

(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
2016 年 12 月 1 日 (01.12.2016)



(10) 国际公布号
WO 2016/187892 A1

- (51) 国际专利分类号:
H04L 9/00 (2006.01)
- (21) 国际申请号: PCT/CN2015/080322
- (22) 国际申请日: 2015 年 5 月 29 日 (29.05.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510267013.X 2015 年 5 月 22 日 (22.05.2015) 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: 董志伟 (DONG, Zhiwei); 中国广东省深圳市南山区科技园北区梦溪道 2 号, Guangdong 518057 (CN)。 刘碧波 (LIU, Bibo); 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: 广州三环专利代理有限公司 (GUANG-ZHOU SCIHEAD PATENT AGENT CO., LTD); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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。
- (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)。

[见续页]

(54) Title: DATA TRANSMISSION METHOD AND TERMINAL

(54) 发明名称: 一种数据传输的方法及终端

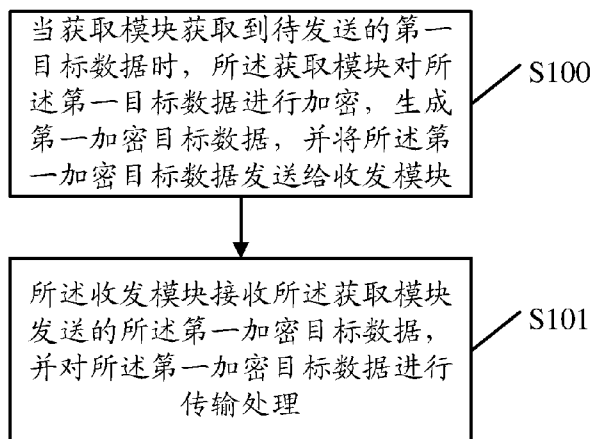


图 1

- S100 When an acquiring module acquires first target data to be sent, the acquiring module encrypts the first target data to generate first encrypted target data, and sends the first encrypted target data to a transceiver module
- S101 The transceiver module receives the first encrypted target data sent by the acquiring module, and transmits the first encrypted target data

(57) Abstract: Disclosed is a data transmission method. The method comprises: when an acquiring module acquires first target data to be sent, the acquiring module encrypts the first target data to generate first encrypted target data, and sends the first encrypted target data to a transceiver module; and the transceiver module receives the first encrypted target data sent by the acquiring module, and transmits the first encrypted target data, so that a reception end connected to the transceiver module obtains the first target data. Also disclosed is a terminal. By using the present invention, a terminal can encrypt internally transmitted data, so as to prevent data from being thieved and improve security of the data.

(57) 摘要: 本发明实施例公开了一种数据传输的方法, 包括: 当获取模块获取到待发送的第一目标数据时, 所述获取模块对所述第一目标数据进行加密, 生成第一加密目标数据, 并将所述第一加密目标数据发送给收发模块; 所述收发模块接收所述获取模块发送的所述第一加密目标数据, 并对所述第一加密目标数据进行传输处理, 以使与所述收发模块连接的接收端获得所述第一目标数据。本发明实施例还公开了终端。采用本发明, 可使得终端可对内部传输的数据进行加密, 从而避免数据被监听窃取, 提高数据的安全性。



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种数据传输的方法及终端

本申请要求于 2015 年 5 月 22 日提交中国专利局，申请号为 201510267013.X、发明名称为“一种数据传输的方法及终端”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

5

技术领域

本发明涉及电子技术领域，尤其涉及一种数据的传输方法及终端。

背景技术

10 目前，终端上的需与其他接收端进行交互的待发送数据，例如：用户在终端的操作页面上输入操作指令以控制与终端连接的接收端，该操作指令需由终端发送给接收端，以使接收端响应操作指令实现终端的控制。其中，待发送数据在终端内部的现有传输路径具体为：终端的获取模块获取到待发送数据，获取模块对待发送数据不进行任何处理，直接将待发送数据发送给终端的收发模
15 块，以使收发模块通过空口传输给接收端。在具体应用中可以是，用户在应用层上输入数据，该数据需发送给接收端，而终端的应用层可以将该数据直接传输给基带处理器（Modem），基带处理器将该数据通过空口传输给接收端；还可以是，短信应用通过短信收发的接口向基带处理器发送明文短信，基带处理器将短信发送到对应的接收端。其中，为了提高待发送的数据的安全性，收发
20 模块还可对待发送的数据进行加密，并将加密后的数据传输给接收端。

但是，由于获取模块是對待发送数据不进行任何处理即将待发送数据发送给收发模块，这使得获取模块向收发模块发送的待发送数据是明文内容，而目前存在的第三方木马程序可以进行监听获取模块的接口和收发模块的接口，即
25 是，第三方木马程序可以监听获取模块与收发模块的传输过程，这使得当获取模块向收发模块发送的是明文内容时，第三方木马程序可通过监听系统广播等方式在收发模块获取到待发送数据之前，即可从中拦截到待发送数据，从而造成用户数据的丢失。

同样，终端上的与其他发送端进行交互的接收数据，例如：终端接收到发送端发送的操作指令。其中，接收数据在终端内部的现有传输路径具体为：终端的收发模块获取到接收数据，当接收数据不是加密数据时，收发模块可对接
30

收数据不进行任何处理，直接将接收数据发送给终端的获取模块；当接收数据是加密数据时，收发模块可对接收数据进行解密，并将解密后的接收数据发送给终端的获取模块。

但是，由于收发模块是将明文内容发送给获取模块，而目前存在的第三方木马程序可以进行监听获取模块与收发模块的传输过程，这使得当收发模块向获取模块发送的是明文内容时，第三方木马程序可通过监听系统广播等方式在收发模块获取到待发送数据之前，即可从中拦截到接收数据，也造成用户数据的丢失。

因此，现有的获取模块与收发模块之间在进行数据传输时无法保证数据的安全性，从而导致数据丢失，造成数据泄露，给用户带来了不便。

发明内容

本发明实施例所要解决的技术问题在于，提供一种数据传输的方法及终端。可使得终端可对内部传输的数据进行加密，从而避免数据被监听窃取，提高数据的安全性。

为了解决上述技术问题，本发明实施例提供了一种数据传输的方法，包括：

当获取模块获取到待发送的第一目标数据时，所述获取模块对所述第一目标数据进行加密，生成第一加密目标数据，并将所述第一加密目标数据发送给收发模块；

所述收发模块接收所述获取模块发送的所述第一加密目标数据，并对所述第一加密目标数据进行传输处理，以使与所述收发模块连接的接收端获得所述第一目标数据。

其中，所述第一加密目标数据携带第一加密标识符；

所述收发模块接收所述获取模块发送的所述第一加密目标数据，并对所述第一加密目标数据进行传输处理包括：

所述收发模块将所述第一加密目标数据发送给所述接收端，或者，

所述收发模块解析所述第一加密目标数据获得所述第一加密标识符；

所述收发模块根据所述第一加密标识符获取所述第一加密标识符所对应的第一解密规则；

所述收发模块根据所述第一解密规则对所述第一加密目标数据进行解密，

获得所述第一目标数据。

其中，所述方法还包括：

当所述收发模块接收到与所述收发模块连接的发送端发送的第二目标数据时，所述收发模块对所述第二目标数据进行加密，生成第二加密目标数据，
5 并将所述第二加密目标数据发送给所述获取模块；

所述获取模块接收所述收发模块发送的所述第二加密目标数据，对所述第二加密目标数据进行解密，获得所述第二目标数据；

所述获取模块处理所述第二目标数据。

其中，所述第二加密目标数据携带第二加密标识符；

10 所述获取模块接收所述收发模块发送的所述第二加密目标数据，对所述第二加密目标数据进行解密，获得所述第二目标数据包括：

所述获取模块根据所述第二加密标识符获取所述第二加密标识符对应的第二解密规则；

15 所述获取模块根据所述第二解密规则对所述第二加密目标数据进行解密，获得所述第二目标数据。

其中，所述获取模块接收所述收发模块发送的所述第二加密目标数据，对所述第二加密目标数据进行解密，获得所述第二目标数据之前包括：

验证模块对所述获取模块进行验证，确定所述获取模块合法。

20 相应地，本发明实施例还提供了一种终端，所述终端包括获取模块和与所述获取模块连接的收发模块，其中，

所述获取模块，用于当获取到待发送的第一目标数据时，对所述第一目标数据进行加密，生成第一加密目标数据，并将所述第一加密目标数据发送给收发模块；

25 所述收发模块接收所述获取模块发送的所述第一加密目标数据，并对所述第一加密目标数据进行传输处理，以使与所述收发模块连接的接收端获得所述第一目标数据。

其中，所述第一加密目标数据携带第一加密标识符；

所述收发模块具体用于：

将所述第一加密目标数据发送给所述接收端，或者，

30 解析所述第一加密目标数据获得所述第一加密标识符；

根据所述第一加密标识符获取所述第一加密标识符所对应的第一解密规则；

根据所述第一解密规则对所述第一加密目标数据进行解密，获得所述第一目标数据。

5 其中，

所述收发模块具体用于：

当接收到与所述收发模块连接的发送端发送的第二目标数据时，对所述第二目标数据进行加密，生成第二加密目标数据，并将所述第二加密目标数据发送给所述获取模块；

10 所述获取模块具体用于：

接收所述收发模块发送的所述第二加密目标数据，对所述第二加密目标数据进行解密，获得所述第二目标数据；

处理所述第二目标数据。

其中，所述第二加密目标数据携带第二加密标识符；

15 所述获取模块具体用于：

根据所述第二加密标识符获取所述第二加密标识符对应的第二解密规则；

根据所述第二解密规则对所述第二加密目标数据进行解密，获得所述第二目标数据。

其中，所述终端还包括验证模块，其中，

20 所述验证模块用于对所述获取模块进行验证，确定所述获取模块合法。

实施本发明实施例，具有如下有益效果：

在本发明实施例中，当获取模块获取到待发送的第一目标数据时，获取模块对第一目标数据进行加密，生成第一加密目标数据，并将第一加密目标数据发送给收发模块，收发模块接收第一加密目标数据，并对第一加密目标数据进行传输处理，以使与所收发模块连接的接收端获得所述第一目标数据，这使得终端可对内部传输的数据进行加密，从而避免数据被监听窃取，提高数据的安全性。

25

附图说明

30 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一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本发明一种数据传输的方法的第一实施例流程示意图；

5 图 2 是本发明一种数据传输的方法的第二实施例流程示意图；

图 3 是本发明一种终端的第一实施结构图；

图 4 是本发明一种终端的第二实施结构图。

具体实施方式

10 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，都属于本发明保护的范围。

15 本发明所提及到的获取模块、收发模块和验证模块都属于同一个终端中的模块。其中，终端可包括：手机、平板电脑、掌上电脑或者移动互联网设备（Mobile Internet Device, MID）等，上述终端仅是举例，而非穷举，包含但不限于上述终端。

请参见图 1，为本发明一种数据传输的方法的第一实施例流程示意图。如图 1 所示，本实施例所述的一种数据传输的方法包括步骤：

20 S100，当获取模块获取到待发送的第一目标数据时，所述获取模块对所述第一目标数据进行加密，生成第一加密目标数据，并将所述第一加密目标数据发送给收发模块。

在本发明实施例中，获取模块可以是终端中获取终端的待发送数据的模块，其中，终端需将待发送数据送给与终端建立网络通信连接的接收端。在具
25 体应用中，获取模块可以是终端的应用层，应用层可包括终端提供应用服务的应用程序，如：短信应用程序、互联网应用程序和电子邮件应用程序等。进一步的，获取模块还可以是终端的会话层，会话层可包括终端提供会话的应用程序，如：通话应用程序。进一步的，由于待发送数据需通过终端的基带处理器（Modem）来进行网络交互，获取模块还可以是其他与 Modem 进行交互的模
30 块，在此不再赘述。

在本发明实施例中，第一目标数据可以包括短信、彩信、控制信息和数据业务信息（电子邮件、上网浏览记录）等可以向接收端发送的数据。获取模块获取第一目标数据具体可以是：当用户通过短信应用程序输入需要进行发送的短信时，应用层的短信应用程序将获取该短信；当用户通过浏览器输入网址进行浏览网页时，浏览器可获取该网址。

在本发明实施例中，当获取模块获取到第一目标数据时，获取模块可以读取终端预设的使用模式，判断是否需对第一目标数据进行加密处理。其中，终端可提供设置页面供用户进行选择设置使用模式，使用模式包括安全传输模式和普通传输模式，终端可根据用户在设置页面选择设置的使用模式，提供相应的显示界面，并且获取模块也根据用户在设置页面选择设置的使用模式，而进行相应的处理。当获取模块读取到用户设置的使用模式为安全传输模式时，获取模块将第一目标数据进行加密；当获取模块读取到用户设置的使用模式为普通传输模式时，获取模块将不对第一目标数据进行处理，直接将第一目标数据发送给收发模块。

在本发明实施例中，当获取模块需对第一目标数据进行加密时，获取模块调用了相应的第一加密规则对第一目标数据进行加密处理。终端可预置获取模块的第一加密规则，其中，第一加密规则可包括密钥、加密算法、加密算法类型等。当获取模块需将第一目标数据进行加密时，获取模块可以根据预置的第一加密规则对第一目标数据进行加密，生成第一加密目标数据，如采用预置的CP_DECODE_SI加密算法进行加密；或者，获取模块可以获取第一目标数据的重要等级，根据重要等级获取相应的第一加密规则，从而根据第一加密规则对第一目标数据进行加密，生成第一加密目标数据，其中，获取模块可以根据第二目标数据判断重要等级，终端可预置重要等级与第二加密规则的对应关系；或者，终端可提供设置页面由用户进行选择第一加密规则，从而获取模块根据用户选择的第一加密规则对第一目标数据进行加密，生成第一加密目标数据，并将第一加密目标数据发送给收发模块。其中，收发模块可以是终端的Modem，其中，Modem负责终端的网络通信。终端打电话、上网和发短信等，其过程均是由上层系统将指令发送给Modem处理执行，Modem完成处理后就会在终端和接收端建立一条网络通道。获取模块可将话音、短信或上网数据包发送给Modem，Modem可将该数据通过网络通道向接收端发送。从而使得即

使终端存在第三方应用程序对获取模块发送的数据进行监听，其监听到的数据为加密后的数据，从而提高了数据的安全性。

进一步的，在本发明实施例中，当获取模块获取到第一加密规则对第一目标数据进行加密后，获取模块还可获取第一加密规则对应的第一加密标识符，
5 并将第一加密标识符添加至第一加密目标数据中，其中，第一加密标识符用于标识第一加密规则。

S101，所述收发模块接收所述获取模块发送的所述第一加密目标数据，并对所述第一加密目标数据进行传输处理，以使与所述收发模块连接的接收端获得所述第一目标数据。

10 在本发明实施例中，接收端可以是手机、平板电脑和基站等接收端，其中，接收端可与终端建立蓝牙连接、WIFI（Wireless Fidelity，无线保真技术）连接和 NFC（Near Field Communication，近距离无线通信）通信连接等通信连接，其中，接收端可与终端的收发模块建立通信连接。当收发模块接收到第一加密目标数据后，收发模块可直接将第一加密目标数据通过通信网络转发给接收
15 端，以使接收端可对第一加密目标数据进行解密，获得第一目标数据，从而根据第一目标数据进行处理。

进一步的，当收发模块接收到第一加密目标数据后，收发模块可对第一加密目标数据进行解密，获得第一目标数据，从而将第一目标数据通过通信网络发送给接收端，以使接收端根据第一目标数据进行处理。

20 其中，收发模块对第一加密目标数据进行解密可以是：收发模块根据预置的第一解密规则对第一加密目标数据进行解密，获得第一目标数据，如采用预置的 CP_DECODE_SI 解密算法进行解密。进一步的，还可以是，收发模块解析第一加密目标数据，获得第一加密标识符，收发模块根据该第一加密标识符获得相应的第一解密规则，如第一加密标识符标识 CP_DECODE_SI 加密算法，
25 收发模块可根据 CP_DECODE_SI 加密算法查找对应的 CP_DECODE_SI 解密算法。从而收发模块根据获得的第一解密规则对所述第一加密目标数据进行解密，获得所述第一目标数据。

在本发明实施例中，当获取模块获取到待发送的第一目标数据时，获取模块对第一目标数据进行加密，生成第一加密目标数据，并将第一加密目标数据
30 发送给收发模块，收发模块接收第一加密目标数据，并对第一加密目标数据进

行传输处理,以使与所收发模块连接的接收端获得所述第一目标数据,这使得终端可对内部传输的数据进行加密,从而避免数据被监听窃取,提高数据的安全性。

请参见图 2,为本发明一种数据传输的方法的第二实施例流程示意图。如

5 图 2 所示,本实施例所述的一种数据传输的方法包括步骤:

S200,当所述收发模块接收到与所述收发模块连接的发送端发送的第二目标数据时,所述收发模块对所述第二目标数据进行加密,生成第二加密目标数据,并将所述第二加密目标数据发送给所述获取模块。

在本发明实施例中,发送端可以是与终端建立通信连接的发送端,发送端
10 可以是手机、平板电脑和基站等发送端。其中,发送端可与终端建立通信连接,其中,通信连接可以是蓝牙通信连接、WIFI 通信连接和 NFC 通信连接等网络通信连接,具体的,发送端可以与终端的收发模块建立通信连接。当发送端向终端发送第二目标数据时,终端的收发模块接收到第二目标数据,如当基站向终端发送短信时,终端的收发模块将通过空口接收来自基站发送的短信。其中,
15 第二目标数据可以包括基站向终端发送的短信、彩信、控制信息和数据业务信息(电子邮件)等基站可以向终端发送的数据。

在本发明实施例中,当收发模块获取到第二目标数据时,收发模块可以读取终端预设的使用模式,判断是否需对第二目标数据进行加密处理。其中,终端可提供设置页面供用户进行选择设置使用模式,使用模式包括安全传输模式
20 和普通传输模式,终端可根据用户在设置页面选择设置的使用模式,提供相应的显示界面,并且收发模块也根据用户在设置页面选择设置的使用模式,而进行相应的处理。当收发模块读取到用户设置的使用模式为安全传输模式时,收发模块将第二目标数据进行加密;当收发模块读取到用户设置的使用模式为普通传输模式时,收发模块将不对第二目标数据进行处理,直接将第二目标数据
25 发送给获取模块。

在本发明实施例中,当收发模块需对第二目标数据进行加密时,收发模块调用了相应的第二加密规则对第二目标数据进行加密处理。其中,终端可预置收发模块的第二加密规则,其中,第二加密规则可包括密钥、加密算法、加密算法类型等。收发模块可以根据预置的第二加密规则对第二目标数据进行加
30 密,生成第二加密目标数据,如收发模块采用预置的 CP_DECODE_SI 加密算

法进行加密；或者，收发模块可以获取第二目标数据的重要等级，根据重要等级获取相应的第二加密规则，从而根据第二加密规则对第二目标数据进行加密，生成第二加密目标数据，其中，第二目标数据可携带重要等级，终端可预置重要等级与第二加密规则的对应关系；或者，终端可以设置页面由用户进行选择加密规则，从而收发模块根据用户选择的第二加密规则对第二目标数据进行加密，生成第二加密目标数据，并将第二加密目标数据发送给获取模块。

进一步的，在本发明实施例中，当收发模块获取到第二加密规则对第二目标数据进行加密后，获取模块还可获取第二加密规则对应的第二加密标识符，并将第二加密标识符添加至第二加密目标数据中，其中，第二加密标识符用于标识第二加密规则。

S201，所述获取模块接收所述收发模块发送的所述第二加密目标数据，对所述第二加密目标数据进行解密，获得所述第二目标数据。

在本发明实施例中，在获取模块接收收发模块发送的第二加密目标数据之前，终端还可检验获取模块是否合法。其中，可以是终端的检验模块检验获取模块是否合法。具体的，当接收到第二加密目标数据的获取模块是应用程序时，检验模块判断该应用程序是否包含检验模块所信任的安全信息，如认证证书。当应用程序包含检验模块所信任的安全信息时，检验模块可确认应用程序合法。当检验模块判断获取模块合法时，检验模块可允许获取模块调用第二加密规则对第二加密目标数据进行解密，如提供 API（Application Programming Interface，应用程序编程接口）给已经授权的应用程序进行解密；当检验模块判断获取模块不合法时，检验模块将不允许获取模块对第二加密目标数据进行解密，从而有效提高数据的安全性。

在本发明实施例中，当检验模块允许获取模块调用第二加密规则对第二加密目标数据进行解密时，获取模块可以根据预置的第二解密规则对第二加密目标数据进行解密，获得第二目标数据，如采用预置的 CP_DECODE_SI 解密算法进行解密。进一步的，还可以是，获取模块解析第二加密目标数据，获得第二加密标识符，获取模块根据第二加密标识符获得相应的第二解密规则，如第二加密标识符标识 CP_DECODE_SI 加密算法，获取模块可根据 CP_DECODE_SI 加密算法查找对应的 CP_DECODE_SI 解密算法。从而获取模块调用第二解密规则对第二加密目标数据进行解密，获得第二目标数据。

S202, 所述获取模块处理所述第二目标数据。

当获取模块获取到第二目标数据后, 获取模块可根据本身的功能以及第二目标数据的属性进行相应的处理。例如: 当获取模块是短信应用程序, 第二目标数据是短信时, 短信应用程序将短信显示在用户界面上, 以使用户阅读短信;
5 当获取模块是设置应用程序, 第二目标数据是设置参数时, 设置应用程序将根据设置参数修改自身的参数。

在本发明实施例中, 当所述收发模块接收到与所述收发模块连接的发送端发送的第二目标数据时, 所述收发模块对所述第二目标数据进行加密, 生成第二加密目标数据, 并将所述第二加密目标数据发送给所述获取模块, 所述获取
10 模块接收所述第二加密目标数据, 对所述第二加密目标数据进行解密, 获得所述第二目标数据, 所述获取模块处理所述第二目标数据, 这使得终端可对内部传输的数据进行加密, 从而避免数据被监听窃取, 提高数据的安全性。

参见图 3, 是本发明实施例的一种终端的第一实施例结构示意图。本实施例中所述的终端, 包括:

15 获取模块 100, 用于当获取到待发送的第一目标数据时, 对所述第一目标数据进行加密, 生成第一加密目标数据, 并将所述第一加密目标数据发送给收发模块。

收发模块 200, 用于接收所述获取模块发送的所述第一加密目标数据, 并对所述第一加密目标数据进行传输处理, 以使与所述收发模块连接的接收端获
20 得所述第一目标数据。

在本发明实施例中, 获取模块 100 可以是终端中获取终端的待发送数据的模块, 其中, 终端需将待发送数据送给与终端建立网络通信连接的接收端。在具体应用中, 获取模块 100 可以是终端的应用层, 应用层可包括终端提供应用服务的应用程序, 如: 短信应用程序、互联网应用程序和电子邮件应用程序等。
25 进一步的, 获取模块 100 还可以是终端的会话层, 会话层可包括终端提供会话的应用程序, 如: 通话应用程序。进一步的, 由于待发送数据需通过终端的基带处理器 (Modem) 来进行网络交互, 获取模块 100 还可以是其他与 Modem 进行交互的模块, 在此不再赘述。

在本发明实施例中, 第一目标数据可以包括短信、彩信、控制信息和数据
30 业务信息 (电子邮件、上网浏览记录) 等可以向接收端发送的数据。获取模块

100 获取第一目标数据具体可以是：当用户通过短信应用程序输入需要进行发送的短信时，应用层的短信应用程序将获取该短信；当用户通过浏览器输入网址进行浏览网页时，浏览器可获取该网址。

在本发明实施例中，当获取模块 100 获取到第一目标数据时，获取模块
5 100 可以读取终端预设的使用模式，判断是否需对第一目标数据进行加密处理。其中，终端可提供设置页面供用户进行选择设置使用模式，使用模式包括安全传输模式和普通传输模式，终端可根据用户在设置页面选择设置的使用模式，提供相应的显示界面，并且获取模块 100 也根据用户在设置页面选择设置的使用模式，而进行相应的处理。当获取模块 100 读取到用户设置的使用模式
10 为安全传输模式时，获取模块 100 将第一目标数据进行加密；当获取模块 100 读取到用户设置的使用模式为普通传输模式时，获取模块 100 将不对第一目标数据进行处理，直接将第一目标数据发送给收发模块。

在本发明实施例中，当获取模块 100 需对第一目标数据进行加密时，获取模块 100 了调用相应的第一加密规则对第一目标数据进行加密处理。终端可预
15 置获取模块 100 的第一加密规则，其中，第一加密规则可包括密钥、加密算法、加密算法类型等。当获取模块 100 需将第一目标数据进行加密时，获取模块 100 可以根据预置的第一加密规则对第一目标数据进行加密，生成第一加密目标数据，如采用预置的 CP_DECODE_SI 加密算法进行加密；或者，获取模块 100 可以获取第一目标数据的重要等级，根据重要等级获取相应的第一加密规则，从而根据第一加密规则对第一目标数据进行加密，生成第一加密目标数据，
20 其中，获取模块 100 可以根据第二目标数据判断重要等级，终端可预置重要等级与第二加密规则的对应关系；或者，终端可提供设置页面由用户进行选择第一加密规则，从而获取模块 100 根据用户选择的第一加密规则对第一目标数据进行加密，生成第一加密目标数据，并将第一加密目标数据发送给收发模块。
25 其中，收发模块可以是终端的 Modem，其中，Modem 负责终端的网络通信。终端打电话、上网和发短信等，其过程均是由上层系统将指令发送给 Modem 处理执行，Modem 完成处理后就会在终端和接收端建立一条网络通道。获取模块 100 可将话音、短信或上网数据包发送给 Modem，Modem 可将该数据通过网络通道向接收端发送。从而使得即使终端存在第三方应用程序对获取模块
30 100 发送的数据进行监听，其监听到的数据为加密后的数据，从而提高了数据

的安全性。

进一步的，在本发明实施例中，当获取模块 100 获取到第一加密规则对第一目标数据进行加密后，获取模块 100 还可获取第一加密规则对应的第一加密标识符，并将第一加密标识符添加至第一加密目标数据中，其中，第一加密标识符用于标识第一加密规则。

在本发明实施例中，接收端可以是手机、平板电脑和基站等接收端，其中，接收端可与终端建立蓝牙连接、WIFI（Wireless Fidelity，无线保真技术）连接等通信连接，其中，接收端可与终端的收发模块 200 建立通信连接。当收发模块 200 接收到第一加密目标数据后，收发模块 200 可直接将第一加密目标数据通过通信网络转发给接收端，以使接收端可对第一加密目标数据进行解密，获得第一目标数据，从而根据第一目标数据进行处理。

进一步的，当收发模块 200 接收到第一加密目标数据后，收发模块 200 可对第一加密目标数据进行解密，获得第一目标数据，从而将第一目标数据通过通信网络发送给接收端，以使接收端根据第一目标数据进行处理。

其中，收发模块 200 对第一加密目标数据进行解密可以是：收发模块 200 根据预置的第一解密规则对第一加密目标数据进行解密，获得第一目标数据，如采用预置的 CP_DECODE_SI 解密算法进行解密。进一步的，还可以是，收发模块 200 解析第一加密目标数据，获得第一加密标识符，收发模块 200 根据该第一加密标识符获得相应的第一解密规则，如第一加密标识符标识 CP_DECODE_SI 加密算法，收发模块 200 可根据 CP_DECODE_SI 加密算法查找对应的 CP_DECODE_SI 解密算法。从而收发模块 200 根据获得的第一解密规则对所述第一加密目标数据进行解密，获得所述第一目标数据。

在本发明实施例中，当获取模块 100 获取到待发送的第一目标数据时，获取模块 100 对第一目标数据进行加密，生成第一加密目标数据，并将第一加密目标数据发送给收发模块 200，收发模块 200 接收第一加密目标数据，并对第一加密目标数据进行传输处理，以使与所收发模块 200 连接的接收端获得所述第一目标数据，这使得终端可对内部传输的数据进行加密，从而避免数据被监听窃取，提高数据的安全性。

参见图 4，是本发明实施例的一种终端的第一实施例结构示意图。本实施例中所述的终端包括获取模块 100 和收发模块 200，其中，

所述收发模块 200 具体用于：

当接收到与所述收发模块连接的发送端发送的第二目标数据时，对所述第二目标数据进行加密，生成第二加密目标数据，并将所述第二加密目标数据发送给所述获取模块；

5 所述获取模块 100 具体用于：

接收所述收发模块发送的所述第二加密目标数据，对所述第二加密目标数据进行解密，获得所述第二目标数据；

处理所述第二目标数据。

其中，所述终端还包括：

10 验证模块 300，其中，

所述验证模块 300 用于对所述获取模块进行验证，确定所述获取模块合法。

在本发明实施例中，发送端可以是与终端建立通信连接的发送端，发送端可以是手机、平板电脑和基站等发送端。其中，发送端可与终端建立通信连接，15 其中，通信连接可以是蓝牙通信连接、WIFI 通信连接和 NFC 通信连接等网络通信连接，具体的，发送端可以与终端的收发模块 200 建立通信连接。当发送端向终端发送第二目标数据时，终端的收发模块 200 接收到第二目标数据，如当基站向终端发送短信时，终端的收发模块 200 将通过空口接收来自基站发送的短信。其中，第二目标数据可以包括基站向终端发送的短信、彩信、控制信20 息和数据业务信息（电子邮件）等基站可以向终端发送的数据。

在本发明实施例中，当收发模块 200 获取到第二目标数据时，收发模块 200 可以读取终端预设的使用模式，判断是否需对第二目标数据进行加密处理。其中，终端可提供设置页面供用户进行选择设置使用模式，使用模式包括安全传输模式和普通传输模式，终端可根据用户在设置页面选择设置的使用模25 式，提供相应的显示界面，并且收发模块 200 也根据用户在设置页面选择设置的使用模式，而进行相应的处理。当收发模块 200 读取到用户设置的使用模式为安全传输模式时，收发模块 200 将第二目标数据进行加密；当收发模块 200 读取到用户设置的使用模式为普通传输模式时，收发模块 200 将不对第二目标数据进行处理，直接将第二目标数据发送给获取模块。

30 在本发明实施例中，当收发模块 200 需对第二目标数据进行加密时，收发

模块 200 了调用相应的第二加密规则对第二目标数据进行加密处理。其中，终端可预置收发模块 200 的第二加密规则，其中，第二加密规则可包括密钥、加密算法、加密算法类型等。收发模块 200 可以根据预置的第二加密规则对第二目标数据进行加密，生成第二加密目标数据，如收发模块 200 采用预置的
5 CP_DECODE_SI 加密算法进行加密；或者，收发模块 200 可以获取第二目标数据的重要等级，根据重要等级获取相应的第二加密规则，从而根据第二加密规则对第二目标数据进行加密，生成第二加密目标数据，其中，第二目标数据可携带重要等级，终端可预置重要等级与第二加密规则的对应关系；或者，终端可以设置页面由用户进行选择加密规则，从而收发模块 200 根据用户选择的
10 第二加密规则对第二目标数据进行加密，生成第二加密目标数据，并将第二加密目标数据发送给获取模块。

进一步的，在本发明实施例中，当收发模块 200 获取到第二加密规则对第二目标数据进行加密后，获取模块还可获取第二加密规则对应的第二加密标识符，并将第二加密标识符添加至第二加密目标数据中，其中，第二加密标识符
15 用于标识第二加密规则。

在本发明实施例中，在获取模块 200 接收收发模块 100 发送的第二加密目标数据之前，终端还可检验获取模块 100 是否合法。其中，可以是终端的检验模块 300 检验获取模块 100 是否合法。具体的，当接收到第二加密目标数据的获取模块 100 是应用程序时，检验模块 300 判断该应用程序是否包含检验模块
20 所信任的安全信息，如认证证书。当应用程序包含检验模块所信任的安全信息时，检验模块 300 可确认应用程序合法。当检验模块 300 判断获取模块 100 合法时，检验模块 300 可允许获取模块 100 调用第二加密规则对第二加密目标数据进行解密，如提供 API（Application Programming Interface，应用程序编程接口）给已经授权的应用程序进行解密；当检验模块 300 判断获取模块 100
25 不合法时，检验模块 300 将不允许获取模块 100 对第二加密目标数据进行解密，从而有效提高数据的安全性。

在本发明实施例中，当检验模块 300 允许获取模块 100 调用第二加密规则对第二加密目标数据进行解密时，获取模块 100 可以根据预置的第二解密规则对第二加密目标数据进行解密，获得第二目标数据，如采用预置的
30 CP_DECODE_SI 解密算法进行解密。进一步的，还可以是，获取模块 100 解

析第二加密目标数据, 获得第二加密标识符, 获取模块 100 根据第二加密标识符获得相应的第二解密规则, 如第二加密标识符标识 CP_DECODE_SI 加密算法, 获取模块 100 可根据 CP_DECODE_SI 加密算法查找对应的 CP_DECODE_SI 解密算法。从而获取模块 100 调用第二解密规则对第二加密目标数据进行解密, 获得第二目标数据。

当获取模块 100 获取到第二目标数据后, 获取模块 100 可根据本身的功能以及第二目标数据的属性进行相应的处理。例如: 当获取模块 100 是短信应用程序, 第二目标数据是短信时, 短信应用程序将短信显示在用户界面上, 以使用户阅读短信; 当获取模块 100 是设置应用程序, 第二目标数据是设置参数时, 设置应用程序将根据设置参数修改自身的参数。

在本发明实施例中, 当所述收发模块 200 接收到与所述收发模块 200 连接的发送端发送的第二目标数据时, 所述收发模块 200 对所述第二目标数据进行加密, 生成第二加密目标数据, 并将所述第二加密目标数据发送给所述获取模块 100, 所述获取模块 100 接收所述第二加密目标数据, 对所述第二加密目标数据进行解密, 获得所述第二目标数据, 所述获取模块 100 处理所述第二目标数据, 这使得终端可对内部传输的数据进行加密, 从而避免数据被监听窃取, 提高数据的安全性。

本领域普通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, 所述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, 所述的存储介质可为磁碟、光盘、只读存储记忆体 (Read-Only Memory, ROM) 或随机存储记忆体 (Random Access Memory, RAM) 等。

以上所揭露的仅为本发明较佳实施例而已, 当然不能以此来限定本发明之权利范围, 因此依本发明权利要求所作的等同变化, 仍属本发明所涵盖的范围。

权 利 要 求

1、一种数据传输的方法，其特征在于，所述方法包括：

5 当获取模块获取到待发送的第一目标数据时，所述获取模块对所述第一目标数据进行加密，生成第一加密目标数据，并将所述第一加密目标数据发送给收发模块；

所述收发模块接收所述获取模块发送的所述第一加密目标数据，并对所述第一加密目标数据进行传输处理，以使与所述收发模块连接的接收端获得所述第一目标数据。

10

2、如权利要求 1 所述的方法，其特征在于，所述第一加密目标数据携带第一加密标识符；

所述收发模块接收所述获取模块发送的所述第一加密目标数据，并对所述第一加密目标数据进行传输处理包括：

15 所述收发模块将所述第一加密目标数据发送给所述接收端，或者，

所述收发模块解析所述第一加密目标数据获得所述第一加密标识符；

所述收发模块根据所述第一加密标识符获取所述第一加密标识符所对应的第一解密规则；

20 所述收发模块根据所述第一解密规则对所述第一加密目标数据进行解密，获得所述第一目标数据。

3、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

25 当所述收发模块接收到与所述收发模块连接的发送端发送的第二目标数据时，所述收发模块对所述第二目标数据进行加密，生成第二加密目标数据，并将所述第二加密目标数据发送给所述获取模块；

所述获取模块接收所述收发模块发送的所述第二加密目标数据，对所述第二加密目标数据进行解密，获得所述第二目标数据；

所述获取模块处理所述第二目标数据。

30 4、如权利要求 3 所述的方法，其特征在于，所述第二加密目标数据携带

第二加密标识符;

所述获取模块接收所述收发模块发送的所述第二加密目标数据, 对所述第二加密目标数据进行解密, 获得所述第二目标数据包括:

5 所述获取模块根据所述第二加密标识符获取所述第二加密标识符对应的第二解密规则;

所述获取模块根据所述第二解密规则对所述第二加密目标数据进行解密, 获得所述第二目标数据。

10 5、如权利要求 4 所述的方法, 其特征在于, 所述获取模块接收所述收发模块发送的所述第二加密目标数据, 对所述第二加密目标数据进行解密, 获得所述第二目标数据之前包括:

验证模块对所述获取模块进行验证, 确定所述获取模块合法。

15 6、一种终端, 其特征在于, 所述终端包括获取模块和与所述获取模块连接的收发模块, 其中,

所述获取模块, 用于当获取到待发送的第一目标数据时, 对所述第一目标数据进行加密, 生成第一加密目标数据, 并将所述第一加密目标数据发送给收发模块;

20 所述收发模块, 用于接收所述获取模块发送的所述第一加密目标数据, 并对所述第一加密目标数据进行传输处理, 以使与所述收发模块连接的接收端获得所述第一目标数据。

7、如权利要求 6 所述的终端, 其特征在于, 所述第一加密目标数据携带第一加密标识符;

25 所述收发模块具体用于:

将所述第一加密目标数据发送给所述接收端, 或者,

解析所述第一加密目标数据获得所述第一加密标识符;

根据所述第一加密标识符获取所述第一加密标识符所对应的第一解密规则;

30 根据所述第一解密规则对所述第一加密目标数据进行解密, 获得所述第一

目标数据。

8、如权利要求 6 所述的终端，其特征在于，

所述收发模块具体用于：

- 5 当接收到与所述收发模块连接的发送端发送的第二目标数据时，对所述第二目标数据进行加密，生成第二加密目标数据，并将所述第二加密目标数据发送给所述获取模块；

所述获取模块具体用于：

- 10 接收所述收发模块发送的所述第二加密目标数据，对所述第二加密目标数据进行解密，获得所述第二目标数据；
处理所述第二目标数据。

9、如权利要求 8 所述的终端，其特征在于，所述第二加密目标数据携带第二加密标识符；

- 15 所述获取模块具体用于：

根据所述第二加密标识符获取所述第二加密标识符对应的第二解密规则；
根据所述第二解密规则对所述第二加密目标数据进行解密，获得所述第二目标数据。

- 20 10、如权利要求 9 所述的终端，其特征在于，所述终端还包括验证模块，其中，

所述验证模块用于对所述获取模块进行验证，确定所述获取模块合法。

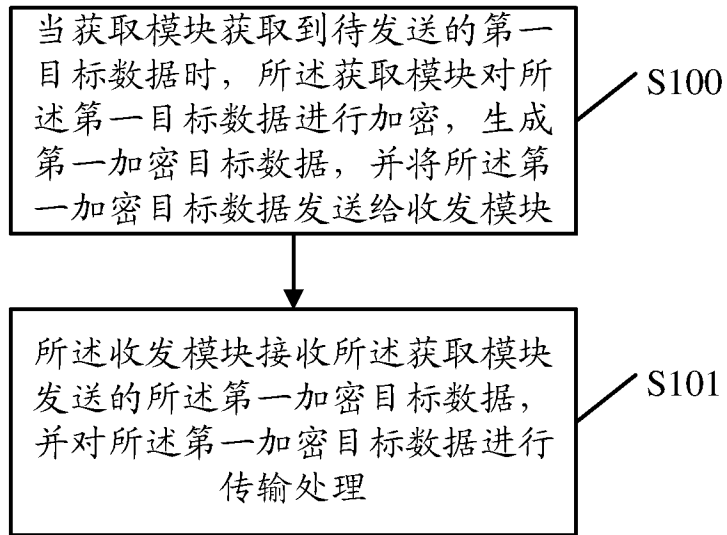


图 1

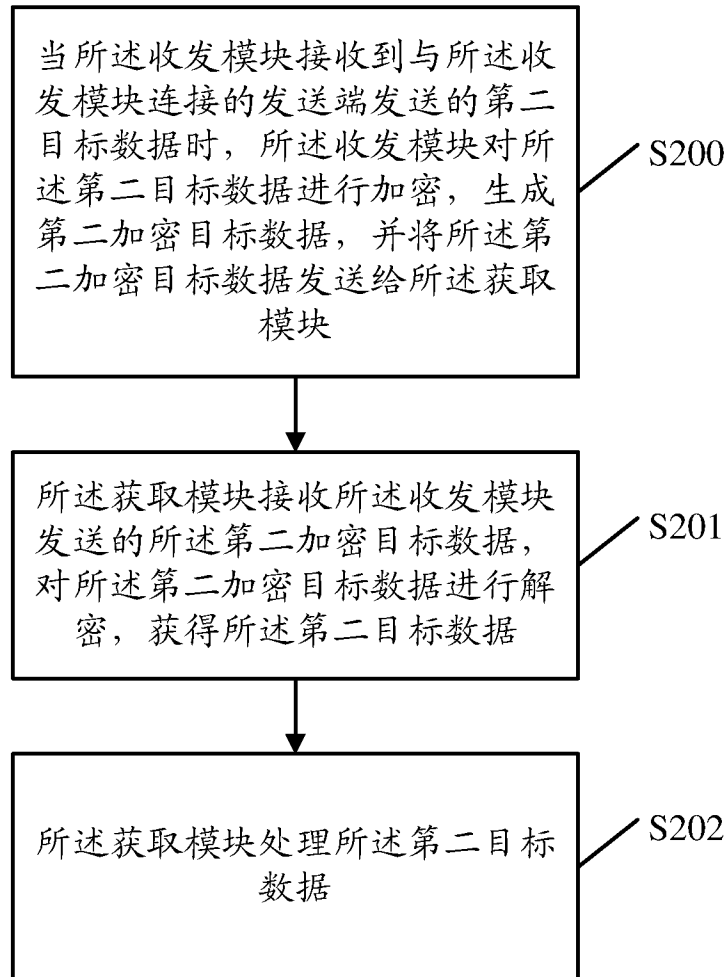


图 2

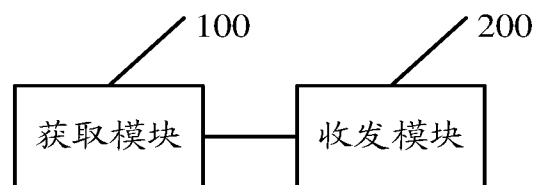


图 3

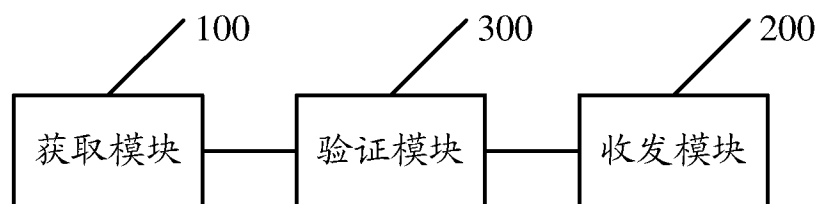


图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/080322

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/00 (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)

H04W; H04Q; H04L; H04B; H04J; H04M; 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, CNKI, WPI, EPODOC, IEEE: terminal, user equipment, UE, +phone, internal, data, transmission, encrypt, cockhorse, virus, monitor, intercept, filch

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101064595 A (LENOVO BEIJING CO., LTD.) 31 October 2007 (31.10.2007) description, page 2, the fourth paragraph to page 5, the tenth paragraph, page 13, the fifth paragraph to page 14, the third paragraph, and figures 1, and 4	1-10
X	CN 101236591 A (LENOVO BEIJING CO., LTD.) 06 August 2008 (06.08.2008) description, page 2, the fifth paragraph to page 5, the first paragraph, and figures 2, and 4	1-10
X	CN 103986711 A (TENDYRON TECHNOLOGY CO., LTD.) 13 August 2014 (13.08.2014) description, paragraphs [0002] to [0005], and figure 1	1-10
X	CN 103974243 A (TENDYRON TECHNOLOGY CO., LTD.) 06 August 2014 (06.08.2014) description, paragraphs [0002] to [0005], and [0027] to [0043]	1-10
A	CN 102790676 A (HUANG, Zhijun) 21 November 2012 (21.11.2012) the whole document	1-10

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	"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
"A" document defining the general state of the art which is not considered to be of particular relevance	"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
"E" earlier application or patent but published on or after the international filing date	"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
"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)	"&" document member of the same patent family
"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	

Date of the actual completion of the international search 15 January 2016	Date of mailing of the international search report 23 February 2016
Name and mailing address of the ISA 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 ZHAO, Jian Telephone No. (86-10) 61648266

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2015/080322

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101064595 A	31 October 2007	None	
CN 101236591 A	06 August 2008	US 2008181409 A1	31 July 2008
CN 103986711 A	13 August 2014	HK 1199986 A1	24 July 2015
CN 103974243 A	06 August 2014	None	
CN 102790676 A	21 November 2012	None	

A. 主题的分类 H04L 9/00 (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) H04W, H04Q, H04L, H04B, H04J, H04M, 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, CNKI, WPI, EPDOC, IEEE: 终端, 用户设备, 手机, 内部, 数据, 传输, 加密, 木马, 病毒, 监听, 窃取, terminal, user equipment, UE, +phone, internal, data, transmission, encrypt, cockhorse, virus, monitor, intercept, filch																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 101064595 A (联想北京有限公司) 2007年 10月 31日 (2007 - 10 - 31) 说明书第2页第4段至第5页第10段, 第13页第5段至第14页第3段, 图1, 图4</td> <td>1-10</td> </tr> <tr> <td>X</td> <td>CN 101236591 A (联想北京有限公司) 2008年 8月 6日 (2008 - 08 - 06) 说明书第2页第5段至第5页第1段, 图2, 图4</td> <td>1-10</td> </tr> <tr> <td>X</td> <td>CN 103986711 A (天地融科技股份有限公司) 2014年 8月 13日 (2014 - 08 - 13) 说明书第[0002]-[0005]段, 图1</td> <td>1-10</td> </tr> <tr> <td>X</td> <td>CN 103974243 A (天地融科技股份有限公司) 2014年 8月 6日 (2014 - 08 - 06) 说明书第[0002]-[0005], [0027]-[0043]段</td> <td>1-10</td> </tr> <tr> <td>A</td> <td>CN 102790676 A (黄志军) 2012年 11月 21日 (2012 - 11 - 21) 全文</td> <td>1-10</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 101064595 A (联想北京有限公司) 2007年 10月 31日 (2007 - 10 - 31) 说明书第2页第4段至第5页第10段, 第13页第5段至第14页第3段, 图1, 图4	1-10	X	CN 101236591 A (联想北京有限公司) 2008年 8月 6日 (2008 - 08 - 06) 说明书第2页第5段至第5页第1段, 图2, 图4	1-10	X	CN 103986711 A (天地融科技股份有限公司) 2014年 8月 13日 (2014 - 08 - 13) 说明书第[0002]-[0005]段, 图1	1-10	X	CN 103974243 A (天地融科技股份有限公司) 2014年 8月 6日 (2014 - 08 - 06) 说明书第[0002]-[0005], [0027]-[0043]段	1-10	A	CN 102790676 A (黄志军) 2012年 11月 21日 (2012 - 11 - 21) 全文	1-10
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
X	CN 101064595 A (联想北京有限公司) 2007年 10月 31日 (2007 - 10 - 31) 说明书第2页第4段至第5页第10段, 第13页第5段至第14页第3段, 图1, 图4	1-10																		
X	CN 101236591 A (联想北京有限公司) 2008年 8月 6日 (2008 - 08 - 06) 说明书第2页第5段至第5页第1段, 图2, 图4	1-10																		
X	CN 103986711 A (天地融科技股份有限公司) 2014年 8月 13日 (2014 - 08 - 13) 说明书第[0002]-[0005]段, 图1	1-10																		
X	CN 103974243 A (天地融科技股份有限公司) 2014年 8月 6日 (2014 - 08 - 06) 说明书第[0002]-[0005], [0027]-[0043]段	1-10																		
A	CN 102790676 A (黄志军) 2012年 11月 21日 (2012 - 11 - 21) 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 2016年 1月 15日		国际检索报告邮寄日期 2016年 2月 23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		授权官员 赵剑 电话号码 (86-10) 61648266																		

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/080322

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	101064595	A	2007年 10月 31日	无	
CN	101236591	A	2008年 8月 6日	US 2008181409 A1	2008年 7月 31日
CN	103986711	A	2014年 8月 13日	HK 1199986 A1	2015年 7月 24日
CN	103974243	A	2014年 8月 6日	无	
CN	102790676	A	2012年 11月 21日	无	

表 PCT/ISA/210 (同族专利附件) (2009年7月)