(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
2017 年 3 月 9 日 (09.03.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/035899 A1

(51) 国际专利分类号:
H04L 9/14 (2006.01)

(21) 国际申请号: PCT/CN2015/091355

(22) 国际申请日: 2015 年 9 月 30 日 (30.09.2015)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510542374.0 2015 年 8 月 28 日 (28.08.2015) CN

(71) 申请人: 宇龙计算机通信科技（深圳）有限公司 (YULONG COMPUTER TELECOMMUNICATION SCIENTIFIC (SHENZHEN) CO., LTD.) [CN/CN]; 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(72) 发明人: 钟焰涛 (ZHONG, Yantao); 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 傅文治 (FU, Wenzhi); 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。

(74) 代理人: 北京友联知识产权代理事务所（普通合伙） (YOULINK INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区学清路 8 号科技财富中心 A 座 506 室尚志峰, Beijing 100192 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

[见续页]

(54) Title: DATA SECURITY PROCESSING METHOD, APPARATUS AND SYSTEM

(54) 发明名称 : 一种数据安全处理方法、装置和系统

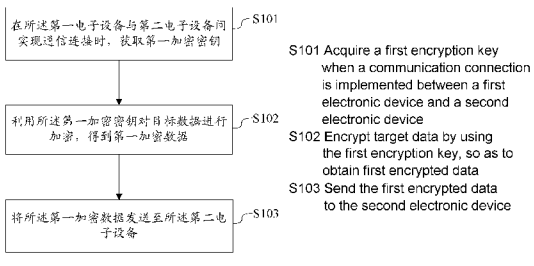

图 1

(57) Abstract: Disclosed are a data security processing method, apparatus and system. The method comprises: acquiring an encryption key when a first electronic device using the method detects a communication connection between the first electronic device and a second electronic device; encrypting target data by using the encryption key; and finally, securely transmitting the encrypted data to the second electronic device for storage. Accordingly, when the present application is used, by encrypting collected physiological data of a user, a wearable medical health device can securely transmit collected data at a high privacy level to an external electronic device (for example, a mobile phone of the user) for storage, thereby implementing security protection on data with user privacy.

(57) 摘要: 本申请公开一种数据安全处理方法、装置和系统，应用所述方法的第一电子设备在检测到其与第二电子设备间实现通信连接时，获取一个加密密钥，并利用该加密密钥对目标数据进行加密，最后，将加密数据安全传输至所述第二电子设备进行存储。可见，应用本申请时，可穿戴医疗健康设备可通过对采集的用户生理数据进行加密，实现将私密性较高的采集数据安全传输至一外部的电子设备(例如用户手机等)，进行存储，实现了对用户私密性数据的安全保护。

WO 2017/035899 A1

(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))。

说 明 书

一种数据安全处理方法、装置和系统

技术领域

本发明属于终端设备的信息安全技术领域，尤其涉及一种数据安全处理方法、装置和系统。

背景技术

可穿戴医疗健康设备实现了将可穿戴技术应用于医疗健康领域。该设备可通过采集用户的心跳、血压、体温、血糖等多种生理数据，实现对用户的身体情况、运动数据、健康状况进行实时监测。

用户的生理数据具有极强的私密性，可穿戴医疗健康设备在采集用户的心跳、血压、体温、血糖等多种生理数据后，如何对采集的这些私密性数据进行安全处理，进而实现对用户私密性数据进行安全保护，成为该领域的一个热点问题。

发明内容

有鉴于此，本发明的目的在于提供一种数据安全处理方法、装置和系统，旨在解决可穿戴医疗健康设备所采集的用户私密性数据的安全保护问题。

为此，本发明公开如下技术方案:

一种数据安全处理方法，应用于第一电子设备，所述方法包括:

在所述第一电子设备与第二电子设备间实现通信连接时，获取第一加密密钥;

利用所述第一加密密钥对目标数据进行加密，得到第一加密数据;

将所述第一加密数据发送至所述第二电子设备。

上述方法，优选的，所述获取第一加密密钥包括：采用预设的密钥协商机制，与所述第二电子设备进行密钥协商，得到第一加密密钥。

上述方法，优选的，所述第一电子设备为可穿戴医疗健康设备，所述目标数据为所述可穿戴医疗健康设备采集的用户生理数据。

一种数据安全处理方法，应用于第二电子设备，所述方法包括:

接收来自第一电子设备的第一加密数据;

采用第一解密密钥对所述第一加密数据进行解密，得到目标数据;

存储所述目标数据。

上述方法，优选的，所述第一解密密钥为所述第二电子设备预先采用预设的密钥协商机制，与所述第一电子设备进行密钥协商后所得的密钥。

上述方法，优选的，当所述第二电子设备具有安全系统时，所述接收来自第一电子设备的加密数据包括：在所述第二电子设备的安全系统中，接收来自第一电子设备的第一加密数据。

上述方法，优选的，所述存储所述目标数据包括:

获取第二加密密钥;

采用所述第二加密密钥对所述目标数据进行加密，得到第二加密数据;

存储所述第二加密数据。

上述方法，优选的，所述获取第二加密密钥包括:

检测目标存储位置是否存储有预先生成的第二加密密钥;

如果检测结果为是，则从所述目标存储位置读取所述第二加密密钥;

如果检测结果为否，则生成第二加密密钥，并将所述第二加密密钥存储至所述目标存储位置。

一种数据安全处理装置，应用于第一电子设备，所述装置包括:

密钥获取模块，用于在所述第一电子设备与第二电子设备间实现通信连接时，获取第一加密密钥;

数据加密模块，用于利用所述第一加密密钥对目标数据进行加密，得到第一加密数据;

数据发送模块，用于将所述第一加密数据发送至所述第二电子设备。

上述装置，优选的，所述密钥获取模块包括:

密钥协商单元，用于采用预设的密钥协商机制，与所述第二电子设备进行密钥协商，得到第一加密密钥。

一种数据安全处理装置，应用于第二电子设备，所述装置包括:

数据接收模块，用于接收来自第一电子设备的第一加密数据;

数据解密模块，用于采用第一解密密钥对所述第一加密数据进行解密，

得到目标数据;

数据存储模块，用于存储所述目标数据。

上述装置，优选的，当所述第二电子设备具有安全系统时，所述数据接收模块包括:

安全接收单元，用于在所述第二电子设备的安全系统中，接收来自第一电子设备的第一加密数据。

上述装置，优选的，所述数据存储模块包括:

获取单元，用于获取第二加密密钥;

加密单元，用于采用所述第二加密密钥对所述目标数据进行加密，得到第二加密数据;

存储单元，用于存储所述第二加密数据。

上述装置，优选的，所述获取单元包括:

检测子单元，用于检测目标存储位置是否存储有预先生成的第二加密密钥;

读取子单元，用于在检测结果为是时，从所述目标存储位置读取所述第二加密密钥;

生成子单元，用于在检测结果为否时，生成第二加密密钥，并将所述第二加密密钥存储至所述目标存储位置。

一种数据安全处理系统，其特征在于，包括如上所述的两种数据安全处理装置。

由以上方案可知，本申请公开一种数据安全处理方法、装置和系统，应用所述方法的第一电子设备在检测到其与第二电子设备间实现通信连接时，获取一个加密密钥，并利用该加密密钥对目标数据进行加密，最后，将加密数据安全传输至所述第二电子设备进行存储。可见，应用本申请时，可穿戴医疗健康设备可通过对采集的用户生理数据进行加密，实现将私密性较高的采集数据安全传输至一外部的电子设备（例如用户手机等），进行存储，实现了对用户私密性数据的安全保护。

附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例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，下面描述中的附图仅仅是本发明的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

图1是本发明实施例一公开的应用于第一电子设备的数据安全处理方法流程图；

图2是本发明实施例一公开的应用于第二电子设备的数据安全处理方法流程图；

图3是本发明实施例二公开的数据安全存储流程图；

图4是本发明实施例三公开的应用于第一电子设备的数据安全处理装置的结构示意图；

图5是本发明实施例三公开的应用于第二电子设备的数据安全处理装置的结构示意图。

具体实施方式

下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

实施例一

本实施例公开一种数据安全处理方法，该方法可应用于第一电子设备，例如，具体可以应用于可穿戴医疗健康设备中，参考图1，所述方法包括以下步骤：

S101：在所述第一电子设备与第二电子设备间实现通信连接时，获取第一加密密钥；

S102：利用所述第一加密密钥对目标数据进行加密，得到第一加密数据；

S103：将所述第一加密数据发送至所述第二电子设备。

用户手机等终端设备，可以为可穿戴医疗健康设备提供大容量的数据存

储支持，基于此，本申请借助用户手机等终端设备，来解决可穿戴医疗健康设备所采集的用户私密性数据的安全保护问题。接下来，以应用于可穿戴医疗健康设备为例，对本申请的数据安全处理方法进行描述。

可穿戴医疗健康设备在采集用户的心跳、血压、体温、血糖等多种生理数据的基础上，实时检测其与用户的智能手机等终端设备间的通信连接情况，当检测到两设备间通过某种通信方式建立通信连接后，例如通过蓝牙等近距离无线通信技术建立连接后，可穿戴医疗健康设备通过预设的密钥协商机制，与建立连接的终端设备进行密钥协商，最终基于两者间的密钥协商过程，动态生成一对用于对用户生理数据进行加/解密的密钥：加密密钥和解密密钥，以实现为后续可穿戴医疗健康设备向终端设备安全传输数据提供支持。

为了保证加/解密速度，本申请采用对称密钥实现加、解密，具体地，本实施例使用DIffie-Hellman密钥协商机制，在可穿戴设备和用户终端设备之间建立一个共享的密钥，该密钥同时作为加密密钥和解密密钥。

密钥协商完成后，可穿戴医疗健康设备利用动态协商的密钥对采集的用户生理数据进行加密，在此基础上，可穿戴医疗健康设备可实现生理数据向用户手机等终端设备的加密传输。由于进行数据的加密传输时，采用的密钥为动态密钥，即每次进行数据传输时，可穿戴医疗健康设备及终端设备均采用预定的密钥协商机制，生成本次传输所需的实时密钥，从而极大程度地确保了数据传输的安全性，实现了传输环节的数据安全保护。

相对应地，本实施例同时公开另一种数据安全处理方法，该方法应用于第二电子设备，例如具体可应用于智能手机等终端设备中，参考图2，所述方法包括以下步骤：

S201：接收来自第一电子设备的第一加密数据；

S202：采用第一解密密钥对所述第一加密数据进行解密，得到目标数据；

S203：存储所述目标数据。

应用本申请方法的所述终端设备，可以为可穿戴医疗健康设备采集的用户生理数据提供大容量的数据存储支持。

当可穿戴医疗健康设备利用协商生成的密钥对用户生理数据进行加密，并启动与用户终端设备间的数据传输后，终端设备接收来自可穿戴医疗健康设备的加密数据，同时，利用相同密钥，即两设备协商的所述密钥，对接收

的加密数据进行解密，得到用户生理数据，并对其进行存储。

由以上方案可知，应用本申请数据安全处理方法的第一电子设备在检测到其与第二电子设备间实现通信连接时，获取一个加密密钥，并利用该加密密钥对目标数据进行加密，最后，将加密数据安全传输至所述第二电子设备进行存储。可见，应用本申请时，可穿戴医疗健康设备可通过对采集的用户生理数据进行加密，实现将私密性较高的采集数据安全传输至一外部的电子设备（例如用户手机等），进行存储，实现了对用户私密性数据的安全保护。

实施例二

本实施例中，参考图3，所述步骤S203可以通过以下步骤实现：

S301：获取第二加密密钥；

S302：采用所述第二加密密钥对所述目标数据进行加密，得到第二加密数据；

S303：存储所述第二加密数据。

为了保证数据存储过程的安全，本实施例中，终端设备在利用协商的密钥对接收的加密数据进行解密后，继续采用本地密钥（即所述第二加密密钥）对解密后所得的用户生理数据进行加密，从而实现加密存储。

所述本地密钥，可以是终端设备在每次完成接收并解密来自可穿戴医疗健康设备的生理数据时，依据一定的密钥生成机制生成的动态密钥，也可以针对每次接收的数据，均采用一相同的静态密钥。

本实施例优先采用静态密钥实现对接收的用户生理数据进行加密存储，具体地，终端设备在完成接收并解密来自可穿戴医疗健康设备的生理数据时，可首先检测目标存储位置是否存储有预先生成的密钥，如果检测结果为否，例如端设备第一次使用该功能时，可依据设定的密钥生成机制生成一密钥，之后在利用该密钥对生理数据进行加密存储的同时，将该密钥作为一静态密钥进行存储，后续，终端设备每次获得用户生理数据后，可读取该静态密钥，对用户生理数据进行加密并存储，确保了数据存储环节用户私密性数据的安全。

本实施例中，加密存储环节同样采用对称密钥，即加密密钥及后续解密时采用的解密密钥为同一密钥，均为所述静态密钥。需要说明的是，终端设

备应将静态密钥与用户加密数据分别存储在不同区域，以提升加密存储的安全程度，确保存储过程中，用户私密性数据不易遭受窃取或破坏等非法攻击。

在用户需打开存储的加密数据进行查看时，终端设备利用存储的所述静态密钥对用户选定的数据进行解密，从而实现为用户呈现可读信息。

实际应用场景中，如果用于为可穿戴医疗健康设备提供数据存储支持的终端设备为双系统设备，即所述终端设备除了包含安全级别相对较低的普通系统外，例如，安卓操作系统等，还包括一安全级别相对较高的安全系统，此时，为进一步加强用户生理数据等私密性数据的安全程度，可选择在终端设备的安全系统中，对来自可穿戴医疗健康设备的采集数据，执行安全接收及加密存储等过程。

实施例三

本实施例三，首先公开一种应用于可穿戴医疗健康设备等电子设备的数据安全处理装置，参考图3，所述装置包括密钥获取模块301、数据加密模块302和数据发送模块303。

密钥获取模块301，用于在所述第一电子设备与第二电子设备间实现通信连接时，获取第一加密密钥。

所述密钥获取模块301包括密钥协商单元，用于采用预设的密钥协商机制，与所述第二电子设备进行密钥协商，得到第一加密密钥。

数据加密模块302，用于利用所述第一加密密钥对目标数据进行加密，得到第一加密数据。

数据发送模块303，用于将所述第一加密数据发送至所述第二电子设备。

相对应地，本实施例还公开一种应用于智能手机等终端设备的数据安全处理装置，参考图4，所述装置包括数据接收模块401、数据解密模块402和数据存储模块403。

数据接收模块401，用于接收来自第一电子设备的第一加密数据。

其中，当所述第二电子设备具有安全系统时，所述数据接收模块410包括安全接收单元，用于在所述第二电子设备的安全系统中，接收来自第一电子设备的第一加密数据。

数据解密模块402，用于采用第一解密密钥对所述第一加密数据进行解

密，得到目标数据。

数据存储模块403，用于存储所述目标数据。

所述数据存储模块403包括获取单元、加密单元和存储单元。获取单元，用于获取第二加密密钥；加密单元，用于采用所述第二加密密钥对所述目标数据进行加密，得到第二加密数据；存储单元，用于存储所述第二加密数据。

所述获取单元包括检测子单元、读取子单元和生成子单元。检测子单元，用于检测目标存储位置是否存储有预先生成的第二加密密钥；读取子单元，用于在检测结果为是时，从所述目标存储位置读取所述第二加密密钥；生成子单元，用于在检测结果为否时，生成第二加密密钥，并将所述第二加密密钥存储至所述目标存储位置。

对于本发明实施例三公开的数据安全处理装置而言，由于其与实施例一至实施例二公开的数据安全处理方法相对应，所以描述的比较简单，相关相似之处请参见实施例一至实施例二中数据安全处理方法部分的说明即可，此处不再详述。

实施例四

本实施例公开一种数据安全处理系统，该系统包括如实施例三所提供的两种数据处理装置：应用于可穿戴医疗健康设备的数据处理装置；及应用于用户手机等终端设备的数据处理装置。

应用本系统可实现对可穿戴医疗健康设备采集的用户私密性数据，进行安全传输及安全存储，解决了用户私密性数据的安全保护问题。

需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。

为了描述的方便，描述以上系统或装置时以功能分为各种模块或单元分别描述。当然，在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品

的形式体现出来，该计算机软件产品可以存储在存储介质中，如ROM/RAM、磁碟、光盘等，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例或者实施例的某些部分所述的方法。

最后，还需要说明的是，在本文中，诸如第一、第二、第三和第四等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

以上所述仅是本发明的优选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本发明原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本发明的保护范围。

权 利 要 求 书

1、一种数据安全处理方法，其特征在于，应用于第一电子设备，所述方法包括:

在所述第一电子设备与第二电子设备间实现通信连接时，获取第一加密密钥;

利用所述第一加密密钥对目标数据进行加密，得到第一加密数据;

将所述第一加密数据发送至所述第二电子设备。

2、根据权利要求1所述的方法，其特征在于，所述获取第一加密密钥包括：采用预设的密钥协商机制，与所述第二电子设备进行密钥协商，得到第一加密密钥。

3、根据权利要求1所述的方法，其特征在于，所述第一电子设备为可穿戴医疗健康设备，所述目标数据为所述可穿戴医疗健康设备采集的用户生理数据。

4、一种数据安全处理方法，其特征在于，应用于第二电子设备，所述方法包括:

接收来自第一电子设备的第一加密数据;

采用第一解密密钥对所述第一加密数据进行解密，得到目标数据;

存储所述目标数据。

5、根据权利要求4所述的方法，其特征在于，所述第一解密密钥为所述第二电子设备预先采用预设的密钥协商机制，与所述第一电子设备进行密钥协商后所得的密钥。

6、根据权利要求4所述的方法，其特征在于，当所述第二电子设备具有安全系统时，所述接收来自第一电子设备的加密数据包括：在所述第二电子设备的安全系统中，接收来自第一电子设备的第一加密数据。

7、根据权利要求4所述的方法，其特征在于，所述存储所述目标数据包括:

获取第二加密密钥;

采用所述第二加密密钥对所述目标数据进行加密，得到第二加密数据;

存储所述第二加密数据。

8、根据权利要求7所述的方法，其特征在于，所述获取第二加密密钥包

括:

检测目标存储位置是否存储有预先生成的第二加密密钥;

如果检测结果为是，则从所述目标存储位置读取所述第二加密密钥;

如果检测结果为否，则生成第二加密密钥，并将所述第二加密密钥存储至所述目标存储位置。

9、一种数据安全处理装置，其特征在于，应用于第一电子设备，所述装置包括:

密钥获取模块，用于在所述第一电子设备与第二电子设备间实现通信连接时，获取第一加密密钥;

数据加密模块，用于利用所述第一加密密钥对目标数据进行加密，得到第一加密数据;

数据发送模块，用于将所述第一加密数据发送至所述第二电子设备。

10、根据权利要求9所述的装置，其特征在于，所述密钥获取模块包括:

密钥协商单元，用于采用预设的密钥协商机制，与所述第二电子设备进行密钥协商，得到第一加密密钥。

11、一种数据安全处理装置，其特征在于，应用于第二电子设备，所述装置包括:

数据接收模块，用于接收来自第一电子设备的第一加密数据;

数据解密模块，用于采用第一解密密钥对所述第一加密数据进行解密，得到目标数据;

数据存储模块，用于存储所述目标数据。

12、根据权利要求11所述的装置，其特征在于，当所述第二电子设备具有安全系统时，所述数据接收模块包括:

安全接收单元，用于在所述第二电子设备的安全系统中，接收来自第一电子设备的第一加密数据。

13、根据权利要求11所述的装置，其特征在于，所述数据存储模块包括:

获取单元，用于获取第二加密密钥;

加密单元，用于采用所述第二加密密钥对所述目标数据进行加密，得到第二加密数据;

存储单元，用于存储所述第二加密数据。

14、根据权利要求13所述的装置，其特征在于，所述获取单元包括:

检测子单元，用于检测目标存储位置是否存储有预先生成的第二加密密钥;

读取子单元，用于在检测结果为是时，从所述目标存储位置读取所述第二加密密钥;

生成子单元，用于在检测结果为否时，生成第二加密密钥，并将所述第二加密密钥存储至所述目标存储位置。

15、一种数据安全处理系统，其特征在于，包括如权利要求9-10任意一项所述的装置，以及如权利要求11-14任意一项所述的装置。

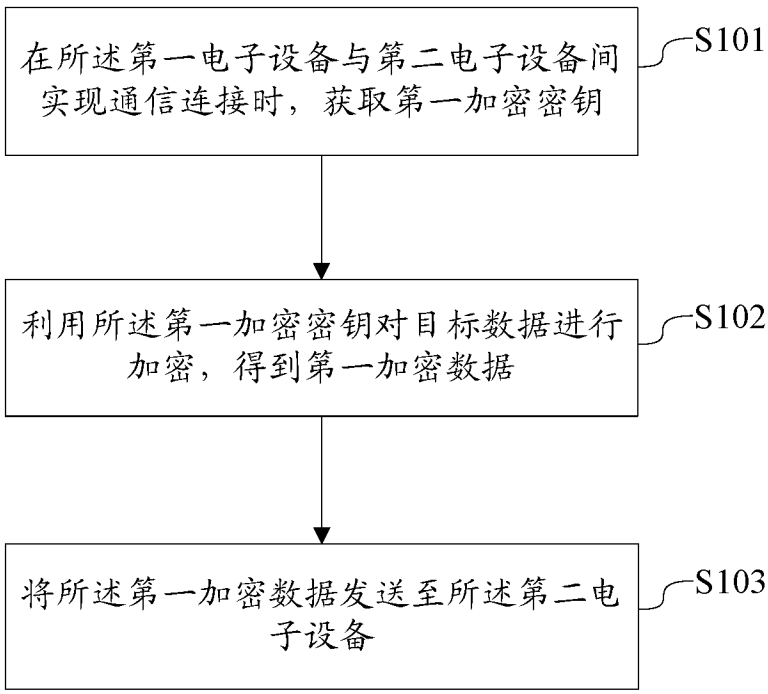
在所述第一电子设备与第二电子设备间实现通信连接时，获取第一加密密钥
S101
利用所述第一加密密钥对目标数据进行加密，得到第一加密数据
S102
将所述第一加密数据发送至所述第二电子设备
S103

图 1

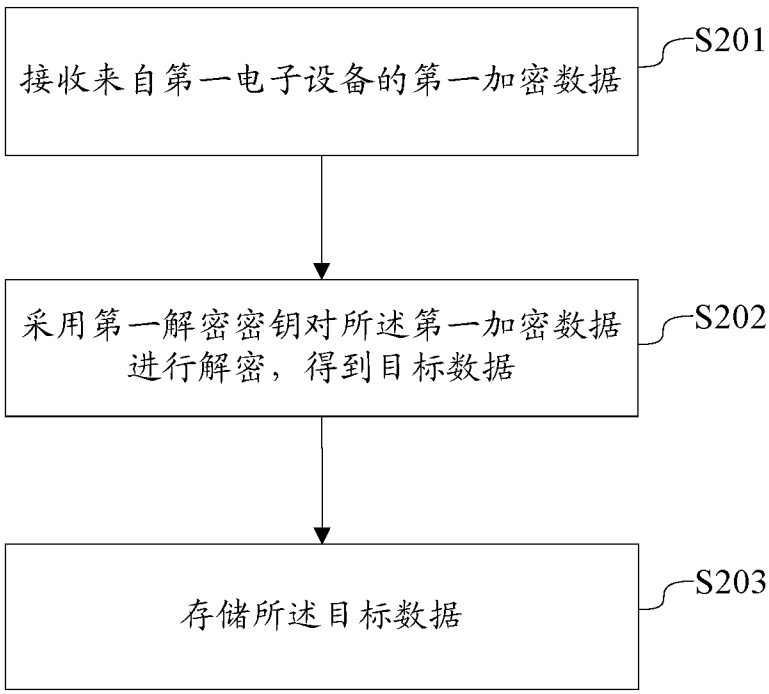
接收来自第一电子设备的第一加密数据
S201
采用第一解密密钥对所述第一加密数据进行解密，得到目标数据
S202
存储所述目标数据
S203

图 2

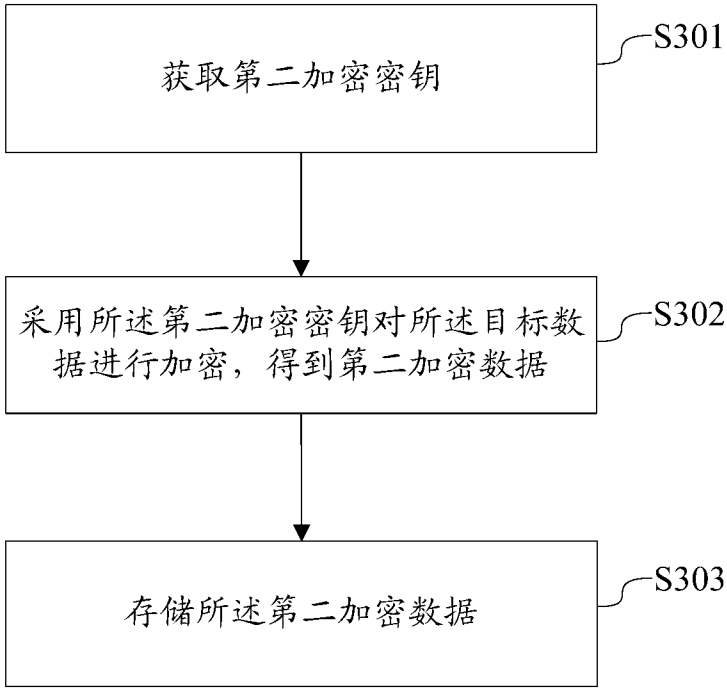
获取第二加密密钥
S301
采用所述第二加密密钥对所述目标数据进行加密，得到第二加密数据
S302
存储所述第二加密数据
S303

图 3

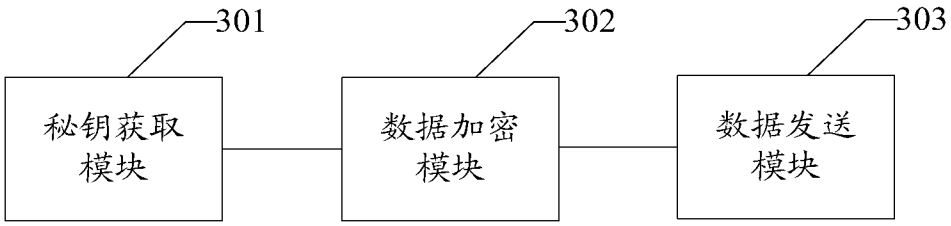
301
302
303
秘钥获取模块
数据加密模块
数据发送模块

图 4

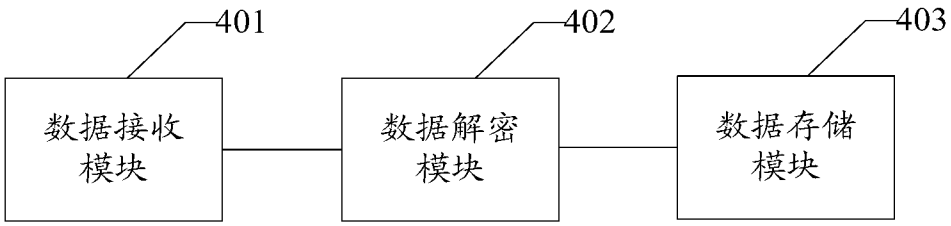
401
402
403
数据接收模块
数据解密模块
数据存储模块

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/091355

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/14 (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; H04W

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)

CNTXT; CNABS: body area network, wearable, medical, encrypt, decrypt, key, data, security

VEN; USTXT: body area network, medical, encrypt, decrypt, key, data, security

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103457722 A (JILIN UNIVERSITY), 18 December 2013 (18.12.2013), description, paragraphs [0002]-[0003], [0006]-[0011], [0014]-[0017] and [0030]-[0062]	1-15
X	CN 103929741 A (CHONGQING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS), 16 July 2014 (16.07.2014), description, paragraphs [0013]-[0018]	1-15
X	CN 104053152 A (NINGBO UNIVERSITY OF TECHNOLOGY), 17 September 2014 (17.09.2014), description, paragraphs [0035]-[0046]	1-15
A	CN 104685322 A (PROTEUS DIGITAL HEALTH, INC.), 03 June 2015 (03.06.2015), the whole document	1-15

☐ 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
25 April 2016 (25.04.2016)	**03 May 2016 (03.05.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **WANG, Rui** Telephone No.: (86-10) **62089564**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/091355

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103457722 A	18 December 2013	None	
CN 103929741 A	16 July 2014	None	
CN 104053152 A	17 September 2014	None	
CN 104685322 A	03 June 2015	WO 2014047205 A1	27 March 2014
		US 2015248833 A1	03 September 2015
		KR 20150047630 A	04 May 2015
		EP 2898297 A1	29 July 2015
		AU 2013318130 A1	16 April 2015
		CA 2885704 A1	27 March 2014
		SG 11201502203 A1	29 April 2015
		IL 237834 A	31 May 2015
		JP 2015531954 A	05 November 2015
		KR 1571688 B1	25 November 2015

国际检索报告

国际申请号
PCT/CN2015/091355

A. 主题的分类

H04L 9/14(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; H04W

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））

CNTXT;CNABS:体域网，可穿戴，医疗，加密，解密，密钥，解密，数据，安全 VEN;USTXT:body area network, medical, encrypt, decrypt, key, data, security

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
X	CN 103457722 A (吉林大学) 2013年 12月 18日 (2013-12-18) 说明书[0002]-[0003]，[0006]-[0011]，[0014]-[0017]，[0030]-[0062]段	1-15
X	CN 103929741 A (重庆邮电大学) 2014年 7月 16日 (2014-07-16) 说明书第[0013]-[0018]段	1-15
X	CN 104053152 A (宁波工程学院) 2014年 9月 17日 (2014-09-17) 说明书第[0035]-[0046]段	1-15
A	CN 104685322 A (普罗秋斯数字健康公司) 2015年 6月 3日 (2015-06-03) 全文	1-15

☐ 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
2016年 4月 25日	2016年 5月 3日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(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 王瑞 电话号码 (86-10)62089564

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/091355

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	103457722	A	2013年 12月 18日	无			
CN	103929741	A	2014年 7月 16日	无			
CN	104053152	A	2014年 9月 17日	无			
CN	104685322	A	2015年 6月 3日	WO	2014047205	A1	2014年 3月 27日
				US	2015248833	A1	2015年 9月 3日
				KR	20150047630	A	2015年 5月 4日
				EP	2898297	A1	2015年 7月 29日
				AU	2013318130	A1	2015年 4月 16日
				CA	2885704	A1	2014年 3月 27日
				SG	11201502203	A1	2015年 4月 29日
				IL	237834	A	2015年 5月 31日
				JP	2015531954	A	2015年 11月 5日
				KR	1571688	B1	2015年 11月 25日