术问题，本申请实施例采用的技术方案是：

[0008] 第一方面，提供了一种信息交互方法，该方法包括：

[0009] 当检测到用户请求与第二节点进行信息交互时，第一节点获取第二节点的第二数字证书，采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文；

[0010] 获取第一节点私钥，采用第一节点私钥对第一初始密文进行加密，生成交互密文，将交互密文传输至电子病历存储设备；

[0011] 接收电子病历存储设备返回的信息密文，采用第二节点公钥对信息密文进行解密，信息密文由第二节点接收到电子病历存储设备传输的交互密文后生成并传输至电子病历存储设备；

[0012] 如果采用第二节点公钥对信息密文进行解密成功，则在对信息密文进行解密得到的第二初始密文中提取交互信息，存储交互信息，第二初始密文由第二节点基于交互信息加密得到。

[0013] 第二方面，提供了提供了一种信息交互方法，该方法包括：

[0014] 当接收到第一节点传输的交互密文时，电子病历存储设备确定第一节点请求进行信息交互的第二节点，第一节点和第二节点为进行信息交互的节点，交互密文由第一节点基于携带待交互信息标识的信息交互请求生成的；

[0015] 将交互密文传输至第二节点；

[0016] 如果接收到第二节点在接收到交互密文后返回的信息密文，则将信息密文返回给第一节点，信息密文由第二节点基于待交互信息标识指示的交互信息生成。

[0017] 第三方面，一种信息交互方法，该方法包括：

[0018] 当接收到电子病历存储设备传输的交互密文时，第二节点获取第一节点的第一数字证书，采用第一数字证书中的第一节点公钥对交互密文进行解密，交互密

文由第一节点基于携带待交互信息标识的信息交互请求生成的，第一节点为请求与第二节点进行信息交互的节点；

[0019] 如果采用第一节点公钥对交互密文进行解密成功，则在解密后的交互密文中提取第一初始密文，第一初始密文由第一节点对信息交互请求加密后生成；

[0020] 获取第二节点私钥，采用第二节点私钥对第一初始密文进行解密，得到待交互信息标识；

[0021] 提取待交互信息标识指示的交互信息，基于交互信息生成信息密文，将信息密文传输至电子病历存储设备。

[0022] 第四方面，提供了一种信息交互装置，该装置包括：

[0023] 第一加密模块，用于当检测到用户请求与第二节点进行信息交互时，第一节点获取第二节点的第二数字证书，采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文；

[0024] 第二加密模块，用于获取第一节点私钥，采用第一节点私钥对第一初始密文进行加密，生成交互密文，将交互密文传输至电子病历存储设备；

[0025] 解密模块，用于接收电子病历存储设备返回的信息密文，采用第二节点公钥对信息密文进行解密，信息密文由第二节点接收到电子病历存储设备传输的交互密文后生成并传输至电子病历存储设备；

[0026] 存储模块，用于如果采用第二节点公钥对信息密文进行解密成功，则在对信息密文进行解密得到的第二初始密文中提取交互信息，存储交互信息，第二初始密文由第二节点基于交互信息加密得到。

[0027] 第五方面，提供了一种信息交互装置，该装置包括：

[0028] 确定模块，用于当接收到第一节点传输的交互密文时，电子病历存储设备确定第一节点请求进行信息交互的第二节点，第一节点和第二节点为进行信息交互的节点，交互密文由第一节点基于携带待交互信息标识的信息交互请求生成的；

[0029] 第一传输模块，用于将交互密文传输至第二节点；

[0030] 返回模块，用于如果接收到第二节点在接收到交互密文后返回的信息密文，则将信息密文返回给第一节点，信息密文由第二节点基于待交互信息标识指示的

交互信息生成。

[0031] 第六方面，提供了一种信息交互装置，该装置包括：

[0032] 第一解密模块，用于当接收到电子病历存储设备传输的交互密文时，第二节点获取第一节点的第一数字证书，采用第一数字证书中的第一节点公钥对交互密文进行解密，交互密文由第一节点基于携带待交互信息标识的信息交互请求生成的，第一节点为请求与第二节点进行信息交互的节点；

[0033] 提取模块，用于如果采用第一节点公钥对交互密文进行解密成功，则在解密后的交互密文中提取第一初始密文，第一初始密文由第一节点对信息交互请求加密后生成；

[0034] 第二解密模块，用于获取第二节点私钥，采用第二节点私钥对第一初始密文进行解密，得到待交互信息标识；

[0035] 传输模块，用于提取待交互信息标识指示的交互信息，基于交互信息生成信息密文，将信息密文传输至电子病历存储设备。

[0036] 第七方面，提供了一种计算机设备，包括存储器、处理器以及存储在存储器中并可在处理器上运行的计算机可读指令，处理器执行计算机可读指令时实现上述第一方面或第二方面或第三方面的方法的步骤。

[0037] 第八方面，提供了一种计算机非易失性可读存储介质，计算机非易失性可读存储介质存储有计算机可读指令，计算机可读指令被处理器执行时实现上述第一方面或第二方面或第三方面的方法的步骤。

[0038] 本申请提供的一种信息交互方法、装置、计算机设备及可读存储介质，与目前采用纸质或者电子版的形式将待交互的信息传输给其他医院的方式相比，本申请在需要进行信息交互时，第一节点对待交互信息标识进行加密，并将加密后的待交互信息标识传输给需要进行交互的第二节点，由第二节点在允许信息交互的情况下，将交互信息进行传输，使得采用多层加密的形式保证了交互信息在传输过程中的安全，提高信息交互过程中的私密性，信息不容易泄露，信息的安全性较好。

发明的有益效果

对附图的简要说明

附图说明

[0039] 图1A示出了本申请实施例提供的一种信息交互方法流程示意图；

[0040] 图1B示出了本申请实施例提供的一种信息交互方法流程示意图；

[0041] 图1C示出了本申请实施例提供的一种信息交互方法流程示意图；

[0042] 图2A示出了本申请实施例提供的一种信息交互方法流程示意图；

[0043] 图2B示出了本申请实施例提供的一种信息交互方法流程示意图；

[0044] 图3A示出了本申请实施例提供的一种信息交互方装置的结构示意图；

[0045] 图4A示出了本申请实施例提供的一种信息交互方装置的结构示意图；

[0046] 图5A示出了本申请实施例提供的一种信息交互方装置的结构示意图；

[0047] 图6示出了本申请实施例提供的一种计算机设备的装置结构示意图。

发明实施例

本发明的实施方式

[0048] 本申请实施例提供了一种信息交互方法，如图1A所示，该方法包括：

[0049] 101、当检测到用户请求与第二节点进行信息交互时，第一节点获取第二节点的第二数字证书，采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文。

[0050] 在本申请实施例中，当第一节点检测到用户请求进行信息交互时，为了保证请求进行信息交互的过程的安全性，第一节点获取待进行信息交互的第二节点的第二数字证书，并采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，从而生成第一初始密文，以便后续基于该第一初始密文实现信息交互。

[0051] 102、第一节点获取第一节点私钥，采用第一节点私钥对第一初始密文进行加密，生成交互密文，将交互密文传输至电子病历存储设备。

[0052] 在本申请实施例中，为了给第二节点一个对进行信息交互的凭证的验证机会，且公私钥之间具有可以相互加密或者解密的特性，因此，第一节点获取自身的第一节点私钥，并采用该第一节点私钥对第一初始密文进行加密，生成交互密文，从而将该交互密文传输至电子病历存储设备。

[0053] 103、第一节点接收电子病历存储设备返回的信息密文，采用第二节点公钥对信息密文进行解密，信息密文由第二节点接收到电子病历存储设备传输的交互

密文后生成并传输至电子病历存储设备。

[0054] 在本申请实施例中，当第一节点接收到电子病历存储设备返回的信息密文时，采用第二节点公钥对信息密文进行解密，也即对接收到的信息密文进行验证，从而判断信息密文是否在传输的过程中被篡改。

[0055] 104、如果第一节点采用第二节点公钥对信息密文进行解密成功，则在对信息密文进行解密得到的第二初始密文中提取交互信息，存储交互信息，第二初始密文由第二节点基于交互信息加密得到。

[0056] 在本申请实施例中，如果第一节点采用第二节点公钥对信息密文进行解密成功，则表示第二节点给第一节点传输的信息密文在传输的过程中并没有被篡改，第一节点可以接收并存储第二节点返回的交互信息。

[0057] 本申请实施例提供了另一种信息交互方法，如图1B所示，该方法包括：

[0058] 105、当接收到第一节点传输的交互密文时，电子病历存储设备确定第一节点请求进行信息交互的第二节点，第一节点和第二节点为进行信息交互的节点，交互密文由第一节点基于携带待交互信息标识的信息交互请求生成的。

[0059] 在本申请实施例中，当电子病历存储设备接收到第一节点传输的交互密文时，便可以确定第一节点请求进行信息交互的第二节点，以便后续将交互密文传输至第二节点。

[0060] 106、电子病历存储设备将交互密文传输至第二节点。

[0061] 在本申请实施例中，电子病历存储设备将接收到的第一节点传输的交互密文传输至第二节点。

[0062] 107、如果电子病历存储设备接收到第二节点在接收到交互密文后返回的信息密文，则将信息密文返回给第一节点，信息密文由第二节点基于待交互信息标识指示的交互信息生成。

[0063] 在本申请实施例中，如果电子病历存储设备接收到第二节点在接收到交互密文后返回的信息密文，则表示第一节点与第二节点之间进行的信息交互成功，电子病历存储设备将信息密文返回给第一节点。

[0064] 本申请实施例提供了另一种信息交互方法，如图1C所示，该方法包括：

[0065] 108、当接收到电子病历存储设备传输的交互密文时，第二节点获取第一节点

的第一数字证书，采用第一数字证书中的第一节点公钥对交互密文进行解密，交互密文由第一节点基于携带待交互信息标识的信息交互请求生成的，第一节点为请求与第二节点进行信息交互的节点。

[0066] 在本申请实施例中，当第二节点接收到电子病历存储设备传输的交互密文时，第二节点通过获取第一节点的第一数字证书，采用第一数字证书中的第一节点公钥对交互密文进行解密，来实现对交互密文的验证，确定交互密文在传输的过程中是否被更改。

[0067] 109、如果第二节点采用第一节点公钥对交互密文进行解密成功，则在解密后的交互密文中提取第一初始密文，第一初始密文由第一节点对信息交互请求加密后生成。

[0068] 在本申请实施例中，如果第二节点采用第一节点公钥对交互密文进行解密成功，则表示交互密文在传输的过程中并没有被篡改，第二节点可以在解密后的交互密文中提取第一初始密文。

[0069] 110、第二节点获取第二节点私钥，采用第二节点私钥对第一初始密文进行解密，得到待交互信息标识。

[0070] 在本申请实施例中，第二节点在对交互密文进行解密成功后，便可以获取第二节点私钥，采用第二节点私钥对第一初始密文进行解密，得到待交互信息标识。

[0071] 111、第二节点提取待交互信息标识指示的交互信息，基于交互信息生成信息密文，将信息密文传输至电子病历存储设备。

[0072] 在本申请实施例中，当第二节点获取到待交互信息标识后，第二节点便可以提取到该待交互信息标识指示的交互信息，并基于交互信息生成信息密文，将信息密文传输至电子病历存储设备，从而实现与第一节点之间进行信息交互。

[0073] 本申请实施例提供了另一种信息交互方法，如图2A和图2B所示，该方法包括：

[0074] 201、第一节点基于第二节点的第二节点标识，生成证书查询请求，将证书查询请求传输至电子病历存储设备。

[0075] 在本申请实施例中，电子病历存储设备是基于区块链技术实现电子病历存储的

设备，其中存储有大量用户的电子病历。由于通常来说只有医院才可以在用户治疗的过程中生成电子病历，因此，大量医院以节点的方式接入到电子病历存储设备中，且这些医院作为节点将用户的电子病历上传到电子病历存储设备中。在实际应用的过程中，为了实现对医院的认证，避免盲目的允许医院接入到电子病历存储设备中造成的信息不安全，电子病历存储设备会为接入其中的节点提供注册服务，并只有在电子病历存储设备中成功注册的节点才可以基于电子病历存储设备实现一系列的操作。在本申请实施例中，以交互的节点为第一节点和第二节点为例进行说明，第一节点和第二节点均为在电子病历存储设备中成功注册的节点。

[0076] 通常来说，指示节点在电子病历存储设备中注册成功的标志便是电子病历存储设备中存储有该节点的数字证书，也即电子病历存储设备中存储有每一个成功在电子病历存储设备中注册的节点的数字证书。节点的数字证书中通常包括证书公钥，该证书公钥与节点自身保留的证书私钥是相互对应的，采用证书公钥进行加密的信息可以采用证书私钥进行解密，且采用证书私钥加密的信息可以采用证书公钥解密，因此，为了保证在请求进行信息交互时各种信息的安全性，可以基于公私钥的特性对交互的信息进行加密，并基于加密后的信息进行交互。

[0077] 由于每个节点的数字证书都存储在电子病历存储设备中，因此，为了对交互过程涉及到的信息进行加密，当第一节点希望与第二节点进行信息交互时，需要向电子病历存储设备请求第二节点的第二数字证书，以便基于该第二数字证书中的第二证书公钥实现在交互过程中对信息的加密。其中，第一节点在向电子病历存储设备请求第二节点的第二数字证书时，由于电子病历存储设备中注册有大量的节点，使得电子病历存储设备中存储有大量的数字证书，因此，第一节点基于第二节点的第二节点标识，生成证书查询请求，也即生成包括第二节点标识的证书查询请求，并将该证书查询请求传输给电子病历存储设备，以便电子病历存储设备基于该证书查询请求为第一节点提供第二节点的数字证书。

[0078] 202、当电子病历存储设备接收到第一节点传输的证书查询请求时，在证书查询请求中提取第二节点标识，获取第二节点标识指示的第二数字证书，将第二

数字证书传输至第一节点。

[0079] 在本申请实施例中，当电子病历存储设备接收到第一节点传输的证书查询请求时，便可以基于该证书查询请求获取到第二节点的第二数字证书，并将该第二数字证书提供给第一节点。其中，由于证书查询请求中携带了第二节点标识，因此，首先，电子病历存储设备在证书查询请求中提取第二节点标识；随后，基于该第二节点标识进行查询，从而获取到该第二节点标识指示的第二数字证书，并将该第二数字证书传输至第一节点。

[0080] 203、第一节点接收电子病历存储设备在接收到证书查询请求后返回的第二数字证书。

[0081] 在本申请实施例中，由于电子病历存储设备会将获取到的第二节点的数字证书返回给第一节点，因此，第一节点会接收到电子病历存储设备在接收到证书查询请求后返回的第二数字证书。

[0082] 204、当第一节点检测到用户请求与第二节点进行信息交互时，获取第二节点的第二数字证书，采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文。

[0083] 在本申请实施例中，为了给第一节点的用户提供请求进行信息交互的机会，第一节点所搭载的终端中可以提供信息交互入口，当检测到用户触发该信息交互入口时，确定检测到用户请求进行信息交互，此时，便可以显示交互信息输入页面，并在检测到用户对该交互信息输入页面确认时，获取用户填入交互信息输入页面中的待交互信息标识，以便交互该待交互信息标识指示的交互信息。具体地，该待交互信息标识可为病历信息标识、员工信息标识以及学术文件标识等，本申请实施例对待交互信息标识具体包括哪些内容不进行限定。

[0084] 为了保证信息交互过程的安全性，第一节点在向第二节点传输希望进行信息交互的待交互信息标识时，基于第二节点的第二数字证书对该待交互信息标识进行加密。考虑到每个节点的数字证书都会包括该节点的证书公钥，因此，当第一节点检测到用户请求进行信息交互时，便可以在获取到的第二节点的第二数字证书中提取到该第二节点的第二节点公钥。由于每一个节点均具有一对证书公钥和证书私钥，且证书公钥和证书私钥具有采用证书公钥加密后的信息可以

采用证书私钥进行解密的特性，为了避免待交互信息标识在传输的过程中被篡改，第一节点在获取到第二节点的第二节点公钥后，便可以将该第二节点公钥作为加密公钥，采用第二节点公钥对待交互信息标识进行加密，从而生成第一初始密文。

[0085] 205、第一节点获取第一节点私钥，采用第一节点私钥对第一初始密文进行加密，生成交互密文，将交互密文传输至电子病历存储设备。

[0086] 在本申请实施例中，在生成了第一初始密文后，考虑到第一初始密文仍旧存在在传输过程中被篡改的可能，且第一节点的第一数字证书中包括的第一证书公钥是公开的，为了在后续给第二节点提供一个可以验证接收到的密文是否未被篡改的机会，因此，第一节点在生成第一初始密文后，还可以采用自身的第一节点私钥对该第一初始密文进行签名，生成查询密文，并将该查询密文传输给电子病历存储设备，以便电子病历存储设备将该查询密文传输给第二节点，使得第二节点可以基于第二节点公开的第一证书公钥对该交互密文进行验证，既保证了信息交互过程的安全性，还给第二节点提供了对交互密文进行验证的机会，实现了双重保护。

[0087] 在实际应用的过程中，为了使电子病历存储设备在接收到交互密文时，可以确定将该交互密文传输给哪一个节点，第一节点还可以采用第二节点标识对交互密文进行标记，以便电子病历存储设备在接收到交互密文时，可以确定将该交互密文传输给第二节点，避免电子病历存储设备将交互密文传输错误。

[0088] 206、当电子病历存储设备接收到第一节点传输的交互密文时，确定第一节点请求进行信息交互的第二节点，将交互密文传输至第二节点。

[0089] 在本申请实施例中，当电子病历存储设备接收到第一节点传输的交互密文时，便可以确定第一节点请求进行信息交互的第二节点，并直接将该交互密文传输至第二节点。其中，如果第一节点采用了第二节点标识对交互密文进行了标记，则电子病历存储设备在接收到交互密文时，可以根据交互密文标记的第二节点标识来确定第二节点，并直接将该交互密文传输至第二节点。

[0090] 207、当第二节点接收到电子病历存储设备传输的交互密文时，获取第一节点的第一数字证书，采用第一数字证书中的第一节点公钥对交互密文进行解密，

如果采用第一节点公钥对交互密文进行解密成功，则执行下述步骤208至步骤211；如果采用第一节点公钥对交互密文进行解密失败，则执行下述步骤215至步骤216。

[0091] 在本申请实施例中，由于交互密文是采用第一节点的第一节点私钥进行加密生成的，因此，在第二节点接收到交互密文后，第二节点可以采用第一节点公钥对交互密文进行解密，并通过解密是否成功来实现对交互密文的验证，从而确定交互密文是否被篡改。其中，第一节点的第二节点公钥是公开的，且是以第一数字证书的形式存储在电子病历存储设备中的，因此，第二节点在获取第一节点公钥时，可以请求电子病历存储设备提供，具体过程与上述步骤201至步骤202 中第一节点向电子病历存储设备请求第二节点公钥的过程一致，此处不再进行赘述。

[0092] 其中，如果第二节点采用第一节点公钥对交互密文进行解密成功，则表示交互密文并没有被篡改，这时，第二节点便可以对该交互密文进行解密，得到该交互密文中的第一初始密文，并基于该第一初始密文为第一节点提供交互信息，也即执行下述步骤208至步骤211。如果第二节点采用第一节点公钥对交互密文进行签名失败，则表示该交互密文在传输的过程中很可能被篡改了，需要第一节点重新发送交互密文才可以进行信息的交互，也即执行下述步骤215至步骤216。

[0093] 在实际应用的过程中，当第二节点接收到交互密文时，如果第二节点并不希望与第一节点进行信息交互，则第二节点无需执行采用第一节点公钥对交互密文进行解密的过程，直接执行下述步骤215至步骤216的过程，告知第一节点信息交互失败即可。

[0094] 208、如果第二节点采用第一节点公钥对交互密文进行解密成功，则在解密后的交互密文中提取第一初始密文，获取第二节点私钥，采用第二节点私钥对第一初始密文进行解密，得到待交互信息标识。

[0095] 在本申请实施例中，如果第二节点采用第一节点公钥对交互密文进行签名成功，则表示交互密文并没有被篡改，这时，第二节点便可以通过对交互密文进行解密，在解密后的交互密文中提取第一初始密文。另外，由于第一初始密文采

用第二节点的第二节点公钥加密生成，基于公私钥互相加密解密的特性，因此，第二节点可以采用第二节点私钥对第一初始密文进行解密，得到第一初始密文中包括的待查询信息标识，以便第二节点后续可以根据该待查询信息标识确定目标信息，并基于该目标信息，生成信息密文。

[0096] 209、第二节点根据待交互信息标识进行信息查询，获取待交互信息标识指示的交互信息，采用第一节点公钥对交互信息进行加密，生成第二初始密文，并采用第二节点私钥对第二初始密文进行加密，生成信息密文，并将信息密文传输给电子病历存储设备。

[0097] 在本申请实施例中，当第二节点获取到待交互信息标识后，便可以基于该待交互信息标识进行信息查询，获取该待交互信息标识指示的交互信息。为了保证将交互信息交互给第一节点的过程中交互信息的安全性，第二节点在将交互信息传输给第一节点之前，可以对交互信息进行加密。由于第一节点的第一节点公钥是公开的，且第二节点已经获取到了第一节点的第一证书公钥，因此，为了保证交互信息的安全性，第二节点可以采用第一节点公钥对交互信息进行加密，生成第二初始密文。随后，为了使第一节点在接收到第二初始密文时可以验证该第二初始密文是否未被其他的恶意节点篡改，第二节点可给第一节点提供对接收到的密文进行验证的机会，也即第二节点采用自身的第二节点私钥，对第二初始密文进行加密，生成信息密文，并将该信息密文传输给电子病历存储设备，使得电子病历存储可以将该信息密文传输给第一节点。

[0098] 210、电子病历存储设备将信息密文返回给第一节点。

[0099] 在本申请实施例中，当电子病历存储设备接收到第二节点传输的信息密文后，便可以将该信息密文传输给第一节点，以便第二节点基于该信息密文获取到第二节点为第一节点提供的交互信息。

[0100] 211、第一节点接收电子病历存储设备返回的信息密文，采用第二节点公钥对信息密文进行解密，如果采用第二节点公钥对信息密文进行解密成功，则执行下述步骤212；如果采用第二节点公钥对信息密文进行解密失败，则执行下述步骤213至步骤214。

[0101] 在本申请实施例中，当第一节点接收到电子病历存储设备返回的信息密文后，

由于信息密文是由第二节点获取交互信息，并首先采用第一节点的第一节点公钥加密，随后采用自身的第二节点私钥进行加密生成的，因此，第一节点可以先采用第二节点公钥对信息密文进行解密，实现对信息密文的验证，并仅在基于第二节点公钥对信息密文进行解密成功后，再继续进行其他的操作。如果采用第二节点公钥对信息密文进行解密成功，则表示信息密文在传输的过程中并没有被篡改，因此，第一节点便可以通过对信息密文进行解密，在解密后的信息密文中提取第二初始密文，也即执行下述步骤212；如果第一节点采用第二节点公钥对信息密文进行解密失败，则表示信息密文很可能在传输的过程中内容被篡改，因此，该信息密文便无法正常使用，此时，需要第二节点重新发送信息密文，也即执行下述步骤213至步骤214。

[0102] 212、如果第一节点采用第二节点公钥对信息密文进行解密成功，则获取对信息密文解密后的第二初始密文，采用第一节点私钥对第二初始密文进行解密，得到交互信息，并存储交互信息。

[0103] 在本申请实施例中，如果采用第二节点公钥对信息密文进行解密成功，则表示信息密文在传输的过程中并没有被篡改，因此，第一节点便可以通过对信息密文进行解密，在解密后的信息密文中提取第二初始密文。其中，由于第二初始密文由第二节点采用第一节点的第一节点公钥对交互信息进行加密生成的，因此，在提取到第二初始密文后，第一节点便可以采用自身的第一节点私钥对该第二初始密文进行解密，从而得到交互信息，并将得到的交互信息进行存储，从而完成与第二节点之间进行的信息交互。

[0104] 213、如果第一节点采用第二节点公钥对信息密文进行解密失败，则生成第一失败响应，将第一失败响应返回至电子病历存储设备。

[0105] 在本申请实施例中，如果第一节点采用第二节点公钥对信息密文进行解密失败，则表示信息密文很可能在传输的过程中内容被篡改，因此，该信息密文便无法正常使用，此时，需要第二节点重新发送信息密文。为了提醒第二节点重新发送信息密文，第一节点生成第一失败响应，并将第二失败响应返回给电子病历存储设备，以便电子病历存储设备将该第一失败响应传输给第二节点。

[0106] 其中，为了使第二节点在接收到第一失败响应时可以确定哪一个信息密文交互

失败了，第一节点生成的第一失败响应中可以携带待交互信息标识，以便第二节点根据第一失败响应携带的待交互信息标识重新发送对应的信息密文。

[0107] 214、电子病历存储设备将第一失败响应返回至第二节点。

[0108] 在本申请实施例中，当电子病历存储设备接收到第一失败响应后，便可以将该第一失败响应返回给第二节点，以便第二节点在接收到第一失败响应后可以重新发送信息密文。

[0109] 215、如果第二节点采用第一节点公钥对交互密文进行解密失败，则生成第二失败响应，将第二失败响应传输至电子病历存储设备。

[0110] 在本申请实施例中，如果第二节点采用第一节点公钥对交互密文进行解密失败，则表示该交互密文在传输的过程中很可能被篡改了，需要第一节点重新发送交互密文，因此，第二节点生成第二失败响应，并将该第二失败响应传输给电子病历存储设备，以便电子病历存储设备将该第二失败响应传输给第一节点，使得第一节点可以重新生成并发送交互密文。

[0111] 216、电子病历存储设备将第二失败响应返回至第一节点。

[0112] 在本申请实施例中，电子病历存储设备在接收到第二节点传输的第二失败响应后，便可将该第二失败响应传输给第一节点，使得第一节点在接收到第二失败响应后可以重新生成并发送交互密文。

[0113] 通过执行上述步骤201至步骤216中的过程，便可以实现第一节点与第二节点之间进行的信息交互。而在实际应用的过程中，为了防止不法分子的节点也可以在电子病历存储设备中与其他节点进行信息交互，从而导致节点中存储的数据被盗取，接入到电子病历存储设备中的节点均需要进行注册，并且只有成功注册的节点才可以基于电子病历存储设备实现与其他节点进行信息交互。其中，以第一节点为例，第一节点在电子病历存储设备中进行注册的过程如图2B所示，该方法包括：

[0114] 217、当第一节点检测到用户请求注册时，将第一节点身份信息以及第一节点公钥传输至电子病历存储设备。

[0115] 在本申请实施例中，第一节点所依赖的终端中可以为用户提供注册入口，当该终端检测到用户触发该注册入口时，确定检测到用户请求注册，显示注册页面

。其中，由于电子病历存储设备中为节点提供注册服务所依赖的凭证是数字证书，而电子病历存储设备为节点生成数字证书时是基于每个节点的节点公钥的，因此，第一节点在检测到用户请求注册时，将第一节点身份信息以及自身的第一节点公钥传输至电子病历存储设备，以便电子病历存储设备基于第一节点身份信息以及第一节点公钥为第一节点提供注册服务。

[0116] 具体地，第一节点身份信息可以包括医院名称信息、医院属性信息等，这样，还可为相同属性的医院提供更加便捷且清晰的信息交互服务。第一节点公钥可由第一节点自身生成或者获取到，一般来说，第一节点可以将自身可以公开的信息作为第一节点公钥，例如，医院编号、医院股票代码等；或者还可以随机生成一串字符串，将该字符串作为第一节点公钥。本申请实施例对第一节点获取第一节点公钥的方法不进行限定。

[0117] 218、当电子病历存储设备接收到第一节点传输的第一节点身份信息以及第一节点公钥时，将第一节点身份信息以及第一节点公钥进行绑定。

[0118] 在本申请实施例中，当电子病历存储设备接收到第一节点传输的第一节点身份信息以及第一节点公钥时，由于可能存在大量的节点在同一时间向电子病历存储设备请求注册的情况，使得电子病历存储设备可能在同一时间接收到大量的节点身份信息以及节点公钥，因此，为了区分接收到的节点身份信息以及节点公钥，电子病历存储设备将接收到的第一节点身份信息以及第一节点公钥进行绑定，以便后续基于该第一节点身份信息以及第一节点公钥实现对第一节点的注册。

[0119] 219、电子病历存储设备采用第一节点公钥对绑定后的第一节点身份信息以及第一节点公钥进行签名，生成并注册第一数字证书，将第一数字证书传输至第一节点，并将第一节点身份信息以及第一数字证书对应存储。

[0120] 在本申请实施例中，当电子病历存储设备将接收到的第一节点身份信息和第一节点公钥进行绑定后，为了给每一个节点生成与其相关的数字证书，并在后续可以基于数字证书对节点的身份进行验证，电子病历存储设备采用第一节点公钥对绑定后的第一节点身份信息以及第一节点公钥进行签名，生成第一数字证书，并基于该第一数字证书实现对第一节点的注册。在实际应用的过程中，为

了避免数字证书与节点之间对应关系的混淆，电子病历存储设备将生成的第一节点身份信息与第一数字证书对应存储，或者采用第一节点身份信息对第一数字证书进行标记，从而建立第一节点身份信息与第一数字证书之间的对应关系。

[0121] 在完成了给第一节点生成数字证书后，为了使第一节点可以获知自身已经完成了在电子病历存储设备中的注册，电子病历存储设备将第一数字证书传输至第一节点。

[0122] 220、第一节点接收电子病历存储设备在基于接收到第一节点身份信息以及第一节点公钥完成注册后返回的第一数字证书，并存储第一数字证书。

[0123] 第一数字证书由电子病历存储设备对第一节点身份信息以及第一节点公钥进行签名后生成。

[0124] 在本申请实施例中，第一节点接收到电子病历存储设备返回的第一数字证书后，便可以存储第一数字证书，从而完成在电子病历存储设备中的注册。

[0125] 本申请实施例提供的方法，在需要进行信息交互时，第一节点对待交互信息标识进行加密，并将加密后的待交互信息标识传输给需要进行交互的第二节点，由第二节点在允许信息交互的情况下，将交互信息进行传输，使得采用多层加密的形式保证了交互信息在传输过程中的安全，提高信息交互过程中的私密性，信息不容易泄露，信息的安全性较好。

[0126] 需要说明的是，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

[0127] 进一步地，作为图1A所述方法的具体实现，本申请实施例提供了一种信息交互装置，如图3A所示，所述装置包括：

[0128] 第一加密模块301，用于当检测到用户请求与第二节点进行信息交互时，第一节点获取第二节点的第二数字证书，采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文；

[0129] 第二加密模块302，用于获取第一节点私钥，采用第一节点私钥对第一初始密文进行加密，生成交互密文，将交互密文传输至电子病历存储设备；

[0130] 解密模块303，用于接收电子病历存储设备返回的信息密文，采用第二节点公钥对信息密文进行解密，信息密文由第二节点接收到电子病历存储设备传输的交互密文后生成并传输至电子病历存储设备；

[0131] 存储模块304，用于如果采用第二节点公钥对信息密文进行解密成功，则在对信息密文进行解密得到的第二初始密文中提取交互信息，存储交互信息，第二初始密文由第二节点基于交互信息加密得到。

[0132] 在具体的应用场景中，该装置还包括：

[0133] 传输模块305，用于当检测到用户请求注册时，将第一节点身份信息以及第一节点公钥传输至所述电子病历存储设备，所述第一节点身份信息至少包括医院名称信息、医院属性信息；

[0134] 接收模块306，用于接收所述电子病历存储设备返回的第一数字证书，并存储所述第一数字证书，所述第一数字证书由所述电子病历存储设备对所述第一节点身份信息以及所述第一节点公钥进行签名后生成。

[0135] 在具体的应用场景中，该第一加密模块301，包括：

[0136] 生成单元3011，用于基于第二节点的第二节点标识，生成证书查询请求，将证书查询请求传输至电子病历存储设备；

[0137] 接收单元3012，用于接收电子病历存储设备在接收到证书查询请求后返回的第二数字证书。

[0138] 在具体的应用场景中，该装置还包括：

[0139] 生成模块307，用于如果采用所述第二节点公钥对所述信息密文进行解密失败，则生成第一失败响应，将所述第一失败响应返回至所述电子病历存储设备。

[0140] 在具体的应用场景中，该存储模块304，包括：

[0141] 该获取单元3041，用于如果采用所述第二节点公钥对所述信息密文进行解密成功，则获取对所述信息密文解密后的所述第二初始密文；

[0142] 该解密单元3042，用于采用所述第一节点私钥对所述第二初始密文进行解密，得到所述交互信息，并存储所述交互信息。

[0143] 进一步地，作为图1B所述方法的具体实现，本申请实施例提供了一种信息交互装置，如图4A所示，所述装置包括：

[0144] 确定模块401，用于当接收到第一节点传输的交互密文时，电子病历存储设备确定所述第一节点请求进行信息交互的第二节点，所述第一节点和所述第二节点为进行信息交互的节点，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的；

[0145] 第一传输模块402，用于将所述交互密文传输至所述第二节点；

[0146] 返回模块403，用于如果接收到所述第二节点在接收到所述交互密文后返回的信息密文，则将所述信息密文返回给所述第一节点，所述信息密文由所述第二节点基于所述待交互信息标识指示的交互信息生成。

[0147] 在具体的应用场景中，该装置还包括：

[0148] 绑定模块404，用于当接收到所述第一节点传输的第一节点身份信息以及第一节点公钥时，将所述第一节点身份信息以及所述第一节点公钥进行绑定；

[0149] 签名模块405，用于采用所述第一节点公钥对绑定后的所述第一节点身份信息以及所述第一节点公钥进行签名，生成并注册第一数字证书；

[0150] 存储模块406，用于将所述第一数字证书传输至所述第一节点，并将所述第一节点身份信息以及所述第一数字证书对应存储。

[0151] 在具体的应用场景中，该装置还包括：

[0152] 提取模块407，用于当接收到所述第一节点传输的证书查询请求时，在所述证书查询请求中提取第二节点标识；

[0153] 第二传输模块408，用于获取所述第二节点标识指示的第二数字证书，将所述第二数字证书传输至所述第一节点。

[0154] 在具体的应用场景中，该返回模块403，还用于如果接收到所述第一节点返回的第一失败响应，则将所述第一失败响应返回至所述第二节点；或，如果接收到所述第二节点返回的第二失败响应，则将所述第二失败响应返回至所述第一节点。

[0155] 进一步地，作为图1C所述方法的具体实现，本申请实施例提供了一种信息交互装置，如图5A所示，所述装置包括：

[0156] 第一解密模块501，用于当接收到电子病历存储设备传输的交互密文时，第二节点获取第一节点的第一数字证书，采用所述第一数字证书中的第一节点公钥

对所述交互密文进行解密，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的，所述第一节点为请求与所述第二节点进行信息交互的节点；

[0157] 提取模块502，用于如果采用所述第一节点公钥对所述交互密文进行解密成功，则在解密后的所述交互密文中提取第一初始密文，所述第一初始密文由所述第一节点对所述信息交互请求加密后生成；

[0158] 第二解密模块503，用于获取第二节点私钥，采用所述第二节点私钥对所述第一初始密文进行解密，得到所述待交互信息标识；

[0159] 传输模块504，用于提取所述待交互信息标识指示的交互信息，基于所述交互信息生成信息密文，将所述信息密文传输至所述电子病历存储设备。

[0160] 在具体的应用场景中，该传输模块504，包括：

[0161] 查询单元5041，用于根据所述待交互信息标识进行信息查询，获取所述待交互信息标识指示的交互信息；

[0162] 第一加密单元5042，用于采用所述第一节点公钥对所述交互信息进行加密，生成第二初始密文；

[0163] 第二加密单元5043，用于采用所述第二节点私钥对所述第二初始密文进行加密，生成所述信息密文。

[0164] 在具体的应用场景中，该装置还包括：

[0165] 生成模块505，用于如果采用所述第一节点公钥对所述交互密文进行解密失败，则生成第二失败响应，将所述第二失败响应传输至所述电子病历存储设备。

[0166] 需要说明的是，本申请实施例提供的一种信息交互装置所涉及各功能单元的其他相应描述，可以参考图1A至图1C和图2A至图2B中的对应描述，在此不再赘述。

[0167] 在示例性实施例中，参见图6，还提供了一种设备，该设备600包括通信总线、处理器、存储器和通信接口，还可以包括、输入输出接口和显示设备，其中，各个功能单元之间可以通过总线完成相互间的通信。该存储器存储有计算机可读指令，处理器，用于执行存储器上所存放的程序，执行上述实施例中任一实施例中第一节点、电子病历存储设备或第二节点分别对应的信息交互方法。

[0168] 一种计算机非易失性可读存储介质，其上存储有计算机可读指令，所述计算机可读指令被处理器执行时实现所述任一实施例中第一节点、电子病历存储设备或第二节点分别对应的信息交互方法的步骤。

[0169] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本申请可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是CD-ROM，U盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施场景所述的方法。

[0170] 本领域技术人员可以理解附图只是一个优选实施场景的示意图，附图中的模块或流程并不一定是实施本申请所必须的。上述实施场景的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

权利要求书

[权利要求 1] 一种信息交互方法，其特征在于，包括：

当检测到用户请求与第二节点进行信息交互时，第一节点获取所述第二节点的第二数字证书，采用所述第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文；

获取第一节点私钥，采用所述第一节点私钥对所述第一初始密文进行加密，生成交互密文，将所述交互密文传输至电子病历存储设备；

接收所述电子病历存储设备返回的信息密文，采用所述第二节点公钥对所述信息密文进行解密，所述信息密文由所述第二节点接收到所述电子病历存储设备传输的所述交互密文后生成并传输至所述电子病历存储设备；

如果采用所述第二节点公钥对所述信息密文进行解密成功，则在对所述信息密文进行解密得到的第二初始密文中提取交互信息，存储所述交互信息，所述第二初始密文由所述第二节点基于所述交互信息加密得到。

[权利要求 2] 根据权利要求1所述的方法，其特征在于，所述当检测到用户请求与第二节点进行信息交互时，第一节点获取所述第二节点的第二数字证书，采用所述第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文之前，所述方法还包括：

当检测到用户请求注册时，将第一节点身份信息以及第一节点公钥传输至所述电子病历存储设备，所述第一节点身份信息至少包括医院名称信息、医院属性信息；

接收所述电子病历存储设备返回的第一数字证书，并存储所述第一数字证书，所述第一数字证书由所述电子病历存储设备对所述第一节点身份信息以及所述第一节点公钥进行签名后生成。

[权利要求 3] 根据权利要求1所述的方法，其特征在于，所述第一节点获取所述第二节点的第二数字证书，包括：

基于所述第二节点的第二节点标识，生成证书查询请求，将所述证书

查询请求传输至所述电子病历存储设备；

接收所述电子病历存储设备在接收到所述证书查询请求后返回的所述第二数字证书。

[权利要求 4] 根据权利要求1所述的方法，其特征在于，所述接收所述电子病历存储设备返回的信息密文，采用所述第二节点公钥对所述信息密文进行解密之后，所述方法还包括：

如果采用所述第二节点公钥对所述信息密文进行解密失败，则生成第一失败响应，将所述第一失败响应返回至所述电子病历存储设备。

[权利要求 5] 根据权利要求1所述的方法，其特征在于，所述如果采用所述第二节点公钥对所述信息密文进行解密成功，则在对所述信息密文进行解密得到的第二初始密文中提取交互信息，存储所述交互信息，包括：

如果采用所述第二节点公钥对所述信息密文进行解密成功，则获取对所述信息密文解密后的所述第二初始密文；

采用所述第一节点私钥对所述第二初始密文进行解密，得到所述交互信息，并存储所述交互信息。

[权利要求 6] 一种信息交互方法，其特征在于，包括：

当接收到第一节点传输的交互密文时，电子病历存储设备确定所述第一节点请求进行信息交互的第二节点，所述第一节点和所述第二节点为进行信息交互的节点，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的；

将所述交互密文传输至所述第二节点；

如果接收到所述第二节点在接收到所述交互密文后返回的信息密文，则将所述信息密文返回给所述第一节点，所述信息密文由所述第二节点基于所述待交互信息标识指示的交互信息生成。

[权利要求 7] 根据权利要求6所述的方法，其特征在于，所述方法还包括：

当接收到所述第一节点传输的第一节点身份信息以及第一节点公钥时，将所述第一节点身份信息以及所述第一节点公钥进行绑定；

采用所述第一节点公钥对绑定后的所述第一节点身份信息以及所述第

一节点公钥进行签名，生成并注册第一数字证书；

将所述第一数字证书传输至所述第一节点，并将所述第一节点身份信息以及所述第一数字证书对应存储。

[权利要求 8] 根据权利要求6所述的方法，其特征在于，所述当接收到第一节点传输的交互密文时，电子病历存储设备确定所述第一节点指示的第二节点之前，所述方法还包括：

当接收到所述第一节点传输的证书查询请求时，在所述证书查询请求中提取第二节点标识；

获取所述第二节点标识指示的第二数字证书，将所述第二数字证书传输至所述第一节点。

[权利要求 9] 根据权利要求6所述的方法，其特征在于，所述方法还包括：

如果接收到所述第一节点返回的第一失败响应，则将所述第一失败响应返回至所述第二节点；或，

如果接收到所述第二节点返回的第二失败响应，则将所述第二失败响应返回至所述第一节点。

[权利要求 10] 一种信息交互方法，其特征在于，包括：

当接收到电子病历存储设备传输的交互密文时，第二节点获取第一节点的第一数字证书，采用所述第一数字证书中的第一节点公钥对所述交互密文进行解密，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的，所述第一节点为请求与所述第二节点进行信息交互的节点；

如果采用所述第一节点公钥对所述交互密文进行解密成功，则在解密后的所述交互密文中提取第一初始密文，所述第一初始密文由所述第一节点对所述信息交互请求加密后生成；

获取第二节点私钥，采用所述第二节点私钥对所述第一初始密文进行解密，得到所述待交互信息标识；

提取所述待交互信息标识指示的交互信息，基于所述交互信息生成信息密文，将所述信息密文传输至所述电子病历存储设备。

[权利要求 11] 一种信息交互装置，其特征在于，包括：

第一加密模块，用于当检测到用户请求与第二节点进行信息交互时，第一节点获取所述第二节点的第二数字证书，采用所述第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文；

第二加密模块，用于获取第一节点私钥，采用所述第一节点私钥对所述第一初始密文进行加密，生成交互密文，将所述交互密文传输至电子病历存储设备；

解密模块，用于接收所述电子病历存储设备返回的信息密文，采用所述第二节点公钥对所述信息密文进行解密，所述信息密文由所述第二节点接收到所述电子病历存储设备传输的所述交互密文后生成并传输至所述电子病历存储设备；

存储模块，用于如果采用所述第二节点公钥对所述信息密文进行解密成功，则在对所述信息密文进行解密得到的第二初始密文中提取交互信息，存储所述交互信息，所述第二初始密文由所述第二节点基于所述交互信息加密得到。

[权利要求 12] 一种信息交互装置，其特征在于，包括：

确定模块，用于当接收到第一节点传输的交互密文时，电子病历存储设备确定所述第一节点请求进行信息交互的第二节点，所述第一节点和所述第二节点为进行信息交互的节点，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的；

第一传输模块，用于将所述交互密文传输至所述第二节点；

返回模块，用于如果接收到所述第二节点在接收到所述交互密文后返回的信息密文，则将所述信息密文返回给所述第一节点，所述信息密文由所述第二节点基于所述待交互信息标识指示的交互信息生成。

[权利要求 13] 一种信息交互装置，其特征在于，包括：

第一解密模块，用于当接收到电子病历存储设备传输的交互密文时，第二节点获取第一节点的第一数字证书，采用所述第一数字证书中的第一节点公钥对所述交互密文进行解密，所述交互密文由所述第一节

点基于携带待交互信息标识的信息交互请求生成的，所述第一节点为请求与所述第二节点进行信息交互的节点；

提取模块，用于如果采用所述第一节点公钥对所述交互密文进行解密成功，则在解密后的所述交互密文中提取第一初始密文，所述第一初始密文由所述第一节点对所述信息交互请求加密后生成；

第二解密模块，用于获取第二节点私钥，采用所述第二节点私钥对所述第一初始密文进行解密，得到所述待交互信息标识；

传输模块，用于提取所述待交互信息标识指示的交互信息，基于所述交互信息生成信息密文，将所述信息密文传输至所述电子病历存储设备。

[权利要求 14] 一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

当检测到用户请求与第二节点进行信息交互时，第一节点获取所述第二节点的第二数字证书，采用所述第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文；

获取第一节点私钥，采用所述第一节点私钥对所述第一初始密文进行加密，生成交互密文，将所述交互密文传输至电子病历存储设备；

接收所述电子病历存储设备返回的信息密文，采用所述第二节点公钥对所述信息密文进行解密，所述信息密文由所述第二节点接收到所述电子病历存储设备传输的所述交互密文后生成并传输至所述电子病历存储设备；

如果采用所述第二节点公钥对所述信息密文进行解密成功，则在对所述信息密文进行解密得到的第二初始密文中提取交互信息，存储所述交互信息，所述第二初始密文由所述第二节点基于所述交互信息加密得到。

[权利要求 15] 根据权利要求14所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

当检测到用户请求注册时，将第一节点身份信息以及第一节点公钥传输至所述电子病历存储设备，所述第一节点身份信息至少包括医院名称信息、医院属性信息；

接收所述电子病历存储设备返回的第一数字证书，并存储所述第一数字证书，所述第一数字证书由所述电子病历存储设备对所述第一节点身份信息以及所述第一节点公钥进行签名后生成。

[权利要求 16] 一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

当接收到第一节点传输的交互密文时，电子病历存储设备确定所述第一节点请求进行信息交互的第二节点，所述第一节点和所述第二节点为进行信息交互的节点，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的；

将所述交互密文传输至所述第二节点；

如果接收到所述第二节点在接收到所述交互密文后返回的信息密文，则将所述信息密文返回给所述第一节点，所述信息密文由所述第二节点基于所述待交互信息标识指示的交互信息生成。

[权利要求 17] 一种计算机设备，包括存储器、处理器以及存储在所述存储器中并可在所述处理器上运行的计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

当接收到电子病历存储设备传输的交互密文时，第二节点获取第一节点的第一数字证书，采用所述第一数字证书中的第一节点公钥对所述交互密文进行解密，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的，所述第一节点为请求与所述第二节点进行信息交互的节点；

如果采用所述第一节点公钥对所述交互密文进行解密成功，则在解密后的所述交互密文中提取第一初始密文，所述第一初始密文由所述第一节点对所述信息交互请求加密后生成；

获取第二节点私钥，采用所述第二节点私钥对所述第一初始密文进行解密，得到所述待交互信息标识；

提取所述待交互信息标识指示的交互信息，基于所述交互信息生成信息密文，将所述信息密文传输至所述电子病历存储设备。

[权利要求 18] 一种计算机非易失性可读存储介质，所述计算机非易失性可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现如下步骤：

当检测到用户请求与第二节点进行信息交互时，第一节点获取所述第二节点的第二数字证书，采用所述第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文；

获取第一节点私钥，采用所述第一节点私钥对所述第一初始密文进行加密，生成交互密文，将所述交互密文传输至电子病历存储设备；

接收所述电子病历存储设备返回的信息密文，采用所述第二节点公钥对所述信息密文进行解密，所述信息密文由所述第二节点接收到所述电子病历存储设备传输的所述交互密文后生成并传输至所述电子病历存储设备；

如果采用所述第二节点公钥对所述信息密文进行解密成功，则在对所述信息密文进行解密得到的第二初始密文中提取交互信息，存储所述交互信息，所述第二初始密文由所述第二节点基于所述交互信息加密得到。

[权利要求 19] 一种计算机非易失性可读存储介质，所述计算机非易失性可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现如下步骤：

当接收到第一节点传输的交互密文时，电子病历存储设备确定所述第一节点请求进行信息交互的第二节点，所述第一节点和所述第二节点为进行信息交互的节点，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的；

将所述交互密文传输至所述第二节点；

如果接收到所述第二节点在接收到所述交互密文后返回的信息密文，则将所述信息密文返回给所述第一节点，所述信息密文由所述第二节点基于所述待交互信息标识指示的交互信息生成。

[权利要求 20] 一种计算机非易失性可读存储介质，所述计算机非易失性可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被处理器执行时实现如下步骤：

当接收到电子病历存储设备传输的交互密文时，第二节点获取第一节点的第一数字证书，采用所述第一数字证书中的第一节点公钥对所述交互密文进行解密，所述交互密文由所述第一节点基于携带待交互信息标识的信息交互请求生成的，所述第一节点为请求与所述第二节点进行信息交互的节点；

如果采用所述第一节点公钥对所述交互密文进行解密成功，则在解密后的所述交互密文中提取第一初始密文，所述第一初始密文由所述第一节点对所述信息交互请求加密后生成；

获取第二节点私钥，采用所述第二节点私钥对所述第一初始密文进行解密，得到所述待交互信息标识；

提取所述待交互信息标识指示的交互信息，基于所述交互信息生成信息密文，将所述信息密文传输至所述电子病历存储设备。

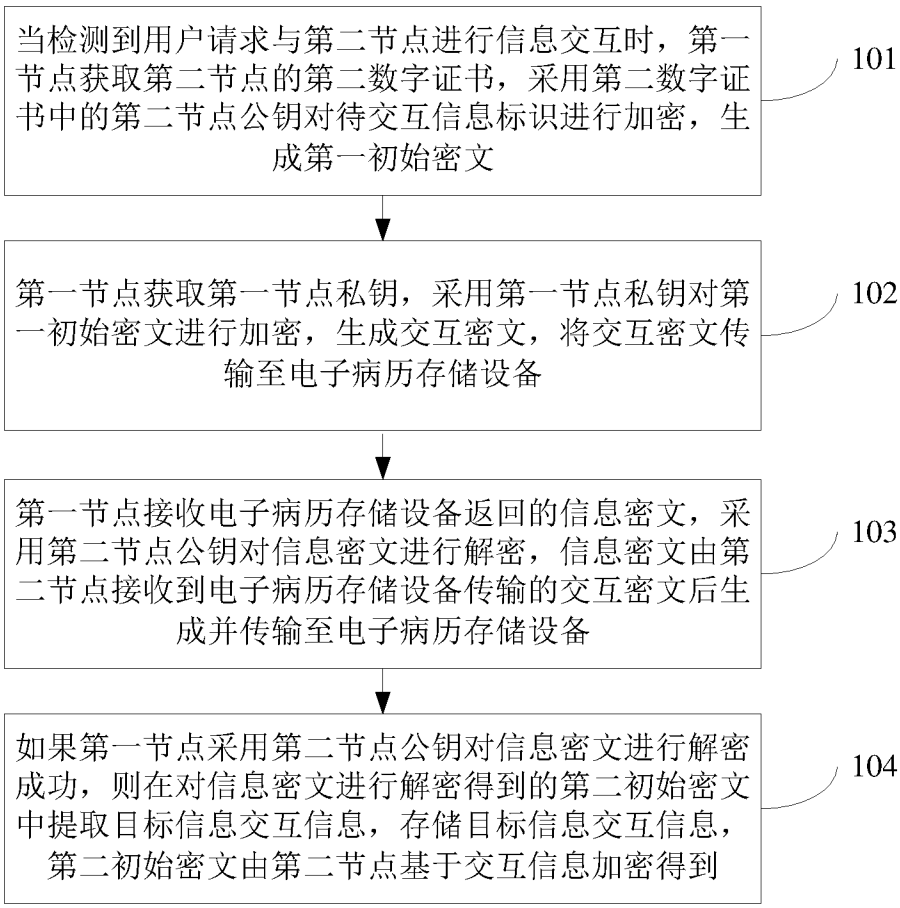
当检测到用户请求与第二节点进行信息交互时，第一节点获取第二节点的第二数字证书，采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文
101
第一节点获取第一节点私钥，采用第一节点私钥对第一初始密文进行加密，生成交互密文，将交互密文传输至电子病历存储设备
102
第一节点接收电子病历存储设备返回的信息密文，采用第二节点公钥对信息密文进行解密，信息密文由第二节点接收到电子病历存储设备传输的交互密文后生成并传输至电子病历存储设备
103
如果第一节点采用第二节点公钥对信息密文进行解密成功，则在对信息密文进行解密得到的第二初始密文中提取目标信息交互信息，存储目标信息交互信息，第二初始密文由第二节点基于交互信息加密得到
104

图 1A

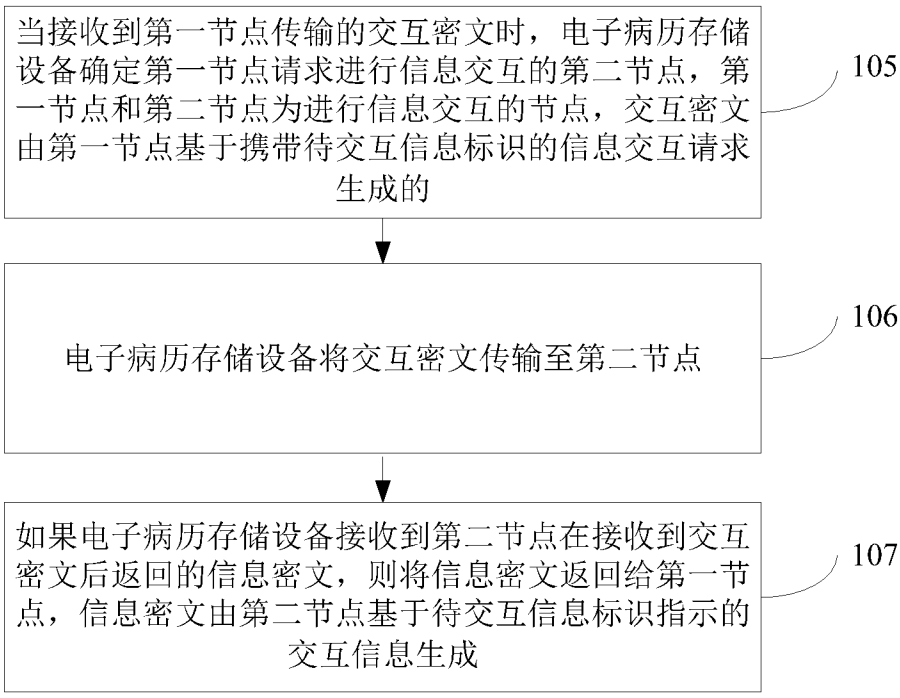
当接收到第一节点传输的交互密文时，电子病历存储设备确定第一节点请求进行信息交互的第二节点，第一节点和第二节点为进行信息交互的节点，交互密文由第一节点基于携带待交互信息标识的信息交互请求生成的
105
电子病历存储设备将交互密文传输至第二节点
106
如果电子病历存储设备接收到第二节点在接收到交互密文后返回的信息密文，则将信息密文返回给第一节点，信息密文由第二节点基于待交互信息标识指示的交互信息生成
107

图 1B

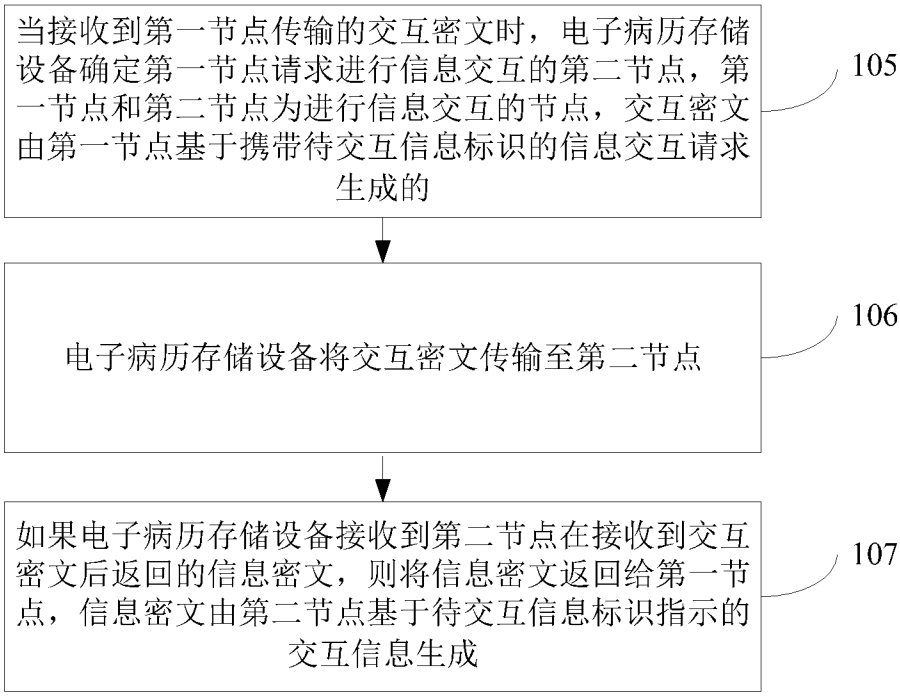
当接收到第一节点传输的交互密文时，电子病历存储设备确定第一节点请求进行信息交互的第二节点，第一节点和第二节点为进行信息交互的节点，交互密文由第一节点基于携带待交互信息标识的信息交互请求生成的
105
电子病历存储设备将交互密文传输至第二节点
106
如果电子病历存储设备接收到第二节点在接收到交互密文后返回的信息密文，则将信息密文返回给第一节点，信息密文由第二节点基于待交互信息标识指示的交互信息生成
107

图 1C

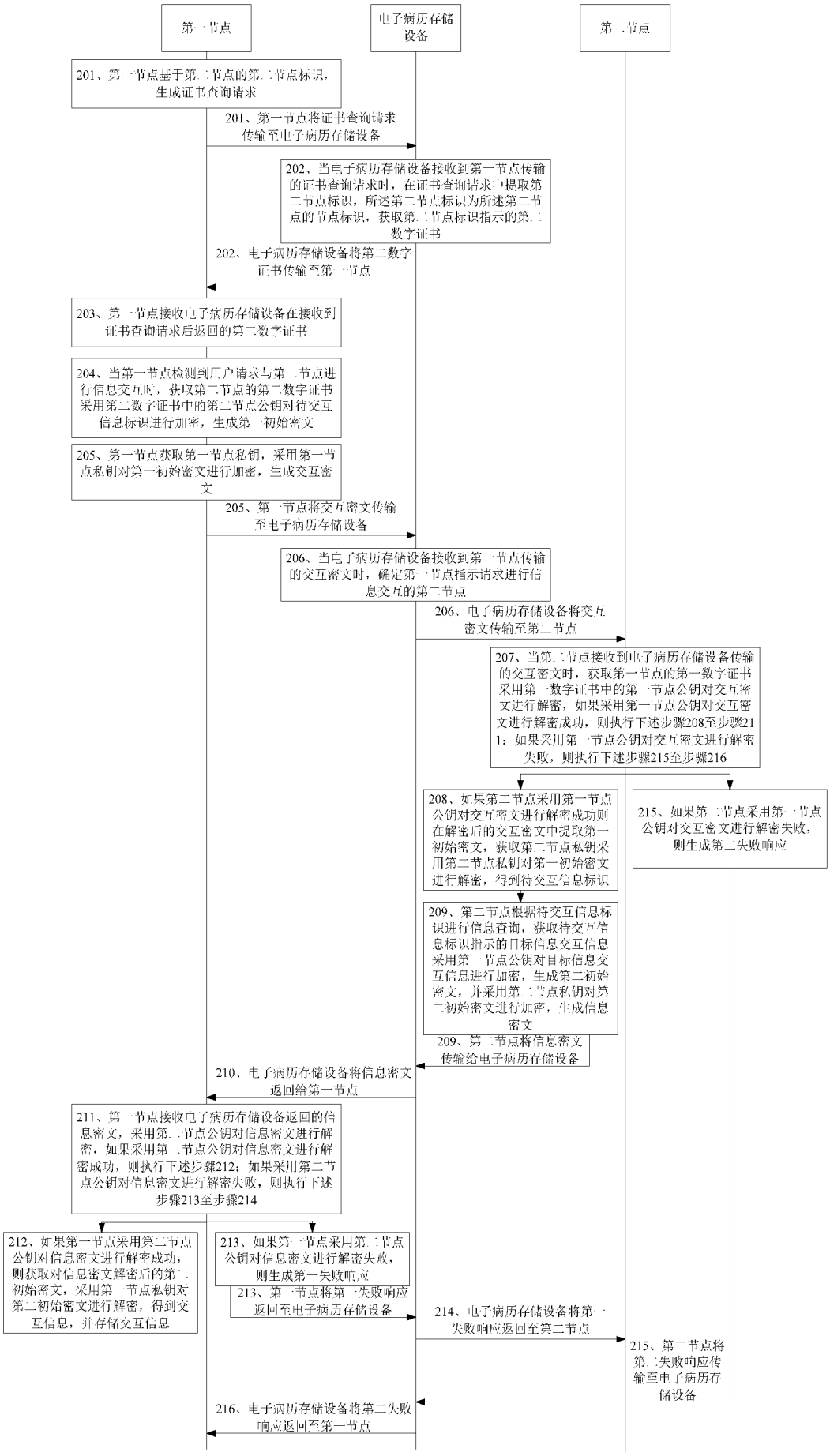
第一节点
电子病历存储设备
第二节点
201、第一节点基于第二节点的第二节点标识，生成证书查询请求
201、第一节点将证书查询请求传输至电子病历存储设备
202、当电子病历存储设备接收到第一节点传输的证书查询请求时，在证书查询请求中提取第二节点标识，所述第二节点标识为所述第二节点的节点标识，获取第二节点标识指示的第二数字证书
202、电子病历存储设备将第二数字证书传输至第一节点
203、第一节点接收电子病历存储设备在接收到证书查询请求后返回的第二数字证书
204、当第一节点检测到用户请求与第二节点进行信息交互时，获取第二节点的第二数字证书采用第二数字证书中的第二节点公钥对待交互信息标识进行加密，生成第一初始密文
205、第一节点获取第一节点私钥，采用第一节点私钥对第一初始密文进行加密，生成交互密文
205、第一节点将交互密文传输至电子病历存储设备
206、当电子病历存储设备接收到第一节点传输的交互密文时，确定第一节点指示请求进行信息交互的第二节点
206、电子病历存储设备将交互密文传输至第二节点
207、当第二节点接收到电子病历存储设备传输的交互密文时，获取第一节点的第一数字证书采用第一数字证书中的第一节点公钥对交互密文进行解密，如果采用第一节点公钥对交互密文进行解密成功，则执行下述步骤208至步骤211；如果采用第一节点公钥对交互密文进行解密失败，则执行下述步骤215至步骤216
208、如果第二节点采用第一节点公钥对交互密文进行解密成功则在解密后的交互密文中提取第一初始密文，获取第二节点私钥采用第二节点私钥对第一初始密文进行解密，得到待交互信息标识
209、第二节点根据待交互信息标识进行信息查询，获取待交互信息标识指示的目标信息交互信息采用第一节点公钥对目标信息交互信息进行加密，生成第二初始密文，并采用第二节点私钥对第二初始密文进行加密，生成信息密文
209、第二节点将信息密文传输给电子病历存储设备
210、电子病历存储设备将信息密文返回给第一节点
211、第一节点接收电子病历存储设备返回的信息密文，采用第二节点公钥对信息密文进行解密，如果采用第二节点公钥对信息密文进行解密成功，则执行下述步骤212；如果采用第二节点公钥对信息密文进行解密失败，则执行下述步骤213至步骤214
212、如果第一节点采用第二节点公钥对信息密文进行解密成功，则获取对信息密文解密后的第二初始密文，采用第一节点私钥对第二初始密文进行解密，得到交互信息，并存储交互信息
213、如果第一节点采用第二节点公钥对信息密文进行解密失败，则生成第一失败响应
213、第一节点将第一失败响应返回至电子病历存储设备
214、电子病历存储设备将第一失败响应返回至第二节点
215、如果第二节点采用第一节点公钥对交互密文进行解密失败，则生成第二失败响应
215、第二节点将第二失败响应传输至电子病历存储设备
216、电子病历存储设备将第二失败响应返回至第一节点

图 2A

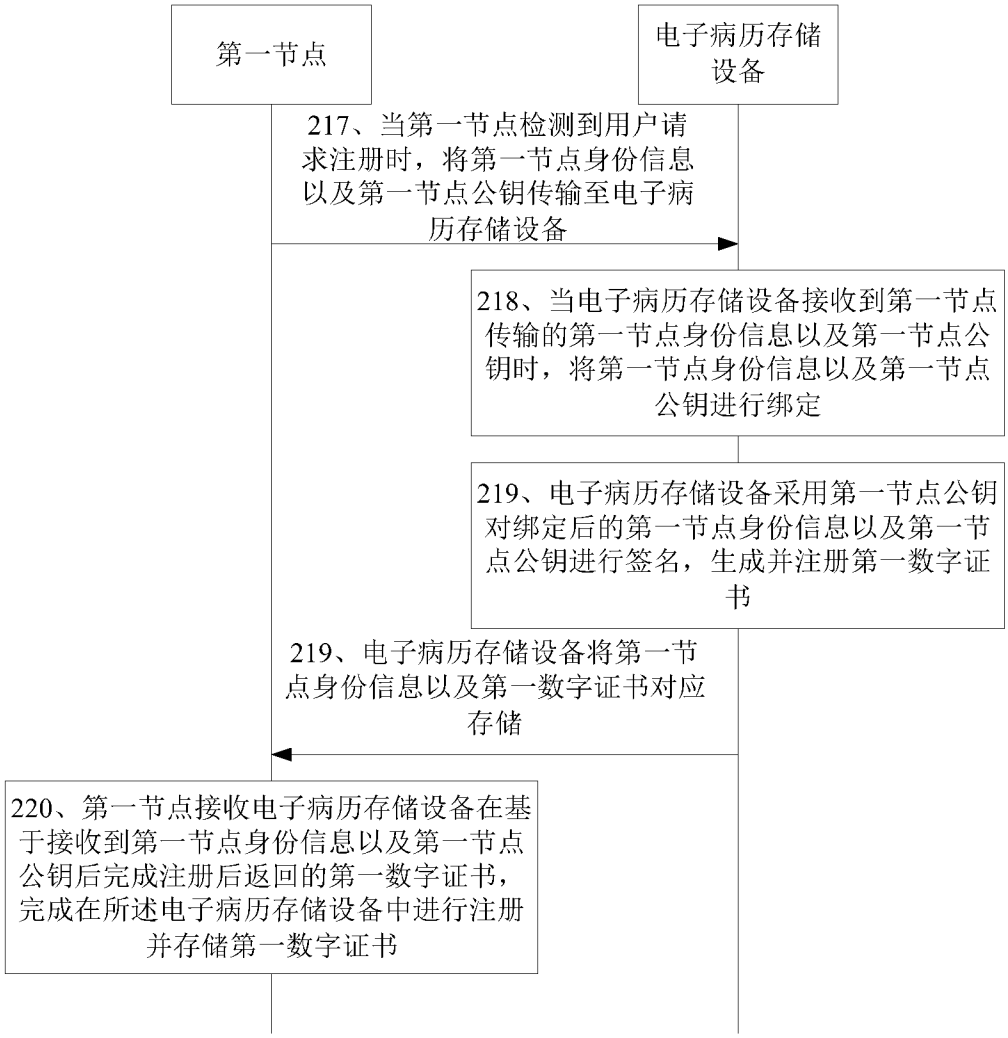
第一节点
电子病历存储设备
217、当第一节点检测到用户请求注册时，将第一节点身份信息以及第一节点公钥传输至电子病历存储设备
218、当电子病历存储设备接收到第一节点传输的第一节点身份信息以及第一节点公钥时，将第一节点身份信息以及第一节点公钥进行绑定
219、电子病历存储设备采用第一节点公钥对绑定后的第一节点身份信息以及第一节点公钥进行签名，生成并注册第一数字证书
219、电子病历存储设备将第一节点身份信息以及第一数字证书对应存储
220、第一节点接收电子病历存储设备在基于接收到第一节点身份信息以及第一节点公钥后完成注册后返回的第一数字证书，完成在所述电子病历存储设备中进行注册并存储第一数字证书

图 2B

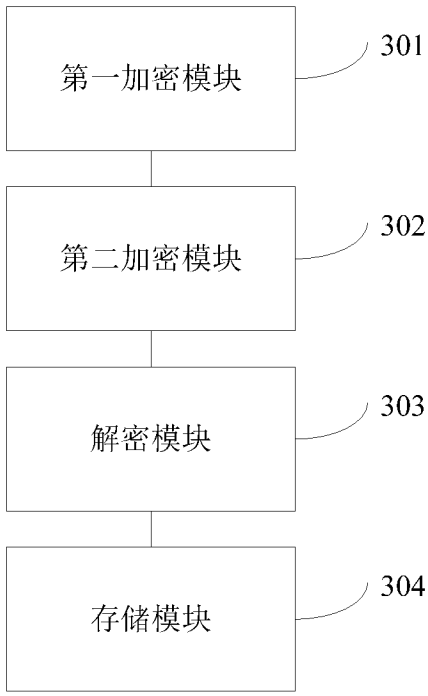
第一加密模块
301
第二加密模块
302
解密模块
303
存储模块
304

图 3A

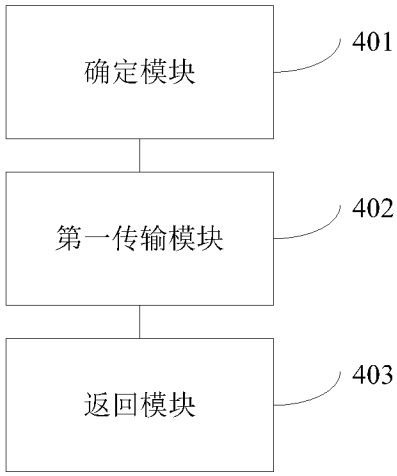
确定模块
401
第一传输模块
402
返回模块
403

图 4A

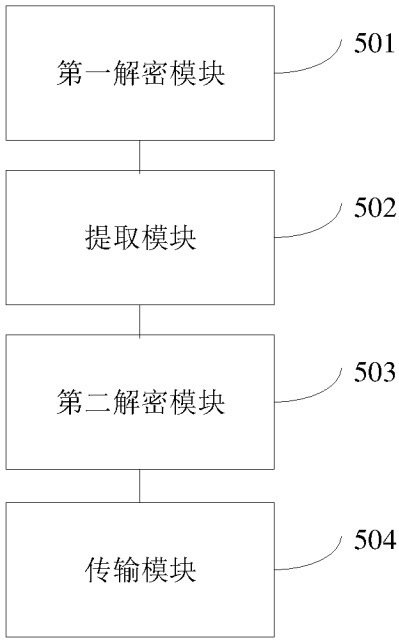
第一解密模块
501
提取模块
502
第二解密模块
503
传输模块
504

图 5A

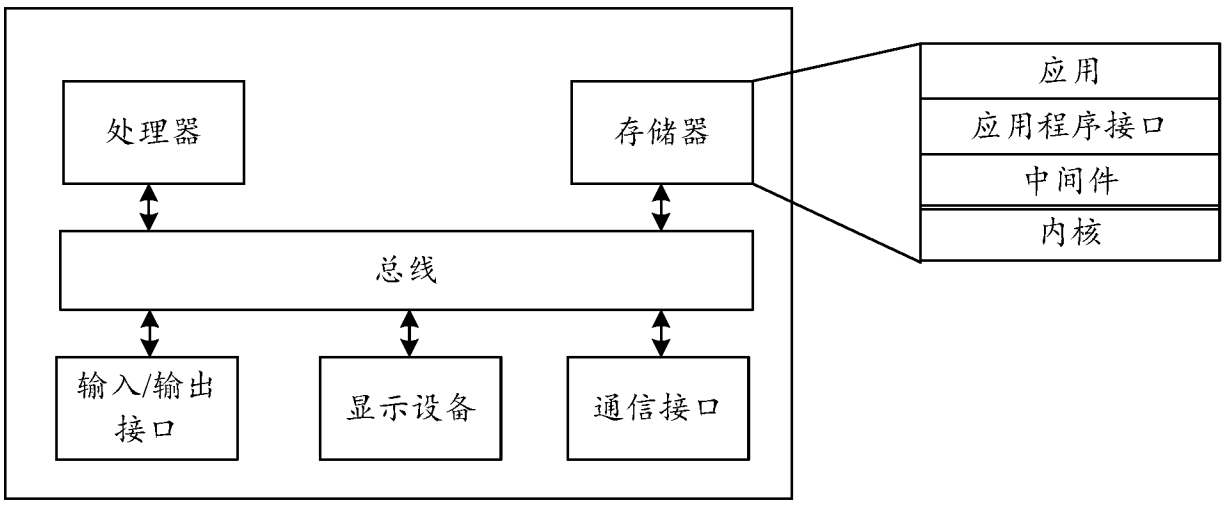
处理器
存储器
应用
应用程序接口
中间件
内核
总线
输入/输出接口
显示设备
通信接口

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/123141

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; H04L 9/32(2006.01)n

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

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

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

CNPAT, WPI, EPODOC, CNKI: 电子, 病历, 诊断, 医院, 医疗, 医生, 病人, 病患, 访问, 交互, 请求, 证书, 公钥, 私钥, 密钥, 加密, 解密, 密文, 签名, 注册, 身份, electronic, prescription, medical, hospital, doctor, patient, visit, interactive, obtain, request, CA, certification, public, private, key, encrypt, decrypt, signature, register, identity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110224989 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 10 September 2019 (2019-09-10) description, paragraphs [0111]-[0231]	1-20
PX	CN 110049016 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 23 July 2019 (2019-07-23) description, paragraphs [0086]-[0169]	1-20
X	CN 106295393 A (ALIBABA GROUP HOLDING LIMITED) 04 January 2017 (2017-01-04) description, paragraphs [0260]-[0322], and figures 6 and 7	6, 9, 12, 16, 19
Y	CN 106295393 A (ALIBABA GROUP HOLDING LIMITED) 04 January 2017 (2017-01-04) description, paragraphs [0260]-[0322], and figures 6 and 7	1-5, 7, 8, 10, 11, 13-15, 17, 18, 20
Y	CN 109544331 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 29 March 2019 (2019-03-29) description, paragraphs [0038]-[0065]	1-5, 7, 8, 10, 11, 13-15, 17, 18, 20
A	WO 2016180264 A1 (ALIBABA GROUP HOLDING LIMITED) 17 November 2016 (2016-11-17) 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
26 February 2020	**06 March 2020**

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

International application No.
PCT/CN2019/123141

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2016277374 A1 (REID CONSULTING GROUP) 22 September 2016 (2016-09-22) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/123141

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110224989 A	10 September 2019	None	
CN 110049016 A	23 July 2019	None	
CN 106295393 A	04 January 2017	WO 2016210347 A1	29 December 2016
		TW 201701226 A	01 January 2017
		US 2016378949 A1	29 December 2016
CN 109544331 A	29 March 2019	None	
WO 2016180264 A1	17 November 2016	CN 106302312 A	04 January 2017
		US 2018159833 A1	07 June 2018
		EP 3297244 A1	21 March 2018
US 2016277374 A1	22 September 2016	WO 2016277374 A1	22 September 2016
		WO 2017210563 A1	07 December 2017

国际检索报告

国际申请号 PCT/CN2019/123141

A. 主题的分类

H04L 29/06(2006.01)i; H04L 9/32(2006.01)n

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,WPI,EPODOC,CNKI:电子，病历，诊断，医院，医疗，医生，病人，病患，访问，交互，请求，证书，公钥，私钥，密钥，加密，解密，密文，签名，注册，身份，electronic, prescription, medical, hospital, doctor, patient, visit, interactive, obtain, request, CA, certification, public, private, key, encrypt, decrypt, signature, register, identity

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 110224989 A (深圳壹账通智能科技有限公司) 2019年 9月 10日 (2019-09-10) 说明书第[0111]-[0231]段	1-20
PX	CN 110049016 A (深圳壹账通智能科技有限公司) 2019年 7月 23日 (2019-07-23) 说明书第[0086]-[0169]段	1-20
X	CN 106295393 A (阿里巴巴集团控股有限公司) 2017年 1月 4日 (2017-01-04) 说明书第[0260]-[0322]段、图6-7	6，9，12，16，19
Y	CN 106295393 A (阿里巴巴集团控股有限公司) 2017年 1月 4日 (2017-01-04) 说明书第[0260]-[0322]段、图6-7	1-5，7-8，10-11，13-15，17-18，20
Y	CN 109544331 A (深圳壹账通智能科技有限公司) 2019年 3月 29日 (2019-03-29) 说明书第[0038]-[0065]段	1-5，7-8，10-11，13-15，17-18，20
A	WO 2016180264 A1 (阿里巴巴集团控股有限公司) 2016年 11月 17日 (2016-11-17) 全文	1-20
A	US 2016277374 A1 (REID CONSULTING GROUP) 2016年 9月 22日 (2016-09-22) 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
2020年 2月 26日	2020年 3月 6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 罗啸 电话号码 86-(10)-53961774

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/123141

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	110224989	A	2019年 9月 10日	无			
CN	110049016	A	2019年 7月 23日	无			
CN	106295393	A	2017年 1月 4日	WO	2016210347	A1	2016年 12月 29日
				TW	201701226	A	2017年 1月 1日
				US	2016378949	A1	2016年 12月 29日
CN	109544331	A	2019年 3月 29日	无			
WO	2016180264	A1	2016年 11月 17日	CN	106302312	A	2017年 1月 4日
				US	2018159833	A1	2018年 6月 7日
				EP	3297244	A1	2018年 3月 21日
US	2016277374	A1	2016年 9月 22日	WO	2016277374	A1	2016年 9月 22日
				WO	2017210563	A1	2017年 12月 7日