(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 119856444 A
(43)申请公布日 2025.04.18

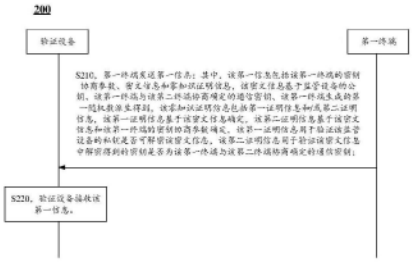
(21)申请号 202280100138.1
(22)申请日 2022.09.22
(85)PCT国际申请进入国家阶段日
2025.03.17
(86)PCT国际申请的申请数据
PCT/CN2022/120646 2022.09.22
(87)PCT国际申请的公布数据
WO2024/060149 ZH 2024.03.28
(71)申请人 OPPO广东移动通信有限公司
地址 523860 广东省东莞市长安镇乌沙海滨路18号
(72)发明人 甘露 刘雪峰 邹继鹏 石聪 杨宁
(74)专利代理机构 北京远志博慧知识产权代理有限公司 11680
专利代理师 李翠雅
(51)Int.Cl.
H04L 9/08(2006.01)
H04L 41/00(2006.01)
H04W 12/00(2006.01)

(54)发明名称

密钥验证方法、密钥获取方法及设备

(57)摘要

本申请实施例提供了一种密钥验证方法、密钥获取方法及设备,验证设备可以基于零知识证明信息验证监管设备的私钥是否可解密密文信息,以及验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥,从而,可以确保监管设备在获取到密文信息之后可以解密得到第一终端与第二终端协商确定的通信密钥,进而,监管设备可以监听第一终端与第二终端之间的侧行通信。



CN 119856444 A

(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
2024 年 3 月 28 日 (28.03.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/060149 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) ***H04W 12/00*** (2021.01)
H04L 41/00 (2022.01)

(21) 国际申请号: PCT/CN2022/120646

(22) 国际申请日: 2022 年 9 月 22 日 (22.09.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: **OPPO** 广东移动通信有限公司 **(GUANGDONG OPPO MOBILE TELECOMMUNICATIONS CORP., LTD.)** [CN/CN]; 中国广东省东莞市长安镇乌沙海滨路 18 号, Guangdong 523860 (CN)。

(72) 发明人: 甘露 **(GAN, Lu)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。 刘雪峰 **(LIU, Xuefeng)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。 邹继鹏 **(ZOU, Jipeng)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。 石聪 **(SHI, Cong)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。 杨宁 **(YANG, Ning)**; 中国广东省东莞市长安镇乌沙海滨路18号, Guangdong 523860 (CN)。

(74) 代理人: 北京知帆远景知识产权代理有限公司 **(ZHIFAN & PARTNERS)**; 中国北京市海淀区阜成路73号裕惠大厦B座805, Beijing 100142 (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, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, 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,

(54) **Title:** KEY VERIFICATION METHODS, KEY ACQUISITION METHOD, AND DEVICES

(54) 发明名称: 密钥验证方法、密钥获取方法及设备

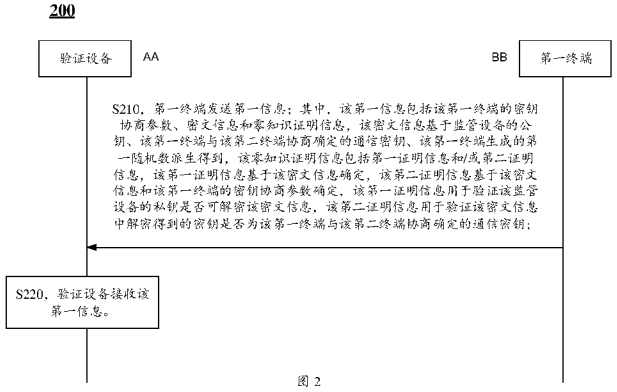


图 2

S210 A first terminal sends first information, the first information comprising key negotiation parameters of the first terminal, ciphertext information and zero-knowledge proof information; the ciphertext information is derived on the basis of a public key of a supervisory device, a communication key determined by means of a negotiation between the first terminal and a second terminal, and a first random number generated by the first terminal; the zero-knowledge proof information comprises first proof information and/or second proof information, the first proof information being determined on the basis of the ciphertext information, the second proof information being determined on the basis of the ciphertext information and the key negotiation parameters of the first terminal, the first proof information being used for verifying whether a private key of the supervisory device can decipher the ciphertext information, and the second proof information being used for verifying whether a key obtained by means of deciphering the ciphertext information is the communication key determined by means of the negotiation between the first terminal and the second terminal
S220 A verification device receives the first information
AA Verification device
BB First terminal

(57) **Abstract:** Provided in the embodiments of the present application are key verification methods, a key acquisition method, and devices. On the basis of zero-knowledge proof information, a verification device can verify whether a private key of a supervisory device can decipher ciphertext information, and whether a key obtained by means of deciphering the ciphertext information is a communication key determined by means of a negotiation between a first terminal and a second terminal, thereby ensuring that after acquiring the ciphertext information, the supervisory device can decipher same to obtain the communication key determined by means of the negotiation between the first terminal and the second terminal, and then the supervisory device can monitor sidelink communication between the first terminal and the second terminal.

(57) 摘要: 本申请实施例提供了一种密钥验证方法、密钥获取方法及设备，验证设备可以基于零知识证明信息验证监管设备的私钥是否可解密密文信息，以及验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥，从而，可以确保监管设备在获取到密文信息之后可以解密得到第一终端与第二终端协商确定的通信密钥，进而，监管设备可以监听第一终端与第二终端之间的侧行通信。

WO 2024/060149 A1

[见续页]

SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, 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))。

密钥验证方法、密钥获取方法及设备

技术领域

本申请实施例涉及通信领域，并且更具体地，涉及一种密钥验证方法、密钥获取方法及设备。

背景技术

监管设备可以监管第三代合作伙伴计划（The 3rd Generation Partnership Project，3GPP）通信场景，然而，并未涉及终端至终端中继（UE to UE Relay）场景的监管，按照行业发展趋势，针对终端至终端中继（UE to UE Relay）场景的监管在未来是不可避免的。如何针对终端至终端中继（UE to UE Relay）场景的进行监管，是一个需要解决的问题。

发明内容

本申请实施例提供了一种密钥验证方法、密钥获取方法及设备，监管设备可以通过零知识证明获取 UE to UE Relay 场景中监听所需的通信密钥，实现了对 UE to UE Relay 场景的监听。

第一方面，提供了一种密钥验证方法，应用于验证设备，该方法包括：

该验证设备接收第一信息；

其中，该第一信息包括第一终端的密钥协商参数、密文信息和零知识证明信息，该密文信息基于监管设备的公钥、该第一终端与第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该零知识证明信息包括第一证明信息和/或第二证明信息，该第一证明信息基于该密文信息确定，该第二证明信息基于该密文信息和该第一终端的密钥协商参数确定，该第一证明信息用于验证该监管设备的私钥是否可解密该密文信息，该第二证明信息用于验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥，该第一终端与该第二终端之间通过中继终端进行侧行通信。

第二方面，提供了一种密钥验证方法，应用于第一终端，该第一终端与第二终端之间通过中继终端进行侧行通信，该方法包括：

该第一终端发送第一信息；

其中，该第一信息包括该第一终端的密钥协商参数、密文信息和零知识证明信息，该密文信息基于监管设备的公钥、该第一终端与该第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该零知识证明信息包括第一证明信息和/或第二证明信息，该第一证明信息基于该密文信息确定，该第二证明信息基于该密文信息和该第一终端的密钥协商参数确定，该第一证明信息用于验证该监管设备的私钥是否可解密该密文信息，该第二证明信息用于验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥。

第三方面，提供了一种密钥获取方法，应用于监管设备，该方法包括：

该监管设备接收密文信息；其中，该密文信息基于该监管设备的公钥、第一终端与第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该第一终端与该第二终端之间通过中继终端进行侧行通信；

该监管设备根据该监管设备的私钥解密该密文信息，得到该第一终端与该第二终端协商确定的通信密钥。

第四方面，提供了一种验证设备，用于执行上述第一方面中的方法。

具体地，该验证设备包括用于执行上述第一方面中的方法的功能模块。

第五方面，提供了一种终端设备，用于执行上述第二方面中的方法。

具体地，该终端设备包括用于执行上述第二方面中的方法的功能模块。

第六方面，提供了一种监管设备，用于执行上述第三方面中的方法。

具体地，该监管设备包括用于执行上述第三方面中的方法的功能模块。

第七方面，提供了一种验证设备，包括处理器和存储器；该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，使得该验证设备执行上述第一方面中的方法。

第八方面，提供了一种终端设备，包括处理器和存储器；该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，使得该终端设备执行上述第二方面中的方法。

第九方面，提供了一种监管设备，包括处理器和存储器；该存储器用于存储计算机程序，该处理器用于调用并运行该存储器中存储的计算机程序，使得该监管设备执行上述第三方面中的方法。

第十方面，提供了一种装置，用于实现上述第一方面至第三方面中的任一方面中的方法。

具体地，该装置包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有该装置的设备执行如上述第一方面至第三方面中的任一方面中的方法。

第十一方面，提供了一种计算机可读存储介质，用于存储计算机程序，该计算机程序使得计算机执行上述第一方面至第三方面中的任一方面中的方法。

第十二方面，提供了一种计算机程序产品，包括计算机程序指令，所述计算机程序指令使得计算机执行上述第一方面至第三方面中的任一方面中的方法。

第十三方面，提供了一种计算机程序，当其在计算机上运行时，使得计算机执行上述第一方面至第三方面中的任一方面中的方法。

通过上述技术方案，验证设备可以基于零知识证明信息验证监管设备的私钥是否可解密密文信息，以及验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥，从而，可以确保监管设备在获取到密文信息之后可以解密得到第一终端与第二终端协商确定的通信密钥，进而，监管设备可以监听第一终端与第二终端之间的侧行通信。

附图说明

图 1 是本申请实施例应用的一种通信系统架构的示意性图。

图 2 是根据本申请实施例提供的一种密钥验证方法的示意性流程图。

图 3 是根据本申请实施例提供的第一终端与第二终端协商确定通信密钥的示意性流程图。

图 4 是根据本申请实施例提供的一种密钥获取方法的示意性流程图。

图 5 是根据本申请实施例提供的一种验证设备的示意性框图。

图 6 是根据本申请实施例提供的一种终端设备的示意性框图。

图 7 是根据本申请实施例提供的一种监管设备的示意性框图。

图 8 是根据本申请实施例提供的一种通信设备的示意性框图。

图 9 是根据本申请实施例提供的一种装置的示意性框图。

图 10 是根据本申请实施例提供的一种通信系统的示意性框图。

具体实施方式

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。针对本申请中的实施例，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，都属于本申请保护的范围。

本申请实施例的技术方案可以应用于各种通信系统，例如：全球移动通讯（Global System of Mobile communication，GSM）系统、码分多址（Code Division Multiple Access，CDMA）系统、宽带码分多址（Wideband Code Division Multiple Access，WCDMA）系统、通用分组无线业务（General Packet Radio Service，GPRS）、长期演进（Long Term Evolution，LTE）系统、先进的长期演进（Advanced long term evolution，LTE-A）系统、新无线（New Radio，NR）系统、NR 系统的演进系统、非授权频谱上的 LTE（LTE-based access to unlicensed spectrum，LTE-U）系统、非授权频谱上的 NR（NR-based access to unlicensed spectrum，NR-U）系统、非地面通信网络（Non-Terrestrial Networks，NTN）系统、通用移动通信系统（Universal Mobile Telecommunication System，UMTS）、无线局域网（Wireless Local Area Networks，WLAN）、物联网（internet of things，IoT）、无线保真（Wireless Fidelity，WiFi）、第五代通信（5th-Generation，5G）系统、第六代通信（6th-Generation，6G）系统或其他通信系统等。

通常来说，传统的通信系统支持的连接数有限，也易于实现，然而，随着通信技术的发展，移动通信系统将不仅支持传统的通信，还将支持例如，设备到设备（Device to Device，D2D）通信，机器到机器（Machine to Machine，M2M）通信，机器类型通信（Machine Type Communication，MTC），车辆间（Vehicle to Vehicle，V2V）通信，侧行（sidelink，SL）通信，车联网（Vehicle to everything，V2X）通信等，本申请实施例也可以应用于这些通信系统。

在一些实施例中，本申请实施例中的通信系统可以应用于载波聚合（Carrier Aggregation，CA）场景，也可以应用于双连接（Dual Connectivity，DC）场景，还可以应用于独立（Standalone，SA）布网场景，或者应用于非独立（Non-Standalone，NSA）布网场景。

在一些实施例中，本申请实施例中的通信系统可以应用于非授权频谱，其中，非授权频谱也可以认为是共享频谱；或者，本申请实施例中的通信系统也可以应用于授权频谱，其中，授权频谱也可以认为是非共享频谱。

在一些实施例中，本申请实施例中的通信系统可以应用于 FR1 频段（对应频段范围 410 MHz 到 7.125 GHz），也可以应用于 FR2 频段（对应频段范围 24.25 GHz 到 52.6 GHz），还可以应用于新的频段例如对应 52.6 GHz 到 71 GHz 频段范围或对应 71GHz 到 114.25 GHz 频段范围的高频频段。

本申请实施例结合终端设备（如第一终端、第二终端和中继终端）描述了各个实施例，其中，终端设备也可以称为用户设备（User Equipment，UE）、接入终端、用户单元、用户站、移动站、移动

台、远方站、远程终端、移动设备、用户终端、终端、无线通信设备、用户代理或用户装置等。

终端设备可以是WLAN中的站点（STATION，ST），可以是蜂窝电话、无绳电话、会话启动协议（Session Initiation Protocol，SIP）电话、无线本地环路（Wireless Local Loop，WLL）站、个人数字助理（Personal Digital Assistant，PDA）设备、具有无线通信功能的手持设备、计算设备或连接到无线调制解调器的其它处理设备、车载设备、可穿戴设备、下一代通信系统例如NR网络中的终端设备，或者未来演进的公共陆地移动网络（Public Land Mobile Network，PLMN）网络中的终端设备等。

在本申请实施例中，终端设备可以部署在陆地上，包括室内或室外、手持、穿戴或车载；也可以部署在水面上（如轮船等）；还可以部署在空中（例如飞机、气球和卫星上等）。

在本申请实施例中，终端设备可以是手机（Mobile Phone）、平板电脑（Pad）、带无线收发功能的电脑、虚拟现实（Virtual Reality，VR）终端设备、增强现实（Augmented Reality，AR）终端设备、工业控制（industrial control）中的无线终端设备、无人驾驶（self driving）中的无线终端设备、远程医疗（remote medical）中的无线终端设备、智能电网（smart grid）中的无线终端设备、运输安全（transportation safety）中的无线终端设备、智慧城市（smart city）中的无线终端设备或智慧家庭（smart home）中的无线终端设备、车载通信设备、无线通信芯片/专用集成电路（application specific integrated circuit，ASIC）/系统级芯片（System on Chip，SoC）等。

作为示例而非限定，在本申请实施例中，该终端设备还可以是可穿戴设备。可穿戴设备也可以称为穿戴式智能设备，是应用穿戴式技术对日常穿戴进行智能化设计、开发出可以穿戴的设备的总称，如眼镜、手套、手表、服饰及鞋等。可穿戴设备即直接穿在身上，或是整合到用户的衣服或配件的一种便携式设备。可穿戴设备不仅仅是一种硬件设备，更是通过软件支持以及数据交互、云端交互来实现强大的功能。广义穿戴式智能设备包括功能全、尺寸大、可不依赖智能手机实现完整或者部分的功能，例如：智能手表或智能眼镜等，以及只专注于某一类应用功能，需要和其它设备如智能手机配合使用，如各类进行体征监测的智能手环、智能首饰等。

在本申请实施例中，网络设备可以是用于与移动设备通信的设备，网络设备可以是WLAN中的接入点（Access Point，AP），GSM或CDMA中的基站（Base Transceiver Station，BTS），也可以是WCDMA中的基站（NodeB，NB），还可以是LTE中的演进型基站（Evolutional Node B，eNB或eNodeB），或者中继站或接入点，或者车载设备、可穿戴设备以及NR网络中的网络设备或者基站（gNB）或者发送接收点（Transmission Reception Point，TRP），或者未来演进的PLMN网络中的网络设备或者NTN网络中的网络设备等。

作为示例而非限定，在本申请实施例中，网络设备可以具有移动特性，例如网络设备可以为移动的设备。在一些实施例中，网络设备可以为卫星、气球站。例如，卫星可以为低地球轨道（low earth orbit，LEO）卫星、中地球轨道（medium earth orbit，MEO）卫星、地球同步轨道（geostationary earth orbit，GEO）卫星、高椭圆轨道（High Elliptical Orbit，HEO）卫星等。在一些实施例中，网络设备还可以为设置在陆地、水域等位置的基站。

在本申请实施例中，网络设备可以为小区提供服务，终端设备通过该小区使用的传输资源（例如，频域资源，或者说，频谱资源）与网络设备进行通信，该小区可以是网络设备（例如基站）对应的小区，小区可以属于宏基站，也可以属于小小区（Small cell）对应的基站，这里的小小区可以包括：城市小区（Metro cell）、微小区（Micro cell）、微微小区（Pico cell）、毫微微小区（Femto cell）等，这些小小区具有覆盖范围小、发射功率低的特点，适用于提供高速率的数据传输服务。

示例性的，本申请实施例应用的通信系统100可以如图1所示。该通信系统100可以包括第一终端110、中继终端120和第二终端130，第一终端110与第二终端130之间通过中继终端120进行侧行通信。中继终端120可以为特定的地理区域提供通信覆盖，并且可以与位于该覆盖区域内的终端设备进行通信。

在一些实施例中，该通信系统100还可以包括接入网设备、网络控制器、移动管理实体等其他网络实体，本申请实施例对此不作限定。

应理解，本申请实施例中网络/系统中具有通信功能的设备可称为通信设备。以图1示出的通信系统100为例，通信设备可包括具有通信功能的第一终端110、中继终端120和第二终端130，第一终端110、中继终端120和第二终端130可以为上文所述的具体设备，此处不再赘述；通信设备还可包括通信系统100中的其他设备，例如网络控制器、移动管理实体等其他网络实体，本申请实施例中对此不做限定。

应理解，本文中术语“系统”和“网络”在本文中常被可互换使用。本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本文中字符“/”，一般表示前后关联对象是

一种“或”的关系。

应理解，本文涉及第一通信设备和第二通信设备，第一通信设备可以是终端设备，例如手机，机器设施，用户前端设备（Customer Premise Equipment，CPE），工业设备，车辆等；第二通信设备可以是第一通信设备的对端通信设备，例如终端设备，手机，工业设备，车辆等。在本申请实施例中，第一通信设备可以是第一终端，且第二通信设备可以第二终端（即侧行通信）。

本申请的实施方式部分使用的术语仅用于对本申请的具体实施例进行解释，而非旨在限定本申请。本申请的说明书和权利要求书及所述附图中的术语“第一”、“第二”、“第三”和“第四”等是用于区别不同对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。

应理解，在本申请的实施例中提到的“指示”可以是直接指示，也可以是间接指示，还可以是表示具有关联关系。举例说明，A 指示 B，可以表示 A 直接指示 B，例如 B 可以通过 A 获取；也可以表示 A 间接指示 B，例如 A 指示 C，B 可以通过 C 获取；还可以表示 A 和 B 之间具有关联关系。

在本申请实施例的描述中，术语“对应”可表示两者之间具有直接对应或间接对应的关系，也可以表示两者之间具有关联关系，也可以是指示与被指示、配置与被配置等关系。

本申请实施例中，“预定义”或“预配置”可以通过在设备（例如，包括终端设备和网络设备）中预先保存相应的代码、表格或其他可用于指示相关信息的方式来实现，本申请对于其具体的实现方式不做限定。比如预定义可以是指协议中定义的。

本申请实施例中，所述“协议”可以指通信领域的标准协议，例如可以是对现有 LTE 协议、NR 协议、Wi-Fi 协议或者与之相关的其它通信系统相关的协议的演进，本申请不对协议类型进行限定。

为便于理解本申请实施例的技术方案，以下通过具体实施例详述本申请的技术方案。以下相关技术作为可选方案与本申请实施例的技术方案可以进行任意结合，其均属于本申请实施例的保护范围。本申请实施例包括以下内容中的至少部分内容。

监管设备可以监管第三代合作伙伴计划（The 3rd Generation Partnership Project，3GPP）通信场景，然而，并未涉及终端至终端中继（UE to UE Relay）场景的监管，按照行业发展趋势，针对终端至终端中继（UE to UE Relay）场景的监管在未来是不可避免的。届时，如果监管设备没有手段获取通信密钥，如加密密钥，就无法进行监听。

DH（Diffie-Hellman）密钥交换协议/算法是 3GPP 中进行端到端密钥协商时比较常见的技术手段，并可用于终端至终端中继（UE to UE Relay）场景下两个 UE 之间的密钥协商，确定通信密钥。然而，当前的终端至终端中继（UE to UE Relay）场景并未涉及监听的方案，如果通信密钥是直接在两个 UE 之间协商的，中继终端和其他设备无法获取通信密钥，也无法向监管设备提供通信密钥。

DH（Diffie-Hellman）密钥交换协议/算法是一种确保共享密钥安全穿越不安全网络的方法，由 Whitefield 与 Martin Hellman 在 1976 年提出。DH（Diffie-Hellman）密钥交换协议/算法的巧妙在于需要安全通信的双方在完全没有对方任何预先信息的条件下通过不安全信道建立起双方共享的密钥，可以用这个方法确定对称密钥，然后可以用这个密钥进行加密和解密。但是，需要注意的是，DH（Diffie-Hellman）密钥交换协议/算法只能用于密钥的交换，而不能进行消息的加密和解密。通信双方确定要用的密钥后，要使用其他对称密钥操作加密算法实现加密和解密消息。

Elgamal 算法是公钥密码算法，可用于 DH 密钥交换协议/算法中建立双方共享密钥。

为便于更好的理解本申请实施例，对本申请所解决的问题进行说明。

当前 3GPP 中如果在两个设备之间直接通过 DH 密钥交换协议/算法协商密钥，例如 3GPP 中的终端至终端中继（UE to UE Relay）场景，并未涉及监听的方案。

DH 密钥交换协议/算法如果没有恰当的算法辅助计算密钥，容易出现以下问题:

1、没有提供双方身份的任何信息;

2、DH 密钥交换协议/算法是计算密集性的，因此容易遭受阻塞性攻击，即对手请求大量的密钥，受攻击者花费了相对多的计算资源来求解无用的幂系数而不是在做真正的工作;

3、没办法防止重演攻击（Replay attack）;

4、容易遭受中间人的攻击。

具体例如，设备 A 与设备 B 之间通过设备 C 进行侧行通信，设备 C 在与设备 A 通信时扮演设备 B；设备 C 在与设备 B 通信时扮演设备 A。设备 A 和设备 B 都与设备 C 协商了一个密钥，然后设备 C 就可以监听和传递通信量。中间人的攻击按如下进行:

（1）设备 B 在给设备 A 的报文中发送设备 B 的公开密钥。

（2）设备 C 截获并解析该报文。设备 C 将设备 B 的公开密钥保存下来并给设备 A 发送报文，该报文具有设备 B 的用户标识（Identity，ID）但使用设备 C 的公开密钥 YC，仍按照好像是来自设备 B

的样子被发送出去。设备 A 收到设备 C 的报文后，将 YC 和设备 B 的用户 ID 存储在一块。类似地，设备 C 使用 YC 向设备 B 发送好像来自设备 A 的报文。

（3）设备 B 基于私有密钥 XB 和 YC 计算秘密密钥 K1。设备 A 基于私有密钥 XA 和 YC 计算秘密密钥 K2。设备 C 使用私有密钥 XC 和 YB 计算 K1，并使用 XC 和 YA 计算 K2。

（4）从现在开始，设备 C 就可以转发设备 A 发给设备 B 的报文或转发设备 B 发给设备 A 的报文，在途中根据需要修改它们的密文。使得设备 A 和设备 B 都不知道他们在和设备 C 共享通信。

基于上述问题，本申请提出了一种监管设备获取 UE to UE Relay 场景中监听所需的通信密钥的方案，监管设备可以通过零知识证明获取 UE to UE Relay 场景中监听所需的通信密钥，实现了对 UE to UE Relay 场景的监听。

以下通过具体实施例详述本申请的技术方案。

图 2 是根据本申请实施例的密钥验证方法 200 的示意性流程图。具体的，在该密钥验证方法 200 中，第一终端与第二终端之间通过中继终端进行侧行通信，如图 2 所示，该密钥验证方法 200 可以包括如下内容中的至少部分内容：

S210，该第一终端发送第一信息；其中，该第一信息包括该第一终端的密钥协商参数、密文信息和零知识证明信息，该密文信息基于监管设备的公钥、该第一终端与该第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该零知识证明信息包括第一证明信息和/或第二证明信息，该第一证明信息基于该密文信息确定，该第二证明信息基于该密文信息和该第一终端的密钥协商参数确定，该第一证明信息用于验证该监管设备的私钥是否可解密该密文信息，该第二证明信息用于验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥；

S220，验证设备接收该第一信息。

在本申请实施例中，验证设备可以基于零知识证明信息验证监管设备的私钥是否可解密密文信息，以及验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥，从而，可以确保监管设备在获取到密文信息之后可以解密得到第一终端与第二终端协商确定的通信密钥，进而，监管设备可以监听第一终端与第二终端之间的侧行通信。

在一些实施例中，该验证设备为该中继终端，或者，该验证设备为第三方网络设备。可选地，此种情况下，该零知识证明信息包括该第一证明信息和该第二证明信息。

具体例如，该验证设备为该中继终端，也即，该中继终端接收该第一终端发送的该第一信息，且该中继终端存储该第一信息所包含的全部信息，以及在验证通过之后，该中继终端将该第一信息所包含的部分或全部信息上传至区块链，以便监管设备可以获取监听所需的相关信息。其中，该第一信息通过以下之一承载：侧行控制信息（Sidelink Control Information，SCI）、PC5-无线资源控制（Radio Resource Control，RRC）。

具体例如，该验证设备为第三方网络设备，也即，该第三方网络设备接收该第一终端发送的该第一信息，且该第三方网络设备存储该第一信息所包含的全部信息，以及在验证通过之后，该第三方网络设备将该第一信息所包含的部分或全部信息上传至区块链，以便监管设备可以获取监听所需的相关信息。其中，该第三方网络设备与该第一终端之间的信息传递方式可以是无线通信传递，也可以是有线通信传递，也可以是通过其他媒介传递，本申请实施例对此并不限定。

具体例如，该验证设备为第三方网络设备，也即，该第一终端向该中继终端发送该第一信息，以及该第三方网络设备接收该中继终端发送的该第一信息，且该第三方网络设备存储该第一信息所包含的全部信息，以及在验证通过之后，该第三方网络设备将该第一信息所包含的部分或全部信息上传至区块链，以便监管设备可以获取监听所需的相关信息。其中，该第三方网络设备与该中继终端之间的信息传递方式可以是无线通信传递，也可以是有线通信传递，也可以是通过其他媒介传递，本申请实施例对此并不限定。

在一些实施例中，该验证设备为该监管设备。可选地，此种情况下，该零知识证明信息包括该第二证明信息。

具体例如，该第一终端向该中继终端发送该第一信息，以及，该监管设备接收该中继终端发送的该第一信息，或者，该监管设备通过区块链获取该第一信息。其中，该监管设备与该中继终端之间的信息传递方式可以是无线通信传递，也可以是有线通信传递，也可以是通过其他媒介传递，本申请实施例对此并不限定。

在一些实施例中，监管设备可以是得到监听授权的设备，具体例如，该监管设备可以是终端设备，也可以是接入网设备或基站，还可以是核心网设备，还可以是第三方网络设备，还可以是其他设备，本申请实施例对此并不限定。

在一些实施例中，该第一终端与该第二终端可以基于 DH 密钥交换协议/算法协商确定通信密钥。

在一些实施例中，本申请实施例除了应用于第一终端与第二终端之间通过中继终端进行侧行通信，即 UE to UE Relay 场景，也可以应用于其他场景。

例如，本申请实施例还可以应用于 UE（如第一终端）和 UE（如第二终端）直连通信的场景，此种场景下，验证设备可以是第三方网络设备或监管设备，也即，验证设备可以从第一终端或第二终端获取第一信息，在验证通过之后，监管设备可以获取第一终端与第二终端之间的通信密钥，第一终端和第二终端不需要知道监管设备的行为。

又例如，本申请实施例还可以应用于 UE（如第一终端）和零功耗设备（如第二终端）直连通信的场景，此种场景下，验证设备可以是第三方网络设备或监管设备，也即，验证设备可以从第一终端或第二终端获取第一信息，在验证通过之后，监管设备可以获取第一终端与第二终端之间的通信密钥，第一终端和第二终端不需要知道监管设备的行为。

再例如，本申请实施例还可以应用于 UE（如第一终端）和车载无线设备（如第二终端）直连通信的场景，此种场景下，验证设备可以是第三方网络设备或监管设备，也即，验证设备可以从第一终端或第二终端获取第一信息，在验证通过之后，监管设备可以获取第一终端与第二终端之间的通信密钥，第一终端和第二终端不需要知道监管设备的行为。

再例如，本申请实施例还可以应用于 UE（如第一终端）和感知设备（如第二终端）直连通信的场景，此种场景下，验证设备可以是第三方网络设备或监管设备，也即，验证设备可以从第一终端或第二终端获取第一信息，在验证通过之后，监管设备可以获取第一终端与第二终端之间的通信密钥，第一终端和第二终端不需要知道监管设备的行为。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥基于该第一终端生成的第二随机数和该第二终端的密钥协商参数确定。例如，第二终端可以将第二终端的密钥协商参数发送给第一终端，之后，第一终端生成第二随机数，并且，该第一终端基于该第二随机数和该第二终端的密钥协商参数确定该第一终端与该第二终端之间的通信密钥。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥基于该第二终端生成的第三随机数和该第一终端的密钥协商参数确定。例如，第一终端可以将第一终端的密钥协商参数发送给第二终端，之后，第二终端生成第三随机数，并且，该第二终端基于该第三随机数和该第一终端的密钥协商参数确定该第一终端与该第二终端之间的通信密钥。

在一些实施例中，该第一终端的密钥协商参数可以基于该第一终端生成的第二随机数确定。可选地，第一终端生成的第二随机数为 a，且第一终端的密钥协商参数为 $g_0^a \bmod p$，其中，$a \in Z^*$，Z^*为正整数域，g_0 为生成元，p 为随机质数，mod 表示取模运算。

在一些实施例中，该第二终端的密钥协商参数可以基于该第二终端生成的第三随机数确定。可选地，第二终端生成的第三随机数为 b，且第二终端的密钥协商参数为 $g_0^b \bmod p$，其中，$b \in Z^*$，Z^*为正整数域，g_0 为生成元，p 为随机质数，mod 表示取模运算。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥为 $g_0^{ab} \bmod p$;

其中，该第一终端的密钥协商参数为 $g_0^a \bmod p$，该第二终端的密钥协商参数为 $g_0^b \bmod p$，a 为该第一终端生成的第二随机数，b 为该第二终端生成的第三随机数，p 为随机质数，mod 表示取模运算。

在一些实施例中，该密文信息基于 Elgamal 算法加密得到。

在一些实施例中，该密文信息为（$(g_0^{ab} \bmod p)h^r, g_1^r$）；

其中，该密文信息的第一部分为$(g_0^{ab} \bmod p)h^r$，该密文信息的第二部分为 g_1^r;

其中，g_0 和 g_1 均为生成元，a 为该第一终端生成的第二随机数，b 为该第二终端生成的第三随机数，p 为随机质数，$h=g_1^x$，r 为该第一终端生成的第一随机数，g_1 和 h 均为该监管设备的公钥，x 为该监管设备的私钥，mod 表示取模运算。

例如，g_1 为 G 的一个生成元，G 为 g_1 的 q 阶循环群。

在一些实施例中，g_0 可以等于 g_1。例如，g_0 为 G 的一个生成元。

在一些实施例中，$x \in [1,q-1]$。

需要说明的是，该监管设备的私钥由监管设备保存，也即，x 由监管设备保存。

需要说明的是，g_0 和 p 为 DH 密钥交换协议/算法公开的信息。G、q、g_1 和 h 为 Elgamal 算法加密的公钥。

在一些实施例中，该第一终端生成该密文信息。具体的，第一终端生成第一随机数 r，$r \in [1,q-1]$，第一终端计算 $c_1=(g_0^{ab} \bmod p)h^r$，第一终端计算 $c_2= g_1^r$，（c_1, c_2）即为密文信息。

在一些实施例中，该监管设备可以解密该密文信息。具体的，监管设备计算 $s=c_2^x$，之后，计算 $m= c_1 \times s^{-1}$，m 即为解密后的信息，即 $m= g_0^{ab} \bmod p$，其中，$c_1=(g_0^{ab} \bmod p)h^r$，$c_2= g_1^r$，x 为监管设备的私钥。

在一些实施例中，第一终端与第二终端之间协商确定通信密钥的流程可以如图 3 所示，具体可以包括 S11 至 S18 中的部分或全部。

S11，第一终端生成随机数 a，以及基于随机数 a 计算第一终端的密钥协商参数 $g_0^a \bmod p$；

S12，第一终端向中继终端发送 $g_0^a \bmod p$；

S13，中继终端向第二终端发送 $g_0^a \bmod p$；

S14，第二终端生成随机数 b，以及基于随机数 b 计算第二终端的密钥协商参数 $g_0^b \bmod p$，基于随机数 b 和 $g_0^a \bmod p$ 计算第一终端与第二终端之间的通信密钥 $g_0^{ab} \bmod p$；

S15，第二终端向中继终端发送 $g_0^b \bmod p$ 和 $g_0^{ab} \bmod p$；

S16，中继终端保存 $g_0^b \bmod p$ 和 $g_0^{ab} \bmod p$；

S17，中继终端向第一终端发送 $g_0^b \bmod p$；

S18，第一终端基于随机数 a 和 $g_0^b \bmod p$ 计算第一终端与第二终端之间的通信密钥 $g_0^{ab} \bmod p$。

在一些实施例中，该验证设备根据该第一证明信息验证该监管设备的私钥是否可解密该密文信息；在该第一证明信息对应的验证结果指示该监管设备的私钥可解密该密文信息的情况下，该验证设备根据该第二证明信息验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥；在该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥的情况下，该验证设备向该监管设备发送该密文信息。

可选地，该验证设备可以通过区块链向该监管设备发送该密文信息。当然，该验证设备也可以通过其他方式向该监管设备发送该密文信息，本申请实施例对此并不限定。

在一些实现方式中，该验证设备为该中继终端，或者，该验证设备为第三方网络设备。也即，验证设备可以基于第一证明信息验证监管设备的私钥是否可解密密文信息，以及基于第二证明信息验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥，在验证通过的情况下，验证设备向监管设备发送密文信息，从而，监管设备可以通过其私钥解密密文信息，并获取第一终端与第二终端协商确定的通信密钥。

在一些实现方式中，该验证设备根据该第一证明信息进行零知识验证，以及在验证结果为该密文信息的第一部分中的第一随机数与该密文信息的第二部分中的第一随机数的取值相同的情况下，该第一证明信息对应的验证结果指示该监管设备的私钥可解密该密文信息。例如，密文信息为（c_1, c_2），也即，密文信息的第一部分为 c_1，密文信息的第二部分为 c_2，其中，$c_1=(g_0^{ab} \bmod p)h^r$，$c_2= g_1^r$，具体的，验证设备根据第一证明信息进行零知识验证，在验证结果为 c_1 和 c_2 中的随机数 r 相同时可以指示该监管设备的私钥可解密该密文信息。

在一些实现方式中，该验证设备根据该第二证明信息进行零知识验证，以及在验证结果为该密文信息中解密得到的密钥中的第二随机数与该第一终端的密钥协商参数中的第二随机数的取值相同的情况下，该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥。例如，密文信息中解密得到的密钥为 $g_0^{ab} \bmod p$，第一终端的密钥协商参数为 $g_0^a \bmod p$，具体的，验证设备根据第二证明信息进行零知识验证，在验证结果为 $g_0^{ab} \bmod p$ 和 $g_0^a \bmod p$ 中的随机数 a 相同时可以指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥。

在一些实施例中，该验证设备根据该监管设备的私钥解密该密文信息；该验证设备根据该第二证明信息验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥；在该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥的情况下，该验证设备根据该监管设备的私钥解密该密文信息，以获取该第一终端与该第二终端协商确定的通信密钥。

可选地，该验证设备接收该中继设备发送的该第一信息。当然，该验证设备也可以通过其他设备获取该第一信息，本申请实施例对此并不限定。

在一些实现方式中，该验证设备为该监管设备。也即，该监管设备根据该监管设备的私钥解密该密文信息；以及该监管设备根据该第二证明信息验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥；在该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥的情况下，该监管设备根据该监管设备的私钥解密该密文信息，以获取该第一终端与该第二终端协商确定的通信密钥。

在一些实现方式中，该验证设备根据该第二证明信息进行零知识验证，以及在验证结果为该密文信息中解密得到的密钥中的第二随机数与该第一终端的密钥协商参数中的第二随机数的取值相同的情况下，该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终

端协商确定的通信密钥。例如，密文信息中解密得到的密钥为 $g_0^{ab} \bmod p$，第一终端的密钥协商参数为 $g_0^a \bmod p$，具体的，验证设备根据第二证明信息进行零知识验证，在验证结果为 $g_0^{ab} \bmod p$ 和 $g_0^a \bmod p$ 中的随机数 a 相同时可以指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥。

在一些实施例中，本申请实施例所使用的零知识证明为线性等式证明，其中，线性等式证明可以如公式 1 所示。

$$\mathrm{POK}\left\{(x_1,\mathrm{L}\ ,x_l):\mathrm{y}=\sum_{i=1}^{l} g_i^{x_i},\sum_{i=1}^{l} a_i x_i=c\right\} \qquad \text{公式 1}$$

其中，在线性等式证明算法中，$c, a_1, \cdots, a_l$ 为公开数值，证明者在不泄露 $x_1,\mathrm{L}\ ,x_l$ 情况下，使得验证者确信其拥有 $x_1,\mathrm{L}\ ,x_l$ 且满足 $\sum_{i=1}^{l} a_i x_i = c$。

具体的，证明者向验证者证明元素 y 是（$x_1,\mathrm{L}\ ,x_l$）以 $g_1,\mathrm{L}\ ,g_l \in \mathrm{G}$ 为底的离散对数值，且满足线性等式 $\sum_{i=1}^{l} a_i x_i = c$，其中，c 与 a_i 为公开值。例如，证明者可以是第一终端，验证者可以是验证设备。

在一些实施例中，证明密文信息（c_1, c_2）中 c_1 和 c_2 中的随机数 r 相等，其中，$c_1=(g_0^{ab} \bmod p)h^r$，$c_2= g_1^r$。具体的，等式构造：令 c_1 中 $g_0^a \bmod p$ 为 g、b 为 m、h 为 y、r 为 r_1，以及令 c_2 中 g_1 为 h、r 为 r_2，也即，$c_1 = g^m y^{r_1}$，$c_2 = h^{r_2}$，构造等式 $x= c_1 \times c_2$，由此证明，$0\cdot \mathrm{m}+1\cdot r_1+(-1)\cdot r_2=0$（即证明 $r_1=r_2$）。

证明方：从 Z^* 中选取随机数 v_1,v_2,v_3；计算承诺 $t = g^{v_1} y^{v_2} h^{v_3}$，满足 $0\cdot v_1+1\cdot v_2+(-1)\cdot v_3=0$；计算挑战 $c=\mathrm{H}(g,y,h,t,x)$；计算响应 $s_1 = v_1 - cm$，$s_2 = v_2 - cr_1$，$s_3 = v_3 - cr_2$，构造证明信息 (s_1,s_2,s_3,t)，即第一证明信息为 (s_1,s_2,s_3,t)，并将证明信息 (s_1,s_2,s_3,t) 发送给验证方。

验证方：检查等式 $g^{s_1} y^{s_2} h^{s_3} x^c = t$ 是否成立（当且仅当 $x = c_1 \times c_2$ 时成立）；检查等式 $0\cdot s_1+1\cdot s_2+(-1)\cdot s_3=0$ 是否成立（当且仅当 $r_1 = r_2$ 时成立）。也即，当且仅当 $x = c_1 \times c_2$ 时，等式 $g^{s_1} y^{s_2} h^{s_3} x^c = t$ 成立，以及当且仅当 $r_1 = r_2$ 时 $0\cdot s_1+1\cdot s_2+(-1)\cdot s_3=0$ 成立，换句话说，在 $0\cdot s_1+1\cdot s_2+(-1)\cdot s_3=0$ 成立的情况下，验证结果为 c_1 和 c_2 中的随机数 r 相同，此时可以指示监管设备的私钥可解密密文信息。

在一些实施例中，密文信息为（c_1, c_2），其中，$c_1=(g_0^{ab} \bmod p)h^r$，$c_2= g_1^r$，证明 $(g_0^{ab} \bmod p)h^r$ 和 $g_0^a \bmod p$ 中的随机数 a 相等。具体的，等式构造：令 $(g_0^{ab} \bmod p)h^r$ 中 h 为 g、r 为 m、g_0^b 为 y、a 为 r_1，以及令 $g_0^a \bmod p$ 中 g_0 为 h、a 为 r_2，也即，$c_1 = g^m y^{r_1}$，$c_2 = h^{r_2}$，构造等式 $x= c_1 \times c_2$，由此证明，$0\cdot \mathrm{m}+1\cdot r_1+(-1)\cdot r_2=0$（即证明 $r_1=r_2$）。

证明方：从 Z^* 中选取随机数 v_1,v_2,v_3；计算承诺 $t = g^{v_1} y^{v_2} h^{v_3}$，满足 $0\cdot v_1+1\cdot v_2+(-1)\cdot v_3=0$；计算挑战 $c=\mathrm{H}(g,y,h,t,x)$；计算响应 $s_1 = v_1 - cm$，$s_2 = v_2 - cr_1$，$s_3 = v_3 - cr_2$，构造证明信息 (s_1,s_2,s_3,t)，即第二证明信息为 (s_1,s_2,s_3,t)，并将证明信息 (s_1,s_2,s_3,t) 发送给验证方。

验证方：检查等式 $g^{s_1} y^{s_2} h^{s_3} x^c = t$ 是否成立（当且仅当 $x = c_1 \times c_2$ 时成立）；检查等式 $0\cdot s_1+1\cdot s_2+(-1)\cdot s_3=0$ 是否成立（当且仅当 $r_1 = r_2$ 时成立）。也即，当且仅当 $x = c_1 \times c_2$ 时，等式 $g^{s_1} y^{s_2} h^{s_3} x^c = t$ 成立，以及当且仅当 $r_1 = r_2$ 时 $0\cdot s_1+1\cdot s_2+(-1)\cdot s_3=0$ 成立，换句话说，在 $0\cdot s_1+1\cdot s_2+(-1)\cdot s_3=0$ 成立的情况下，验证结果为 $(g_0^{ab} \bmod p)h^r$ 和 $g_0^a \bmod p$ 中的随机数 a 相等，此时可以指示密文信息中解密得到的密钥为第一终端与第二终端协商确定的通信密钥。

因此，在本申请实施例中，验证设备可以基于零知识证明信息验证监管设备的私钥是否可解密密文信息，以及验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥，从而，

可以确保监管设备在获取到密文信息之后可以解密得到第一终端与第二终端协商确定的通信密钥，进而，监管设备可以监听第一终端与第二终端之间的侧行通信。

上文结合图 2 至图 3，详细描述了本申请的验证设备侧实施例，下文结合图 4，详细描述本申请的监管设备侧实施例，应理解，监管设备侧实施例与验证设备侧实施例相互对应，类似的描述可以参照验证设备侧实施例。

图 4 是根据本申请实施例的密钥获取方法 300 的示意性流程图。具体的，如图 4 所示，该密钥获取方法 300 可以包括如下内容中的至少部分内容:

S310，监管设备接收密文信息；其中，该密文信息基于该监管设备的公钥、第一终端与第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该第一终端与该第二终端之间通过中继终端进行侧行通信;

S320，该监管设备根据该监管设备的私钥解密该密文信息，得到该第一终端与该第二终端协商确定的通信密钥。

在一些实施例中，该监管设备接收零知识证明信息验证通过的确认信息。具体的，如上述密钥验证方法 200 所述，验证设备基于零知识证明信息验证监管设备的私钥是否可解密密文信息，以及验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥，在验证通过之后，验证设备可以发送验证通过的确认信息。

在一些实施例中，该监管设备在验证该确认信息有效后解密该密文信息。也即，上述 S320 在该监管设备在验证该确认信息有效后执行。

在一些实施例中，该监管设备通过区块链接收该密文信息和/或该确认信息。当然，该监管设备也可以通过其他方式获取该密文信息。可选地，该密文信息和/或改确认信息可以由验证设备提供。

在本申请实施例中，验证设备可以基于零知识证明信息验证监管设备的私钥是否可解密密文信息，以及验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥，从而，可以确保监管设备在获取到密文信息之后可以解密得到第一终端与第二终端协商确定的通信密钥，进而，监管设备可以监听第一终端与第二终端之间的侧行通信。

可选地，验证设备可以在验证通过后生成确认信息，以及，将验证通过的确认信息发送给监管设备，或者，将验证通过的确认信息上传区块链，以便监管设备通过区块链获取该确认信息。

在一些实施例中，该验证设备为该中继终端，或者，该验证设备为第三方网络设备。

具体例如，该验证设备为该中继终端，也即，该中继终端接收该第一终端发送的第一信息，且该中继终端存储该第一信息所包含的全部信息，以及在验证通过之后，该中继终端将密文信息上传至区块链，以便监管设备可以获取密文信息。可选的，中继设备和监管设备之间的信息传递方式可以是无线通信传递，也可以是有线通信传递，也可以是通过其他媒介传递，本申请实施例对此并不限定，

其中，该第一信息包括该第一终端的密钥协商参数、密文信息和零知识证明信息，该密文信息基于监管设备的公钥、该第一终端与该第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该零知识证明信息包括第一证明信息和/或第二证明信息，该第一证明信息基于该密文信息确定，该第二证明信息基于该密文信息和该第一终端的密钥协商参数确定，该第一证明信息用于验证该监管设备的私钥是否可解密该密文信息，该第二证明信息用于验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥。该第一信息通过以下之一承载: SCI、PC5- RRC。

具体例如，该验证设备为第三方网络设备，也即，该第三方网络设备接收该第一终端发送的该第一信息，且该第三方网络设备存储该第一信息所包含的全部信息，以及在验证通过之后，该第三方网络设备将该第一信息所包含的密文信息上传至区块链，以便监管设备可以获取密文信息。其中，该第三方网络设备与该第一终端之间的信息传递方式可以是无线通信传递，也可以是有线通信传递，也可以是通过其他媒介传递，本申请实施例对此并不限定。

具体例如，该验证设备为第三方网络设备，也即，该第一终端向该中继终端发送该第一信息，以及该第三方网络设备接收该中继终端发送的该第一信息，且该第三方网络设备存储该第一信息所包含的全部信息，以及在验证通过之后，该第三方网络设备将该第一信息所包含的密文信息上传至区块链，以便监管设备可以获取密文信息。其中，该第三方网络设备与该中继终端之间的信息传递方式可以是无线通信传递，也可以是有线通信传递，也可以是通过其他媒介传递，本申请实施例对此并不限定。

在一些实施例中，监管设备可以是得到监听授权的设备，该监管设备可以是终端设备，也可以是接入网设备，还可以是核心网设备，还可以是其他设备，本申请实施例对此并不限定。

在一些实施例中，该第一终端与该第二终端可以基于 DH 密钥交换协议/算法协商确定通信密钥。

在一些实施例中，本申请实施例除了应用于第一终端与第二终端之间通过中继终端进行侧行通信，即 UE to UE Relay 场景，也可以应用于其他场景。

例如，本申请实施例还可以应用于 UE（如第一终端）和 UE（如第二终端）直连通信的场景，此种场景下，验证设备可以是第三方网络设备或监管设备，也即，验证设备可以从第一终端或第二终端获取第一信息，在验证通过之后，监管设备可以获取第一终端与第二终端之间的通信密钥，第一终端和第二终端不需要知道监管设备的行为。

又例如，本申请实施例还可以应用于 UE（如第一终端）和零功耗设备（如第二终端）直连通信的场景，此种场景下，验证设备可以是第三方网络设备或监管设备，也即，验证设备可以从第一终端或第二终端获取第一信息，在验证通过之后，监管设备可以获取第一终端与第二终端之间的通信密钥，第一终端和第二终端不需要知道监管设备的行为。

再例如，本申请实施例还可以应用于 UE（如第一终端）和车载无线设备（如第二终端）直连通信的场景，此种场景下，验证设备可以是第三方网络设备或监管设备，也即，验证设备可以从第一终端或第二终端获取第一信息，在验证通过之后，监管设备可以获取第一终端与第二终端之间的通信密钥，第一终端和第二终端不需要知道监管设备的行为。

再例如，本申请实施例还可以应用于 UE（如第一终端）和感知设备（如第二终端）直连通信的场景，此种场景下，验证设备可以是第三方网络设备或监管设备，也即，验证设备可以从第一终端或第二终端获取第一信息，在验证通过之后，监管设备可以获取第一终端与第二终端之间的通信密钥，第一终端和第二终端不需要知道监管设备的行为。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥基于该第一终端生成的第二随机数和该第二终端的密钥协商参数确定。例如，第二终端可以将第二终端的密钥协商参数发送给第一终端，之后，第一终端生成第二随机数，并且，该第一终端基于该第二随机数和该第二终端的密钥协商参数确定该第一终端与该第二终端之间的通信密钥。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥基于该第二终端生成的第三随机数和该第一终端的密钥协商参数确定。例如，第一终端可以将第一终端的密钥协商参数发送给第二终端，之后，第二终端生成第三随机数，并且，该第二终端基于该第三随机数和该第一终端的密钥协商参数确定该第一终端与该第二终端之间的通信密钥。

在一些实施例中，该第一终端的密钥协商参数可以基于该第一终端生成的第二随机数确定。可选地，第一终端生成的第二随机数为 a，且第一终端的密钥协商参数为 $g_0^a \bmod p$，其中，$a \in Z^*$，Z^*为正整数域，g_0 为生成元，p 为随机质数，mod 表示取模运算。

在一些实施例中，该第二终端的密钥协商参数可以基于该第二终端生成的第三随机数确定。可选地，第二终端生成的第三随机数为 b，且第二终端的密钥协商参数为 $g_0^b \bmod p$，其中，$b \in Z^*$，Z^*为正整数域，g_0 为生成元，p 为随机质数，mod 表示取模运算。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥为 $g_0^{ab} \bmod p$;

其中，该第一终端的密钥协商参数为 $g_0^a \bmod p$，该第二终端的密钥协商参数为 $g_0^b \bmod p$，a 为该第一终端生成的第二随机数，b 为该第二终端生成的第三随机数，p 为随机质数，mod 表示取模运算。

在一些实施例中，该密文信息基于 Elgamal 算法加密得到。

在一些实施例中，该密文信息为（$(g_0^{ab} \bmod p)h^r, g_1^r$）；

其中，该密文信息的第一部分为$(g_0^{ab} \bmod p)h^r$，该密文信息的第二部分为 g_1^r;

其中，g_0 和 g_1 均为生成元，a 为该第一终端生成的第二随机数，b 为该第二终端生成的第三随机数，p 为随机质数，$h=g_1^x$，r 为该第一终端生成的第一随机数，g_1 和 h 均为该监管设备的公钥，x 为该监管设备的私钥，mod 表示取模运算。

例如，g_1 为 G 的一个生成元，G 为 g_1 的 q 阶循环群。

在一些实施例中，g_0 可以等于 g_1。例如，g_0 为 G 的一个生成元。

在一些实施例中，$x \in [1,q-1]$。

需要说明的是，该监管设备的私钥由监管设备保存，也即，x 由监管设备保存。

需要说明的是，g_0 和 p 为 DH 密钥交换协议/算法公开的信息。G、q、g_1 和 h 为 Elgamal 算法加密的公钥。

在一些实施例中，该第一终端生成该密文信息。具体的，第一终端生成第一随机数 r，$r \in [1,q-1]$，第一终端计算 $c_1=(g_0^{ab} \bmod p)h^r$，第一终端计算 $c_2= g_1^r$，（c_1, c_2）即为密文信息。

在一些实施例中，该监管设备可以解密该密文信息。具体的，监管设备计算 $s=c_2^x$，之后，计算 $m= c_1 \times s^{-1}$，m 即为解密后的信息，即 $m= g_0^{ab} \bmod p$，其中，$c_1=(g_0^{ab} \bmod p)h^r$，$c_2= g_1^r$，x 为监管设备的私钥。

因此，在本申请实施例中，验证设备可以基于零知识证明信息验证监管设备的私钥是否可解密密文信息，以及验证密文信息中解密得到的密钥是否为第一终端与第二终端协商确定的通信密钥，从而，

可以确保监管设备在获取到密文信息之后可以解密得到第一终端与第二终端协商确定的通信密钥，进而，监管设备可以监听第一终端与第二终端之间的侧行通信。

上文结合图 2 至图 4，详细描述了本申请的方法实施例，下文结合图 5 至图 10，详细描述本申请的装置实施例，应理解，装置实施例与方法实施例相互对应，类似的描述可以参照方法实施例。

图 5 示出了根据本申请实施例的验证设备 400 的示意性框图。如图 5 所示，该验证设备 400 包括：

通信单元 410，用于接收第一信息；

其中，该第一信息包括第一终端的密钥协商参数、密文信息和零知识证明信息，该密文信息基于监管设备的公钥、该第一终端与第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该零知识证明信息包括第一证明信息和第二证明信息，该第一证明信息基于该密文信息确定，该第二证明信息基于该密文信息和/或该第一终端的密钥协商参数确定，该第一证明信息用于验证该监管设备的私钥是否可解密该密文信息，该第二证明信息用于验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥，该第一终端与该第二终端之间通过中继终端进行侧行通信。

在一些实施例中，该验证设备 400 还包括：处理单元 420；

该处理单元 420 用于根据该第一证明信息验证该监管设备的私钥是否可解密该密文信息；

在该第一证明信息对应的验证结果指示该监管设备的私钥可解密该密文信息的情况下，该处理单元 420 用于根据该第二证明信息验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥；

在该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥的情况下，该通信单元 410 还用于向该监管设备发送该密文信息。

在一些实施例中，该通信单元 410 具体用于：

通过区块链向该监管设备发送该密文信息。

在一些实施例中，该验证设备为该中继终端，或者，该验证设备为第三方网络设备。

在一些实施例中，该验证设备 400 还包括：处理单元 420；

该处理单元 420 用于根据该监管设备的私钥解密该密文信息；

该处理单元 420 用于根据该第二证明信息验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥；

在该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥的情况下，该处理单元 420 用于获取该第一终端与该第二终端协商确定的通信密钥。

在一些实施例中，该通信单元 410 具体用于：

接收该中继设备发送的该第一信息。

在一些实施例中，该验证设备为该监管设备。

在一些实施例中，该处理单元 420 具体用于：

根据该第一证明信息进行零知识验证，以及在验证结果为该密文信息的第一部分中的第一随机数与该密文信息的第二部分中的第一随机数的取值相同的情况下，该第一证明信息对应的验证结果指示该监管设备的私钥可解密该密文信息。

在一些实施例中，该处理单元 420 具体用于：

根据该第二证明信息进行零知识验证，以及在验证结果为该密文信息中解密得到的密钥中的第二随机数与该第一终端的密钥协商参数中的第二随机数的取值相同的情况下，该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥基于该第一终端生成的第二随机数和该第二终端的密钥协商参数确定；和/或，

该第一终端与该第二终端协商确定的通信密钥基于该第二终端生成的第三随机数和该第一终端的密钥协商参数确定。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥为 $g_0^{ab} \bmod p$；

其中，该第一终端的密钥协商参数为 $g_0^{a} \bmod p$，该第二终端的密钥协商参数为 $g_0^{b} \bmod p$，a 为该第二随机数，b 为该第三随机数，p 为随机质数，mod 表示取模运算。

在一些实施例中，该密文信息为 $((g_0^{ab} \bmod p)h^r, g_1^r)$；

其中，该密文信息的第一部分为 $(g_0^{ab} \bmod p)h^r$，该密文信息的第二部分为 g_1^r；

其中，g_0 和 g_1 均为生成元，a 为该第一终端生成的第二随机数，b 为该第二终端生成的第三随机数，p 为随机质数，$h=g_1^x$，r 为该第一终端生成的第一随机数，g_1 和 h 均为该监管设备的公钥，x 为

该监管设备的私钥，mod 表示取模运算。

在一些实施例中，上述通信单元可以是通信接口或收发器，或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

应理解，根据本申请实施例的验证设备 400 可对应于本申请方法实施例中的验证设备，并且验证设备 400 中的各个单元的上述和其它操作和/或功能分别为了实现图 2 所示方法 200 中验证设备的相应流程，为了简洁，在此不再赘述。

图 6 示出了根据本申请实施例的终端设备 500 的示意性框图。该终端设备 500 为第一终端，所述第一终端与第二终端之间通过中继终端进行侧行通信，如图 6 所示，该终端设备 500 包括:

通信单元 510，用于发送第一信息;

其中，该第一信息包括该第一终端的密钥协商参数、密文信息和零知识证明信息，该密文信息基于监管设备的公钥、该第一终端与该第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该零知识证明信息包括第一证明信息和/或第二证明信息，该第一证明信息基于该密文信息确定，该第二证明信息基于该密文信息和该第一终端的密钥协商参数确定，该第一证明信息用于验证该监管设备的私钥是否可解密该密文信息，该第二证明信息用于验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥。

在一些实施例中，该第一证明信息用于验证该监管设备的私钥是否可解密该密文信息，包括:

该第一证明信息用于验证设备进行零知识验证，以及在验证结果为该密文信息的第一部分中的第一随机数与该密文信息的第二部分中的第一随机数的取值相同的情况下，该第一证明信息对应的验证结果指示该监管设备的私钥可解密该密文信息。

在一些实施例中，该第二证明信息用于验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥，包括:

该第二证明信息用于该验证设备进行零知识验证，以及在验证结果为该密文信息中解密得到的密钥中的第二随机数与该第一终端的密钥协商参数中的第二随机数的取值相同的情况下，该第二证明信息对应的验证结果指示该密文信息中解密得到的密钥为该第一终端与该第二终端协商确定的通信密钥。

在一些实施例中，该验证设备为该中继终端，或者，该验证设备为第三方网络设备，或者，该验证设备为该监管设备。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥基于该第一终端生成的第二随机数和该第二终端的密钥协商参数确定；和/或，

该第一终端与该第二终端协商确定的通信密钥基于该第二终端生成的第三随机数和该第一终端的密钥协商参数确定。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥为 $g_0^{ab} \bmod p$;

其中，该第一终端的密钥协商参数为 $g_0^{a} \bmod p$，该第二终端的密钥协商参数为 $g_0^{b} \bmod p$，a 为该第二随机数，b 为该第三随机数，p 为随机质数，mod 表示取模运算。

在一些实施例中，该密文信息为（$(g_0^{ab} \bmod p)h^r, g_1^r$）;

其中，该密文信息的第一部分为$(g_0^{ab} \bmod p)h^r$，该密文信息的第二部分为 g_1^r;

其中，g_0 和 g_1 均为生成元，a 为该第一终端生成的第二随机数，b 为该第二终端生成的第三随机数，p 为随机质数，$h=g_1^x$，r 为该第一终端生成的第一随机数，g_1 和 h 均为该监管设备的公钥，x 为该监管设备的私钥，mod 表示取模运算。

在一些实施例中，上述通信单元可以是通信接口或收发器，或者是通信芯片或者片上系统的输入输出接口。

应理解，根据本申请实施例的终端设备 500 可对应于本申请方法实施例中的第一终端，并且终端设备 500 中的各个单元的上述和其它操作和/或功能分别为了实现图 2 所示方法 200 中第一终端的相应流程，为了简洁，在此不再赘述。

图 7 示出了根据本申请实施例的监管设备 600 的示意性框图。如图 7 所示，该监管设备 600 包括:

通信单元 610，用于接收密文信息；其中，该密文信息基于该监管设备的公钥、第一终端与第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该第一终端与该第二终端之间通过中继终端进行侧行通信;

处理单元 620，用于根据该监管设备的私钥解密该密文信息，得到该第一终端与该第二终端协商确定的通信密钥。

在一些实施例中，该通信单元 610 具体用于:

通过区块链接收该密文信息。

在一些实施例中，该通信单元 610 还用于接收零知识证明信息验证通过的确认信息，其中，该零知识证明信息用于验证该监管设备的私钥是否可解密该密文信息，以及验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥；

该处理单元 620 具体用于：

在验证该确认信息有效之后，根据该监管设备的私钥解密该密文信息。

在一些实施例中，该通信单元 610 具体用于：

通过区块链接收该零知识证明信息验证通过的该确认信息。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥基于该第一终端生成的第二随机数和该第二终端的密钥协商参数确定；和/或，

该第一终端与该第二终端协商确定的通信密钥基于该第二终端生成的第三随机数和该第一终端的密钥协商参数确定。

在一些实施例中，该第一终端与该第二终端协商确定的通信密钥为 $g_0^{ab} \bmod p$；

其中，该第一终端的密钥协商参数为 $g_0^{a} \bmod p$，该第二终端的密钥协商参数为 $g_0^{b} \bmod p$，a 为该第二随机数，b 为该第三随机数，p 为随机质数，mod 表示取模运算。

在一些实施例中，该密文信息为（$(g_0^{ab} \bmod p)h^r, g_1^r$）；

其中，该密文信息的第一部分为$(g_0^{ab} \bmod p)h^r$，该密文信息的第二部分为 g_1^r；

其中，g_0 和 g_1 均为生成元，a 为该第一终端生成的第二随机数，b 为该第二终端生成的第三随机数，p 为随机质数，$h=g_1^x$，r 为该第一终端生成的第一随机数，g_1 和 h 均为该监管设备的公钥，x 为该监管设备的私钥，mod 表示取模运算。

在一些实施例中，上述通信单元可以是通信接口或收发器，或者是通信芯片或者片上系统的输入输出接口。上述处理单元可以是一个或多个处理器。

应理解，根据本申请实施例的监管设备 600 可对应于本申请方法实施例中的监管设备，并且监管设备 600 中的各个单元的上述和其它操作和/或功能分别为了实现图 4 所示方法 300 中监管设备的相应流程，为了简洁，在此不再赘述。

图 8 是本申请实施例提供的一种通信设备 700 示意性结构图。图 8 所示的通信设备 700 包括处理器 710，处理器 710 可以从存储器中调用并运行计算机程序，以实现本申请实施例中的方法。

在一些实施例中，如图 8 所示，通信设备 700 还可以包括存储器 720。其中，处理器 710 可以从存储器 720 中调用并运行计算机程序，以实现本申请实施例中的方法。

其中，存储器 720 可以是独立于处理器 710 的一个单独的器件，也可以集成在处理器 710 中。

在一些实施例中，如图 8 所示，通信设备 700 还可以包括收发器 730，处理器 710 可以控制该收发器 730 与其他设备进行通信，具体地，可以向其他设备发送信息或数据，或接收其他设备发送的信息或数据。

其中，收发器 730 可以包括发射机和接收机。收发器 730 还可以进一步包括天线，天线的数量可以为一个或多个。

在一些实施例中，处理器 710 可以实现验证设备中的处理单元的功能，或者，处理器 710 可以实现终端设备中的处理单元的功能，或者，处理器 710 可以实现监管设备中的处理单元的功能，为了简洁，在此不再赘述。

在一些实施例中，收发器 730 可以实现终端设备中的通信单元的功能，为了简洁，在此不再赘述。

在一些实施例中，收发器 730 可以实现验证设备中的通信单元的功能，为了简洁，在此不再赘述。

在一些实施例中，收发器 730 可以实现监管设备中的通信单元的功能，为了简洁，在此不再赘述。

在一些实施例中，该通信设备 700 具体可为本申请实施例的验证设备，并且该通信设备 700 可以实现本申请实施例的各个方法中由验证设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该通信设备 700 具体可为本申请实施例的终端设备，并且该通信设备 700 可以实现本申请实施例的各个方法中由终端设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该通信设备 700 具体可为本申请实施例的监管设备，并且该通信设备 700 可以实现本申请实施例的各个方法中由监管设备实现的相应流程，为了简洁，在此不再赘述。

图 9 是本申请实施例的装置的示意性结构图。图 9 所示的装置 800 包括处理器 810，处理器 810 可以从存储器中调用并运行计算机程序，以实现本申请实施例中的方法。

在一些实施例中，如图 9 所示，装置 800 还可以包括存储器 820。其中，处理器 810 可以从存储器 820 中调用并运行计算机程序，以实现本申请实施例中的方法。

其中，存储器 820 可以是独立于处理器 810 的一个单独的器件，也可以集成在处理器 810 中。

在一些实施例中，该装置 800 还可以包括输入接口 830。其中，处理器 810 可以控制该输入接口

830 与其他设备或芯片进行通信，具体地，可以获取其他设备或芯片发送的信息或数据。可选地，处理器 810 可以位于芯片内或芯片外。

在一些实施例中，处理器 810 可以实现终端设备中的处理单元的功能，或者，处理器 810 可以实现验证设备中的处理单元的功能，或者，处理器 810 可以实现监管设备中的处理单元的功能，为了简洁，在此不再赘述。

在一些实施例中，输入接口 830 可以实现终端设备中的通信单元的功能，或者，输入接口 830 可以实现验证设备中的通信单元的功能，或者，输入接口 830 可以实现监管设备中的通信单元的功能。

在一些实施例中，该装置 800 还可以包括输出接口 840。其中，处理器 810 可以控制该输出接口 840 与其他设备或芯片进行通信，具体地，可以向其他设备或芯片输出信息或数据。可选地，处理器 810 可以位于芯片内或芯片外。

在一些实施例中，输出接口 840 可以实现终端设备中的通信单元的功能，或者，输出接口 840 可以实现监管设备中的通信单元的功能，或者，输出接口 840 可以实现验证设备中的通信单元的功能。

在一些实施例中，该装置可应用于本申请实施例中的验证设备，并且该装置可以实现本申请实施例的各个方法中由验证设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该装置可应用于本申请实施例中的监管设备，并且该装置可以实现本申请实施例的各个方法中由监管设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该装置可应用于本申请实施例中的终端设备，并且该装置可以实现本申请实施例的各个方法中由终端设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，本申请实施例提到的装置也可以是芯片。例如可以是系统级芯片，系统芯片，芯片系统或片上系统芯片等。

图 10 是本申请实施例提供的一种通信系统 900 的示意性框图。如图 10 所示，该通信系统 900 包括第一终端 910、中继终端 920、第二终端 930 和监管设备 940。

其中，该第一终端 910 可以用于实现上述方法中由第一终端实现的相应的功能，该中继终端 920 可以用于实现上述方法中由中继终端实现的相应的功能，以及该监管设备 940 可以用于实现上述方法中由监管设备实现的相应的功能，为了简洁，在此不再赘述。

应理解，本申请实施例的处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理器（Digital Signal Processor，DSP）、专用集成电路（Application Specific Integrated Circuit，ASIC）、现成可编程门阵列（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。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

可以理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（Read-Only Memory，ROM）、可编程只读存储器（Programmable ROM，PROM）、可擦除可编程只读存储器（Erasable PROM，EPROM）、电可擦除可编程只读存储器（Electrically EPROM，EEPROM）或闪存。易失性存储器可以是随机存取存储器（Random Access Memory，RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态随机存取存储器（Static RAM，SRAM）、动态随机存取存储器（Dynamic RAM，DRAM）、同步动态随机存取存储器（Synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（Double Data Rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（Enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（Synchlink DRAM，SLDRAM）和直接内存总线随机存取存储器（Direct Rambus RAM，DR RAM）。应注意，本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

应理解，上述存储器为示例性但不是限制性说明，例如，本申请实施例中的存储器还可以是静态随机存取存储器（static RAM，SRAM）、动态随机存取存储器（dynamic RAM，DRAM）、同步动态随机存取存储器（synchronous DRAM，SDRAM）、双倍数据速率同步动态随机存取存储器（double data rate SDRAM，DDR SDRAM）、增强型同步动态随机存取存储器（enhanced SDRAM，ESDRAM）、同步连接动态随机存取存储器（synch link DRAM，SLDRAM）以及直接内存总线随机存取存储器（Direct Rambus RAM，DR RAM）等等。也就是说，本申请实施例中的存储器旨在包括但不限于这

些和任意其它适合类型的存储器。

本申请实施例还提供了一种计算机可读存储介质，用于存储计算机程序。

在一些实施例中，该计算机可读存储介质可应用于本申请实施例中的验证设备，并且该计算机程序使得计算机执行本申请实施例的各个方法中由验证设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机可读存储介质可应用于本申请实施例中的终端设备，并且该计算机程序使得计算机执行本申请实施例的各个方法中由终端设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机可读存储介质可应用于本申请实施例中的监管设备，并且该计算机程序使得计算机执行本申请实施例的各个方法中由监管设备实现的相应流程，为了简洁，在此不再赘述。

本申请实施例还提供了一种计算机程序产品，包括计算机程序指令。

在一些实施例中，该计算机程序产品可应用于本申请实施例中的验证设备，并且该计算机程序指令使得计算机执行本申请实施例的各个方法中由验证设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机程序产品可应用于本申请实施例中的终端设备，并且该计算机程序指令使得计算机执行本申请实施例的各个方法中由终端设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机程序产品可应用于本申请实施例中的监管设备，并且该计算机程序指令使得计算机执行本申请实施例的各个方法中由监管设备实现的相应流程，为了简洁，在此不再赘述。

本申请实施例还提供了一种计算机程序。

在一些实施例中，该计算机程序可应用于本申请实施例中的验证设备，当该计算机程序在计算机上运行时，使得计算机执行本申请实施例的各个方法中由验证设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机程序可应用于本申请实施例中的终端设备，当该计算机程序在计算机上运行时，使得计算机执行本申请实施例的各个方法中由终端设备实现的相应流程，为了简洁，在此不再赘述。

在一些实施例中，该计算机程序可应用于本申请实施例中的监管设备，当该计算机程序在计算机上运行时，使得计算机执行本申请实施例的各个方法中由监管设备实现的相应流程，为了简洁，在此不再赘述。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、或者计算机软件和电子硬件的结合来实现。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

所属领域的技术人员可以清楚地了解到，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统、装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。针对这样的理解，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或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，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例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory，ROM）、随机存取存储器（Random Access Memory，RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应所述以权利要求的保护范围为准。

权利要求

1、一种密钥验证方法，其特征在于，应用于验证设备，所述方法包括:

所述验证设备接收第一信息;

其中，所述第一信息包括第一终端的密钥协商参数、密文信息和零知识证明信息，所述密文信息基于监管设备的公钥、所述第一终端与第二终端协商确定的通信密钥、所述第一终端生成的第一随机数派生得到，所述零知识证明信息包括第一证明信息和第二证明信息，所述第一证明信息基于所述密文信息确定，所述第二证明信息基于所述密文信息和/或所述第一终端的密钥协商参数确定，所述第一证明信息用于验证所述监管设备的私钥是否可解密所述密文信息，所述第二证明信息用于验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥，所述第一终端与所述第二终端之间通过中继终端进行侧行通信。

2、如权利要求 1 所述的方法，其特征在于，所述方法还包括:

所述验证设备根据所述第一证明信息验证所述监管设备的私钥是否可解密所述密文信息;

在所述第一证明信息对应的验证结果指示所述监管设备的私钥可解密所述密文信息的情况下，所述验证设备根据所述第二证明信息验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥;

在所述第二证明信息对应的验证结果指示所述密文信息中解密得到的密钥为所述第一终端与所述第二终端协商确定的通信密钥的情况下，所述验证设备向所述监管设备发送所述密文信息。

3、如权利要求 2 所述的方法，其特征在于，

所述验证设备向所述监管设备发送所述密文信息，包括:

所述验证设备通过区块链向所述监管设备发送所述密文信息。

4、如权利要求 2 或 3 所述的方法，其特征在于，

所述验证设备为所述中继终端，或者，所述验证设备为第三方网络设备。

5、如权利要求 1 所述的方法，其特征在于，所述方法还包括:

所述验证设备根据所述监管设备的私钥解密所述密文信息;

所述验证设备根据所述第二证明信息验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥;

在所述第二证明信息对应的验证结果指示所述密文信息中解密得到的密钥为所述第一终端与所述第二终端协商确定的通信密钥的情况下，所述验证设备获取所述第一终端与所述第二终端协商确定的通信密钥。

6、如权利要求 5 所述的方法，其特征在于，所述验证设备接收第一信息，包括:

所述验证设备接收所述中继设备发送的所述第一信息。

7、如权利要求 5 或 6 所述的方法，其特征在于，所述验证设备为所述监管设备。

8、如权利要求 2 至 4 中任一项所述的方法，其特征在于，

所述验证设备根据所述第一证明信息验证所述监管设备的私钥是否可解密所述密文信息，包括:

所述验证设备根据所述第一证明信息进行零知识验证，以及在验证结果为所述密文信息的第一部分中的第一随机数与所述密文信息的第二部分中的第一随机数的取值相同的情况下，所述第一证明信息对应的验证结果指示所述监管设备的私钥可解密所述密文信息。

9、如权利要求 2 至 8 中任一项所述的方法，其特征在于，

所述验证设备根据所述第二证明信息验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥，包括:

所述验证设备根据所述第二证明信息进行零知识验证，以及在验证结果为所述密文信息中解密得到的密钥中的第二随机数与所述第一终端的密钥协商参数中的第二随机数的取值相同的情况下，所述第二证明信息对应的验证结果指示所述密文信息中解密得到的密钥为所述第一终端与所述第二终端协商确定的通信密钥。

10、如权利要求 1 至 9 中任一项所述的方法，其特征在于，

所述第一终端与所述第二终端协商确定的通信密钥基于所述第一终端生成的第二随机数和所述第二终端的密钥协商参数确定; 和/或，

所述第一终端与所述第二终端协商确定的通信密钥基于所述第二终端生成的第三随机数和所述第一终端的密钥协商参数确定。

11、如权利要求 10 所述的方法，其特征在于，

所述第一终端与所述第二终端协商确定的通信密钥为 $g_0^{ab} \bmod p$;

其中，所述第一终端的密钥协商参数为 $g_0^{a} \bmod p$，所述第二终端的密钥协商参数为 $g_0^{b} \bmod p$，a

为所述第二随机数，b 为所述第三随机数，p 为随机质数，mod 表示取模运算。

12、如权利要求 1 至 11 中任一项所述的方法，其特征在于，

所述密文信息为（$(g_0^{ab} \bmod p)h^r, g_1^r$）；

其中，所述密文信息的第一部分为$(g_0^{ab} \bmod p)h^r$，所述密文信息的第二部分为 g_1^r；

其中，g_0和 g_1均为生成元，a 为所述第一终端生成的第二随机数，b 为所述第二终端生成的第三随机数，p 为随机质数，$h=g_1^x$，r 为所述第一终端生成的第一随机数，g_1和 h 均为所述监管设备的公钥，x 为所述监管设备的私钥，mod 表示取模运算。

13、一种密钥验证方法，其特征在于，应用于第一终端，所述第一终端与第二终端之间通过中继终端进行侧行通信，所述方法包括:

所述第一终端发送第一信息;

其中，所述第一信息包括所述第一终端的密钥协商参数、密文信息和零知识证明信息，所述密文信息基于监管设备的公钥、所述第一终端与所述第二终端协商确定的通信密钥、所述第一终端生成的第一随机数派生得到，所述零知识证明信息包括第一证明信息和/或第二证明信息，所述第一证明信息基于所述密文信息确定，所述第二证明信息基于所述密文信息和所述第一终端的密钥协商参数确定，所述第一证明信息用于验证所述监管设备的私钥是否可解密所述密文信息，所述第二证明信息用于验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥。

14、如权利要求 13 所述的方法，其特征在于，

所述第一证明信息用于验证所述监管设备的私钥是否可解密所述密文信息，包括:

所述第一证明信息用于验证设备进行零知识验证，以及在验证结果为所述密文信息的第一部分中的第一随机数与所述密文信息的第二部分中的第一随机数的取值相同的情况下，所述第一证明信息对应的验证结果指示所述监管设备的私钥可解密所述密文信息。

15、如权利要求 13 所述的方法，其特征在于，所述第二证明信息用于验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥，包括:

所述第二证明信息用于所述验证设备进行零知识验证，以及在验证结果为所述密文信息中解密得到的密钥中的第二随机数与所述第一终端的密钥协商参数中的第二随机数的取值相同的情况下，所述第二证明信息对应的验证结果指示所述密文信息中解密得到的密钥为所述第一终端与所述第二终端协商确定的通信密钥。

16、如权利要求 14 或 15 所述的方法，其特征在于，所述验证设备为所述中继终端，或者，所述验证设备为第三方网络设备，或者，所述验证设备为所述监管设备。

17、如权利要求 13 至 16 中任一项所述的方法，其特征在于，

所述第一终端与所述第二终端协商确定的通信密钥基于所述第一终端生成的第二随机数和所述第二终端的密钥协商参数确定；和/或，

所述第一终端与所述第二终端协商确定的通信密钥基于所述第二终端生成的第三随机数和所述第一终端的密钥协商参数确定。

18、如权利要求 17 所述的方法，其特征在于，

所述第一终端与所述第二终端协商确定的通信密钥为 $g_0^{ab} \bmod p$;

其中，所述第一终端的密钥协商参数为 $g_0^a \bmod p$，所述第二终端的密钥协商参数为 $g_0^b \bmod p$，a 为所述第二随机数，b 为所述第三随机数，p 为随机质数，mod 表示取模运算。

19、如权利要求 13 至 18 中任一项所述的方法，其特征在于，

所述密文信息为（$(g_0^{ab} \bmod p)h^r, g_1^r$）；

其中，所述密文信息的第一部分为$(g_0^{ab} \bmod p)h^r$，所述密文信息的第二部分为 g_1^r；

其中，g_0和 g_1均为生成元，a 为所述第一终端生成的第二随机数，b 为所述第二终端生成的第三随机数，p 为随机质数，$h=g_1^x$，r 为所述第一终端生成的第一随机数，g_1和 h 均为所述监管设备的公钥，x 为所述监管设备的私钥，mod 表示取模运算。

20、一种密钥获取方法，其特征在于，应用于监管设备，所述方法包括:

所述监管设备接收密文信息；其中，所述密文信息基于所述监管设备的公钥、第一终端与第二终端协商确定的通信密钥、所述第一终端生成的第一随机数派生得到，所述第一终端与所述第二终端之间通过中继终端进行侧行通信;

所述监管设备根据所述监管设备的私钥解密所述密文信息，得到所述第一终端与所述第二终端协商确定的通信密钥。

21、如权利要求 20 所述的方法，其特征在于，

所述监管设备接收密文信息，包括:

所述监管设备通过区块链接收所述密文信息。

22、如权利要求 20 或 21 所述的方法，其特征在于，所述方法还包括:

所述监管设备接收零知识证明信息验证通过的确认信息，其中，所述零知识证明信息用于验证所述监管设备的私钥是否可解密所述密文信息，以及验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥;

所述监管设备根据所述监管设备的私钥解密所述密文信息，包括:

所述监管设备在验证所述确认信息有效之后，根据所述监管设备的私钥解密所述密文信息。

23、如权利要求 22 所述的方法，其特征在于，所述监管设备接收零知识证明信息验证通过的确认信息，包括:

所述监管设备通过区块链接收所述零知识证明信息验证通过的所述确认信息。

24、如权利要求 20 至 23 中任一项所述的方法，其特征在于，

所述第一终端与所述第二终端协商确定的通信密钥基于所述第一终端生成的第二随机数和所述第二终端的密钥协商参数确定; 和/或，

所述第一终端与所述第二终端协商确定的通信密钥基于所述第二终端生成的第三随机数和所述第一终端的密钥协商参数确定。

25、如权利要求 24 所述的方法，其特征在于，

所述第一终端与所述第二终端协商确定的通信密钥为 $g_0^{ab} \bmod p$;

其中，所述第一终端的密钥协商参数为 $g_0^{a} \bmod p$，所述第二终端的密钥协商参数为 $g_0^{b} \bmod p$，a 为所述第二随机数，b 为所述第三随机数，p 为随机质数，mod 表示取模运算。

26、如权利要求 20 至 25 中任一项所述的方法，其特征在于，

所述密文信息为（$(g_0^{ab} \bmod p)h^r, g_1^r$）;

其中，所述密文信息的第一部分为$(g_0^{ab} \bmod p)h^r$，所述密文信息的第二部分为 g_1^r;

其中，g_0 和 g_1 均为生成元，a 为所述第一终端生成的第二随机数，b 为所述第二终端生成的第三随机数，p 为随机质数，$h=g_1^x$，r 为所述第一终端生成的第一随机数，g_1 和 h 均为所述监管设备的公钥，x 为所述监管设备的私钥，mod 表示取模运算。

27、一种验证设备，其特征在于，包括:

通信单元，用于接收第一信息;

其中，所述第一信息包括第一终端的密钥协商参数、密文信息和零知识证明信息，所述密文信息基于监管设备的公钥、所述第一终端与第二终端协商确定的通信密钥、所述第一终端生成的第一随机数派生得到，所述零知识证明信息包括第一证明信息和第二证明信息，所述第一证明信息基于所述密文信息确定，所述第二证明信息基于所述密文信息和/或所述第一终端的密钥协商参数确定，所述第一证明信息用于验证所述监管设备的私钥是否可解密所述密文信息，所述第二证明信息用于验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥，所述第一终端与所述第二终端之间通过中继终端进行侧行通信。

28、一种终端设备，其特征在于，所述终端设备为第一终端，所述第一终端与第二终端之间通过中继终端进行侧行通信，所述终端设备包括:

通信单元，用于发送第一信息;

其中，所述第一信息包括所述第一终端的密钥协商参数、密文信息和零知识证明信息，所述密文信息基于监管设备的公钥、所述第一终端与所述第二终端协商确定的通信密钥、所述第一终端生成的第一随机数派生得到，所述零知识证明信息包括第一证明信息和/或第二证明信息，所述第一证明信息基于所述密文信息确定，所述第二证明信息基于所述密文信息和所述第一终端的密钥协商参数确定，所述第一证明信息用于验证所述监管设备的私钥是否可解密所述密文信息，所述第二证明信息用于验证所述密文信息中解密得到的密钥是否为所述第一终端与所述第二终端协商确定的通信密钥。

29、一种监管设备，其特征在于，包括:

通信单元，用于接收密文信息; 其中，所述密文信息基于所述监管设备的公钥、第一终端与第二终端协商确定的通信密钥、所述第一终端生成的第一随机数派生得到，所述第一终端与所述第二终端之间通过中继终端进行侧行通信;

处理单元，用于根据所述监管设备的私钥解密所述密文信息，得到所述第一终端与所述第二终端协商确定的通信密钥。

30、一种验证设备，其特征在于，包括: 处理器和存储器，所述存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，使得所述验证设备执行如权利要求 1 至 12 中任一项所述的方法。

31、一种终端设备，其特征在于，包括：处理器和存储器，所述存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，使得所述终端设备执行如权利要求 13 至 19 中任一项所述的方法。

32、一种监管设备，其特征在于，包括：处理器和存储器，所述存储器用于存储计算机程序，所述处理器用于调用并运行所述存储器中存储的计算机程序，使得所述监管设备执行如权利要求 20 至 26 中任一项所述的方法。

33、一种芯片，其特征在于，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有所述芯片的设备执行如权利要求 1 至 12 中任一项所述的方法，或者，使得安装有所述芯片的设备执行如权利要求 13 至 19 中任一项所述的方法，或者，使得安装有所述芯片的设备执行如权利要求 20 至 26 中任一项所述的方法。

34、一种计算机可读存储介质，其特征在于，用于存储计算机程序，当所述计算机程序被执行时，如权利要求 1 至 12 中任一项所述的方法被实现，或者，如权利要求 13 至 19 中任一项所述的方法被实现，或者，如权利要求 20 至 26 中任一项所述的方法被实现。

35、一种计算机程序产品，其特征在于，包括计算机程序指令，当所述计算机程序指令被执行时，如权利要求 1 至 12 中任一项所述的方法被实现，或者，如权利要求 13 至 19 中任一项所述的方法被实现，或者，如权利要求 20 至 26 中任一项所述的方法被实现。

36、一种计算机程序，其特征在于，当所述计算机程序被执行时，如权利要求 1 至 12 中任一项所述的方法被实现，或者，如权利要求 13 至 19 中任一项所述的方法被实现，或者，如权利要求 20 至 26 中任一项所述的方法被实现。

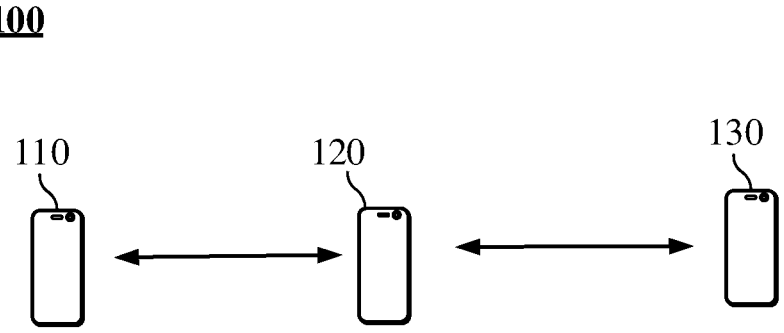

100
110
120
130

图 1

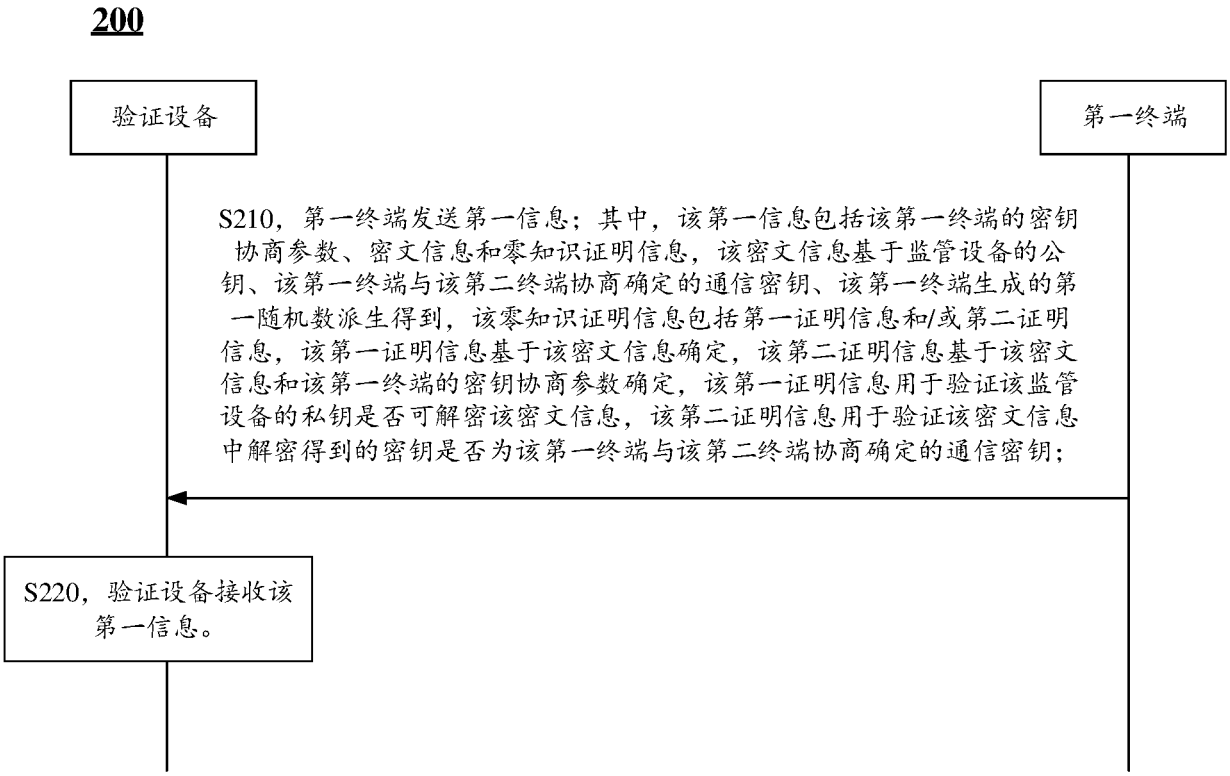

200
验证设备
第一终端
S210，第一终端发送第一信息；其中，该第一信息包括该第一终端的密钥协商参数、密文信息和零知识证明信息，该密文信息基于监管设备的公钥、该第一终端与该第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到，该零知识证明信息包括第一证明信息和/或第二证明信息，该第一证明信息基于该密文信息确定，该第二证明信息基于该密文信息和该第一终端的密钥协商参数确定，该第一证明信息用于验证该监管设备的私钥是否可解密该密文信息，该第二证明信息用于验证该密文信息中解密得到的密钥是否为该第一终端与该第二终端协商确定的通信密钥；
S220，验证设备接收该第一信息。

图 2

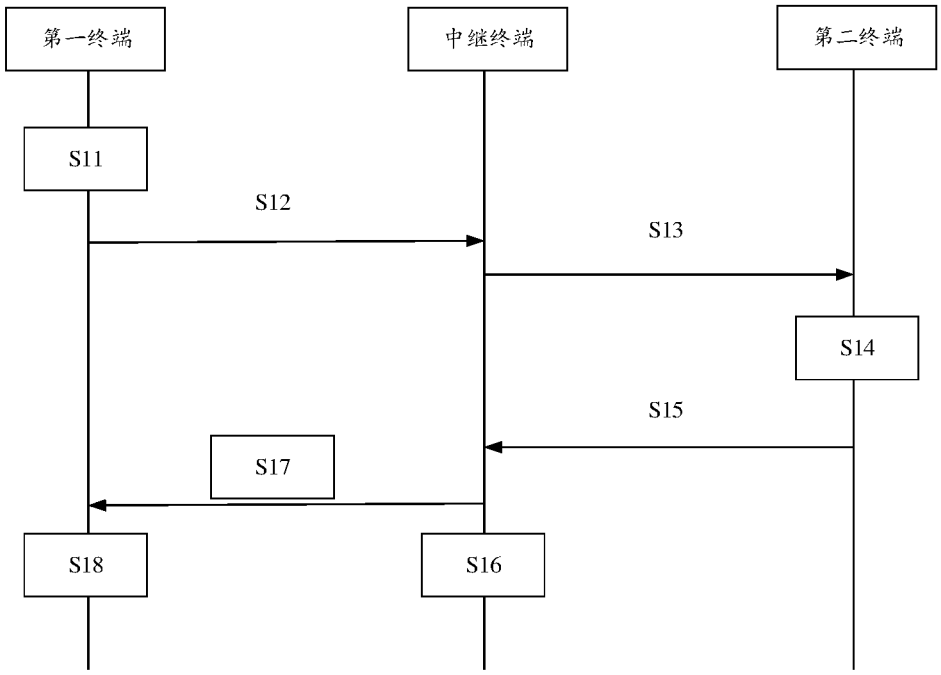

第一终端
中继终端
第二终端
S11
S12
S13
S14
S15
S17
S18
S16

图 3

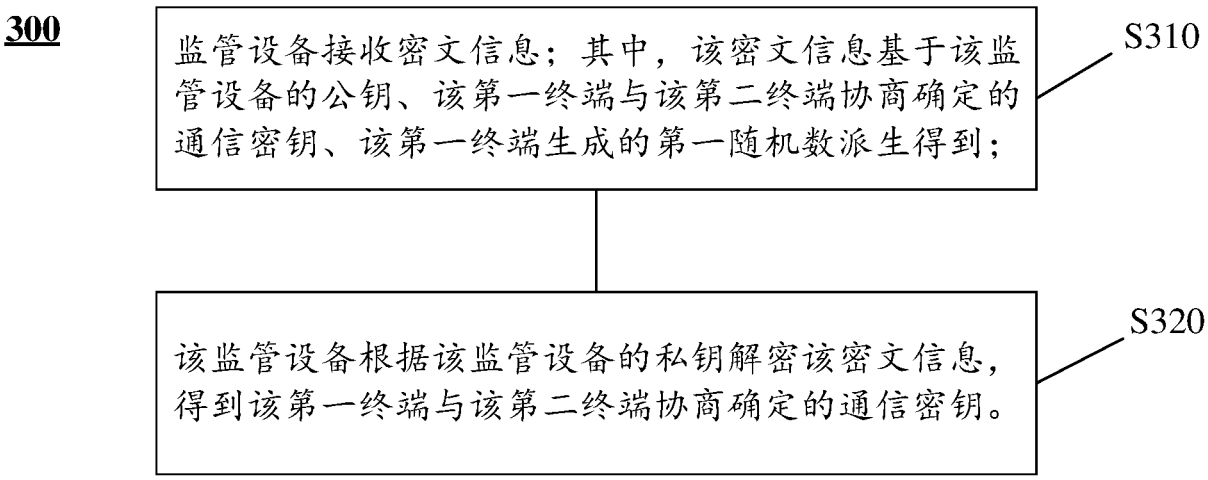

300
监管设备接收密文信息；其中，该密文信息基于该监管设备的公钥、该第一终端与该第二终端协商确定的通信密钥、该第一终端生成的第一随机数派生得到；
S310
该监管设备根据该监管设备的私钥解密该密文信息，得到该第一终端与该第二终端协商确定的通信密钥。
S320

图 4

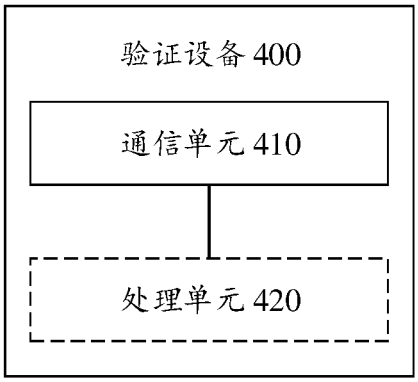

验证设备 400
通信单元 410
处理单元 420

图 5

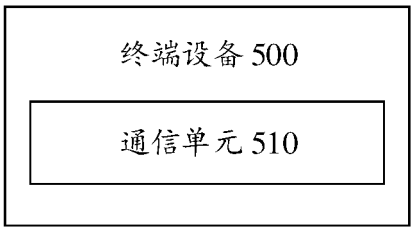

终端设备 500
通信单元 510

图 6

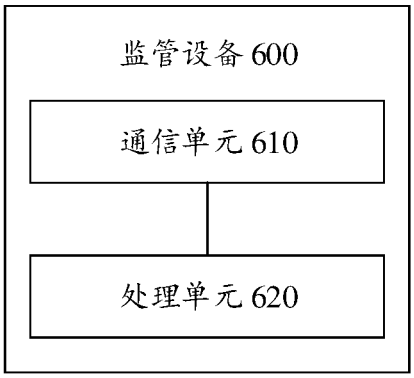

监管设备 600
通信单元 610
处理单元 620

图 7

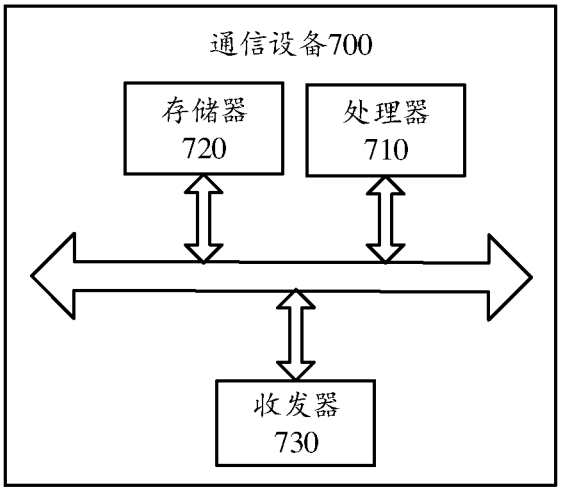

通信设备700
存储器
720
处理器
710
收发器
730

图 8

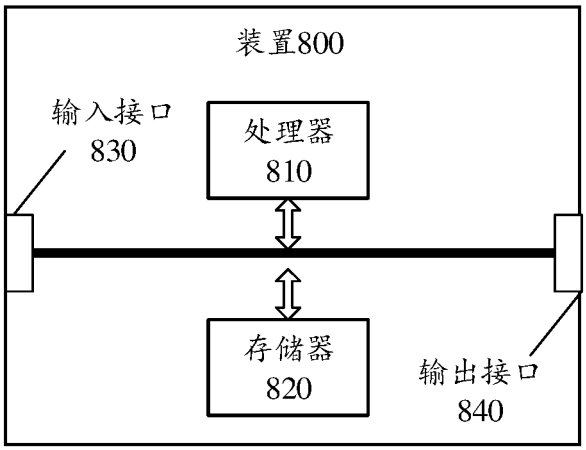

装置800
输入接口
830
处理器
810
存储器
820
输出接口
840

图 9

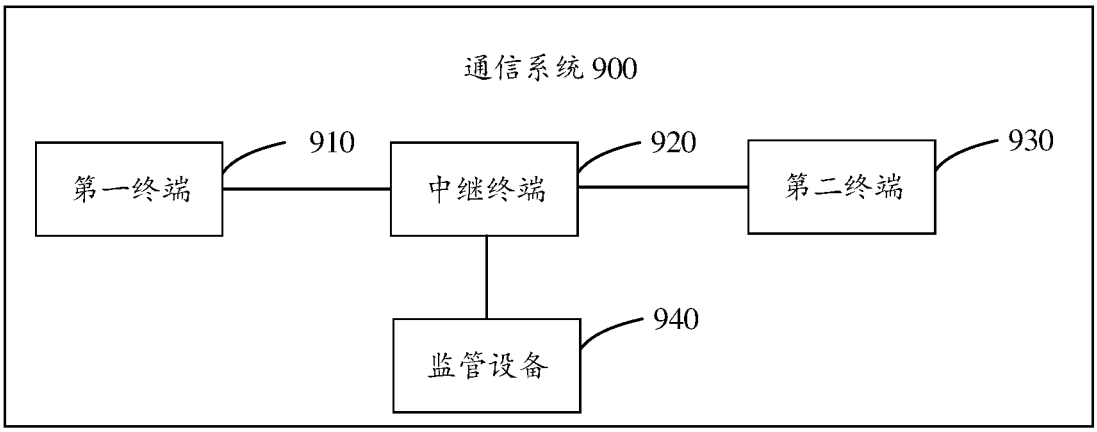


图 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/120646

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i; H04L41/00(2022.01)i; H04W12/00(2021.01)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)

IPC: H04L9/-, H04L41/-, H04W12/-

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

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

CNABS, CNTXT, CNKI, CJFD: 密钥, 验证, 监管, 监督, 侧行, 侧链, 副链, PC5, 车联网, D2D, V2X, P2P, 零知识证明, ZKP; VEN, ENTXT, 3gpp, IEEE: key, certificat+, authenticat+, supervis+, administrator, regulator, sidelink, side link, PC5, D2D, V2X, P2P, zero knowledge proof, ZKP.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 106911513 A (NO.30 RESEARCH INSTITUTE OF CETC) 30 June 2017 (2017-06-30) description, paragraphs [0006]-[0018]	20-21, 29, 32-36
A	CN 105848140 A (XIDIAN UNIVERSITY et al.) 10 August 2016 (2016-08-10) entire document	1-36
A	WO 2021168614 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 02 September 2021 (2021-09-02) entire document	1-36
A	WO 2022001278 A1 (QUALCOMM INC.) 06 January 2022 (2022-01-06) entire document	1-36
A	Benedikt Brecht et al. "A Security Credential Management System for V2X Communications" *IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS,* Vol. 19, No. 12, 31 December 2018 (2018-12-31), entire document	1-36

☐ 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
"D" document cited by the applicant in the international application
"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
08 June 2023	**13 June 2023**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/120646

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 106911513 A	30 June 2017	CN 106911513 B	13 December 2019
CN 105848140 A	10 August 2016	CN 105848140 B	15 March 2019
WO 2021168614 A1	02 September 2021	EP 4087180 A1	09 November 2022
		EP 4087180 A4	04 January 2023
		CN 112602289 A	02 April 2021
		CN 112602289 B	21 December 2021
WO 2022001278 A1	06 January 2022	WO 2022000416 A1	06 January 2022
		TW 202203673 A	16 January 2022
		EP 4176597 A1	10 May 2023
		KR 20230034965 A	10 March 2023
		BR 112022026189 A2	17 January 2023
		IN 202227060795 A	02 December 2022

国际检索报告

国际申请号
PCT/CN2022/120646

A. 主题的分类

H04L9/08(2006.01)i; H04L41/00(2022.01)i; H04W12/00(2021.01)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)

IPC: H04L9/-, H04L41/-, H04W12/-

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS,CNTXT,CNKI,CJFD：密钥，验证，监管，监督，侧行，侧链，副链，PC5，车联网，D2D，V2X，P2P，零知识证明，ZKP； VEN, ENTXT,3gpp,IEEE: key, certificat+, authenticat+, supervis+, administrator, regulator, sidelink, side link, PC5, D2D, V2X, P2P, zero knowledge proof, ZKP.

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 106911513 A (中国电子科技集团公司第三十研究所) 2017年6月30日 (2017-06-30) 说明书第[06]-[18]段	20-21、29、32-36
A	CN 105848140 A (西安电子科技大学等) 2016年8月10日 (2016-08-10) 全文	1-36
A	WO 2021168614 A1 (华为技术有限公司) 2021年9月2日 (2021-09-02) 全文	1-36
A	WO 2022001278 A1 (QUALCOMM INCORPORATED) 2022年1月6日 (2022-01-06) 全文	1-36
A	Benedikt Brecht等. "A Security Credential Management System for V2X Communications" IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, 第19卷，第12期，2018年12月31日 (2018-12-31), 全文	1-36

☐ 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

"D" 申请人在国际申请中引证的文件

"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
2023年6月8日	2023年6月13日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 杨钰娟 电话号码 (+86) 028-62969261

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/120646

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	106911513	A	2017年6月30日	CN	106911513	B	2019年12月13日
CN	105848140	A	2016年8月10日	CN	105848140	B	2019年3月15日
WO	2021168614	A1	2021年9月2日	EP	4087180	A1	2022年11月9日
				EP	4087180	A4	2023年1月4日
				CN	112602289	A	2021年4月2日
				CN	112602289	B	2021年12月21日
WO	2022001278	A1	2022年1月6日	WO	2022000416	A1	2022年1月6日
				TW	202203673	A	2022年1月16日
				EP	4176597	A1	2023年5月10日
				KR	20230034965	A	2023年3月10日
				BR	112022026189	A2	2023年1月17日
				IN	202227060795	A	2022年12月2日