(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
2019 年 7 月 18 日 (18.07.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/137232 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2018/124490

(22) 国际申请日: 2018 年 12 月 27 日 (27.12.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201810036963.5 2018年1月15日 (15.01.2018) CN

(71) 申请人: 华为技术有限公司 (**HUAWEI TECHNOLOGIES CO., LTD.**) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: **朱浩仁(ZHU, Haoren)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **诸华林(ZHU, Hualin)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 **李赫(LI, He)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京同立钧成知识产权代理有限公司 (**LEADER PATENT & TRADEMARK FIRM**); 中国北京市海淀区西直门北大街32号枫蓝国际A座8F-6, Beijing 100082 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, 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,

WO 2019/137232 A1

(54) **Title:** METHOD AND APPARATUS FOR SENDING MESSAGE

(54) **发明名称**: 消息的发送方法和装置

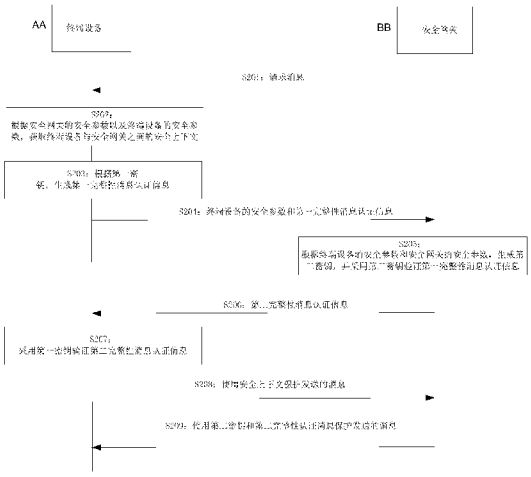

图 2

S201 Request message
S202 Acquire a security context between a terminal device and a security gateway according to a security parameter of the security gateway and a security parameter of the terminal device
S203 Generate first integrity message authentication information according to a first key
S204 The security parameter of the terminal device and the first integrity message authentication information
S205 Generate a second key according to the security parameter of the terminal device and the security parameter of the security gateway, and verify the first integrity message authentication information by means of the second key
S206 Second integrity message authentication information
S207 Verify the second integrity message authentication information by means of the first key
S208 Protect a sent message by means of the security context
S209 Protect the sent message by means of the second key and a second integrity authentication message
AA Terminal device
BB Security gateway

(57) **Abstract:** Provided are a method and apparatus for sending a message. A security gateway sends a request message to a terminal device; and the terminal device acquires a security context between the terminal device and the security gateway according to a security parameter of the security gateway and a security parameter of the terminal device, and protects the sent message by means of the security context, thereby improving the security of the sent message.

(57) **摘要**: 本申请实施例提供一种消息的发送方法和装置，通过安全网关向终端设备发送请求消息，终端设备根据安全网关的安全参数以及终端设备的安全参数，获取终端设备与安全网关之间的安全上下文，使用安全上下文保护发送的消息，从而，提高了发送的消息的安全性。

[见续页]

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))。

消息的发送方法和装置

本申请要求于 2018 年 01 月 15 日提交中国专利局、申请号为 201810036963.5 申请名称为“消息的发送方法和装置”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。

技术领域

本申请涉及通信技术领域，尤其涉及一种消息的发送方法和装置。

背景技术

针对不可信 (Untrusted)非第三代合作伙伴计划(3rd generation partnership project, 3GPP)接入网场景，在 4G 的网络架构中，终端设备在发送消息之前进行接入鉴权，终端设备在接入鉴权过程中，通过无线局域网（Wireless Local Area Networks， WLAN）的方式接入接入网，WLAN 通过 SWa 接口向验证、授权和账号服务器（Authentication、Authorization、Accounting Server ，AAA Server）发起验证请求，以使终端设备获得自身的网络互连协议（Internet Protocol，IP）地址，再采用 IP 地址进行隧道鉴权，从而保证消息的安全传输。

在 5G 的网络架构中，采用接入鉴权和隧道鉴权合一鉴权的方式，即接入鉴权和隧道鉴权同时进行。在合一鉴权完成之前，终端设备和安全网关之间发送的消息的安全性得不到保证。

发明内容

本申请提供一种消息的发送方法和装置，以解决现有技术中发送的消息的安全性不高的问题。

本申请第一方面提供一种消息的发送方法，包括：通过终端设备接收安全网关发送的请求消息，请求消息中包含安全网关的安全参数；终端设备获取到安全网关的安全参数后，根据所述安全网关的安全参数以及所述终端设备的安全参数，使用所述安全上下文保护发送的消息。从而，提高发送的消息的安全性。

可选地，所述请求消息中还包括开始标志位。

可选地，所述请求消息中还包括安全标志位。

可选地，所述安全标志位包含在所述请求消息的头部或者净荷中。

可选地，所述终端设备根据所述安全网关的安全参数以及所述终端设备的安全参数，获取所述终端设备与所述安全网关之间的安全上下文，包括：

所述终端设备根据所述安全网关的安全参数以及所述终端设备的安全参数，生成

第一密钥；并根据所述第一密钥生成第一完整性消息认证信息。

可选地，还包括：

所述终端设备向所述安全网关发送所述终端设备的安全参数和所述第一完整性消息认证信息。

可选地，还包括：

所述终端设备接收所述安全网关发送的第二完整性消息认证信息；

所述终端设备根据所述第一密钥验证所述第二完整性认证信息。

可选地，所述终端设备接收所述安全网关发送的第二完整性消息认证信息，包括：

所述终端设备接收所述安全网关发送的响应消息，所述响应消息中包含所述第二完整性消息认证信息。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

可选地，所述终端设备使用所述安全上下文保护发送的消息，包括：

所述终端设备采用所述第一密钥对向所述安全网关发送的消息进行加密；

所述终端设备采用所述第一完整性消息认证信息对向所述安全网关发送的消息进行完整性保护。

本申请第二方面提供一种消息的发送方法，包括：

安全网关向终端设备发送请求消息，所述请求消息中包含所述安全网关的安全参数，终端设备获取到安全网关的安全参数后，可以根据安全网关的安全参数和自身的安全参数获取所述终端设备与所述安全网关之间的安全上下文；并使用安全上下文保护向安全网关发送的消息，从而，提高发送的消息的安全性。

可选地，所述请求消息中还包括开始标志位。

可选地，所述请求消息中还包括安全标志位。

可选地，所述安全标志位包含在所述请求消息的头部或者净荷中。

可选地，所述安全上下文中包含第一密钥和第一完整性消息认证信息；

所述方法还包括：

所述安全网关接收所述终端设备发送的所述终端设备的安全参数和所述第一完整性消息认证信息；

所述安全网关根据所述终端设备的安全参数和所述安全网关的安全参数，生成第二密钥；

所述安全网关根据所述第二密钥，验证所述第一完整性消息认证信息。

可选地，还包括：

所述安全网关向所述终端设备发送的第二完整性消息认证信息。

可选地，所述安全网关向所述终端设备发送的第二完整性消息认证信息，包括：

所述安全网关向所述终端设备发送的响应消息，所述响应消息中包含所述第二完整性消息认证信息。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括

完整性算法和加密算法之一或全部。

可选地，还包括：

所述安全网关采用所述第二密钥对向所述终端设备发送的消息进行加密；

所述安全网关采用所述第二完整性消息认证信息对向所述终端设备发送的消息进行完整性保护。

本申请第三方面提供一种消息的发送方法，包括：

安全网关接收终端设备发送的第一消息，所述第一消息中包含所述终端设备身份标识和所述终端设备的安全参数；根据所述终端设备的安全参数以及所述安全网关的安全参数，获取所述终端设备与所述安全网关之间的安全上下文；使用所述安全上下文保护向所述终端设备发送的消息。从而，提高发送的消息的安全性。

可选地，所述安全网关根据所述终端设备的安全参数以及所述安全网关的安全参数，获取所述终端设备与所述安全网关之间的安全上下文，包括：

所述安全网关根据所述终端设备的安全参数以及所述安全网关的安全参数，生成第一密钥，并根据所述第一密钥生成第一完整性消息认证信息。

可选地，还包括：

所述安全网关向所述终端设备发送所述安全网关的安全参数和所述第一完整性消息认证信息。

可选地，还包括：

所述安全网关接收所述终端设备发送的第二完整性消息认证信息；

所述安全网关根据所述第一密钥验证所述第二完整性消息认证信息。

可选地，所述安全网关使用所述安全上下文保护发送的消息，包括：

所述安全网关采用所述第一密钥对向所述终端设备发送的消息进行加密；

所述安全网关采用所述第一完整性消息认证信息对向所述终端设备发送的消息进行完整性保护。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

本申请第四方面提供一种消息的发送方法，包括：

终端设备向安全网关发送第一消息，所述第一消息中包含所述终端设备身份标识和所述终端设备的安全参数，所述安全参数用于所述安全网关获取所述终端设备与所述安全网关之间的安全上下文；接收所述安全网关发送的消息，所述消息使用所述终端设备与所述安全网关之间的安全上下文保护。从而，提高发送的消息的安全性。

可选地，所述安全上下文中包含第一密钥和第一完整性消息认证信息；

所述终端设备接收所述安全网关发送的消息之前，还包括：

所述终端设备接收所述安全网关发送的所述安全网关的安全参数和所述第一完整性消息认证信息；

所述终端设备根据所述终端设备的安全参数和所述安全网关的安全参数，生成第二密钥；

所述终端设备根据所述第二密钥，验证所述第一完整性消息。

可选地，还包括：

所述终端设备向所述安全网关发送第二完整性消息认证信息。

可选地，还包括：

所述终端设备采用所述第二密钥对向所述网络设备发送的消息进行加密；

所述终端设备采用所述第二完整性消息认证信息对向所述网络设备发送的消息进行完整性保护。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述协商的算法包括完整性算法和加密算法之一或全部。

本申请第五方面提供一种消息的发送装置，包括：

接收模块，用于接收安全网关发送的请求消息，所述请求消息中包含所述安全网关的安全参数；

处理模块，用于根据所述安全网关的安全参数以及所述消息的发送装置的安全参数，获取所述消息的发送装置与所述安全网关之间的安全上下文；

发送模块，用于使用所述安全上下文和所述第一完整性消息认证信息保护发送的消息。

可选地，所述请求消息中还包括开始标志位。

可选地，所述请求消息中还包括安全标志位。

可选地，所述安全标志位包含在所述请求消息的头部或者净荷中。

可选地，所述处理模块具体用于根据所述安全网关的安全参数以及所述消息的发送装置的安全参数，生成第一密钥，并根据所述第一密钥生成第一完整性消息认证信息。

可选地，所述发送模块还用于向所述安全网关发送所述消息的发送装置的安全参数和所述第一完整性消息认证信息。

可选地，所述接收模块还用于接收所述安全网关发送的第二完整性消息认证信息；

所述处理模块还用于根据所述第一密钥验证所述第二完整性认证信息。

可选地，所述接收模块具体用于接收所述安全网关发送的响应消息，所述响应消息中包含所述第二完整性消息认证信息。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

可选地，所述发送模块具体用于采用所述第一密钥对向所述安全网关发送的消息进行加密；并采用所述第一完整性消息认证信息对向所述安全网关发送的消息进行完整性保护。

本申请第六方面提供一种消息的发送装置，包括：

发送模块，用于向终端设备发送请求消息，所述请求消息中包含所述消息的发送装置的安全参数，其中，所述消息的发送装置的安全参数用于终端设备获取所述终端设备与所述消息的发送装置之间的安全上下文；

接收模块，用于接收所述终端设备发送的消息，所述消息使用所述终端设备与所述消息的发送装置之间的安全上下文保护。

可选地，所述请求消息中还包括开始标志位。

可选地，所述请求消息中还包括安全标志位。

可选地，所述安全标志位包含在所述请求消息的头部或者净荷中。

可选地，所述安全上下文中包含第一密钥和第一完整性消息认证信息；

所述接收模块还用于接收所述终端设备发送的所述终端设备的安全参数和所述第一完整性消息认证信息；

还包括：处理模块；

所述处理模块，用于根据所述终端设备的安全参数和所述消息的发送装置的安全参数，生成第二密钥；并根据所述第二密钥，验证所述第一完整性消息认证信息。

可选地，所述发送模块还用于向所述终端设备发送的第二完整性消息认证信息。

可选地，所述发送模块还用于向所述终端设备发送的响应消息，所述响应消息中包含所述第二完整性消息认证信息。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

可选地，所述发送模块具体用于采用所述第一密钥对向所述终端设备发送的消息进行加密；并采用所述第二完整性消息认证信息对向所述终端设备发送的消息进行完整性保护。

本申请第七方面提供一种消息的发送装置，包括：

接收模块，用于接收终端设备发送的第一消息，所述第一消息中包含所述终端设备身份标识和所述终端设备的安全参数；

处理模块，用于根据所述终端设备的安全参数以及所述消息的发送装置的安全参数，获取所述终端设备与所述消息的发送装置之间的安全上下文；

发送模块，用于使用所述安全上下文保护向所述终端设备发送的消息。

可选地，所述处理模块具体用于根据所述终端设备的安全参数以及所述消息的发送装置的安全参数，生成第一密钥，并根据所述第一密钥生成第一完整性消息认证信息。

可选地，所述发送模块还用于向所述终端设备发送所述消息的发送装置的安全参数和所述第一完整性消息认证信息。

可选地，所述接收模块还用于接收所述终端设备发送的第二完整性消息认证信息；

所述处理模块还用于根据所述第一密钥验证所述第二完整性消息认证信息。

可选地，所述发送模块具体用于采用所述安全上下文对向所述终端设备发送的消息进行加密；并采用所述第一完整性消息认证信息对向所述终端设备发送的消息进行完整性保护。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

本申请第八方面提供一种消息的发送装置，包括：

发送模块，用于向安全网关发送第一消息，所述第一消息中包含所述消息的发送

装置身份标识和所述消息的发送装置的安全参数，所述安全参数用于所述安全网关获取所述消息的发送装置与所述安全网关之间的安全上下文；

接收模块，用于接收所述安全网关发送的消息，所述消息使用所述消息的发送装置与所述安全网关之间的安全上下文保护。

可选地，所述安全上下文中包含第一密钥和第一完整性消息认证信息；

所述接收模块，还用于接收所述安全网关发送的所述安全网关的安全参数和所述第一完整性消息认证信息；

还包括:

处理模块，用于根据所述消息的发送装置的安全参数和所述安全网关的安全参数，生成第二密钥；并根据所述第二密钥，验证所述第一完整性消息。

可选地，所述发送模块，还用于向所述安全网关发送第二完整性消息认证信息。

可选地，所述发送模块还用于采用所述安全上下文对向所述网络设备发送的消息进行加密；并采用所述第二完整性消息认证信息对向所述网络设备发送的消息进行完整性保护。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

本申请第九方面提供一种消息的发送装置，包括：

处理器、存储器和收发器，所述存储器用于存储指令，所述收发器用于和其他设备通信，所述处理器用于执行所述存储器中存储的指令，以使消息的发送装置执行如下第一方面所述的方法。

本申请第十方面提供一种消息的发送装置，包括：

处理器、存储器和收发器，所述存储器用于存储指令，所述收发器用于和其他设备通信，所述处理器用于执行所述存储器中存储的指令，以使消息的发送装置执行如下第二方面所述的方法。

本申请第十一方面提供一种消息的发送装置，包括：

处理器、存储器和收发器，所述存储器用于存储指令，所述收发器用于和其他设备通信，所述处理器用于执行所述存储器中存储的指令，以使消息的发送装置执行如第三方面所述的方法。

本申请第十二方面提供一种消息的发送装置，包括：

处理器、存储器和收发器，所述存储器用于存储指令，所述收发器用于和其他设备通信，所述处理器用于执行所述存储器中存储的指令，以使消息的发送装置执行如下第四方面所述的方法。

本申请第十三方面提供一种计算机可读存储介质所述计算机可读存储介质存储有指令，当所述指令被计算装置执行时，使得消息的发送装置执行如第一方面所述的方法。

本申请第十四方面提供一种计算机可读存储介质，所述计算机可读存储介质存储有指令，当所述指令被计算装置执行时，使得消息的发送装置执行如第二方面所述的方法。

本申请第十五方面提供一种计算机可读存储介质，所述计算机可读存储介质存储有指令，当所述指令被计算装置执行时，使得消息的发送装置执行如第三方面所述的方法。

本申请第十六方面提供一种计算机可读存储介质，所述计算机可读存储介质存储有指令，当所述指令被计算装置执行时，使得消息的发送装置执行如第四方面所述的方法。

本申请第十七方面提供一种程序产品，所述程序产品包括计算机程序，所述计算机程序存储在计算机可读存储介质中，消息的发送装置的至少一个处理器从所述计算机可读存储介质中读取所述计算机程序，所述至少一个处理执行所述计算机程序使得所述消息的发送装置执行如第一方面所述的方法。

本申请第十八方面提供一种程序产品，所述程序产品包括计算机程序，所述计算机程序存储在计算机可读存储介质中，消息的发送装置的至少一个处理器从所述计算机可读存储介质中读取所述计算机程序，所述至少一个处理执行所述计算机程序使得所述消息的发送装置执行如第二方面所述的方法。

本申请第十九方面提供一种程序产品，所述程序产品包括计算机程序，所述计算机程序存储在计算机可读存储介质中，消息的发送装置的至少一个处理器从所述计算机可读存储介质中读取所述计算机程序，所述至少一个处理执行所述计算机程序使得所述消息的发送装置执行如第三方面所述的方法。

本申请第二十方面提供一种程序产品，所述程序产品包括计算机程序，所述计算机程序存储在计算机可读存储介质中，消息的发送装置的至少一个处理器从所述计算机可读存储介质中读取所述计算机程序，所述至少一个处理执行所述计算机程序使得所述消息的发送装置执行如第四方面所述的方法。

附图说明

图 1 为本申请提供的一种 5G 的网络架构示意图；

图 2 为本申请提供的一种消息的发送方法的流程示意图；

图 3a-图 3c 为本申请提供的请求消息的报文结构示意图；

图 4 为本申请提供的另一种消息的发送方法的流程示意图；

图 5 为本申请提供的一种消息的发送装置的结构示意图；

图 6 为本申请提供的另一种消息的发送装置的结构示意图；

图 7 为本申请提供的再一种消息的发送装置的结构示意图；

图 8 为本申请提供的又一种消息的发送装置的结构示意图；

图 9 为本申请提供的又一种消息的发送装置的结构示意图；

图 10 为本申请提供的又一种消息的发送装置的结构示意图；

图 11 为本申请提供的又一种消息的发送装置的结构示意图；

图 12 为本申请提供的又一种消息的发送装置的结构示意图。

具体实施方式

本申请可应用于 5G 以及 5G 之后具有类似功能的网络架构中，本申请以应用于

5G 的网络架构为例进行描述，图 1 为本申请提供的一种 5G 的网络架构示意图，如图 1 所示，本实施例的网络架构中包括：终端设备、不可信的非 3GPP 接入网（untrusted non-3GPP access network）设备、安全网关（security gateway）（图 1 中以 N3IWF 为例示出）、接入与移动性管理功能（Access and Mobility Management Function，AMF）网元、认证服务器功能(Authentication Server Function，AUSF)网元，3GPP 接入网设备、会话管理功能（session management function，SMF）网元、用户面功能（user plane function，UPF）网元和数据网络设备等，其中：

不可信的非 3GPP 接入网设备：该网元允许终端设备和 3GPP 核心网之间采用非 3GPP 技术互连互通，其中，非 3GPP 技术例如：无线保真（WirelessFidelity ，Wi-Fi）、全球微波互联接入（Worldwide Interoperability for Microwave Access ，WiMAX）、码分多址（Code Division Multiple Access，CDMA）网络等，相对于可信的非 3GPP 接入网设备可以直接接入 3GPP 核心网，该网元需要通过安全网关建立的安全隧道来与 3GPP 核心网互连互通，其中，安全网关例如：演进型分组数据网关（Evolved Packet Data Gateway，eDPG）或者非 3GPP 互通功能（Non-3GPP InterWorking Function,N3IWF）网元。

安全网关：该网元通过与终端设备建立安全隧道，使得终端设备能够安全的和 3GPP 核心网之间进行通信，该网元是终端设备和 3GPP 核心网之间通信的中间网元。

AUSF 网元：主要提供认证和鉴权功能。

终端设备：可以为用户设备（user equipment，UE）、手持终端、笔记本电脑、用户单元（subscriber unit）、蜂窝电话（cellular phone）、智能电话（smart phone）、无线数据卡、个人数字助理（personal digital assistant，PDA）电脑、平板型电脑、无线调制解调器（modem）、手持设备（handheld）、膝上型电脑（laptop computer）、无绳电话（cordless phone）或者无线本地环路（wireless local loop，WLL）台、机器类型通信（machine type communication，MTC）终端或是其他可以接入网络的设备。终端设备与接入网设备之间采用某种空口技术相互通信。

3GPP 接入网（radio access network，RAN）设备：主要负责空口侧的无线资源管理、服务质量（quality of service，QoS）管理、数据压缩和加密等功能。所述接入网设备可以包括各种形式的基站，例如：宏基站，微基站（也称为小站），中继站，接入点等。在采用不同的无线接入技术的系统中，具备基站功能的设备的名称可能会有所不同，例如，在第五代（5th generation，5G）系统中，称为 gNB；在 LTE 系统中，称为演进的节点 B（evolved NodeB，eNB 或者 eNodeB）；在第三代（3rd generation，3G）系统中，称为节点 B（Node B）等。

AMF 网元：属于核心网网元，主要负责信令处理部分，例如：接入控制、移动性管理、附着与去附着以及网关选择等功能。AMF 网元为终端设备中的会话提供服务的情况下，会为该会话提供控制面的存储资源，以存储会话标识、与会话标识关联的 SMF 网元标识等。

会话管理功能（session management function，SMF）网元：负责用户面网元选择，用户面网元重定向，因特网协议（internet protocol，IP）地址分配，承载的建立、修改和释放以及 QoS 控制。

UPF 网元：负责终端设备中用户数据的转发和接收。可以从数据网络接收用户数据，通过接入网设备传输给终端设备；UPF 网元还可以通过接入网设备从终端设备接收用户数据，转发到数据网络。UPF 网元中为终端设备提供服务的传输资源和调度功能由 SMF 网元管理控制的。

目前终端设备通过 Y1 接口与不可信的非 3GPP 接入网设备进行通信，不可信的非 3GPP 接入网设备通过 Y2 接口与 N3IWF 网元进行通信，N3IWF 网元通过 N2 接口与 AMF 网元进行通信，AMF 网元通过 N12 接口或者服务化接口与 AUSF 网元进行通信，终端设备通过 N1 接口与 3GPP 接入网设备进行通信，3GPP 接入网设备通过 N2 接口与 AMF 网元进行通信，AMF 网元通过 N11 接口与 SMF 网元进行通信，SMF 网元通过 N4 接口与 UPF 网元进行通信，N3IWF 网元通过 N3 接口与 UPF 网元进行通信，3GPP 接入网设备通过 N3 接口与 UPF 网元进行通信，UPF 网元通过 N6 接口与数据网络设备进行通信。

可以理解的是，在图 1 所示的通信系统中，各网元的功能以及接口仅为示例性的，各个网元在应用于本申请的实施例中时，并非全部功能都是必需的。本实施例中的核心网的全部或者部分网元可以是物理上的实体网元，也可以是虚拟化的网元，在此不做限定。

在本申请的实施例中，“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，在本申请的描述中，“多个”是指两个或多于两个。

在本申请的实施例中，某一网元(例如：A 网元)获取来自另一网元(例如：B 网元)的信息，可以指 A 网元直接从 B 网元接收信息，也可以指 A 网元经其他网元(例如：C 网元)从 B 网元接收信息。当 A 网元经 C 网元从 B 网元接收信息时，C 网元可以对信息进行透传，也可以将信息进行处理，例如：将信息携带在不同的消息中进行传输或者对信息进行筛选，只发送筛选后的信息给 A 网元。类似的，在本申请的各实施例中，A 网元向 B 网元发送信息，可以指 A 网元直接向 B 网元发送信息，也可以指 A 网元经其他网元(例如：C 网元)向 B 网元发送信息。

下面以几个实施例为例对本申请的技术方案进行描述，对于相同或相似的概念或过程可能在某些实施例不再赘述。

图 2 为本申请提供的一种消息的发送方法的流程示意图，如图 2 所示；

S201：安全网关向终端设备发送请求消息。

其中，请求消息中包含安全网关的安全参数。

安全网关是指能够通过建立安全隧道使得终端设备和 3GPP 核心网安全通信的设备，例如：图 1 中所示的 N3IWF 网元。

安全网关的安全参数包括但不限于：生成安全上下文的材料，比如待协商的算法，或者选择出来的算法，以及生成安全上下文所需的参数，比如安全证书，迪菲-赫尔曼（Diffie-Hellman，DH）方法中的安全网关发送的公钥，或者公私钥方法中的网关使用的公钥等。

待协商的算法或者选择出来的算法包括完整性算法和加密算法之一或者全部。

生成安全上下文所需的参数包括但不限 DH 值。

其中，请求消息可以是发送非接入层（Non-access stratum，NAS）消息之前的任一消息，该请求消息可以是现有的请求消息的扩展，也可以是完全新增加的请求消息，对此，本申请不作限制。

请求消息中还可包含安全标志位，安全标志位用于指示该请求消息用于指示建立安全上下文过程，或者，用于指示终端设备建立安全上下文，安全标志位可以包含在请求消息的头部或者净荷中。

安全标志位包含在请求消息的头部中，可以通过定义头部中的空闲比特位中的一个比特或者多个比特来表示安全标志位，例如，可以将图 3a 中的 R 位替换为安全标识位；也可以重新定义头部中已定义过的一个比特或者多个比特来表示安全标志位，对此，本申请不做限制。请求消息以 5G 扩展认证协议（Extensible Authentication Protocol-5G，EAP-5G）消息为例，EAP-5G 报文头部的格式如图 3a-图 3c 所示，图 3a-图 3c 中以第二代互联网秘钥交换协议（Internet Key Exchange version 2，IKEv2）为例，图 3a 为现有的 EAP-5G 报文头部的示意图，将图 3a 中的斜线填充部分拓展成图 3b 所示，图 3b 中的互联网密钥交换协议报文头（IKE header，IKE HDR）部分的完整部分如图 3c 所示。在图 3a 中，S 为开始标志位；C 为完整标志位，F 为失败标志位，R 预留标志位。

请求消息中还包含开始标志位，开始标志位是现有报文头部已有的标志，通过一个比特位表示，当该比特位值为有效时，表示开始传输 NAS 消息；即在这种实现方式中，是通过在现有的请求消息中携带安全参数，以使终端设备获取安全网关的安全参数。

S202：终端设备根据安全网关的安全参数以及终端设备的安全参数，获取终端设备与安全网关之间的安全上下文。

终端设备的安全参数包括但不限于：生成安全上下文的材料，比如待协商的算法，或者选择出来的算法，以及生成安全上下文所需的参数，比如安全证书，DH 方法中的安全网关发送的公钥，或者公私钥方法中的网关使用的公钥等。

待协商的算法或者选择出来的算法包括完整性算法和加密算法之一或者全部。

生成安全上下文所需的参数包括但不限 DH 值。

可选地，安全上下文中包含第一秘钥，终端设备可以根据安全网关的安全参数以及终端设备的安全参数，获取第一密钥。其中，第一密钥包括完整性保护密钥。可选地，第一密钥还包括加密密钥。

S203：终端设备根据第一密钥，生成第一完整性消息认证信息。

其中，完整性消息认证信息是由终端设备即将回复的消息和完整性保护密钥生成。例如，完整性认证信息可以是完整性消息认证码（Message Authentication Code- Integrity，MAC-I），用于对在鉴权过程中终端设备向安全网关的消息进行完整性保护验证。

可选地，终端设备生成第一完整性消息认证信息之后，还可以执行 S204。

S204：终端设备向安全网关发送终端设备的安全参数和第一完整性消息认证信息。

其中，第一完整性消息认证信息是由终端生成的完整性保护密钥，和终端设备即将发送给安全网关的下一条消息生成的。

S205：安全网关根据终端设备的安全参数和安全网关的安全参数，生成第二密钥，

并采用第二密钥验证第一完整性消息认证信息。

第二密钥包含完整性保护密钥。可选地，第二密钥还包含加密保护密钥。进一步地，是否包含加密保护密钥可以由下面几种方法中的至少 1 种确定：根据所述安全标志位，或者选择的保护方法，或者双方提前约定好。其中，选择的保护方法比如是某些特定的公私钥方法。

若第一完整性消息认证信息验证成功，则表明第一密钥与第二密钥相同，则安全网关可以采用第二秘钥对向终端设备发送的消息进行完整性保护，或加密保护。

若第一完整性消息认证信息验证失败，则表明第一秘钥与第二秘钥不同，则需要拒绝终端设备接入核心网，可选地，同时可以返回认证失败的信息。

S206：安全网关向终端设备发送第二完整性消息认证信息。

安全网关根据第二秘钥，生成第二完整性消息认证信息。并向终端设备发送第二完整性消息认证信息。其中，第二完整性消息认证信息是由安全网关生成的第二密钥和即将给终端发送的下一条消息生成的。

S207：终端设备采用第一密钥验证第二完整性消息认证信息。

若第二完整性消息认证信息验证成功，则表明第一密钥与第二密钥相同，则终端设备可以采用第一秘钥对向安全网关发送的消息进行安全保护。其中，安全保护为完整性保护，可选地，如果生成了加密密钥，则也进行加密保护。

若第二完整性消息认证信息验证失败，则表明第一秘钥与第二秘钥不同，则需要则需要拒绝终端设备接入核心网，可选地，同时可以返回认证失败的信息。

S208：终端设备使用安全上下文保护发送的消息。

其中，一种可能的实现方式为：

终端设备采用安全上下文对向安全网关发送的消息进行完整性保护，和/或加密保护；。

其中，发送的消息例如：NAS 消息，NAS 消息例如：NAS 注册请求消息，NAS 认证请求消息等，对此，本申请不做限制。发送的消息还例如 EAP-5G 消息中的消息实体的部分或全部。消息实体是指除了 EAP-5G 头部信息以外的部分。

S209：安全网关使用第二密钥和第二完整性认证消息保护发送的消息。

其中，一种可能的实现方式为：

安全网关采用安全上下文对后续向终端设备发送的消息进行完整性保护，可选地进行加密保护；其中，安全网关后续向终端设备发送的消息包括：后面发送的全部消息或，部分消息。比如，对 EAP-5G 请求（ Request）消息和 EAP 5G 响应（Response）消息进行保护，但是对 EAP 成功（success）消息或 EAP 失败（failure）消息不进行安全保护。

其中，S208 和 S209 的执行顺序不作限制。

本实施例，通过安全网关向终端设备发送请求消息，终端设备根据安全网关的安全参数以及终端设备的安全参数，获取终端设备与安全网关之间的安全上下文，终端设备使用安全上下文保护发送的消息，从而，提高了终端设备向安全网关发送的消息的安全性。并通过终端设备向安全网关发送终端设备的安全参数和第一完整性消息认证信息，安全网关根据终端设备的安全参数和安全网关的安全参数，生成第二密钥，并

采用第二密钥验证第一完整性消息认证信息，安全网关向终端设备发送第二完整性消息认证信息，终端设备采用第一密钥验证第二完整性消息认证信息，安全网关使用安全上下文保护发送的消息，从而，提高了安全网关向终端设备发送的消息的安全性。

图 4 为本申请提供的另一种消息的发送方法的流程示意图，图 4 所示：

S401：终端设备向安全网关发送第一消息。

其中，第一消息中包含终端设备身份标识和终端设备的安全参数。其中，终端设备的身份标识可以是设备标示符、终端设备的永久身份信息、终端设备的永久身份信息的加密结果中的至少 1 种。

其中，第一消息可以是终端设备和非 3GPP 接入网设备交换身份标识过程中的任一消息。

S402：安全网关根据终端设备的安全参数以及安全网关的安全参数，获取终端设备与所述安全网关之间的安全上下文。

所述安全网关根据所述终端设备的安全参数以及所述安全网关的安全参数，生成第一密钥。

S403：安全网关根据第一密钥，生成第一完整性消息认证信息。

其中，完整性消息认证信息是由终端设备即将回复的消息和完整性保护密钥生成。例如，完整性认证信息可以是完整性消息认证码（MAC-I），用于对在鉴权过程中终端设备向安全网关的消息进行完整性保护验证。

S404：安全网关向终端设备发送安全网关的安全参数和所述第一完整性消息认证信息。

其中，第一完整性消息认证信息是由终端生成的完整性保护密钥，和终端设备即将发送给安全网关的下一条消息生成的。

S405：终端设备根据终端设备的安全参数和安全网关的安全参数，生成第二秘钥，并验证第一完整性消息认证信息。

第二密钥包含完整性保护密钥。可选地，第二密钥还包含加密保护密钥。进一步地，是否包含加密保护密钥可以由下面几种方法中的至少 1 种确定：根据所述安全标志位，或者选择的保护方法，或者双方提前约定好。其中，选择的保护方法比如是某些特定的公私钥方法。

若第一完整性消息认证信息验证成功，则表明第一密钥与第二密钥相同，则终端设备可以采用第二秘钥对向终端设备发送的消息进行完整性保护，或加密保护。

若第一完整性消息认证信息验证失败，则表明第一秘钥与第二秘钥不同，则需要则需要拒绝终端设备接入核心网，可选地，同时可以返回认证失败的信息。

S406：终端设备向安全网关发送第二完整性消息认证信息。

终端设备根据第二秘钥，生成第二完整性消息认证信息。并向安全网关发送第二完整性消息认证信息。其中，第二完整性消息认证信息是由安全网关生成的第二密钥和即将给终端发送的下一条消息生成的。

S407：安全网关根据第一密钥验证第二完整性消息认证信息。

若第二完整性消息认证信息验证成功，则表明第一密钥与第二密钥相同，则安全网关可以采用第一秘钥对向终端设备发送的消息进行安全保护。其中，安全保护为完整

性保护，可选地，如果生成了加密密钥，则也进行加密保护。

若第二完整性消息认证信息验证失败，则表明第一秘钥与第二秘钥不同，则需要则需要拒绝终端设备接入核心网，可选地，同时可以返回认证失败的信息。

S408：安全网关使用所述安全上下文保护向所述终端设备发送的消息。

安全网关采用安全上下文对向终端设备发送的消息进行行完整性保护，和/或加密保护。

S409：终端设备使用所述安全上下文保护向所述终端设备发送的消息。

终端设备采用安全上下文对向安全网关发送的消息进行完整性保护，可选地进行加密保护；其中，终端设备后续向安全网关发送的消息包括：后面发送的全部消息或，部分消息。

其中，S408 和 S409 的执行顺序不作限制。

本实施例，通过终端设备向安全网关发送第一消息，安全网关根据终端设备的安全参数以及安全网关的安全参数，获取终端设备与所述安全网关之间的安全上下文，安全网关向终端设备发送安全网关的安全参数和所述第一完整性消息认证信息，终端设备根据终端设备的安全参数和安全网关的安全参数，生成第二秘钥，并验证第一完整性消息认证信息，终端设备向安全网关发送第二完整性消息认证信息，安全网关根据第一密钥验证第二完整性消息认证信息，安全网关使用所述安全上下文保护向所述终端设备发送的消息，终端设备使用所述安全上下文保护向所述终端设备发送的消息，从而，提高发送的消息的安全性，并且，本实施例的第一消息是在终端设备和非 3GPP 接入网设备交换身份标识过程中的任一消息，因此，减少了信令交互过程。

图 5 为本申请提供的一种消息的发送装置的结构示意图，该消息的发送装置可以是终端设备。该装置包括：接收模块 501、处理模块 502 和发送模块 503，其中，接收模块 501 用于接收安全网关发送的请求消息，所述请求消息中包含所述安全网关的安全参数；处理模块 502 用于根据所述安全网关的安全参数以及所述消息的发送装置的安全参数，获取所述消息的发送装置与所述安全网关之间的安全上下文；发送模块 503 用于使用所述安全上下文保护发送的消息。

可选地，所述请求消息中还包括开始标志位。

可选地，所述请求消息中还包括安全标志位。

可选地，所述安全标志位包含在所述请求消息的头部或者净荷中。

可选地，所述处理模块 502 具体用于根据所述安全网关的安全参数以及所述消息的发送装置的安全参数，生成第一密钥；并根据所述第一密钥生成第一完整性消息认证信息。

可选地，所述发送模块还用于向所述安全网关发送所述消息的发送装置的安全参数和所述第一完整性消息认证信息。

可选地，所述接收模块 501 还用于接收所述安全网关发送的第二完整性消息认证信息；

所述处理模块 502 还用于根据所述第一密钥验证所述第二完整性认证信息。

可选地，所述接收模块 501 具体用于接收所述安全网关发送的响应消息，所述响应消息中包含所述第二完整性消息认证信息。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

可选地，所述发送模块 503 具体用于采用所述第一密钥对向所述安全网关发送的消息进行加密；并采用所述第一完整性消息认证信息对向所述安全网关发送的消息进行完整性保护。

本实施例的装置，对应地可用于执行图 2 所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

图 6 为本申请提供的另一种消息的发送装置的结构示意图，该消息的发送装置可以是安全网关。该装置包括发送模块 601 和接收模块 602，其中，发送模块 601 用于向终端设备发送请求消息，所述请求消息中包含所述消息的发送装置的安全参数，其中，所述消息的发送装置的安全参数用于终端设备获取所述终端设备与所述消息的发送装置之间的安全上下文；接收模块 602 用于接收所述终端设备发送的消息，所述消息使用所述终端设备与所述安全网关之间的安全上下文保护。

可选地，所述请求消息中还包括开始标志位。

可选地，所述请求消息中还包括安全标志位。

可选地，所述安全标志位包含在所述请求消息的头部或者净荷中。

可选地，所述安全上下文中包含第一密钥和第一完整性消息认证信息；

所述接收模块 602 还用于接收所述终端设备发送的所述终端设备的安全参数和所述第一完整性消息认证信息；

还包括：处理模块 603；

所述处理模块 603 用于根据所述终端设备的安全参数和所述消息的发送装置的安全参数，生成第二密钥；并根据所述第二密钥，验证所述第一完整性消息认证信息。

可选地，所述发送模块 601 还用于向所述终端设备发送的第二完整性消息认证信息。

可选地，所述发送模块 601 还用于向所述终端设备发送的响应消息，所述响应消息中包含所述第二完整性消息认证信息。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

可选地，所述发送模块 601 具体用于采用所述第二密钥对向所述终端设备发送的消息进行加密；并采用所述第二完整性消息认证信息对向所述终端设备发送的消息进行完整性保护。

本实施例的装置，对应地可用于执行图 2 所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

图 7 为本申请提供的再一种消息的发送装置的结构示意图，该消息发送装置可以是安全网关。该装置包括接收模块 701、处理模块 702 和发送模块 703，其中，接收模块 701 用于接收终端设备发送的第一消息，所述第一消息中包含所述终端设备身份标识和所述终端设备的安全参数；处理模块 702 用于根据所述终端设备的安全参数以

及所述消息的发送装置的安全参数，获取所述终端设备与所述消息的发送装置之间的安全上下文；发送模块 703 用于使用所述安全上下文保护向所述终端设备发送的消息。

可选地，所述处理模块 702 具体用于根据所述终端设备的安全参数以及所述消息的发送装置的安全参数，生成第一密钥，并根据所述第一密钥生成第一完整性消息认证信息。

可选地，所述发送模块 703 还用于向所述终端设备发送所述消息的发送装置的安全参数和所述第一完整性消息认证信息。

可选地，所述接收模块 701 还用于接收所述终端设备发送的第二完整性消息认证信息；

所述处理模块 702 还用于根据所述第一密钥验证所述第二完整性消息认证信息。

可选地，所述发送模块 703 具体用于采用所述第一密钥对向所述终端设备发送的消息进行加密；并采用所述第一完整性消息认证信息对向所述终端设备发送的消息进行完整性保护。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

本实施例的装置，对应地可用于执行图 4 所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

图 8 为本申请提供的又一种消息的发送装置的结构示意图，该消息发送装置可以是终端设备。该装置包括发送模块 801 和接收模块 802，其中，发送模块 801 用于向安全网关发送第一消息，所述第一消息中包含所述消息的发送装置身份标识和所述消息的发送装置的安全参数，所述安全参数用于所述安全网关获取所述消息的发送装置与所述安全网关之间的安全上下文；接收模块 802 用于接收所述安全网关发送的消息，所述消息使用所述消息的发送装置与所述安全网关之间的安全上下文保护。

可选地，所述安全上下文中包含第一密钥和第一完整性消息认证信息；

所述接收模块，还用于接收所述安全网关发送的所述安全网关的安全参数和所述第一完整性消息认证信息；

还包括:

处理模块 803，用于根据所述消息的发送装置的安全参数和所述安全网关的安全参数，生成第二密钥；并根据所述第二密钥，验证所述第一完整性消息。

可选地，所述发送模块 801 还用于向所述安全网关发送第二完整性消息认证信息。

可选地，所述发送模块 801 还用于采用所述安全上下文对向所述网络设备发送的消息进行加密；并采用所述第二完整性消息认证信息对向所述网络设备发送的消息进行完整性保护。

可选地，所述安全参数包括：生成安全上下文所需的参数。

可选地，所述生成安全上下文所需的参数包括协商的算法，所述协商的算法包括完整性算法和加密算法之一或全部。

本实施例的装置，对应地可用于执行图 4 所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

图 9 为本申请提供的又一种消息的发送装置的结构示意图，该消息的发送装置可以是终端设备，该装置包括处理器 901、存储器 902 和收发器 903，所述存储器 902 用于存储指令，所述收发器 903 用于和其他设备通信，所述处理器 901 用于执行所述存储器 902 中存储的指令，以使安全网关执行如图 2 所示的方法实施例的技术方案。

本实施例的装置，对应地可用于执行图 2 所示方法实施例的技术方案，其实现原理和技术效果类似，此处不再赘述。

图 10 为本申请提供的又一种消息的发送装置的结构示意图，所述消息的发送装置可以是安全网关，该装置包括处理器 1001、存储器 1002 和收发器 1003，所述存储器 1002 用于存储指令，所述收发器 1003 用于和其他设备通信，所述处理器 1001 用于执行所述存储器 1002 中存储的指令，以使安全网关执行如图 2 所示的方法实施例的技术方案。

图 11 为本申请提供的又一种消息的发送装置的结构示意图，所述消息的发送装置可以是安全网关，该装置包括处理器 1101、存储器 1102 和收发器 1103，所述存储器 1102 用于存储指令，所述收发器 1103 用于和其他设备通信，所述处理器 1101 用于执行所述存储器 1102 中存储的指令，以使安全网关执行如图 4 所示的方法实施例的技术方案。

图 12 为本申请提供的又一种消息的发送装置的结构示意图，所述消息的发送装置可以是终端设备，该装置包括处理器 1201、存储器 1202 和收发器 1203，所述存储器 1202 用于存储指令，所述收发器 1203 用于和其他设备通信，所述处理器 1201 用于执行所述存储器 1202 中存储的指令，以使安全网关执行如图 4 所示的方法实施例的技术方案。

本申请还提供一种计算机可读存储介质，应用于消息的发送装置中，所述计算机可读存储介质存储有指令，当所述指令被计算装置执行时，使得消息的发送装置执行如图 2 所述的方法。

本申请还提供一种计算机可读存储介质，应用于消息的发送装置中，所述计算机可读存储介质存储有指令，当所述指令被计算装置执行时，使得消息的发送装置执行如图 4 所述的方法。

本申请还提供一种程序产品，所述程序产品包括计算机程序，所述计算机程序存储在计算机可读存储介质中，消息的发送装置的至少一个处理器从所述计算机可读存储介质中读取所述计算机程序，所述至少一个处理执行所述计算机程序使得所述消息的发送装置执行图 2 所述的方法。

本申请还提供一种程序产品，所述程序产品包括计算机程序，所述计算机程序存储在计算机可读存储介质中，消息的发送装置的至少一个处理器从所述计算机可读存储介质中读取所述计算机程序，所述至少一个处理执行所述计算机程序使得所述消息的发送装置执行图 4 所述的方法。

在本申请的实施例中，发送模块和接收模块用于实现处理模块与其他单元或者网元的内容交互。具体的，发送模块和接收模块可以是通信接口，也可以是收发电路或者收发器，还可以是收发信机。发送模块和接收模块还可以是处理模块的通信接口或者收发电路。

处理模块用于实现对数据的处理。处理模块可以是处理电路，也可以是处理器。其中，处理器可以是中央处理器(central processing unit，CPU)，网络处理器(network processor，NP)或者 CPU 和 NP 的组合。处理器还可以进一步包括硬件芯片。上述硬件芯片可以是专用集成电路(application-specific integrated circuit，ASIC)，可编程逻辑器件(programmable logic device，PLD)或其组合。上述 PLD 可以是复杂可编程逻辑器件(complex programmable logic device，CPLD)，现场可编程逻辑门阵列(field-programmable gate array，FPGA)，通用阵列逻辑(Generic Array Logic，GAL)或其任意组合。

处理模块也可以包括多个处理单元或者处理单元包括多个子数据处理单元。具体的，处理器可以是一个单核(single-CPU)处理器，也可以是一个多核(multi-CPU)处理器。

本实施例中的消息的发送装置还可以包括存储单元。存储模块用于存储处理模块执行的计算机指令。存储模块可以是存储电路也可以是存储器。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。存储模块可以是独立于处理模块的单元，也可以是处理模块中的存储单元，在此不做限定。消息的发送装置可以包括多个存储模块或者存储模块包括多个子存储模块。

发送模块和接收模块以及处理模块可以是在物理上相互分离的单元，也可以是集成到一个或者多个物理单元中，在此不做限定。

在本申请所提供的几个实施例中，应该理解到，所揭露的装置和方法，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。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

权 利 要 求 书

1、一种消息的发送方法，其特征在于，包括：

终端设备接收安全网关发送的请求消息，所述请求消息中包含所述安全网关的安全参数；

所述终端设备根据所述安全网关的安全参数以及所述终端设备的安全参数，获取所述终端设备与所述安全网关之间的安全上下文；

所述终端设备使用所述安全上下文保护发送的消息。

2、根据权利要求 1 所述的方法，其特征在于，所述请求消息中还包括开始标志位。

3、根据权利要求 1 所述的方法，其特征在于，所述请求消息中还包括安全标志位。

4、根据权利要求 3 所述的方法，其特征在于，所述安全标志位包含在所述请求消息的头部或者净荷中。

5、根据权利要求 1-4 任一项所述的方法，其特征在于，所述终端设备根据所述安全网关的安全参数以及所述终端设备的安全参数，获取所述终端设备与所述安全网关之间的安全上下文，包括：

所述终端设备根据所述安全网关的安全参数以及所述终端设备的安全参数，生成第一密钥；

所述终端设备根据所述第一密钥，生成第一完整性消息认证信息。

6、根据权利要求 5 所述的方法，其特征在于，还包括：

所述终端设备向所述安全网关发送所述终端设备的安全参数和所述第一完整性消息认证信息。

7、根据权利要求 6 所述的方法，其特征在于，还包括：

所述终端设备接收所述安全网关发送的第二完整性消息认证信息；

所述终端设备根据所述第一密钥验证所述第二完整性认证信息。

8、根据权利要求 7 所述的方法，其特征在于，所述终端设备接收所述安全网关发送的第二完整性消息认证信息，包括：

所述终端设备接收所述安全网关发送的响应消息，所述响应消息中包含所述第二完整性消息认证信息。

9、根据权利要求 1-8 任一项所述的方法，其特征在于，

所述安全参数包括：生成安全上下文所需的参数。

10、根据权利要求 9 所述的方法，其特征在于，

所述生成安全上下文所需的参数包括：协商的算法；

所述协商的算法包括完整性算法和加密算法之一或全部。

11、根据权利要求 5 所述的方法，其特征在于，所述终端设备使用所述安全上下文保护发送的消息，包括：

所述终端设备采用所述第一密钥对向所述安全网关发送的消息进行加密；

所述终端设备采用所述第一完整性消息认证信息对向所述安全网关发送的消息进行完整性保护。

12、一种消息的发送方法，其特征在于，包括：

安全网关向终端设备发送请求消息，所述请求消息中包含所述安全网关的安全参数，其中，所述安全网关的安全参数用于终端设备获取所述终端设备与所述安全网关之间的安全上下文；

所述安全网关接收所述终端设备发送的消息，所述消息使用所述终端设备与所述安全网关之间的安全上下文保护。

13、根据权利要求 12 所述的方法，其特征在于，所述安全上下文中包含第一密钥和第一完整性消息认证信息；

所述方法还包括：

所述安全网关接收所述终端设备发送的所述终端设备的安全参数和所述第一完整性消息认证信息；

所述安全网关根据所述终端设备的安全参数和所述安全网关的安全参数，生成第二密钥；

所述安全网关根据所述第二密钥，验证所述第一完整性消息认证信息。

14、根据权利要求 13 所述的方法，其特征在于，还包括：

所述安全网关向所述终端设备发送的第二完整性消息认证信息。

15、根据权利要求 14 所述的方法，其特征在于，所述安全网关向所述终端设备发送的第二完整性消息认证信息，包括：

所述安全网关向所述终端设备发送的响应消息，所述响应消息中包含所述第二完整性消息认证信息。

16、根据权利要求 12-15 任一项所述的方法，其特征在于，

所述安全参数包括：生成安全上下文所需的参数。

17、根据权利要求 16 所述的方法，其特征在于，还包括：

所述安全网关采用所述第二密钥对向所述终端设备发送的消息进行加密；

所述安全网关采用所述第二完整性消息认证信息对向所述终端设备发送的消息进行完整性保护。

18、一种消息的发送装置，其特征在于，包括：

接收模块，用于接收安全网关发送的请求消息，所述请求消息中包含所述安全网关的安全参数；

处理模块，用于根据所述安全网关的安全参数以及所述消息的发送装置的安全参数，获取所述消息的发送装置与所述安全网关之间的安全上下文；

发送模块，用于使用所述安全上下文保护发送的消息。

19、根据权利要求 18 所述的装置，其特征在于，所述处理模块具体用于根据所述安全网关的安全参数以及所述消息的发送装置的安全参数，生成第一密钥；并根据所述第一密钥，生成第一完整性消息认证信息。

20、根据权利要求 19 所述的装置，其特征在于，所述发送模块还用于向所述安全网关发送所述消息的发送装置的安全参数和所述第一完整性消息认证信息。

21、根据权利要求 20 所述的装置，其特征在于，所述接收模块还用于接收所述安全网关发送的第二完整性消息认证信息；

所述处理模块还用于根据所述第一密钥验证所述第二完整性认证信息。

22、根据权利要求 18-21 任一项所述的装置，其特征在于，

所述发送模块具体用于采用所述第一密钥对向所述安全网关发送的消息进行加密；并采用所述第一完整性消息认证信息对向所述安全网关发送的消息进行完整性保护。

23、一种消息的发送装置，其特征在于，包括：

发送模块，用于向终端设备发送请求消息，所述请求消息中包含所述消息的发送装置的安全参数，其中，所述消息的发送装置的安全参数用于终端设备获取所述终端设备与所述消息的发送装置之间的安全上下文；

接收模块，用于接收所述终端设备发送的消息，所述消息使用所述终端设备与所述消息的发送装置之间的安全上下文保护。

24、根据权利要求 23 所述的装置，其特征在于，所述安全上下文中包含第一密钥和第一完整性消息认证信息；

所述接收模块还用于接收所述终端设备发送的所述终端设备的安全参数和所述第一完整性消息认证信息；

还包括：处理模块；

所述处理模块，用于根据所述终端设备的安全参数和所述消息的发送装置的安全参数，生成第二密钥；并根据所述第二密钥，验证所述第一完整性消息认证信息。

25、根据权利要求 24 所述的装置，其特征在于，

所述发送模块还用于向所述终端设备发送的第二完整性消息认证信息。

26、根据权利要求 25 所述的装置，其特征在于，

所述发送模块具体用于采用所述第二密钥对向所述终端设备发送的消息进行加密；并采用所述第二完整性消息认证信息对向所述终端设备发送的消息进行完整性保护。

27、一种消息的发送装置，其特征在于，包括：

处理器、存储器和收发器，所述存储器用于存储指令，所述收发器用于和其他设备通信，所述处理器用于执行所述存储器中存储的指令，以使消息的发送装置执行如权利要求 1-11 任一项所述的方法。

28、一种消息的发送装置，其特征在于，包括：

处理器、存储器和收发器，所述存储器用于存储指令，所述收发器用于和其他设备通信，所述处理器用于执行所述存储器中存储的指令，以使消息的发送装置执行如权利要求 12-17 任一项所述的方法。

29、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有指令，当所述指令被计算装置执行时，使得消息的发送装置执行如权利要求 1-11 任一项所述的方法。

30、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质存储有指令，当所述指令被计算装置执行时，使得消息的发送装置执行如权利要求 12-17 任一项所述的方法。

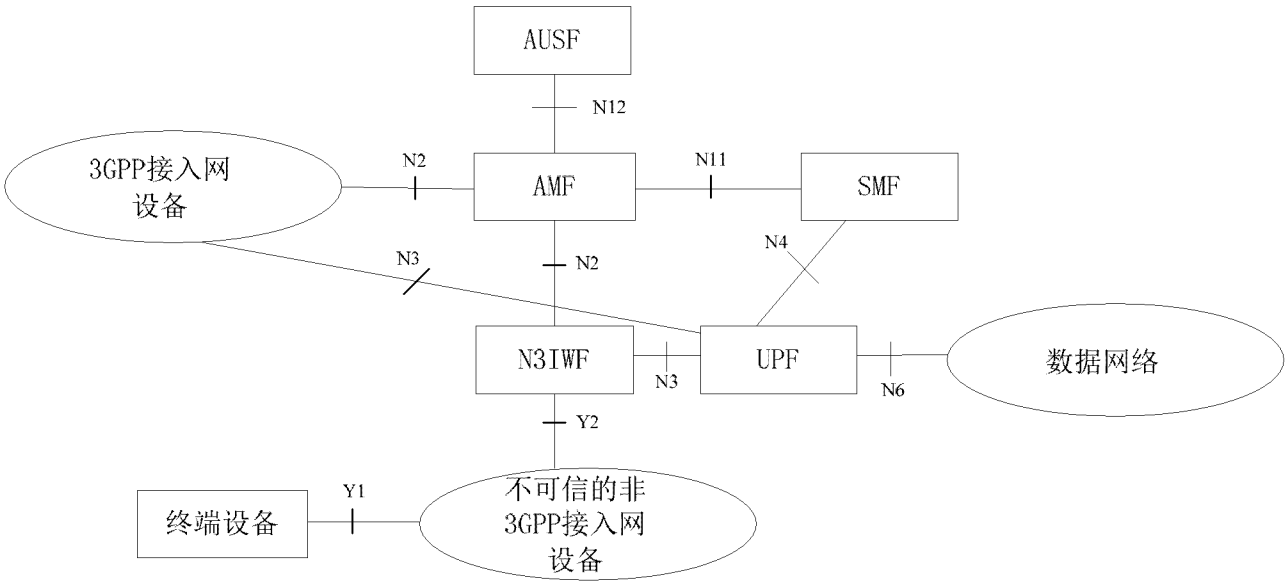
AUSF
N12
3GPP接入网
设备
N2
AMF
N11
SMF
N4
N3
N2
N3IWF
N3
UPF
N6
数据网络
Y2
Y1
终端设备
不可信的非
3GPP接入网
设备

图 1

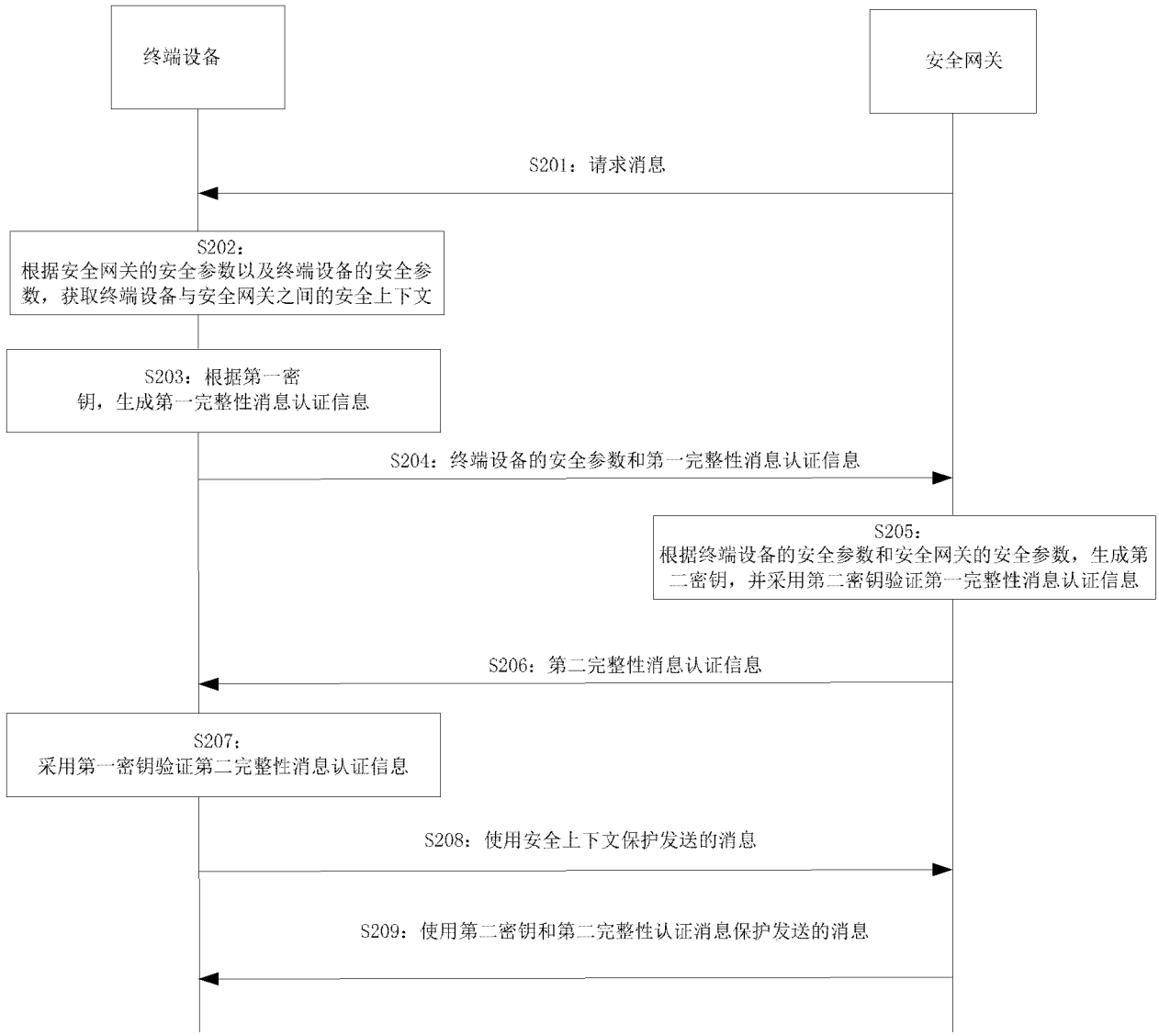
终端设备
安全网关
S201：请求消息
S202：
根据安全网关的安全参数以及终端设备的安全参数，获取终端设备与安全网关之间的安全上下文
S203：根据第一密钥，生成第一完整性消息认证信息
S204：终端设备的安全参数和第一完整性消息认证信息
S205：
根据终端设备的安全参数和安全网关的安全参数，生成第二密钥，并采用第二密钥验证第一完整性消息认证信息
S206：第二完整性消息认证信息
S207：
采用第一密钥验证第二完整性消息认证信息
S208：使用安全上下文保护发送的消息
S209：使用第二密钥和第二完整性认证消息保护发送的消息

图 2

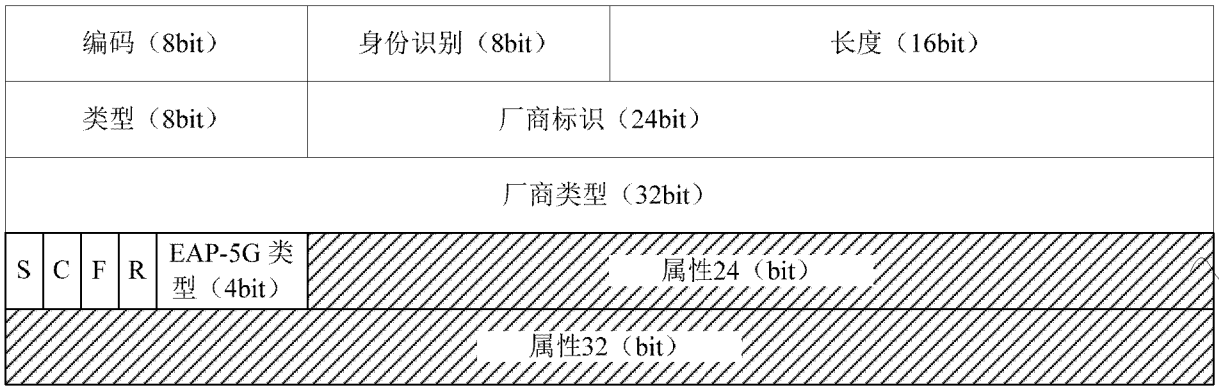
编码（8bit）
身份识别（8bit）
长度（16bit）
类型（8bit）
厂商标识（24bit）
厂商类型（32bit）
S
C
F
R
EAP-5G 类型（4bit）
属性24（bit）
属性32（bit）

图 3a

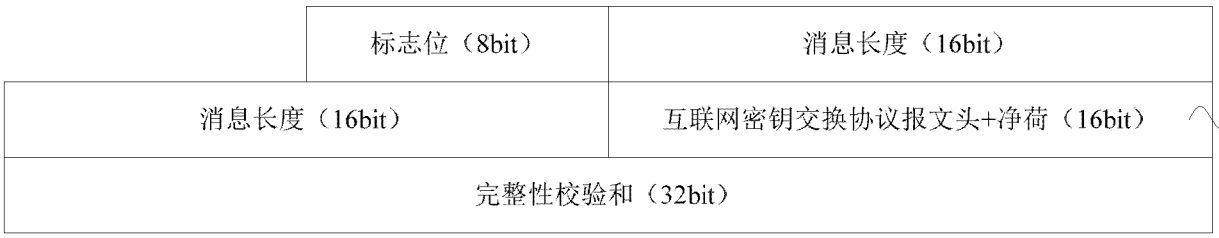
标志位（8bit）
消息长度（16bit）
消息长度（16bit）
互联网密钥交换协议报文头+净荷（16bit）
完整性校验和（32bit）

图 3b


发起者安全联系标识（32bit）
响应者安全联系标识（32bit）
后续负载类型（8bit）
主版本号（4bit）
副版本号（4bit）
交换类型（8bit）
标志位（8bit）
消息标识（32bit）
长度（32bit）

图 3c

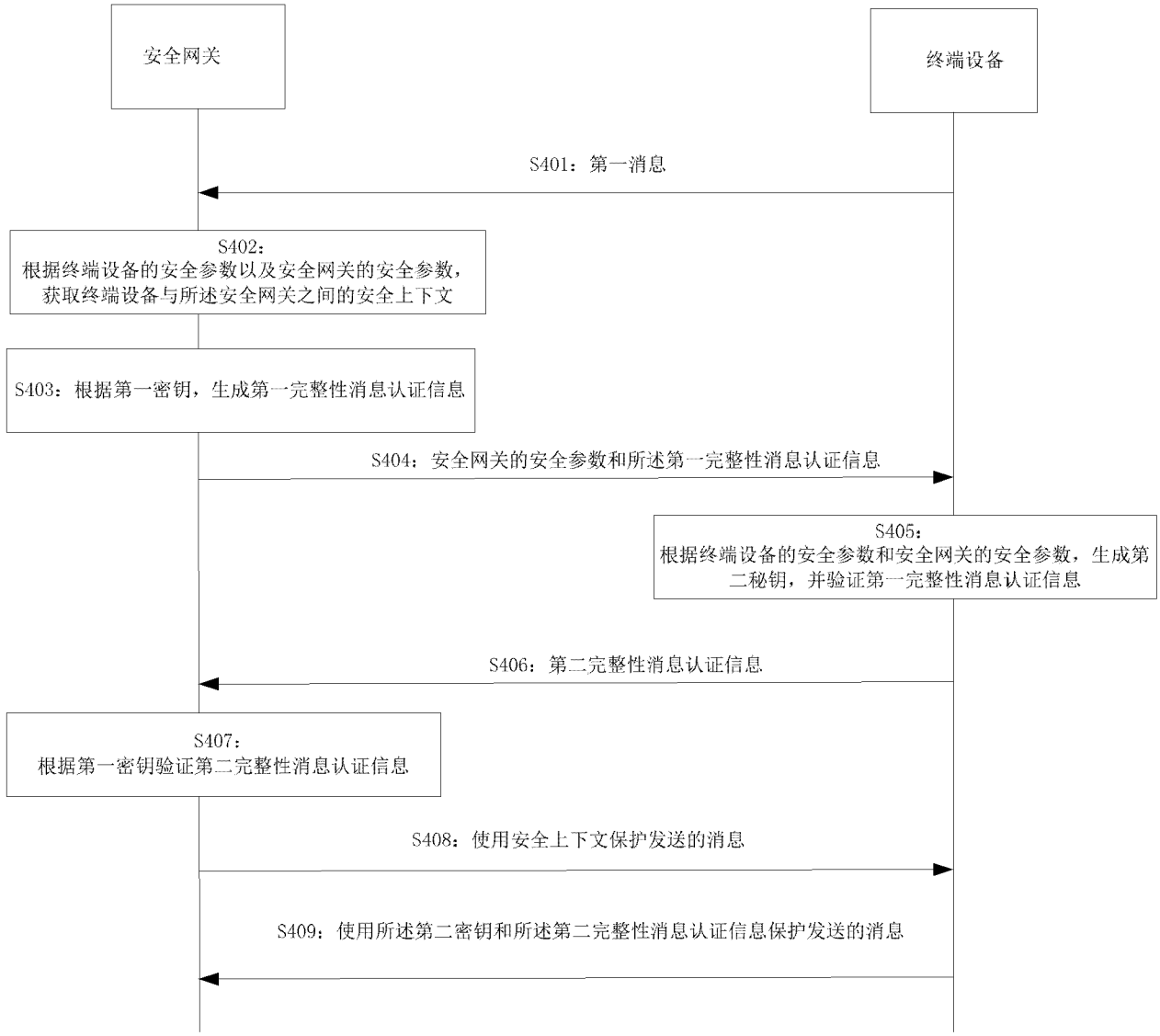
安全网关
终端设备
S401：第一消息
S402：
根据终端设备的安全参数以及安全网关的安全参数，
获取终端设备与所述安全网关之间的安全上下文
S403：根据第一密钥，生成第一完整性消息认证信息
S404：安全网关的安全参数和所述第一完整性消息认证信息
S405：
根据终端设备的安全参数和安全网关的安全参数，生成第二秘钥，并验证第一完整性消息认证信息
S406：第二完整性消息认证信息
S407：
根据第一密钥验证第二完整性消息认证信息
S408：使用安全上下文保护发送的消息
S409：使用所述第二密钥和所述第二完整性消息认证信息保护发送的消息

图 4

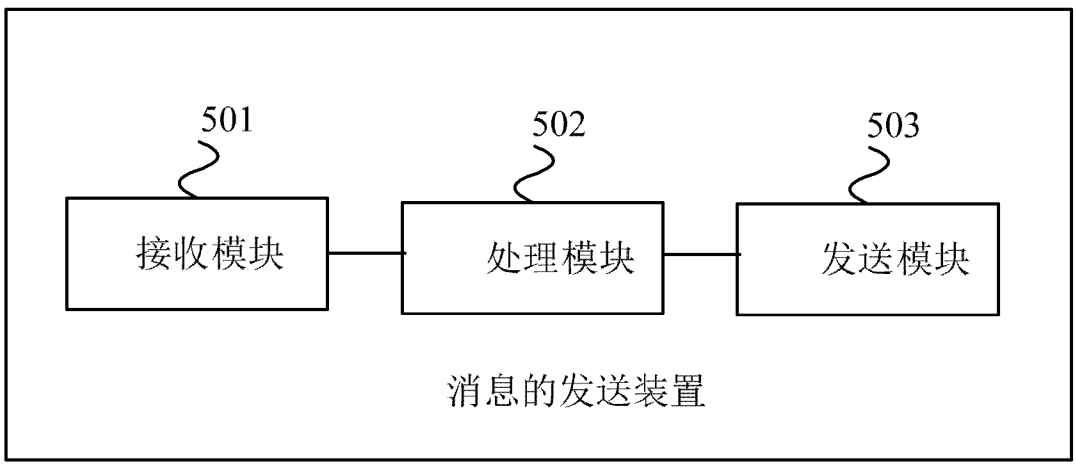
501
502
503
接收模块
处理模块
发送模块
消息的发送装置

图 5

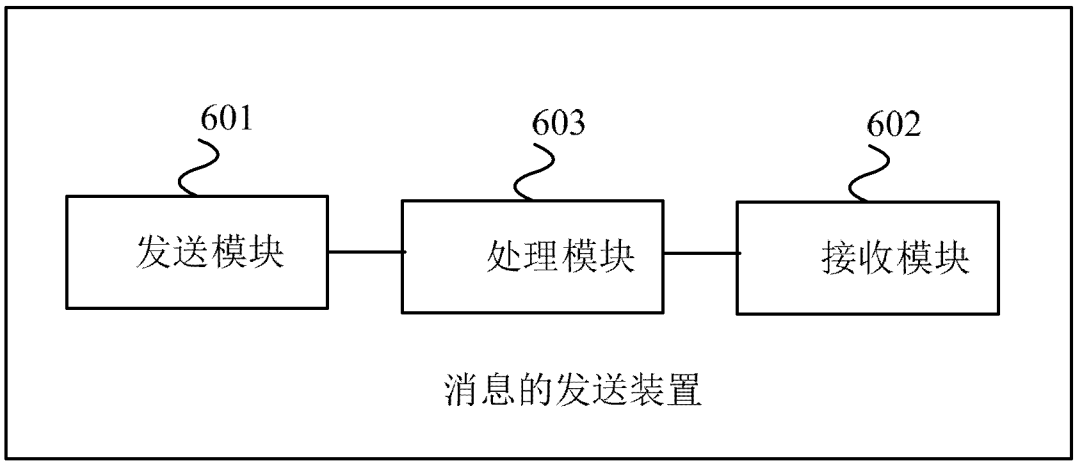
601
603
602
发送模块
处理模块
接收模块
消息的发送装置

图 6

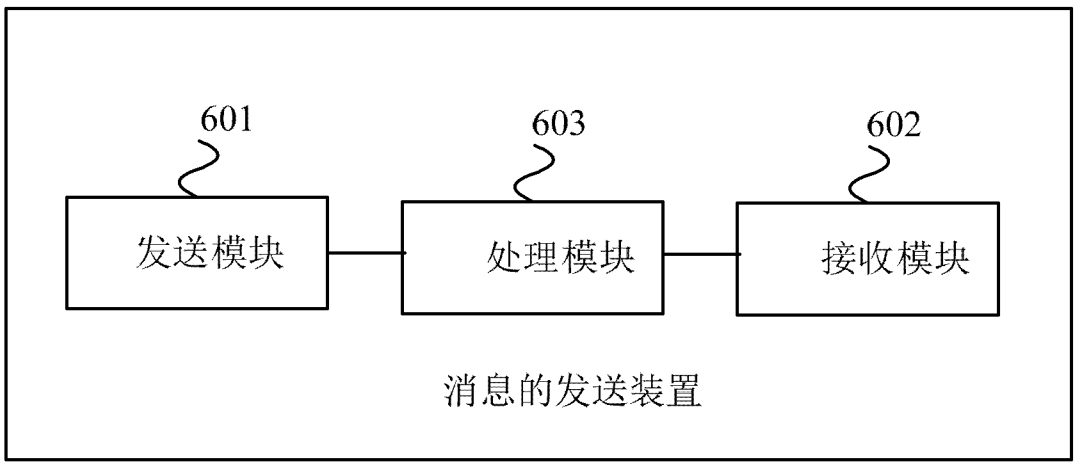
601
603
602
发送模块
处理模块
接收模块
消息的发送装置

图 7

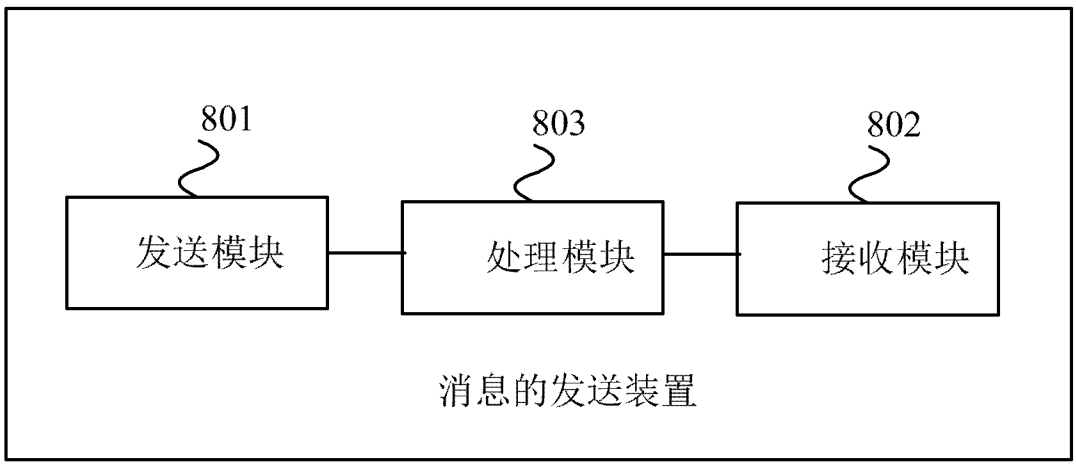
801
803
802
发送模块
处理模块
接收模块
消息的发送装置

图 8

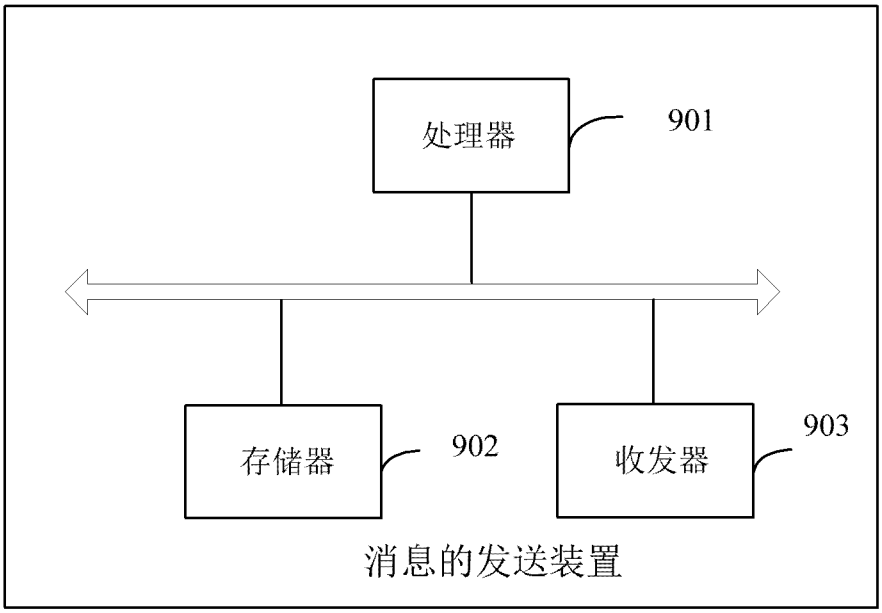
处理器
901
存储器
902
收发器
903
消息的发送装置

图 9

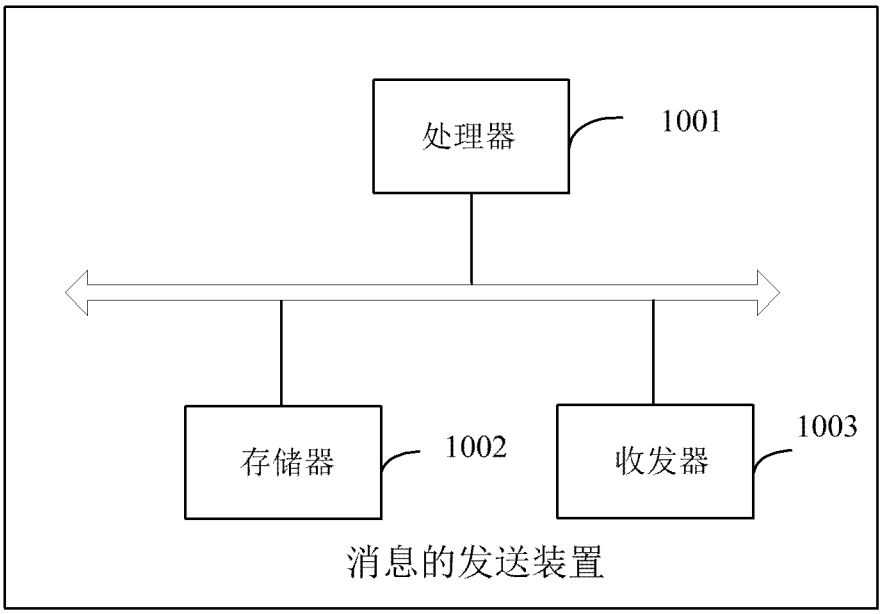
处理器
1001
存储器
1002
收发器
1003
消息的发送装置

图 10

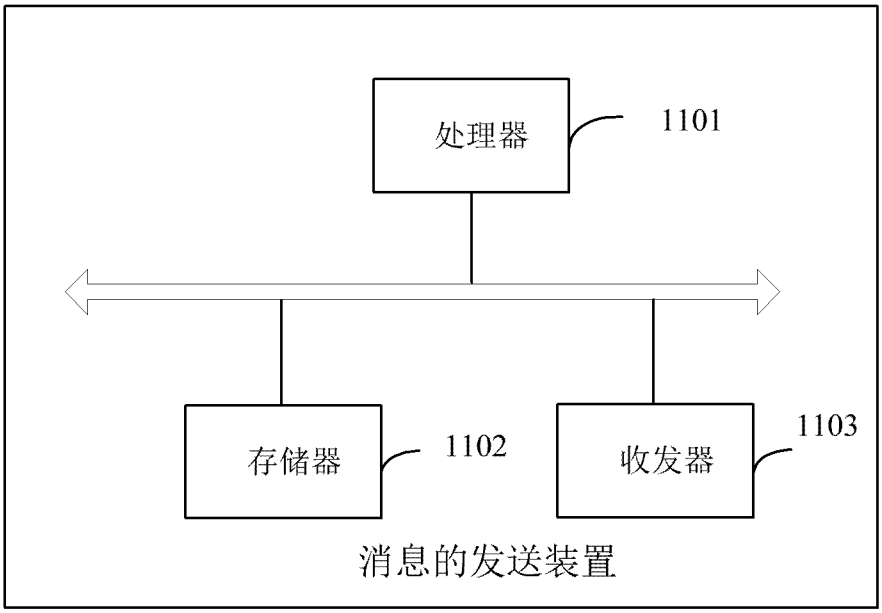
处理器
1101
存储器
1102
收发器
1103
消息的发送装置

图 11

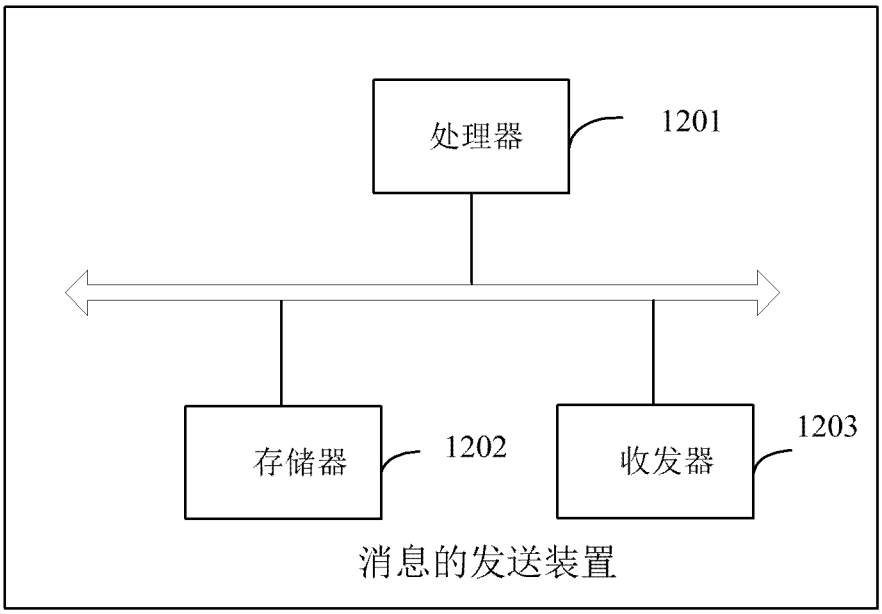
处理器
1201
存储器
1202
收发器
1203
消息的发送装置

图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/124490

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L;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)

CNPAT, CNKI, WPI, EPODOC, 3GPP: 安全, 加密, 密钥, 网关, 请求, 响应, 参数, 上下文, 协商, 保护, 交换, security, gateway, N3IWF, eDPG, SeGW, key, request, response, parameter, context, negotiate, exchange

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101815296 A (HUAWEI TECHNOLOGIES CO., LTD.) 25 August 2010 (2010-08-25) description, paragraphs 0043-0069, and figures 2-3	1-30
A	CN 101631309 A (SHANGHAI HUAWEI TECHNOLOGIES CO., LTD.) 20 January 2010 (2010-01-20) entire document	1-30
A	WO 2006122213 A2 (NETWORK EQUIPMENT TECHNOLOGIES, INC.) 16 November 2006 (2006-11-16) entire document	1-30
A	CN 101754211 A (HUAWEI TECHNOLOGIES CO., LTD.) 23 June 2010 (2010-06-23) entire document	1-30
A	MOTOROLA MOBILITY et al. "Details of EAP-5G Solution for Registration via Untrusted Non-3GPP Access" *3GPP SA WG2 Meeting #123 S2-177681,* 27 October 2017 (2017-10-27), entire document	1-30

☐ 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
11 March 2019	**27 March 2019**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/124490

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	101815296	A	25 August 2010	WO	2010094244	A1	26 August 2010
				EP	2400791	A4	15 February 2012
				EP	2400791	A1	28 December 2011
CN	101631309	A	20 January 2010	CN	101631309	B	20 March 2013
WO	2006122213	A2	16 November 2006	CA	2607665	A1	10 November 2006
				US	2006276139	A1	07 December 2006
				EP	1896982	A4	02 November 2011
				US	2006276138	A1	07 December 2006
				US	8224333	B2	17 July 2012
				EP	1889496	A2	20 February 2008
				US	2006276137	A1	07 December 2006
				WO	2006122226	A2	16 November 2006
				EP	1896982	A2	12 March 2008
				WO	2006122226	A3	03 May 2007
				WO	2006122213	A3	01 November 2007
				US	7885659	B2	08 February 2011
				EP	1941636	A2	09 July 2008
				WO	2006122226	B1	14 June 2007
				CA	2606965	A1	16 November 2006
				EP	1941636	A4	19 October 2016
				CA	2606966	A1	16 November 2006
				EP	1896982	B1	07 January 2015
				WO	2006122213	B1	21 December 2007
				WO	2008048200	A3	02 April 2009
				US	2013064369	A1	14 March 2013
				EP	1889496	A4	26 October 2011
				WO	2008048200	A2	24 April 2008
				US	8750827	B2	10 June 2014
				US	8380167	B2	19 February 2013
CN	101754211	A	23 June 2010	WO	2010069202	A1	24 June 2010

国际检索报告

国际申请号
PCT/CN2018/124490

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L;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）)

CNPAT, CNKI, WPI, EPODOC, 3GPP：安全，加密，密钥，网关，请求，响应，参数，上下文，协商，保护，交换，security, gateway, N3IWF, eDPG, SeGW, key, request, response, parameter, context, negotiate, exchange

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 101815296 A (华为技术有限公司) 2010年 8月 25日 (2010-08-25) 说明书第0043段-第0069段，图2-3	1-30
A	CN 101631309 A (上海华为技术有限公司) 2010年 1月 20日 (2010-01-20) 全文	1-30
A	WO 2006122213 A2 (NETWORK EQUIPMENT TECHNOLOGIES, INC.) 2006年 11月 16日 (2006-11-16) 全文	1-30
A	CN 101754211 A (华为技术有限公司) 2010年 6月 23日 (2010-06-23) 全文	1-30
A	MOTOROLA MOBILITY等. "Details of EAP-5G Solution for registration via untrusted non-3GPP access" 3GPP SA WG2 Meeting #123 S2-177681, 2017年 10月 27日 (2017-10-27), 全文	1-30

☐ 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
2019年 3月 11日	2019年 3月 27日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王侠
传真号 (86-10)62019451	电话号码 86-10-53961750

表 PCT/ISA/210 (第2页) (2015年1月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/124490

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	101815296	A	2010年 8月 25日	WO	2010094244	A1	2010年 8月 26日
				EP	2400791	A4	2012年 2月 15日
				EP	2400791	A1	2011年 12月 28日
CN	101631309	A	2010年 1月 20日	CN	101631309	B	2013年 3月 20日
WO	2006122213	A2	2006年 11月 16日	CA	2607665	A1	2006年 11月 10日
				US	2006276139	A1	2006年 12月 7日
				EP	1896982	A4	2011年 11月 2日
				US	2006276138	A1	2006年 12月 7日
				US	8224333	B2	2012年 7月 17日
				EP	1889496	A2	2008年 2月 20日
				US	2006276137	A1	2006年 12月 7日
				WO	2006122226	A2	2006年 11月 16日
				EP	1896982	A2	2008年 3月 12日
				WO	2006122226	A3	2007年 5月 3日
				WO	2006122213	A3	2007年 11月 1日
				US	7885659	B2	2011年 2月 8日
				EP	1941636	A2	2008年 7月 9日
				WO	2006122226	B1	2007年 6月 14日
				CA	2606965	A1	2006年 11月 16日
				EP	1941636	A4	2016年 10月 19日
				CA	2606966	A1	2006年 11月 16日
				EP	1896982	B1	2015年 1月 7日
				WO	2006122213	B1	2007年 12月 21日
				WO	2008048200	A3	2009年 4月 2日
				US	2013064369	A1	2013年 3月 14日
				EP	1889496	A4	2011年 10月 26日
				WO	2008048200	A2	2008年 4月 24日
				US	8750827	B2	2014年 6月 10日
				US	8380167	B2	2013年 2月 19日
CN	101754211	A	2010年 6月 23日	WO	2010069202	A1	2010年 6月 24日