(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
2021 年 2 月 18 日 (18.02.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/027435 A1

(51) 国际专利分类号:
H04W 12/00 (2009.01) *H04L 29/06* (2006.01)

(21) 国际申请号: PCT/CN2020/100310

(22) 国际申请日: 2020 年 7 月 5 日 (05.07.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910736599.8 2019年8月9日 (09.08.2019) CN
201911088795.5 2019年11月8日 (08.11.2019) 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: 张 博 (**ZHANG, Bo**); 中 国 广 东 省 深 圳 市 龙 岗 区 坂 田 华 为 总 部 办 公 楼, Guangdong 518129 (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, IT, 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, 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, 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)。

(54) **Title:** METHOD AND APPARATUS FOR DETERMINING SECURITY PROTECTION MODE

(54) 发明名称: 一种安全保护方式确定方法及装置

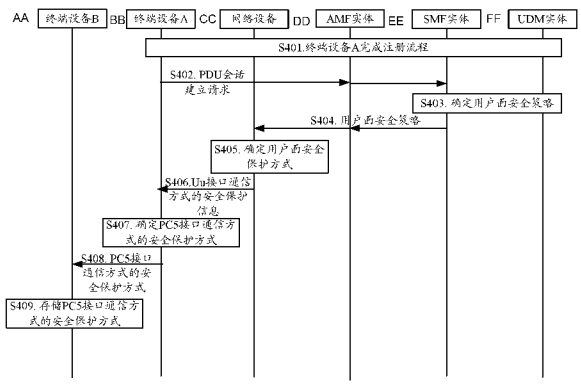

图 4

S401 A terminal device A completes a registration process
S402 PDU session establishment request
S403 Determine a user plane security policy
S404 The user plane security policy
S405 Determine a user plane security protection mode
S406 Security protection information of a Uu interface communication mode
S407 Determine a security protection mode of a PC5 interface communication mode
S408 The security protection mode of the PC5 interface communication mode
S409 Store the security protection mode of the PC5 interface communication mode
AA Terminal device B
BB Terminal device A
CC Network device
DD AMF entity
EE SMF entity
FF UDM entity

(57) **Abstract:** Disclosed are a method and apparatus for determining a security protection mode. In the method, a terminal device may determine a security protection mode of a second communication mode according to security protection information of a first communication mode. Thus, when the terminal device switches from the first communication mode to the second communication mode, the terminal device can directly use the security protection mode of the second communication mode to protect transmitted data, so that the data security of the terminal device after the communication mode is switched can be guaranteed.

(57) 摘要: 本申请实施例公开了一种安全保护方式确定方法及装置，在该方法中，终端设备可以根据第一通信方式的安全保护信息，确定第二通信方式的安全保护方式。这样，当所述终端设备在从第一通信方式切换到所述第二通信方式时，可以直接使用所述第二通信方式的安全保护方式保护传输的数据，从而可以保证通信方式切换后的所述终端设备的数据安全性。

WO 2021/027435 A1

[见续页]

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种安全保护方式确定方法及装置

技术领域

本申请涉及通信技术领域，尤其涉及一种安全保护方式确定方法及装置。

背景技术

随着通信技术的发展，通信系统可以支持终端设备之间通过多种通信方式通信。例如，PC5 接口通信方式、Uu 接口通信方式等。

PC5 接口通信方式：两个终端设备之间可以通过 PC5 接口建立直连链路进行数据通信。

Uu 接口为终端设备与基站之间的通信接口，其中 Uu 接口通信方式：具体可以包括两种场景：

场景一：终端设备 A 和终端设备 B 分别通过 Uu 接口接入为其服务的网络设备 A 和网络设备 B，然后终端设备 A 通过网络设备 A 将数据发送给核心网设备（例如用户面功能（User Plane Function，UPF）实体），再由所述核心网设备通过网络设备 B 转发给终端设备 B。

场景二：终端设备 A 和终端设备 B 分别通过 Uu 接口接入为其服务的网络设备 A 和网络设备 B，然后终端设备 A 通过网络设备 A、核心网设备将数据转发给数据网络（Date Network，DN）中的应用服务器，所述应用服务器再通过核心网设备、网络设备 B，将数据转发给终端设备 B。

目前，通信系统可以支持终端设备切换通信方式。例如，终端设备在使用 Uu 接口通信方式传输业务数据的过程中，可以被触发采用 PC5 接口通信方式传输后续的业务数据。又例如，终端设备在使用 PC5 接口通信方式传输业务数据时，也可以被触发采用 Uu 接口通信方式传输后续的业务数据。

我们知道，为了保证业务数据的安全性，通信系统会采用相应的数据安全保护机制。然而，不同的通信方式对应的数据安全保护方式可能存在差异。例如，终端设备采用 Uu 接口通信方式时，对传输的数据进行了加密，当所述终端设备切换采用 PC5 接口通信方式时，不对传输的数据进行加密，那么在群组通信的情况下，非接收端的其他终端设备也可以窃听到数据，导致终端设备的数据安全性降低。

那么，在支持终端设备切换通信方式的通信系统中，在终端设备切换通信方式后，如何保证数据传输的安全性，是本领域技术人员亟待解决的问题。

发明内容

本申请提供一种安全保护方式确定方法及装置，用于在终端设备切换通信方式后，保证终端设备的数据传输安全性。

第一方面，本申请实施例提供了一种安全保护方式确定方法，该方法可以包括以下步

骤：第一终端设备获取第一通信方式的安全保护信息，其中，所述安全保护信息包含第一安全保护方式，和/或，第一安全策略；所述第一安全保护方式对应所述第一通信方式，用于保护所述第一终端设备采用所述第一通信方式时传输的数据，所述第一安全策略为所述第一终端设备的所述第一通信方式的安全策略；然后，所述第一终端设备根据所述安全保护信息，确定第二安全保护方式，所述第二安全保护方式对应第二通信方式，用于保护所述第一终端设备采用第二通信方式时传输的数据。

通过该方法，第一终端设备可以根据第一通信方式的安全保护信息，确定第二通信方式的安全保护方式。这样，当所述第一终端设备在从第一通信方式切换到所述第二通信方式时，可以直接使用所述第二通信方式的安全保护方式保护传输的数据，从而可以保证通信方式切换后的所述第一终端设备的数据安全性。

在一个可能的设计中，所述第一终端设备可以在请求使用所述第一通信方式时或将要使用所述第一通信方式时，即获取所述第一通信方式的安全保护信息，并根据所述安全保护信息，预先确定第二安全保护方式。这样，当所述第一终端设备在从所述第一通信方式切换到所述第二通信方式时，可以直接使用所述第二安全保护方式进行保护，避免在切换过程中确定所述第二安全保护方式造成的时延，可以提高所述第一终端设备的通信效率。

示例性的，所述第一终端设备可以在 PDU 会话建立流程或者注册中，从网络设备获取 Uu 接口通信方式的安全保护信息，并通过该安全保护信息，确定 PC5 接口通信方式对应的第二安全保护方式。

示例性的，所述第一终端设备还可以在请求使用 PC5 接口通信方式时，从本地或者应用服务器获取 PC5 接口通信方式的安全保护信息，并通过该安全保护信息，确定 Uu 接口通信方式对应的第二安全保护方式。

示例性的，所述第一终端设备还可以在请求使用 PC5 接口通信方式时，从网络设备获取 Uu 接口通信方式的第一安全保护信息以及从本地或者应用服务器获取 PC5 接口通信方式的第二安全保护信息，然后根据第一安全保护信息和第二安全保护信息的优先级选择优先级高的安全保护信息作为目标安全保护信息（例如，以第一安全保护信息为第一优先级，或者以第二安全保护信息为第一优先级），接着根据目标安全保护信息确定 Uu 接口通信方式对应的第二安全保护方式。

在一个可能的设计中，所述第一终端设备可以在确定从所述第一通信方式切换到所述第二通信方式的情况下，获取所述第一通信方式的安全保护信息，并根据所述安全保护信息，预先确定第二安全保护方式。可选的，所述第一终端设备可以在切换前、切换中、切换后，执行上述流程，本申请对此不作限定。可选的，所述第一通信方式的第一安全保护方式可以为所述第一终端设备采用场景一的方法确定的，或者其他方式确定的本申请对此不作限定。

在一个可能的设计中，为了保证所述第一终端设备切换通信方式后，所述第一终端设备的数据传输安全性，所述第一终端设备确定的所述第二安全保护方式的保护等级不低于所述第一通信方式的安全保护信息规定的保护等级。

在一个可能的设计中，当所述安全保护信息为所述第一安全保护方式时，所述第一终端设备根据所述安全保护信息，确定所述第二安全保护方式，包括：

所述第一终端设备确定所述第二安全保护方式与所述第一安全保护方式相同；或者

所述第一终端设备获取第二安全策略，所述第二安全策略为所述第一终端设备的所述

第二通信方式的安全策略；所述第一终端设备根据所述第二安全策略、所述第一安全保护方式，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全保护方式的保护等级。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于第一安全保护方式。另外，当所述第一终端设备能够获取第二安全策略时，进一步保证所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级。

在一个可能的设计中，所述第一终端设备根据所述第二安全策略、所述第一安全保护方式，确定所述第二安全保护方式，包括：

当所述第一安全保护方式的保护等级为需要安全保护，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为优先安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级；

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于所述第二安全策略和所述第一安全保护方式的保护等级。

在一个可能的设计中，当所述安全保护信息为所述第一安全策略时，所述第一终端设备根据所述安全保护信息，确定所述第二安全保护方式，包括：

所述第一终端设备根据所述第一安全策略，确定所述第二安全保护方式；或者

所述第一终端设备获取第二安全策略，所述第二安全策略为所述第一终端设备的所述第二通信方式的安全策略；所述第一终端设备根据所述第二安全策略、所述第一安全策略，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全策略的保护等级。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于第一安全策略。另外，当所述第一终端设备能够获取第二安全策略时，进一步保证所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级。

在一个可能的设计中，所述第一终端设备根据所述第二安全策略、所述第一安全策略，确定所述第二安全保护方式，包括：

当所述第二安全策略的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为优先安全保护或者不需要安全保护时，所述第一终端设备根据所述第一安全策略的保护等级，确定所述第二安全保护方式的保护等级。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于所述第二安全策略和所述第一安全策略的保护等级。

在一个可能的设计中，所述第一终端设备根据所述第一安全策略，确定所述第二安全

保护方式，包括：

当所述第一安全策略的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全策略的保护等级为优先安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级；

当所述第一安全策略保护等级为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于所述第一安全策略的保护等级。

在一个可能的设计中，在所述第一终端设备确定第二安全保护方式之后，所述第一终端设备还可以通过以下方法，确定第四安全保护方式，其中，所述第四安全保护方式用于保护所述第一终端设备与第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据。这样，所述第一终端设备可以在切换到第二通信方式，并与所述第二终端设备进行数据传输时，直接采用所述第四安全保护方式，保护所述第一终端设备与所述第二终端设备之间传输的数据。

方法一：所述第一终端设备向第二终端设备发送所述第二安全保护方式，并接收所述第二终端设备根据所述第二安全保护方式和第三安全保护方式确定的第四安全保护方式。

方法二：所述第一终端设备接收第二终端设备发送的第三安全保护方式，并根据所述第二安全保护方式和所述第三安全保护方式，确定第四安全保护方式。

其中，在以上方式中，所述第四安全保护方式的保护等级不低于所述第二安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；所述第三安全保护方式用于保护所述第二终端设备采用第二通信方式时传输的数据，所述第四安全保护方式用于保护所述第一终端设备与所述第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据。

在一个可能的设计中，所述第一终端设备根据所述第二安全保护方式和所述第三安全保护方式，确定第四安全保护方式，包括：

当所述第二安全保护方式和所述第三安全保护方式中至少一项的保护等级为需要安全保护时，所述第一终端设备确定所述第四安全保护方式的保护等级为需要安全保护；

当所述第二安全保护方式和所述第三安全保护方式的保护等级均为不需要安全保护时，所述第一终端设备确定所述第四安全保护方式的保护等级为不需要安全保护。

通过该设计，可以保证所述第四安全保护方式的保护等级不低于所述第二安全保护方式和所述第三安全保护方式。

在一个可能的设计中，当所述安全保护信息为所述第一安全策略时，所述第二安全保护方式具体用于保护所述第一终端设备与第二终端设备之间采用所述第二通信方式时进行数据传输时传输的数据；所述第一终端设备可以通过以下方法与第二终端设备协商，确定所述第二安全保护方式：

方法一：所述第一终端设备向所述第二终端设备发送所述第一安全策略，并接收所述第二终端设备根据所述第一安全策略和第三安全策略确定的所述第二安全保护方式；或者

方法二：所述第一终端设备接收第二终端设备发送的所述第三安全策略；并根据所述第一安全策略和所述第三安全策略，确定所述第二安全保护方式；

其中，所述第二安全保护方式的保护等级不低于所述第一安全策略的保护等级，且不低于所述第三安全策略的保护等级；所述第三安全策略为所述第二终端设备的所述第一通信方式的保护等级。

在一个可能的设计中，所述第一终端设备根据所述第一安全策略和所述第三安全策略，确定所述第二安全保护方式，包括：

当所述第一安全策略和所述第三安全策略中至少一项的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全策略和所述第三安全策略的保护等级均为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护；

当所述第一安全策略和所述第三安全策略的保护等级均为优先安全保护时，或者当所述第一安全策略和所述第三安全策略中其中一项的保护等级为优先安全保护，另一项的保护等级为不需要安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于所述第一安全策略和所述第三安全策略的保护等级。

在一个可能的设计中，所述第一终端设备确定从第一通信方式切换到第二通信方式时，获取所述第一通信方式的所述安全保护信息。

在一个可能的设计中，当所述第二通信方式为 Uu 接口通信方式时，所述第一终端设备根据所述安全保护信息，确定所述第二安全保护方式，包括：

所述第一终端设备向网络设备发送所述安全保护信息；并从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据所述安全保护信息确定的；或者

所述第一终端设备向应用服务器发送所述安全保护信息，以及向网络设备发送请求消息；所述第一终端设备从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据从所述应用服务器获取的所述安全保护信息确定的。

通过该设计，所述第一终端设备可以从网络设备获取所述第二安全保护方式。

在一个可能的设计中，所述安全保护信息中包含所述第一安全保护方式时，

所述第二安全保护方式与所述第一安全保护方式相同；或者

所述第二安全保护方式的保护等级高于所述第一安全保护方式的保护等级；或者

所述第二安全保护方式为所述网络设备根据所述第一安全保护方式和/或第二安全策略确定的，其中，所述第二安全策略为所述网络设备获得的所述第一终端设备采用所述第二通信方式的保护等级；或者

所述第二安全保护方式为所述网络设备根据所述第一安全保护方式以及第三安全保护方式确定的，其中，所述第三安全保护方式为所述网络设备根据所述第二安全策略确定的。

通过该设计，所述网络设备可以通过多种方法，确定所述第二安全保护方式。

在一个可能的设计中，当所述第二安全策略的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为优先安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为优先安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级由所述网络设备指定；

当所述第二安全策略的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级为不需要安全保护。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于所述第二安全策略和所述第一安全保护方式的保护等级。

在一个可能的设计中，当所述第三安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级为不需要安全保护。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于所述第三安全保护方式和所述第一安全保护方式的保护等级。

在一个可能的设计中，当所述第二通信方式为 PC5 接口通信方式时，所述第二安全保护方式具体用于保护所述第一终端设备与第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据；所述第一终端设备可以通过以下方法与第二终端设备协商，确定所述第二安全保护方式：

方法一：当所述安全保护信息包含所述第一安全保护方式时，所述第一终端设备向第二终端设备发送所述第一安全保护方式，并从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式和第三安全保护方式确定的，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；

方法二：当所述安全保护信息包含所述第一安全保护方式时，所述第一终端设备从所述第二终端设备接收第三安全保护方式，并根据所述第一安全保护方式和所述第三安全保护方式，确定所述第二安全保护方式；其中，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；

方法三：当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，所述第一终端设备向所述第二终端设备发送所述第一安全保护方式和所述第一安全策略；所述第一终端设备从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式、所述第一安全策略，第三安全保护方式，以及第二安全策略确定的；当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级；

方法四：当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，所述第一终端设备从所述第二终端设备接收第三安全保护方式和第二安全策略；所述第一终

端设备根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式；其中，当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级；

在以上方法中，所述第三安全保护方式用于保护所述第二终端设备采用第一通信方式时传输的数据，所述第二安全策略为所述第二终端设备的所述第一通信方式的安全策略。

通过以上方法，可以保证所述第二安全保护方式不低于所述第一终端设备确定的第一通信方式的安全保护信息的保护等级，也不低于所述第二终端设备确定的第一通信方式的安全保护信息的保护等级。

在一个可能的设计中，所述第一终端设备根据所述第一安全保护方式和所述第三安全保护方式，确定所述第二安全保护方式，包括：

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备通过网络设备确定所述第二安全保护方式的保护等级；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护。

通过以上方法，可以保证所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第三安全保护方式的保护等级。

在一个可能的设计中，所述第一终端设备根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式，包括：

当所述第一安全保护方式与所述第三安全保护方式相同时，所述第一终端设备确定所述第二安全保护方式为所述第一安全保护方式；

当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式。

在一个可能的设计中，所述第一终端设备根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式，包括：

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备通过网络设备确定所述第二安全保护方式的

保护等级;

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式。

在一个可能的设计中，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式，包括:

当所述第一安全策略和所述第二安全策略中至少一项的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第一安全策略和所述第二安全策略的保护等级均为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护;

当所述第一安全策略和所述第二安全策略的保护等级均为优先安全保护时，或者当所述第一安全策略和所述第三安全策略中其中一项的保护等级为优先安全保护，另一项的保护等级为不需要安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级。

通过该设计，可以保证所述第二安全保护方式的保护等级不低于所述第一安全策略和所述第二安全策略的保护等级。

在一个可能的设计中，以上任一安全策略包含：机密性保护需求，和/或，完整性保护需求；相应的，以上任一安全保护方式包含：机密性保护需求，和/或，完整性保护需求。

第二方面，本申请实施例提供了一种安全保护方法确定装置，包括用于执行以上第一方面中各个步骤的单元。

第三方面，本申请实施例提供了一种终端设备，包括至少一个处理元件和至少一个存储元件，其中该至少一个存储元件用于存储程序和数据，该至少一个处理元件用于执行本申请第一方面提供的方法。

第四方面，本申请实施例还提供了一种计算机程序，当所述计算机程序在计算机上运行时，使得所述计算机执行上述第一方面提供的方法。

第五方面，本申请实施例还提供了一种计算机存储介质，所述计算机存储介质中存储有计算机程序，当所述计算机程序被计算机执行时，使得所述计算机执行上述第一方面提供的方法。

第六方面，本申请实施例还提供了一种芯片，所述芯片用于读取存储器中存储的计算机程序，执行上述第一方面提供的方法。

第七方面，本申请实施例还提供了一种芯片系统，该芯片系统包括处理器，用于支持计算机装置实现上述第一方面提供的方法。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器用于保存该计算机装置必要的程序和数据。该芯片系统可以由芯片构成，也可以包含芯片和其他分立器件。

附图说明

图 1 为本申请实施例提供的一种通信系统的架构图；

图 2 为申请实施例提供的一种用户面安全保护机制的流程图；

图 3 为本申请实施例提供的一种安全保护方式确定方法的流程图；

图 4 为本申请实施例提供的一种安全保护方式确定实例的流程图；

图 5 为本申请实施例提供的一种安全保护方式确定实例的流程图；

图 6 为本申请实施例提供的一种安全保护方式确定实例的流程图；

图 7 为本申请实施例提供的一种安全保护方式确定实例的流程图；

图 8 为本申请实施例提供的一种安全保护方法确定装置的结构图；

图 9 为本申请实施例提供的一种终端设备的结构图。

具体实施方式

本申请实施例提供一种安全保护方式确定方法及装置，用于在终端设备切换通信方式后，保证终端设备的数据传输安全性。其中，方法和装置是基于同一技术构思的，由于方法及装置解决问题的原理相似，因此装置与方法的实施可以相互参见，重复之处不再赘述。

以下，对本申请中的部分用语进行解释说明，以便于本领域技术人员理解。

1）、网络设备，是通信系统中将终端设备接入到无线网络的设备。所述网络设备作为无线接入网中的节点，又可以称为基站，还可以称为无线接入网（radio access network，RAN）节点（或设备）。

目前，一些网络设备的举例为：gNB、传输接收点（transmission reception point，TRP）、演进型节点 B（evolved Node B，eNB）、无线网络控制器（radio network controller，RNC）、节点 B（Node B，NB）、接入点（access point，AP）基站控制器（base station controller，BSC）、基站收发台（base transceiver station，BTS）、家庭基站（例如，home evolved NodeB，或 home Node B，HNB），或基带单元（base band unit，BBU），企业 LTE 离散窄带聚合（Enterprise LTE Discrete Spectrum Aggregation，eLTE-DSA）基站等。

另外，在一种网络结构中，所述网络设备可以包括集中单元（centralized unit，CU）节点和分布单元（distributed unit，DU）节点。这种结构将长期演进（long term evolution，LTE）系统中 eNB 的协议层拆分开，部分协议层的功能放在 CU 集中控制，剩下部分或全部协议层的功能分布在 DU 中，由 CU 集中控制 DU。比如，该网络设备所要执行的方法可以具体有 CU 来执行，当然也可以有 DU 来执行。

2）、终端设备，是一种向用户提供语音和/或数据连通性的设备。终端设备又可以称为用户设备（user equipment，UE）、移动台（mobile station，MS）、移动终端（mobile terminal，MT）等。

例如，终端设备可以为具有无线连接功能的手持式设备、车载设备等。目前，一些终端设备的举例为：手机（mobile phone）、平板电脑、笔记本电脑、掌上电脑、移动互联网设备（mobile internet device，MID）、智能销售终端（point of sale，POS）、可穿戴设备，虚拟现实（virtual reality，VR）设备、增强现实（augmented reality，AR）设备、工业控制（industrial control）中的无线终端、无人驾驶（self driving）中的无线终端、远程手术（remote medical surgery）中的无线终端、智能电网（smart grid）中的无线终端、运输安全（transportation safety）中的无线终端、智慧城市（smart city）中的无线终端、智慧

家庭（smart home）中的无线终端、各类智能仪表（智能水表、智能电表、智能燃气表）、eLTE-DSA UE、具有接入回传一体化（integrated access and backhaul，IAB）能力的设备等。

3）、Uu接口，为通信系统中终端设备和接入网（即网络设备）之间的接口，又称为空口，主要用于在终端设备和网络设备之间传输用户面数据、控制面相关信令，建立、重新配置和释放各种移动通信无线承载业务。

4）、PC5接口，是在第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）版本12（Rel-12）的D2D项目中引入的终端设备到终端设备之间的直接通信接口。邻近的终端之间可以在PC5接口的有效通信范围内通过直连链路进行数据传输，不需要通过中心节点（例如基站）进行转发，也不需要通过传统的蜂窝链路进行信息传输，通信较为快捷便利。

5）、通信方式，对应通信技术或通信接口，例如Uu接口通信方式、PC5接口通信方式。在通信系统中，终端设备需要采用某通信方式，使用相应的通信技术，通过相应的通信接口与其他终端设备建立通信连接，实现业务传输。

需要说明的是，通信系统可以支持多种通信方式，即终端设备可以通过第一通信方式传输，也可以采用第二通信方式传输。另外，在本申请中，通信系统还可以支持终端设备切换通信方式。例如，终端设备在使用Uu接口通信方式传输业务数据的过程中，可以被触发采用PC5接口通信方式传输后续的业务数据。又例如，终端设备在使用PC5接口通信方式传输业务数据时，也可以被触发采用Uu接口通信方式传输后续的业务数据。

6）通信方式的安全策略，为网络侧规定的终端设备在采用该通信方式时的保护策略。在一个示例中，所述安全策略可以包括机密性保护需求，和/或，完整性保护需求。

安全策略中对任一种保护需求的保护等级可以但不限于以下两种的等级划分方式：

划分方式一：1.需要安全保护、2.不需要安全保护。

划分方式二：1.需要安全保护（required）、2.优先安全保护（preferred）、3.不需要安全保护（not needed）。

7）、通信方式的安全保护方式，用于保护终端设备采用该通信方式时传输的数据，其规定了对数据的保护等级。通常，安全保护方式可以通过安全策略确定。

所述安全保护方式可以包括机密性保护需求，和/或，完整性保护需求。

通常，安全保护方式中的保护等级为需要安全保护，或者为不需要安全保护。

8）、“和/或”，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。字符“/”一般表示前后关联对象是一种“或”的关系。

需要说明的是，本申请中所涉及的多个，是指两个或两个以上。

另外，需要理解的是，在本申请的描述中，“第一”、“第二”等词汇，仅用于区分描述的目的，而不能理解为指示或暗示相对重要性，也不能理解为指示或暗示顺序。

下面结合附图对本申请实施例做进行具体说明。

图1示出了本申请实施例提供的安全保护方式确定方法适用的一种可能的通信系统的架构。参阅图1所示，所述通信系统中包括：终端设备、接入网（access network，AN）、核心网，以及数据网络（data network，DN）。

所述DN可以是因特网（Internet）、IP多媒体业务(IP Multi-media Service，IMS)网络、

区域网络等。其中，所述 DN 中包括应用服务器，所述应用服务器通过与所述终端设备进行数据传输，为所述终端设备提供业务服务。

接入网为终端设备提供无线接入有关的服务。其中，所述无线接入网中包括网络设备，所述网络设备为终端设备提供具体的无线接入服务，实现物理层功能、资源调度和无线资源管理、服务质量（Quality of Service，QoS）管理、无线接入控制以及移动性管理功能。

核心网为通信系统中负责根据终端设备通过接入网发送的呼叫请求或业务请求将所述终端设备接续到不同的数据网络上，以及计费、移动性管理、会话管理等业务。在本申请实施例中，将核心网设备的逻辑功能划分为控制面网元和用户面网元。

其中，用户面网元，又可以称为用户面功能（User Plane Function，UPF）实体，为保持终端设备业务连续性的锚点，负责转发终端设备的用户面数据。

控制面网元主要负责实现会话管理、接入与移动性管理，以及策略控制等具有控制管理功能的网元。所述控制面网元可以但不限于包括：接入与移动性管理功能（Access and Mobility Management Function，AMF）实体、会话管理功能（Session Management Function，SMF）实体，或策略控制功能（Policy Control Function，PCF）实体，统一的数据管理功能（unified data management，UDM）实体、网络开放功能（network exposure function，NEF）实体、和认证服务器功能实体（authentication server function，AUSF）。

下面对所述核心网中控制面网元的功能进行描述。

AMF实体，用于负责所述终端设备的注册、移动性管理、跟踪区更新流程等功能。

SMF 实体，用于负责所述终端设备的会话管理（包括会话的建立、修改和释放），UPF 实体的选择和重选、终端设备的 IP 地址分配、QoS 控制等。

PCF 实体，可用于负责策略控制决策等功能。

UDM 实体，可用于管理终端设备的签约数据、与终端设备相关的注册信息。

AUSF 实体，用于终端设备在注册过程中的认证。

还需要说明的是，核心网中的以上各实体既可以是在专用硬件上实现的网络元件，也可以是在专用硬件上运行的软件实例，或者是在适当平台上虚拟化功能的实例，例如，上述虚拟化平台可以为云平台。另外，以上各实体是按照功能划分，在实际应用中按照逻辑功能，以上任一个功能实体还可以拆分为多个功能实体，或者多个功能实体融合成为一个功能实体，本申请对此不作限定。

在图 1 所示的通信系统中，终端设备与网络设备之间通过 Uu 接口通信，如图中所示。在两个终端设备采用 Uu 接口通信方式进行数据传输的情况下，可以包括以下场景：

场景一：终端设备 a 和终端设备 b 分别通过 Uu 接口接入为其服务的网络设备 A 和网络设备 B，然后终端设备 A 通过网络设备 A 将数据发送给核心网中的 UPF 实体，再由所述 UPF 实体通过网络设备 B 转发给终端设备 B。

场景二：终端设备 a 和终端设备 b 分别通过 Uu 接口接入为其服务的网络设备 A 和网络设备 B，然后终端设备 A 通过网络设备 A 将数据发送给网络设备 B，再由网络设备 B 转发给终端设备 B。

场景三：终端设备 A 和终端设备 B 分别通过 Uu 接口接入为其服务的网络设备 A 和网络设备 B，然后终端设备 A 通过网络设备 A、UPF 实体将数据转发给 DN 中的应用服务器，所述应用服务器再通过 UPF 实体、网络设备 B，将数据转发给终端设备 B。

上述场景中的网络设备 A 和 B 可以相同也可以不同。另外网络设备 A 通信的 UPF，

与网络设备 B 通信的 UPF 可以相同，也可以不同。

另外，当该通信系统还支持边缘连接（sidelink）通信技术时，位置临近的两个终端设备之间可以通过 PC5 接口建立直连链路进行 sidelink 数据传输，即两个终端设备之间采用 PC5 接口通信方式进行数据传输。其中，sidelink 通信技术是一种终端设备之间能够直连的近场通信技术，又称为近距离服务（proximity services，ProSe）通信技术，或 D2D 通信技术。在该通信系统中，所处地理位置较近、且支持 sidelink 通信的多个终端设备可以组成一个子通信系统。在该子通信系统中，终端设备之间可以进行 sidelink 通信。

应了解的是，图 1 所示的通信系统并不构成本申请实施例能够适用的通信系统的限定。本申请实施例提供的方法可以适用于支持多种通信方式的各种通信系统中。所述多种通信方式包含但不限于上述两种通信方式。

此外，还需要注意到是，本申请提供的通信系统可以为移动通信系统和其他任一种系统的耦合的综合性通信系统。其中，本申请并不对移动通信系统的类型和制式进行限定，所述移动通信系统可以为：未来通信系统（例如第六代通信系统，第七代通信系统等），第五代（The 5th Generation，5G）通信系统、长期演进（Long Term Evolution，LTE）通信系统等等。所述其他系统可以但不限于包括：设备到设备 (device to device，D2D）、车到万物（vehicle to everything，V2X）、长期演进-车联网（LTE- vehicle，LTE-V）、车到车（vehicle to vehicle，V2V）、车联网、机器类通信（machine type communications，MTC）、物联网（internet of things，IoT）、长期演进-机器到机器（LTE-machine to machine，LTE-M）、机器到机器（machine to machine，M2M）、企业 LTE 离散窄带聚合（enterprise LTE discrete spectrum aggregation，eLTE-DSA）系统等通信系统。

在图 1 所示的通信系统中，为了保证业务数据传输过程中业务数据的安全性，通信系统针对每种通信方式均采用相应的数据安全保护机制。示例性的，在终端设备采用 Uu 接口通信方式时，终端设备和网络设备可以采用如图 2 所示的用户面安全保护机制保护通过 Uu 接口传输的数据。

参阅图 2 所示，所述通信系统使用用户面安全保护方式的具体流程包括：

S201：在分组数据单元（Packet Data Unit，PDU）会话建立流程中，终端设备通过网络设备向 AMF 实体发送 NAS 消息，其中，所述 NAS 消息中包含单一网络切片选择辅助信息（single network slice selection assistance information，S-NSSAI），数据网络标识（data network number，DNN）等参数。

可选的，所述 NAS 消息中还包含以下至少一项或组合：请求建立的 PDU 会话标识（PDU Session ID）、请求类型（request type）、旧 PDU 会话标识（Old PDU Session ID）、N1 会话管理容器（N1 SM container）。其中，所述 N1 SM container 中包含 PDU 会话建立请求（PDU session establishment request）。

S202：所述 AMF 实体在接收所述 NAS 消息后，向 SMF 实体发送建立 SMF 上下文请求（create SMF context request）或者更新 SMF 上下文请求（update SMF context request），其中携带所述终端设备的用户永久标识符（subscription permanent identifier，SUPI），S-NSSAI，DNN。

可选的，所述建立 SMF 上下文请求或更新 SMF 上下文请求中还可以包含所述 N1 SM container。

S203：所述 SMF 实体向 UDM 实体请求用户面安全策略，具体包括：所述 SMF 实体

向所述 UDM 实体发送用户面安全策略的请求，所述请求中包含 SUPI，DNN 和/或 S-NSSAI。所述 UDM 实体可以根据 SUPI，DNN 和/或 S-NSSAI 确定签约的用户面安全策略，若所述 UDM 能够确定所述用户面安全策略，则将所述用户面安全策略发送给所述 SMF 实体。

需要说明的是，当所述 UDM 实体保存有所述终端设备签约的用户面安全策略的情况下，所述 SMF 实体可以通过本步骤从所述 UDM 实体获取所述用户面安全策略；当所述 UDM 实体未保存所述终端设备签约的用户面安全策略的情况下，所述 SMF 实体通过本步骤无法从所述 UDM 实体获取所述用户面安全策略。

S204：所述 SMF 实体确定最终的用户面安全策略。当所述 SMF 实体可以通过 S203 从所述 UDM 实体获取所述用户面安全策略时，所述 SMF 实体确定获取的所述用户面安全策略为最终的用户面安全策略；当所述 SMF 实体通过 S203 无法从所述 UDM 实体获取所述用户面安全策略时，所述 SMF 实体还可以根据 DNN 和/或 S-NSSAI，在本地存储的用户面安全策略中，确定最终的用户面安全策略。

其中，所述用户面安全策略中包含机密性保护需求和/或完整性保护的需求。

S205：所述 SMF 实体通过所述 AMF 实体将确定的用户面安全策略发送至网络设备。

S206：所述网络设备根据本地安全保护能力（例如完整性保护速率是否支持等），确实最终的用户面安全保护方式。

例如，若所述用户面安全策略为需要安全保护，则所述网络设备确定的用户面安全保护方式为需要安全保护，若所述网络设备确定本地无法执行安全保护时，则所述网络设备向所述 SMF 实体发送拒绝指示。

例如，若所述用户面安全策略为优先安全保护，则所述网络设备确定的用户面安全保护方式是否执行安全保护由所述网络设备根据本地安全保护能力确定。

再例如，若所述用户面安全策略为不需要安全保护，则所述网络设备确定的用户面安全保护方式为不需要安全保护。

需要说明的是，在以上例子中的安全保护可以为机密性保护，或者完整性保护。

S207：所述网络设备向所述终端设备发送用户面安全保护方式。

可选的，所述网络设备可以向所述终端设备发送安全保护指示（例如机密性保护指示，完整性保护指示）所述安全保护指示用于指示是否需要机密性保护，是否需要完整性保护。

可选的安全保护指示还可以指示密钥的长度，或具体机密性保护算法或具体的完整性保护算法。

S208：所述终端设备和所述网络设备根据用户面安全保护方式，对后续传输的用户面数据执行保护。

目前，所述通信系统可以支持终端设备切换通信方式。例如，终端设备在使用 Uu 接口通信方式传输业务数据的过程中，可以被触发采用 PC5 接口通信方式传输后续的业务数据。然而通信系统中的终端设备采用不同的通信方式时，使用的数据安全保护方式可能存在差异。例如，所述终端设备采用 Uu 接口通信方式时的用户面安全保护方式为需要安全保护，而所述终端设备采用 PC5 接口通信方式时的安全保护方式为不需要安全保护，那么当所述终端设备从 Uu 接口通信方式切换到 PC5 接口通信方式时，所述终端设备不能对数据进行加密，当所述终端设备在群组通信的情况下，非接收端的其他终端设备可以窃听到所述终端设备传输的数据，导致所述终端设备的数据安全性降低。另外，如果初始数据有

保护，而切换后数据没有保护，也会导致业务数据的安全性降低。

为了解决上述问题，本申请实施例提供了一种安全保护方式确定方法，该方法可以适用于如图 1 所示的支持多种通信方式、且支持切换通信方式的通信系统中。该方法中涉及的第一终端设备为所述通信系统中的任一个终端设备。参阅图 3 所示，该方法可以包含以下步骤：

S301：第一终端设备获取第一通信方式的安全保护信息。

其中，所述安全保护信息包含第一安全保护方式，和/或，第一安全策略；所述第一安全保护方式对应所述第一通信方式，用于保护所述第一终端设备采用所述第一通信方式时传输的数据，所述第一安全策略为所述第一终端设备的所述第一通信方式的安全策略。

S302：所述第一终端设备根据所述安全保护信息，确定第二安全保护方式，所述第二安全保护方式对应第二通信方式，用于保护所述第一终端设备采用第二通信方式时传输的数据。

根据所述第一终端设备执行上述方法的时机的不同，该方法可以适用于如下两个场景中。

场景一：所述第一终端设备可以在请求使用所述第一通信方式时或将要使用所述第一通信方式时，即获取所述第一通信方式的安全保护信息，并根据所述安全保护信息，预先确定第二安全保护方式。这样，当所述第一终端设备在从所述第一通信方式切换到所述第二通信方式时，可以直接使用所述第二安全保护方式进行保护，避免在切换过程中确定所述第二安全保护方式造成的时延，可以提高所述第一终端设备的通信效率。

示例性的，所述第一终端设备可以在 PDU 会话建立流程或者注册中，从网络设备获取 Uu 接口通信方式的安全保护信息，并通过该安全保护信息，确定 PC5 接口通信方式对应的第二安全保护方式。

示例性的，所述第一终端设备还可以在请求使用 PC5 接口通信方式时，从本地或者应用服务器获取 PC5 接口通信方式的安全保护信息，并通过该安全保护信息，确定 Uu 接口通信方式对应的第二安全保护方式。

场景二：所述第一终端设备可以在确定从所述第一通信方式切换到所述第二通信方式的情况下，获取所述第一通信方式的安全保护信息，并根据所述安全保护信息，预先确定第二安全保护方式。可选的，所述第一终端设备可以在切换前、切换中、切换后，执行上述流程，本申请对此不作限定。可选的，所述第一通信方式的第一安全保护方式可以为所述第一终端设备采用场景一的方法确定的，或者其他方式确定的本申请对此不作限定。

需要说明的是，为了保证所述第一终端设备切换通信方式后，所述第一终端设备的数据传输安全性，所述第一终端设备确定的所述第二安全保护方式的保护等级不低于所述第一通信方式的安全保护信息规定的保护等级。

在场景一的一个实现方式中，当所述安全保护信息为所述第一安全保护方式时，所述第一终端设备可以通过以下方法执行 S302：

方法一：所述第一终端设备确定所述第二安全保护方式与所述第一安全保护方式相同。

方法二：所述第一终端设备获取第二安全策略，所述第二安全策略为所述第一终端设备的所述第二通信方式的安全策略；所述第一终端设备根据所述第二安全策略、所述第一

安全保护方式，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全保护方式的保护等级。

可选的，当所述第二通信方式为 PC5 通信方式时，所述第一终端设备可以从本地或者应用服务器获取所述第二安全策略，当所述第二通信方式为 Uu 通信方式时，所述第一终端设备可以从网络设备获取所述第二安全策略。

在方法二的一个示例中，所述第一终端设备根据所述第二安全策略、所述第一安全保护方式，确定所述第二安全保护方式，包括:

当所述第一安全保护方式的保护等级为需要安全保护，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为优先安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级;

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护。

通过该示例，可以保证所述第一终端设备确定的所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全策略的保护等级。

在场景一的另一个实现方式中，当所述安全保护信息为所述第一安全策略时，所述第一终端设备可以通过以下方法执行 S302:

方法一: 所述第一终端设备根据所述第一安全策略，确定所述第二安全保护方式。

方法二: 所述第一终端设备获取第二安全策略，所述第二安全策略为所述第一终端设备的所述第二通信方式的安全策略; 所述第一终端设备根据所述第二安全策略、所述第一安全策略，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全策略的保护等级。

在方法二的一个示例中，所述第一终端设备根据所述第二安全策略、所述第一安全策略，确定所述第二安全保护方式，包括:

当所述第二安全策略的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第二安全策略的保护等级为不需要安全保护时，所述第一终端设备根据所述第一安全策略的保护等级，确定所述第二安全保护方式的保护等级;

当所述第二安全策略的保护等级为优先安全保护，所述第一终端设备根据所述第一安全策略的保护等级，确定所述第二安全保护方式的保护等级。若所述第一安全策略为需要安全保护，则执行保护。若所述第一安全策略为优先安全保护或者不需要安全保护时，第一终端设备根据优先安全保护的方式，确定是否执行保护。

在方法一和方法二的一个示例中，所述第一终端设备根据所述第一安全策略，确定所述第二安全保护方式，包括:

当所述第一安全策略的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全策略的保护等级为优先安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级；

当所述第一安全策略保护等级为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护。

在场景一的又一个实现方式中，当所述第二通信方式为 PC5 接口通信方式时，在所述第一终端设备确定第二安全保护方式之后，所述第一终端设备还可以与 PC5 接口通信方式的对端设备（为了便于描述，后续可以简称为第二终端设备）进行协商，从而确定第四安全保护方式，其中，所述第四安全保护方式用于保护所述第一终端设备与所述第二终端设备之间采用 PC5 接口通信方式进行数据传输时传输的数据。

具体的协商过程可以包括以下方法：

方法一：所述第一终端设备向第二终端设备发送所述第二安全保护方式，并接收所述第二终端设备根据所述第二安全保护方式和第三安全保护方式确定的第四安全保护方式。

方法二：所述第一终端设备接收第二终端设备发送的第三安全保护方式，并根据所述第二安全保护方式和所述第三安全保护方式，确定第四安全保护方式。

其中，在上述方法中，所述第四安全保护方式的保护等级不低于所述第二安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；所述第三安全保护方式用于保护所述第二终端设备采用第二通信方式时传输的数据。可选的，所述第三安全保护方式可以为所述第二终端设备通过 S301 和 S302 确定的，本申请对此不作限定。

在上述两个方法的一个示例中，所述第一终端设备和所述第二终端设备可以采用相同的方法，根据所述第二安全保护方式和所述第三安全保护方式，确定所述第四安全保护方式。下面以所述第一终端设备为例进行说明：

当所述第二安全保护方式和所述第三安全保护方式中至少一项的保护等级为需要安全保护时，所述第一终端设备确定所述第四安全保护方式的保护等级为需要安全保护；

当所述第二安全保护方式和所述第三安全保护方式的保护等级均为不需要安全保护时，所述第一终端设备确定所述第四安全保护方式的保护等级为不需要安全保护。

通过该示例，可以保证所述第一终端设备确定的所述第四安全保护方式的保护等级不低于所述第二安全保护方式和所述第三安全保护方式的保护等级。

在场景一的又一个实现方式中，当所述第二通信方式为 PC5 接口通信方式时，所述第二安全保护方式具体用于保护所述第一终端设备与第二终端设备之间采用所述第二通信方式时进行数据传输时传输的数据。即所述第一终端设备可以直接根据所述第一通信方式的安全保护信息（第一终端设备的第一通信方式的安全保护信息，后续简称为安全保护信息 1），确定所述第一终端设备与所述第二终端设备采用 PC5 接口通信方式进行通信时的安全保护方式。

可选的，所述第一终端设备在执行 S302 时，可以通过与所述第二终端设备协商的方法，确定所述第二安全保护方式。

具体的协商过程可以包括以下方法：

方法一：所述第一终端设备向所述第二终端设备发送所述安全保护信息 1，并接收所

述第二终端设备根据所述安全保护信息 1 和第二终端设备的第一通信方式的安全保护信息（后续简称为安全保护信息 2）确定的所述第二安全保护方式。

方法二：所述第一终端设备接收第二终端设备发送的安全保护信息 2；并根据所述安全保护信息 1 和所述安全保护信息 2，确定所述第二安全保护方式。

其中，所述第二安全保护方式的保护等级不低于所述安全保护信息 1 的保护等级，且不低于所述安全保护信息 2 的保护等级。安全保护信息 2 中包含第三安全保护方式，和/或，第三安全策略。

在上述两个方法的一个实现方式中，安全保护信息中包含安全保护方式，所述第一终端设备和所述第二终端设备可以采用相同的方法，根据所述第一安全保护方式和所述安全保护信息 2 中的第三安全保护方式，确定所述第二安全保护方式。其中，第三安全保护方式为第二终端设备的第一通信方式的安全保护方式。下面以所述第一终端设备为例进行说明：

当所述第一安全保护方式和所述第三安全保护方式中至少一项的保护等级为需要安全保护时，所述第一终端设备确定所述第三安全保护方式的保护等级为需要安全保护；

当所述第一安全保护方式和所述第三安全保护方式的保护等级均为不需要安全保护时，所述第一终端设备确定所述第三安全保护方式的保护等级为不需要安全保护。

在上述两个方法的另一个实现方式中，安全保护信息中包含安全策略，所述第一终端设备和所述第二终端设备可以采用相同的方法，根据所述第一安全策略和安全保护信息 2 中的第三安全策略，确定所述第二安全保护方式。其中，第三安全策略为第二终端设备的第一通信方式的安全保护方式下面以所述第一终端设备为例进行说明：

当所述第一安全策略和所述第三安全策略中至少一项的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全策略和所述第三安全策略的保护等级均为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护；

当所述第一安全策略和所述第三安全策略的保护等级均为优先安全保护时，或者当所述第一安全策略和所述第三安全策略中其中一项的保护等级为优先安全保护，另一项的保护等级为不需要安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级。

通过该示例，可以保证所述第一终端设备确定的所述第二安全保护方式的保护等级不低于所述第一安全策略和所述第三安全策略的保护等级。

在上述两个方法的又一个实现方式中，安全保护信息中包含安全保护方式和安全策略，所述第一终端设备和所述第二终端设备可以采用相同的方法，根据安全保护信息 1 中的第一安全保护方式和第一安全策略，以及所述安全保护信息 2 中的所述第三安全保护方式和第二安全策略，确定所述第二安全保护方式。下面以所述第一终端设备为例进行说明：

在一个示例中：

当所述第一安全保护方式与所述第三安全保护方式相同时，所述第一终端设备确定所述第二安全保护方式为所述第一安全保护方式；

当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式。

在另一个示例中：

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备通过网络设备确定所述第二安全保护方式的保护等级；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式。

在上述两个示例中，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式，包括：

当所述第一安全策略和所述第二安全策略中至少一项的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全策略和所述第二安全策略的保护等级均为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护；

当所述第一安全策略和所述第二安全策略的保护等级均为优先安全保护时，或者当所述第一安全策略和所述第三安全策略中其中一项的保护等级为优先安全保护，另一项的保护等级为不需要安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级。

在场景二的一个实现方式中，当所述第二通信方式为 Uu 接口通信方式时，所述第一终端设备可以通过以下方法执行 S302：

方法一：所述第一终端设备向网络设备发送所述安全保护信息；并从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据所述安全保护信息确定的。

方法二：所述第一终端设备向应用服务器发送所述安全保护信息，以及向网络设备发送请求消息；所述第一终端设备从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据从所述应用服务器获取的所述安全保护信息确定的。

在方法二中，所述第一终端设备向所述应用服务器发送所述安全保护信息之后，核心网中的 SMF 实体从所述应用服务器中获取所述安全保护信息，在将所述安全保护信息发送给所述网络设备。示例性的，所述网络设备在接收到所述请求消息后，通过向所述 SMF 实体发送 PDU 会话建立请求，请求所述安全保护信息。在另一个示例中，所述第一终端设备可以在向所述应用服务器发送所述安全保护信息时，同时发送所述安全保护信息的标识信息，这样，所述第一终端设备在向所述网络设备发送请求消息时，可以携带所述标识信息，所述网络设备在通过 PDU 会话建立请求将所述标识信息发送给 SMF 实体。这样，所述 SMF 实体可以根据所述标识信息，准确地从所述应用服务器获取所述安全保护信息；或者在所述应用服务器将所述安全保护信息和所述标识信息同时发送给所述 SMF 实体保

存的情况下，所述 SMF 实体可以根据所述标识信息，准确地从本地保存的多个安全保护信息中确定所述第一终端设备的所述标识信息对应的安全保护信息。

可选的，所述安全保护信息的标识信息可以但不限于为：UE 的运营商网络标识，广义公共签约标识（Generic Public Subscription Identifier，GPSI），应用 ID，第一终端设备的应用 ID，第一终端设备的运营商网络 ID 和 PC5 链路标识的至少一项。

在上述两个方法的一个示例中，所述安全保护信息中包含第一安全保护方式；所述网络设备可以通过以下方式确定的第二安全保护方式：

方式一：所述第二安全保护方式与所述第一安全保护方式相同。

方式二：所述第二安全保护方式的保护等级高于所述第一安全保护方式的保护等级。

方式三：所述第二安全保护方式为所述网络设备根据所述第一安全保护方式和/或第二安全策略确定的，其中，所述第二安全策略为所述网络设备获得的所述第一终端设备采用所述第二通信方式的保护等级。

在方式三的一个示例中：

当所述第二安全策略的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为优先安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为优先安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级由所述网络设备指定；

当所述第二安全策略的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级为不需要安全保护。

通过该示例，可以保证所述第二安全保护方式不低于所述第二安全策略和所述第一安全保护方式的保护等级。

方式四：所述第二安全保护方式为所述网络设备根据所述第一安全保护方式以及第三安全保护方式确定的，其中，所述第三安全保护方式为所述网络设备根据所述第二安全策略确定的。

在方式四的一个示例中：

当所述第三安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级为不需要安全保护。

通过该示例，可以保证所述第二安全保护方式不低于所述第一安全保护方式和所述第三安全保护方式的保护等级。

在场景二的又一个实现方式中，当所述第二通信方式为 PC5 接口通信方式时，所述第二安全保护方式具体用于保护所述第一终端设备与第二终端设备之间采用所述第二通信

方式进行数据传输时传输的数据。所述第一终端设备可以通过与所述第二终端设备协商，确定所述第二安全保护方式。其中，在以下协商方法中，所述第三安全保护方式用于保护所述第二终端设备采用第一通信方式时传输的数据，所述第二安全策略为所述第二终端设备的所述第一通信方式的安全策略。

具体的协商方法可以但不限于包括:

方法一: 当所述安全保护信息包含所述第一安全保护方式时，所述第一终端设备向第二终端设备发送所述第一安全保护方式，并从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式和第三安全保护方式确定的，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级。

方法二: 当所述安全保护信息包含所述第一安全保护方式时，所述第一终端设备从所述第二终端设备接收第三安全保护方式，并根据所述第一安全保护方式和所述第三安全保护方式，确定所述第二安全保护方式；其中，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级。

在方法二的一个示例中，所述第一终端设备根据所述第一安全保护方式和所述第三安全保护方式，确定所述第二安全保护方式，包括:

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备通过网络设备确定所述第二安全保护方式的保护等级;

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护。

通过该示例，可以保证所述第二安全保护方式的保护等级不低于所述第三安全保护方式和所述第一安全保护方式的保护等级。

方法三: 当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，所述第一终端设备向所述第二终端设备发送所述第一安全保护方式和所述第一安全策略；所述第一终端设备从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式、所述第一安全策略，第三安全保护方式，以及第二安全策略确定的；当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级。

方法四: 当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，所

述第一终端设备从所述第二终端设备接收第三安全保护方式和第二安全策略；所述第一终端设备根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式；其中，当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级。

在方法四的一个示例中，所述第一终端设备根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式，包括:

当所述第一安全保护方式与所述第三安全保护方式相同时，所述第一终端设备确定所述第二安全保护方式为所述第一安全保护方式;

当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式。

在方法四的另一个示例中，所述第一终端设备根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式，包括:

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备通过网络设备确定所述第二安全保护方式的保护等级;

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式。

在上述两个示例中，所述第一终端设备根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式，包括:

当所述第一安全策略和所述第二安全策略中至少一项的保护等级为需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为需要安全保护;

当所述第一安全策略和所述第二安全策略的保护等级均为不需要安全保护时，所述第一终端设备确定所述第二安全保护方式的保护等级为不需要安全保护;

当所述第一安全策略和所述第二安全策略的保护等级均为优先安全保护时，或者当所述第一安全策略和所述第三安全策略中其中一项的保护等级为优先安全保护，另一项的保护等级为不需要安全保护时，所述第一终端设备根据自身的安全保护能力确定所述第二安全保护方式的保护等级。

还需要说明的是，在以上任一个安全策略中可以包含：机密性保护需求，和/或，完

整性保护需求；相应的，在以上任一个安全保护方式中可以包含：机密性保护需求，和/或，完整性保护需求。另外，当以上任一个安全策略和安全保护方式均包含机密性保护需求和完整性保护需求时，第二安全保护方式中的机密性保护需求可以参考以上示例中的具体方式确定，第二安全保护方式中的完整性保护需求也可以参考以上示例中的具体方式确定。

可选的，针对本申请的安全策略还可以包含：支持256比特等密钥长度（例如支持256比特，192比特等等）。可选的，安全策略还可以包含：支持的完整性保护速率（例如支持64kbps，2Mbps等）。可选的，安全策略还可以包括：密钥生命有效期（例如一天，一小时等）。

本申请实施例提供了一种安全保护方式确定方法，在该方法中，终端设备可以根据第一通信方式的安全保护信息，确定第二通信方式的安全保护方式。这样，当所述终端设备在从第一通信方式切换到所述第二通信方式时，可以直接使用所述第二通信方式的安全保护方式保护传输的数据，从而可以保证通信方式切换后的所述终端设备的数据安全性。进一步的，所述终端设备确定的第二通信方式的安全保护方式的保护等级不低于第一通信方式的安全保护信息的保护等级，这样，可以进一步保证通信方式切换后的所述终端设备的数据安全性。

基于以上实施例，本申请还提供了以下多个安全保护方式确定实例，以下实例均可以适用于如图1所示的通信系统中。

实例1：

参阅图4所示，该实例可以包括以下步骤：

S401：终端设备A完成注册流程，注册到运营商网络。

S402-S405，为网络设备通过PDU会话建立流程，向SMF实体请求用户面安全策略并确定Uu接口通信方式的安全保护信息的流程，具体可以参考图2所示的用户面安全保护机制中的S201-S306，此处不再赘述。

在一个示例中，所述SMF实体在S403中可以按照传统的方法，从UDM实体或本地确定所述用户面安全策略。

在一个示例中，所述SMF实体在S403中还可以向应用服务器发送请求，并从应用服务器侧获取PC5接口通信方式的应用安全策略，并根据应用安全策略确定用户面安全策略。例如，所述SMF实体确定应用安全策略与用户面安全策略相同；或者所述SMF实体根据应用安全策略和所述SMF实体之前确定的用户面安全策略，确定最终的用户面安全策略。在本示例中，在所述SMF实体从所述应用服务器请求应用安全策略的过程中，所述SMF实体可以直接与所述应用服务器进行通信交互，或者所述SMF实体跨越其他网元与所述应用服务器进行通信交互，本申请对此不作限定。

可选的，应用安全策略的等级划分方式可以为：划分方式一：需要安全保护，不需要安全保护；也可以为划分方式二：需要安全保护，优先安全保护，不需要安全保护。

在一个示例中，所述SMF实体确定应用安全策略与用户面安全策略相同，包括：

当应用安全策略的等级划分方式为划分方式一时，若应用安全策略的保护等级为需要安全保护，则所述SMF实体确定用户面安全策略为需要安全保护；若应用安全策略为不需要安全保护，则所述SMF实体确定用户面安全策略为不需要安全保护。

当应用安全策略的等级划分方式为划分方式二时，所述 SMF 实体确定应用安全策略与用户面安全策略可以为相同。

在一个示例中，所述 SMF 实体根据应用安全策略和所述 SMF 实体之前确定的用户面安全策略，确定最终的用户面安全策略；包括：

当应用安全策略的等级划分方式为划分方式一时，若应用安全策略为需要安全保护，则所述 SMF 实体确定用户面安全策略为需要安全保护；当应用安全策略为不需要安全保护，则所述 SMF 实体确定最终的用户面安全策略可以与之前确定的用户面安全策略相同。

当应用安全策略的等级划分方式为划分方式二时，若应用安全策略与 SMF 之前确定用户面安全策略至少一个为需要安全保护，则所述 SMF 实体确定最终的用户面安全策略为需要安全保护；当应用安全策略与 SMF 之前确定的用户面安全策略都是不需要保护，则所述 SMF 实体确定最终的用户面安全策略为不需要保护；其他情况所述 SMF 实体确定最终的用户面安全策略为优先保护。

S406：所述网络设备向所述终端设备 A 发送 Uu 接口通信方式的安全保护信息，其中所述安全保护信息包含：所述用户面安全保护方式，和/或，所述用户面安全策略。

S407：所述终端设备 A 根据所述 Uu 接口通信方式的安全保护信息，确定 PC5 接口通信方式的安全保护方式。其中，所述 PC5 接口通信方式的安全保护方式的保护等级不低于所述 Uu 接口通信方式的安全保护信息的保护等级。

所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的过程可以参考图 3 所示的实施例中的对应的描述。其中，所述 PC5 接口通信方式的安全保护方式的保护等级不低于所述安全保护信息的保护等级。

在一个实现方式中，当所述安全保护信息为所述用户面安全保护方式时，所述终端设备 A 通过如下方法确定所述 PC5 接口通信方式的安全保护方式：

方法一：所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式与所述用户面安全保护方式相同。

方法二：所述终端设备 A 获取所述应用安全策略，并根据所述应用安全策略、所述用户面安全保护方式，确定所述 PC5 接口通信方式的安全保护方式，其中，所述 PC5 接口通信方式的安全保护方式的保护等级不低于所述应用安全策略的保护等级，且不低于所述用户面安全保护方式的保护等级。

在方法二的一个示例中：

当所述用户面安全保护方式的保护等级为需要安全保护，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为需要安全保护；

当所述用户面安全保护方式的保护等级为不需要安全保护，所述应用安全策略的保护等级为需要安全保护时，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为需要安全保护；

当所述用户面安全保护方式的保护等级为不需要安全保护，所述应用安全策略的保护等级为优先安全保护时，所述终端设备 A 根据自身的安全保护能力确定所述 PC5 接口通信方式的安全保护方式的保护等级；

当所述用户面安全保护方式的保护等级为不需要安全保护，所述应用安全策略的保护等级为不需要安全保护时，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为不需要安全保护。

在另一个实现方式中，当所述安全保护信息为所述用户面安全策略时，所述终端设备A通过如下方法确定所述PC5接口通信方式的安全保护方式:

方法一: 所述终端设备A根据所述用户面安全策略，确定所述PC5接口通信方式的安全保护方式，其中，所述PC5接口通信方式的安全保护方式的保护等级不低于所述用户面安全策略的保护等级。

方法二: 所述终端设备A获取应用安全策略，并根据所述应用安全策略、所述用户面安全策略，确定所述PC5接口通信方式的安全保护方式，其中，所述PC5接口通信方式的安全保护方式的保护等级不低于所述应用安全策略的保护等级，且不低于所述用户面安全策略的保护等级。

在上述方法一的一个示例中:

当所述用户面安全策略的保护等级为需要安全保护时，所述终端设备A确定所述PC5接口通信方式的安全保护方式的保护等级为需要安全保护;

当所述用户面安全策略的保护等级为优先安全保护时，所述终端设备A根据自身的安全保护能力确定所述PC5接口通信方式的安全保护方式的保护等级;

当所述用户面安全策略保护等级为不需要安全保护时，所述终端设备A确定所述PC5接口通信方式的安全保护方式的保护等级为不需要安全保护。

在上述方法二的一个示例中:

当所述应用安全策略（或所述用户面安全策略）的保护等级为需要安全保护时，所述终端设备A确定所述PC5接口通信方式的安全保护方式的保护等级为需要安全保护;

当所述应用安全策略（或所述用户面安全策略）的保护等级为优先安全保护或者不需要安全保护时，所述终端设备A根据所述用户面安全策略（或所述应用安全策略）的保护等级，确定所述PC5接口通信方式的安全保护方式的保护等级，如上述示例中的描述。

S408: 所述终端设备A确定采用PC5接口通信方式时的对端设备为所述终端设备B，所述终端设备A向所述终端设备B发送所述PC5接口通信方式的安全保护方式。或者，所述终端设备A广播确定的所述PC5接口通信方式的安全保护方式。

S409: 所述终端设备B接收到所述PC5接口通信方式的安全保护方式后，存储所述PC5接口通信方式的安全保护方式。

这样，当所述终端设备A从Uu接口通信方式切换到PC5接口通信方式时，所述终端设备A可以直接使用所述PC5接口通信方式的安全保护方式，对传输的数据进行保护。

实例2:

在本实例中，终端设备A可以采用图4所示的流程S401-S407确定PC5接口通信方式的安全保护方式1，终端设备B也可以采用如图4所示的流程S401-S407，确定PC5接口通信方式的安全保护方式2。之后，所述终端设备A和所述终端设备B可以通过PC5接口通信方式的安全保护方式1、PC5接口通信方式的安全保护方式2，协商确定所述终端设备A和所述终端设备B在采用PC5接口通信方式时使用的PC5接口通信方式的安全保护方式3。

可选的，终端设备A和所述终端设备B中任一个终端设备可以将本地确定的PC5接口通信方式的安全保护方式，发送给另一个终端设备，由另一个终端设备根据两个PC5接口通信方式的安全保护方式，确定最终的PC5接口通信方式的安全保护方式3。

例如，终端设备 A 可以将确定的 PC5 接口通信方式的安全保护方式 1 发送给终端设备 B，然后终端设备 B 根据 PC5 接口通信方式的安全保护方式 1、PC5 接口通信方式的安全保护方式 2，确定 PC5 接口通信方式的安全保护方式 3，然后向所述终端设备 A 发送所述 PC5 接口通信方式的安全保护方式 3。

需要说明的是，所述 PC5 接口通信方式的安全保护方式 3 的保护等级不低于所述 PC5 接口通信方式的安全保护方式 1 和所述 PC5 接口通信方式的安全保护方式 2 的保护等级。

在一个示例中，终端设备 B 可以通过如下方法，确定所述 PC5 接口通信方式的安全保护方式 3:

当所述 PC5 接口通信方式的安全保护方式 1 和所述 PC5 接口通信方式的安全保护方式 2 中至少一项的保护等级为需要安全保护时，所述终端设备 B 确定所述 PC5 接口通信方式的安全保护方式 3 的保护等级为需要安全保护;

当所述 PC5 接口通信方式的安全保护方式 1 和所述 PC5 接口通信方式的安全保护方式 2 的保护等级均为不需要安全保护时，所述终端设备 B 确定所述 PC5 接口通信方式的安全保护方式 3 的保护等级为不需要安全保护。

实例 3:

在本实例中，终端设备 A 可以采用图 4 所示的流程 S401-S406，获取 Uu 接口通信方式的安全保护信息 1（包含用户面安全策略 1，和/或，用户面安全保护方式 1），终端设备 B 也可以采用如图 4 所示的流程 S401-S406，获取 Uu 接口通信方式的安全保护信息 2（包含用户面安全策略 2，和/或，用户面安全保护方式 2）。之后，所述终端设备 A 和所述终端设备 B 可以通过 Uu 接口通信方式的安全保护信息 1、Uu 接口通信方式的安全保护信息 2，协商确定所述终端设备 A 和所述终端设备 B 在采用 PC5 接口通信方式时使用的安全保护方式（以下简称 PC5 接口通信方式的安全保护方式）。

可选的，终端设备 A 和所述终端设备 B 中任一个终端设备可以将获取的 Uu 接口通信方式的安全保护信息，发送给另一个终端设备，由另一个终端设备根据两个 Uu 接口通信方式的安全保护信息，确定最终的 PC5 接口通信方式的安全保护方式。

需要说明的是，所述安全保护方式 3 的保护等级不低于所述 Uu 接口通信方式的安全保护信息 1 和所述 Uu 接口通信方式的安全保护信息 2 的保护等级。

在一个实现方式中，任一个 Uu 接口通信方式的安全保护信息包含用户面安全策略，任一个终端设备（以终端设备 A 为例）根据用户面安全策略 1 和用户面安全策略 2，确定 PC5 接口通信方式的安全保护方式，包括:

当所述用户面安全策略 1 和所述用户面安全策略 2 中至少一项的保护等级为需要安全保护时，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为需要安全保护;

当所述用户面安全策略 1 和所述用户面安全策略 2 的保护等级均为不需要安全保护时，所述 A 终端设备确定所述 PC5 接口通信方式的安全保护方式的保护等级为不需要安全保护;

当所述用户面安全策略 1 和所述用户面安全策略 2 的保护等级均为优先安全保护时，或者，当所述用户面安全策略 1 和所述用户面安全策略 2 中其中一项的保护等级为优先安全保护，另一项的保护等级为不需要安全保护时，所述终端设备 A 根据自身的安全保护能

力确定所述 PC5 接口通信方式的安全保护方式的保护等级。

在另一个实现方式中，任一个 Uu 接口通信方式的安全保护信息包含用户面安全保护方式，任一个终端设备（以终端设备 A 为例）根据用户面安全保护方式 1 和用户面安全保护方式 2，确定 PC5 接口通信方式的安全保护方式，包括:

当所述用户面安全保护方式 1 和所述用户面安全保护方式 2 中至少一项的保护等级为需要安全保护时，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为需要安全保护;

当所述用户面安全保护方式 1 和所述用户面安全保护方式 2 的保护等级均为不需要安全保护时，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为不需要安全保护。

在又一个实现方式中，任一个 Uu 接口通信方式的安全保护信息包含用户面安全保护策略和用户面安全保护方式，任一个终端设备（以终端设备 A 为例）根据用户面安全策略 1 和用户面安全策略 2，用户面安全保护方式 1 和用户面安全保护方式 2，确定 PC5 接口通信方式的安全保护方式，包括以下方法:

方法一: 当所述用户面安全保护方式 1 与所述用户面安全保护方式 2 相同时，所述 A 终端设备确定所述 PC5 接口通信方式的安全保护方式与所述用户面安全保护方式 1 相同; 当所述用户面安全保护方式 1 与所述用户面安全保护方式 2 不相同时，所述终端设备 A 根据所述用户面安全策略 1 和所述用户面安全策略 2，确定所述 PC5 接口通信方式的安全保护方式。

方法二: 当所述用户面安全保护方式 1 与所述用户面安全保护方式 2 中至少一项保护等级为需要安全保护时，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为需要安全保护; 当所述用户面安全保护方式 1 与所述用户面安全保护方式 2 均为不需要安全保护时，所述终端设备 A 根据所述用户面安全策略 1 和所述用户面安全策略 2，确定所述 PC5 接口通信方式的安全保护方式。

方法三: 当所述用户面安全保护方式 2 的保护等级为需要安全保护，所述用户面安全保护方式 1 的保护等级为需要安全保护时，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为需要安全保护; 当所述用户面安全保护方式 2 的保护等级为需要安全保护，所述用户面安全保护方式 1 的保护等级为不需要安全保护时，所述终端设备 A 通过网络设备确定所述 PC5 接口通信方式的安全保护方式的保护等级; 当所述用户面安全保护方式 2 的保护等级为不需要安全保护，所述用户面安全保护方式 1 的保护等级为需要安全保护时，所述终端设备 A 确定所述 PC5 接口通信方式的安全保护方式的保护等级为需要安全保护; 当所述用户面安全保护方式 2 的保护等级为不需要安全保护，所述用户面安全保护方式 1 的保护等级为不需要安全保护时，所述终端设备 A 根据所述用户面安全策略 1 和所述用户面安全策略 2，确定所述 PC5 接口通信方式的安全保护方式。

以上方式中，所述终端设备 A 根据用户面安全策略 1 和所述用户面安全策略 2，确定所述 PC5 接口通信方式的安全保护方式，可以参见以上实现方式中的描述，此处不再赘述。

实例 4:

参阅图 5 所示，该实例可以包括以下步骤:

S501: 终端设备 A 通过网络设备向 AMF 实体发送注册请求。其中，所述注册请求中

可以包含终端设备 A 的用户隐藏标识符（subscription concealed identifier，SUCI）。其中所述 SUCI 为加密的 SUPI。

可选的，所述注册请求还可以包含以下至少一项或组合：PC5 能力信息、应用标识（例如 V2X 应用 ID）、DNN、S-NSSAI 等。

所述 PC5 能力信息用于通知 AMF 实体本次注册流程与 PC5 接口有关，需要所述 AMF 实体在注册流程中，确定用户面安全策略。

S502：所述终端设备 A 与网络之间执行双向认证过程。该过程为已有技术，网络参与网元包括 AMF 实体，AUSF 实体和 UDM 实体。其中，所述 AMF 实体在该认证过程中，可以根据 SUCI 得到 SUPI。

在本实例中，所述 AMF 实体可以通过以下两种实现方式，确定用户面安全策略。

实现方式 1：

S503：所述 AMF 实体发送请求消息至 UDM 实体。所述请求消息用于请求所述终端设备 A 的用户面安全策略。其中，所述请求消息中包含 SUPI、应用 ID、DNN 和 S-NSSAI 中的至少一项。

S504：所述 UDM 实体接收所述请求消息后，根据所述请求消息中包含的参数，确定用户面安全策略。

在一个示例中，所述 UDM 实体可以采用传统的方式，确定终端设备 A 签约的用户面安全策略。

在另一个示例中，所述 UDM 实体可以通过发送请求，从应用服务器获取应用安全策略，并根据应用安全策略确定用户面安全策略。具体的，所述 UDM 实体可以确定所述用户面安全策略于应用安全策略相同；或者根据应用安全策略和签约的用户面安全策略，确定最终的用户面安全策略。其中，所述 UDM 实体确定最终的用户面安全策略的过程可以参见图 4 所示的实例中所述 SMF 实体确定所述用户面安全策略的过程，此处不再赘述。

在本示例中，在所述 UDM 实体从所述应用服务器请求应用安全策略的过程中，所述 UDM 实体可以直接与所述应用服务器进行通信交互，或者所述 UDM 实体跨越其他网元与所述应用服务器进行通信交互，本申请对此不作限定。

S505：所述 UDM 实体向所述 AMF 实体发送响应消息，所述响应消息中包含确定的用户面安全策略。

实现方式 2：

S506：所述 AMF 实体向 SMF 实体发送第一请求消息。

其中，第一请求消息中包含 SUPI、应用 ID、DNN 和 S-NSSAI 的至少一项。

S507a：所述 SMF 实体向所述 UDM 实体发送第二请求消息。所述第二请求消息中包含 SUPI、应用 ID、DNN 和 S-NSSAI 的至少一项。

S507b：当所述 UDM 实体根据所述第二请求消息中包含的参数，在本地存储的用户面安全策略中，查找所述终端设备的签约的用户面安全策略。若查找到，则向所述 SMF 实体发送携带所述用户面安全策略的第二响应消息。若未找到，则通过第二响应消息或者其他方式通知所述 SMF。

可选的，所述 UDM 实体还可以从应用服务器获取应用安全策略，并根据应用安全策略确定用户面安全策略。具体描述可以参见 S504 中的描述，此处不再赘述。

S508：所述 SMF 实体接收所述第二响应消息，当所述第二响应消息中包含用户面安

全策略时，确定该用户面安全策略为所述终端设备 A 的用户面安全策略；当所述 SMF 实体未从所述 UDM 实体中获取用户面安全策略时，所述 SMF 实体还可以根据 SUPI、应用 ID、DNN 和 S-NSSAI 的至少一项，在本地存储的用户面安全策略中，确定所述终端设备 A 的用户面安全策略。当所述 SMF 实体未从所述 UDM 实体中获取用户面安全策略时，所述 SMF 实体还可以从应用服务器获取应用安全策略，并根据该应用安全策略确定最终的用户面安全策略，具体过程可以参见图 4 所示的实施例中的所述 SMF 实体确定用户面安全策略的描述，此处不再赘述。

S509: 所述 SMF 实体向所述 AMF 实体发送第一响应消息，所述第一响应消息中携带所述 SMF 实体确定的用户面安全策略。

实现方式三:

AMF 实体也可以从应用服务器获得应用安全策略，以及从 SMF 实体获得的之前确定的用户面安全策略，确定最终的用户面安全策略。具体过程可以参见以上对 UDM 实体确定最终的用户面安全策略的描述。

S510: 所述 AMF 实体向所述网络设备发送所述用户面安全策略。

S511: 所述网络设备向所述终端设备 A 发送 Uu 接口通信方式的安全保护信息。其中所述安全保护信息包含: 所述用户面安全保护方式，和/或，所述用户面安全策略。

S512: 所述终端设备 A 根据 Uu 接口通信方式的安全保护信息，确定 PC5 接口通信方式的安全保护方式，具体过程可以参照实例 1-实例 3 中的描述，此处不再赘述。

实例 5:

在本实例中，终端设备 A 和终端设备 B 之间采用 PC5 接口通信方式进行数据传输，并使用安全保护方式 1 保护传输的数据。在终端设备 A 和终端设备 B 中均保持有安全保护方式 1。可选的，所述安全保护方式 1 可以是通过以上实例中的方法确定的，或者根据本地或从应用服务器获取的应用安全策略确定的，本申请对此不作限定。

参阅图 6 所示，该实例可以包括以下步骤:

S601: 终端设备 A 确定从 PC5 接口通信方式切换到 Uu 接口通信方式。

S602a: 终端设备 A 向网络设备发送 PDU 会话建立请求，其中所述 PDU 会话建立请求中包含安全保护方式 1。

S602b: 所述网络设备通过 AMF 实体向所述 SMF 实体发送所述 PDU 会话建立请求。其中，所述 PDU 会话建立请求中包含安全保护方式 1。

在另一个实现方式中，终端设备 A 还可以向 AMF 实体发送携带安全保护方式 1 的 NAS 消息，再由 AMF 实体将所述安全保护方式 1 发送至 SMF 实体。

S603: 在一个实现方式中，所述 SMF 实体确定用户面安全策略，具体过程可以参见图中的 S203 和 S204，此处不再赘述。在另一个实现方式中，所述 SMF 实体还可以从应用服务器获取应用安全策略，并根据所述应用安全策略，确定用户面安全策略，具体过程可以参见图 2 所示的实例中所述 SMF 实体确定用户面安全策略的描述，此处不再赘述。

S604: 所述 SMF 实体向所述网络设备发送用户面安全策略和安全保护方式 1。

S605: 所述网络设备根据用户面安全策略和安全保护方式 1，确定 Uu 接口通信方式的安全保护方式 2。

在本实例中，所述网络设备可以多种实现方式，确定所述安全保护方式 2。

在一个实现方式中，所述网络设备直接根据所述用户面安全策略和所述安全保护方式1，按照最强原则，确定所述安全保护方式2，保证所述安全保护方式2的保护等级不低于所述用户面安全策略和所述安全保护方式1的保护等级。

在另一个实现方式中，所述网络设备先根据所述用户面安全策略，确定用户面安全保护方式；然后根据确定的用户面安全保护方式和所述安全保护方式1，确定所述安全保护方式2。其中，所述安全保护方式2的保护等级不低于所述用户面安全保护方式和所述安全保护方式1的保护等级。

在另一个实现方式中，上述用户面安全策略的确定和发送步骤是可选的，所述网络设备在从终端设备A获取所述安全保护方式1之后，将安全保护方式1作为安全保护方式2。

S606：所述网络设备激活用户面安全机制，根据确定的安全保护方式2，对后续传输的终端设备A的用户面数据，执行用户面保护。

实例6：

在本实例中，终端设备A和终端设备B之间采用PC5接口通信方式进行数据传输，并使用安全保护方式1保护传输的数据。在终端设备A和终端设备B中均保持有安全保护方式1。具体流程可以参考图6所示的实施例，不同的是，所述终端设备A可以通过S602a将安全保护方式1发送给网络设备后，所述网络设备向SMF实体发送PDU会话建立请求时携带所述安全保护方式1是可选的。相应的，所述SMF实体在S604时向网络设备发送安全保护方式1也是可选的。

所述网络设备在S605时，可以通过以下实现方式确定安全保护方式2：

在一种实现方式中，所述网络设备确定安全保护方式2与安全保护方式1相同。

在另一种实现方式中，所述网络设备确定安全保护方式2的保护等级高于安全保护方式1的保护等级。

在又一种实现方式中，所述终端设备根据S604获得的用户面安全策略，以及所述安全保护方式1，确定所述安全保护方式2。其中，所述安全保护方式2的保护等级不低于所述用户面安全策略和所述安全保护方式1的保护等级。

实例7：

在本实例中，终端设备A和终端设备B之间采用PC5接口通信方式进行数据传输，并使用安全保护方式1保护传输的数据。在终端设备A和终端设备B中均保持有安全保护方式1。具体流程可以参考图6所示的实施例，不同的是：所述终端设备A执行S602a时，不在所述PDU会话建立请求中携带所述安全保护方式1，而是预先将所述安全保护方式1发送给应用服务器；所述SMF实体可以从所述应用服务器获取所述安全保护方式1，当所述SMF实体执行S604时，可以将所述用户面安全策略和所述安全保护方式1同时发送给所述网络设备。

可选的，所述终端设备A向所述应用服务器发送所述安全保护方式1时，可以同时发送以下至少一项：UE的运营商网络标识，广义公共签约标识（Generic Public Subscription Identifier，GPSI），应用ID、UE应用ID、UE的运营商网络ID、PC5链路标识。这样，所述应用服务器向所述SMF实体同时发送上述参数和所述安全保护方式1。

所述终端设备A在确定切换通信方式时，可以向SMF实体发送应用ID，UE应用ID，UE的运营商网络ID和PC5链路标识的至少一项，例如将上述参数携带在PDU会话建立请求中。当所述SMF实体接收到所述终端设备发送的应用ID，UE应用ID，UE的运营

商网络 ID 和 PC5 链路标识的至少一项时，所述 SMF 实体可以根据该参数，可以确定所述安全保护方式 1。

实例 8:

基于以上实例 5-7 中的步骤，在所述终端设备 A 和终端设备 B 还保存有 PC5 接口通信方式的应用安全策略的情况下。

在一个实现方式中，所述终端设备 A 还可以在发送安全保护方式 1 时，同时发送所述应用安全策略。这样，所述网络设备在确定所述安全保护方式 2 时，还可以参考所述应用安全策略，其中，所述安全保护方式 2 的保护等级不低于所述应用安全策略。

在另一个实现方式中，实例中的涉及安全保护方式 1 可以替换为所述应用安全策略。

实例 9:

在本实例中，终端设备 A 和终端设备 B 各自采用 Uu 接口通信方式进行数据传输，其中终端设备 A 保存有 Uu 接口通信方式的安全保护信息 1，终端设备 B 保存有 Uu 接口通信方式的安全保护信息 2。其中，安全保护信息 1 中包含安全保护方式 1，和/或，用户面安全策略 1；安全保护信息 2 中包含安全保护方式 2，和/或，用户面安全策略 2。

参阅图 7 所示，该实例可以包括以下步骤:

S701: 终端设备 A 和终端设备确定从 Uu 接口通信方式切换至 PC5 接口通信方式。

S702: 终端设备 A 向终端设备 B 发送安全保护信息 1。

示例性的，所述终端设备 A 可以广播发送所述安全保护信息 1。

示例性的，所述终端设备 A 可以通过设备直通发现等传统的方式，确定终端设备 B 为其采用 PC5 接口通信方式时的对端设备。

示例性的，所述终端设备 A 可以通过用户的输入信息，确定终端设备 B 为其采用 PC5 接口通信方式时的对端设备。

S703: 终端设备 B 根据接收的安全保护信息 1 和本地保存的安全保护信息 2，确定 PC5 接口通信方式的安全保护方式 a。需要说明的是，所述安全保护方式 a 的保护等级不低于所述安全保护信息 1 和所述安全保护信息 2 的保护等级。具体确定过程可以参见以上实施例和实例 3 中的描述，此处不再赘述。

S704: 所述终端设备 B 向所述终端设备 A 发送所述安全保护方式 a，并使用所述安全保护方式 a，保护所述终端设备 A 和所述终端设备 B 之间传输的数据。

实例 10:

基于以上实例中的流程，在本实例中，网络设备或者终端设备可以根据用户面安全策略或应用安全策略确定最终的安全保护方式，而不需要考虑不同通信方式的安全保护方式，这样，该方法可以更好的参考设备的安全保护能力。

实例 11:

基于以上实例中的流程，在本实例中，网络设备或者终端设备可以根据优先级的方式判定是使用用户面安全策略，还是使用应用安全策略确定最终的安全保护方式。例如，如果存在应用安全策略，则仅根据应用安全策略作为判断依据；或者如果存在用户面安全策略，则仅根据用户面安全策略作为判断依据。

实施 12:

在本实例中，终端设备 A 和终端设备 B 各自采用 PC5 接口通信方式进行数据传输，其中终端设备 A 保存有安全保护信息 1，终端设备 B 保存安全保护信息 2。其中，安全保护信息 1 中包含安全保护方式 1，和/或，用户面安全策略 1；安全保护信息 2 中包含安全保护方式 2，和/或，用户面安全策略 2。这里安全保护信息 1 和 2 可以为预置的，或者应用或业务只是给终端的，或者通过其他方式获得的，不做限制。

终端设备 A 还可能保存业务标识 1，这里安全保护信息 1 与业务标识 1 相关。终端设备 A 还可能保存应用标识 1，这里安全保护信息 1 与应用标识 1 相关。

终端设备 B 还可能保存业务标识 1，这里安全保护信息 2 与业务标识 1 相关。终端设备 A 还可能保存应用标识 1，这里安全保护信息 2 与应用标识 1 相关。

该实例可以包括以下步骤:

终端设备 A 向终端设备 B 发送安全保护信息 1。

示例性的，所述终端设备 A 可以广播发送所述安全保护信息 1。

示例性的，所述终端设备 A 可以通过设备直通发现等传统的方式，确定终端设备 B 为其采用 PC5 接口通信方式时的对端设备。

示例性的，所述终端设备 A 可以通过用户的输入信息，确定终端设备 B 为其采用 PC5 接口通信方式时的对端设备。

可选的，除了安全保护信息 1，终端设备 A 还发送业务标识 1;

可选的，除了安全保护信息 1，终端设备 A 还发送应用标识 1;

终端设备 B 根据接收的安全保护信息 1 和本地保存的安全保护信息 2，确定 PC5 接口通信方式的安全保护方式 a。需要说明的是，所述安全保护方式 a 的保护等级不低于所述安全保护信息 1 和所述安全保护信息 2 的保护等级。具体根据安全保护信息 1 和本地保存的安全保护信息 2 确定 PC5 接口的安全保护方式的方法可以参见以上实施例和实例 3 中的描述，此处不再赘述。

可选的，终端设备 B 还接受终端设备 A 发送的业务标识 1，根据业务标识 1 确定本地保护的安全保护信息 2。

可选的，终端设备 B 还接受终端设备 A 发送的应用标识 1，根据应用标识 1 确定本地保护的安全保护信息 2。

所述终端设备 B 向所述终端设备 A 发送所述安全保护方式 a，并使用所述安全保护方式 a，保护所述终端设备 A 和所述终端设备 B 之间传输的数据。

可选的，除了安全保护方式 a，终端设备 B 还发送业务标识 1;

可选的，除了安全保护方式 a，终端设备 B 还发送应用标识 1;

可选的，除了安全保护方式 a，终端设备 B 还发送安全保护信息 1 和/或安全保护信息 2.

针对本申请中所有实例的流程，终端设备之间安全保护方式的确定不仅仅限于两个接入方式的切换场景。两个终端之间也可以基本本地保存的安全保护信息进行协商。

针对本申请中所有实例的流程，终端设备之间安全保护方式的确定也可以基于其中一个终端的安全保护信息。例如，终端设备 A 发送安全保护信息 1，终端设备 B 根据安全保护信息 1 确定双方的安全保护方式。也可能终端设备 A 发送通信请求，终端设备 B 根据安全保护信息 2 确定双方的安全保护方式。也可能终端设备 A 发送通信请求，终端设备 B

发送安全保护信息 2 至终端设备 A。终端设备 A 根据安全保护信息 2 确定双方的安全保护方式。不做限制。

针对本申请中所有实例的流程，终端设备之间安全保护方式确定之后，终端设备 B 发送安全保护信息 1 至终端设备 A，以使终端设备 A 能够校验之前发送的安全保护信息 1 与从终端设备 B 接收到的安全保护信息 2 是否一致。如果不一致，则可选的发送拒绝消息至终端设备 B；或者中断通信等不做限制。还可能终端设备 B 发送安全保护信息 2 至终端设备 A，以使终端设备 A 确定安全保护信息 2 的内容。可选的，这里终端设备 B 发送的安全保护信息 1 和/或安全保护信息 2 需要支持完整性保护，防止被其他攻击者修改。

实施例 12 中描述的业务标识和/或应用标识也适用本申请的其他实施例。具体来讲就是，发送的安全保护信息与业务标识或者应用标识相关，因此协商出来的保护方式也是跟此业务标识或者应用标识一致的。协商出来的保护方式也是适用终端之间的会话粒度，承载粒度，流粒度，切片粒度等。

另外，需要指出的是，实施例 12 中的终端设备 A 或终端设备 B 的结构可参考图 8 或图 9 所示的结构。通过图 8 或图 9 所示的结构可执行实施例 12 所示的方法。

基于同一技术构思，本申请实施例还提供了一种安全保护方式确定装置，所述装置可以应用于如图 1 所示的通信系统中的终端设备，并可以实现以上实施例中的安全保护方式确定方法。参阅图 8 所示，该装置的结构包括通信单元 801 和处理单元 802。下面以所述装置应用的终端设备为第一终端设备为例，对各个单元的功能进行描述。

所述通信单元 801，用于接收和发送数据；

所述处理单元 802，用于通过所述通信单元 801 执行以下步骤：

获取第一通信方式的安全保护信息，其中，所述安全保护信息包含第一安全保护方式，和/或，第一安全策略；所述第一安全保护方式对应所述第一通信方式，用于保护所述第一终端设备采用所述第一通信方式时传输的数据，所述第一安全策略为所述第一终端设备的所述第一通信方式的安全策略；

根据所述安全保护信息，确定第二安全保护方式，所述第二安全保护方式对应第二通信方式，用于保护所述第一终端设备采用第二通信方式时传输的数据。

在一种可能的实现方式中，当所述安全保护信息为所述第一安全保护方式时，所述处理单元 802，在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

确定所述第二安全保护方式与所述第一安全保护方式相同；或者

获取第二安全策略，所述第二安全策略为所述第一终端设备的所述第二通信方式的安全策略；根据所述第二安全策略、所述第一安全保护方式，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全保护方式的保护等级。

在一种可能的实现方式中，所述处理单元 802，在根据所述第二安全策略、所述第一安全保护方式，确定所述第二安全保护方式时，具体用于：

当所述第一安全保护方式的保护等级为需要安全保护，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为优先安全保护时，根据自身的安全保护能力确定所述第二安全保护方式的保护等级；

当所述第一安全保护方式的保护等级为不需要安全保护，所述第二安全策略的保护等级为不需要安全保护时，确定所述第二安全保护方式的保护等级为不需要安全保护。

在一种可能的实现方式中，当所述安全保护信息为所述第一安全策略时，所述处理单元802，在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

根据所述第一安全策略，确定所述第二安全保护方式；或者

获取第二安全策略，所述第二安全策略为所述的所述第二通信方式的安全策略；根据所述第二安全策略、所述第一安全策略，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全策略的保护等级。

在一种可能的实现方式中，所述处理单元802，在根据所述第二安全策略、所述第一安全策略，确定所述第二安全保护方式时，具体用于：

当所述第二安全策略的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为优先安全保护或者不需要安全保护时，根据所述第一安全策略的保护等级，确定所述第二安全保护方式的保护等级。

在一种可能的实现方式中，所述处理单元802，在根据所述第一安全策略，确定所述第二安全保护方式时，具体用于：

当所述第一安全策略的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全策略的保护等级为优先安全保护时，根据自身的安全保护能力确定所述第二安全保护方式的保护等级；

当所述第一安全策略保护等级为不需要安全保护时，确定所述第二安全保护方式的保护等级为不需要安全保护。

在一种可能的实现方式中，所述处理单元802，还用于：

在确定第二安全保护方式之后，通过所述通信单元801向第二终端设备发送所述第二安全保护方式，并接收所述第二终端设备根据所述第二安全保护方式和第三安全保护方式确定的第四安全保护方式；或者

在确定第二安全保护方式之后，通过所述通信单元801接收第二终端设备发送的第三安全保护方式，并根据所述第二安全保护方式和所述第三安全保护方式，确定第四安全保护方式；

其中，所述第四安全保护方式的保护等级不低于所述第二安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；所述第三安全保护方式用于保护所述第二终端设备采用第二通信方式时传输的数据，所述第四安全保护方式用于保护所述与所述第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据。

在一种可能的实现方式中，所述处理单元802，在根据所述第二安全保护方式和所述第三安全保护方式，确定第四安全保护方式时，具体用于：

当所述第二安全保护方式和所述第三安全保护方式中至少一项的保护等级为需要安全保护时，确定所述第四安全保护方式的保护等级为需要安全保护；

当所述第二安全保护方式和所述第三安全保护方式的保护等级均为不需要安全保护时，确定所述第四安全保护方式的保护等级为不需要安全保护。

在一种可能的实现方式中，当所述安全保护信息为所述第一安全策略时，所述第二安全保护方式具体用于保护所述第一终端设备与第二终端设备之间采用所述第二通信方式时进行数据传输时传输的数据；所述处理单元 802，在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

通过所述通信单元 801 向所述第二终端设备发送所述第一安全策略，并接收所述第二终端设备根据所述第一安全策略和第三安全策略确定的所述第二安全保护方式；或者

通过所述通信单元 801 接收第二终端设备发送的所述第三安全策略；并根据所述第一安全策略和所述第三安全策略，确定所述第二安全保护方式；

其中，所述第二安全保护方式的保护等级不低于所述第一安全策略的保护等级，且不低于所述第三安全策略的保护等级；所述第三安全策略为所述第二终端设备的所述第一通信方式的保护等级。

在一种可能的实现方式中，所述处理单元 802，在根据所述第一安全策略和所述第三安全策略，确定所述第二安全保护方式时，具体用于：

当所述第一安全策略和所述第三安全策略中至少一项的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全策略和所述第三安全策略的保护等级均为不需要安全保护时，确定所述第二安全保护方式的保护等级为不需要安全保护；

当所述第一安全策略和所述第三安全策略的保护等级均为优先安全保护时，或者当所述第一安全策略和所述第三安全策略中其中一项的保护等级为优先安全保护，另一项的保护等级为不需要安全保护时，根据自身的安全保护能力确定所述第二安全保护方式的保护等级。

在一种可能的实现方式中，所述处理单元 802，在获取所述第一通信方式的所述安全保护信息时，具体用于：

确定从第一通信方式切换到第二通信方式时，获取所述第一通信方式的所述安全保护信息。

在一种可能的实现方式中，当所述第二通信方式为 Uu 接口通信方式时，所述处理单元 802，在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

通过所述通信单元 801 向网络设备发送所述安全保护信息；并从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据所述安全保护信息确定的；或者

通过所述通信单元 801 向应用服务器发送所述安全保护信息，以及向网络设备发送请求消息；通过所述通信单元 801 从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据从所述应用服务器获取的所述安全保护信息确定的。

在一种可能的实现方式中，所述安全保护信息中包含所述第一安全保护方式时，

所述第二安全保护方式与所述第一安全保护方式相同；或者

所述第二安全保护方式的保护等级高于所述第一安全保护方式的保护等级；或者

所述第二安全保护方式为所述网络设备根据所述第一安全保护方式和/或第二安全策略确定的，其中，所述第二安全策略为所述网络设备获得的所述第一终端设备采用所述第

二通信方式的保护等级；或者

所述第二安全保护方式为所述网络设备根据所述第一安全保护方式以及第三安全保护方式确定的，其中，所述第三安全保护方式为所述网络设备根据所述第二安全策略确定的。

在一种可能的实现方式中，当所述第二安全策略的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为优先安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为优先安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级由所述网络设备指定；

当所述第二安全策略的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第二安全策略的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级为不需要安全保护。

在一种可能的实现方式中，当所述第三安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，所述第二安全保护方式的保护等级为不需要安全保护。

在一种可能的实现方式中，当所述第二通信方式为 PC5 接口通信方式时，所述第二安全保护方式具体用于保护所述第一终端设备与第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据；所述处理单元 802，在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

当所述安全保护信息包含所述第一安全保护方式时，通过所述通信单元 801 向第二终端设备发送所述第一安全保护方式，并从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式和第三安全保护方式确定的，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式时，通过所述通信单元 801 从所述第二终端设备接收第三安全保护方式，并根据所述第一安全保护方式和所述第三安全保护方式，确定所述第二安全保护方式；其中，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，通过所述通信单元 801 向所述第二终端设备发送所述第一安全保护方式和所述第一安全策略；通过所述通信单元 801 从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式、所述第一安全策略，第三安全保护方式，以及第二安全策略确定的；当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全

保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，通过所述通信单元 801 从所述第二终端设备接收第三安全保护方式和第二安全策略；根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式；其中，当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级；

其中，所述第三安全保护方式用于保护所述第二终端设备采用第一通信方式时传输的数据，所述第二安全策略为所述第二终端设备的所述第一通信方式的安全策略。

在一种可能的实现方式中，所述处理单元 802，在根据所述第一安全保护方式和所述第三安全保护方式，确定所述第二安全保护方式时，具体用于：

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，通过网络设备确定所述第二安全保护方式的保护等级；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，确定所述第二安全保护方式的保护等级为不需要安全保护。

在一种可能的实现方式中，所述处理单元 802 在根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式时，具体用于：

当所述第一安全保护方式与所述第三安全保护方式相同时，确定所述第二安全保护方式为所述第一安全保护方式；

当所述第一安全保护方式与所述第三安全保护方式不相同时，根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式。

在一种可能的实现方式中，所述处理单元 802，在根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式时，具体用于：

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，通过网络设备确定所述第二安全保护方式的保护等级；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第三安全保护方式的保护等级为不需要安全保护，所述第一安全保护方式的保护等级为不需要安全保护时，根据所述第一安全策略和所述第二安全策略，确定所述第二

安全保护方式。

在一种可能的实现方式中，所述处理单元802，在根据所述第一安全策略和所述第二安全策略，确定所述第二安全保护方式时，具体用于：

当所述第一安全策略和所述第二安全策略中至少一项的保护等级为需要安全保护时，确定所述第二安全保护方式的保护等级为需要安全保护；

当所述第一安全策略和所述第二安全策略的保护等级均为不需要安全保护时，确定所述第二安全保护方式的保护等级为不需要安全保护；

当所述第一安全策略和所述第二安全策略的保护等级均为优先安全保护时，或者当所述第一安全策略和所述第三安全策略中其中一项的保护等级为优先安全保护，另一项的保护等级为不需要安全保护时，根据自身的安全保护能力确定所述第二安全保护方式的保护等级。

在一种可能的实现方式中，以上安全策略包含：机密性保护需求，和/或，完整性保护需求；以上各安全保护方式包含：机密性保护需求，和/或，完整性保护需求。

本申请实施例提供了一种安全保护方式确定装置，通过该方案，终端设备可以根据第一通信方式的安全保护信息，确定第二通信方式的安全保护方式。这样，当所述终端设备在从第一通信方式切换到所述第二通信方式时，可以直接使用所述第二通信方式的安全保护方式保护传输的数据，从而可以保证通信方式切换后的所述终端设备的数据安全性。进一步的，所述终端设备确定的第二通信方式的安全保护方式的保护等级不低于第一通信方式的安全保护信息的保护等级，这样，可以进一步保证通信方式切换后的所述终端设备的数据安全性。

需要说明的是，本申请以上实施例中对模块的划分是示意性的，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，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，也可以采用软件功能单元的形式实现。

所述集成的单元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。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或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）或处理器（processor）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。

基于同一技术构思，本申请实施例还提供了一种终端设备，所述终端设备可以应用于如图1所示的通信系统中，具有图8所示的安全保护方法确定装置的功能，并可以实现以上实施例中的安全保护方式确定方法。参阅图9所示，所述终端设备900包括：收发器901、处理器902。可选的，所述终端设备900还包括存储器903。其中，所述收发器901、所述处理器902以及所述存储器903之间相互连接。

可选的，所述收发器901、所述处理器902以及所述存储器903之间通过总线904相

互连接。所述总线 904 可以是外设部件互连标准（peripheral component interconnect，PCI）总线或扩展工业标准结构（extended industry standard architecture，EISA）总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图 9 中仅用一条粗线表示，但并不表示仅有一根总线或一种类型的总线。

所述收发器 901，用于接收和发送信号，实现与通信系统中的其他设备之间的通信。可选的，所述收发器 901 可以通过射频装置和天线实现。

所述处理器 902，用于实现如以上各图中的安全保护方式确定方法中终端设备的功能，具体可以参照以上实施例中的描述，此处不再赘述。

其中，处理器 902 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 的组合等等。处理器 902 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。处理器 902 在实现上述功能时，可以通过硬件实现，当然也可以通过硬件执行相应的软件实现。

所述存储器 903，用于存放程序指令等。具体地，程序指令可以包括程序代码，该程序代码包括计算机操作指令。存储器 903 可能包含随机存取存储器（random access memory，RAM），也可能还包括非易失性存储器（non-volatile memory），例如至少一个磁盘存储器。处理器 902 执行存储器 903 所存放的程序指令，实现上述功能，从而实现上述实施例提供的安全保护方式确定方法。

基于以上实施例，本申请实施例还提供了一种计算机程序，当所述计算机程序在计算机上运行时，使得所述计算机执行以上实施例提供的安全保护方式确定方法。

基于以上实施例，本申请实施例还提供了一种计算机存储介质，该计算机存储介质中存储有计算机程序，所述计算机程序被计算机执行时，使得计算机执行以上实施例提供的安全保护方式确定方法。

基于以上实施例，本申请实施例还提供了一种芯片，所述芯片用于读取存储器中存储的计算机程序，实现以上实施例提供的安全保护方式确定方法。

基于以上实施例，本申请实施例提供了一种芯片系统，该芯片系统包括处理器，用于支持计算机装置实现以上实施例提供的安全保护方式确定方法。在一种可能的设计中，所述芯片系统还包括存储器，所述存储器用于保存该计算机装置必要的程序和数据。该芯片系统，可以由芯片构成，也可以包含芯片和其他分立器件。

综上所述，本申请提供了一种安全保护方式确定方法及装置，在该方法中，终端设备可以根据第一通信方式的安全保护信息，确定第二通信方式的安全保护方式。这样，当所述终端设备在从第一通信方式切换到所述第二通信方式时，可以直接使用所述第二通信方式的安全保护方式保护传输的数据，从而可以保证通信方式切换后的所述终端设备的数据安全性。

本领域内的技术人员应明白，本申请的实施例可提供为方法、系统、或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机

可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本申请是参照根据本申请的方法、设备（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的步骤。

显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求 书

1、一种安全保护方式确定方法，其特征在于，包括:

第一终端设备获取第一通信方式的安全保护信息，其中，所述安全保护信息包含第一安全保护方式，和/或，第一安全策略；所述第一安全保护方式对应所述第一通信方式，用于保护所述第一终端设备采用所述第一通信方式时传输的数据，所述第一安全策略为所述第一终端设备的所述第一通信方式的安全策略；

所述第一终端设备根据所述安全保护信息，确定第二安全保护方式，所述第二安全保护方式对应第二通信方式，用于保护所述第一终端设备采用第二通信方式时传输的数据。

2、如权利要求 1 所述的方法，其特征在于，当所述安全保护信息为所述第一安全保护方式时，所述第一终端设备根据所述安全保护信息，确定所述第二安全保护方式，包括:

所述第一终端设备确定所述第二安全保护方式与所述第一安全保护方式相同；或者

所述第一终端设备获取第二安全策略，所述第二安全策略为所述第一终端设备的所述第二通信方式的安全策略；所述第一终端设备根据所述第二安全策略、所述第一安全保护方式，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全保护方式的保护等级。

3、如权利要求 1 所述的方法，其特征在于，当所述安全保护信息为所述第一安全策略时，所述第一终端设备根据所述安全保护信息，确定所述第二安全保护方式，包括:

所述第一终端设备根据所述第一安全策略，确定所述第二安全保护方式；或者

所述第一终端设备获取第二安全策略，所述第二安全策略为所述第一终端设备的所述第二通信方式的安全策略；所述第一终端设备根据所述第二安全策略、所述第一安全策略，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全策略的保护等级。

4、如权利要求 1-3 任一项所述的方法，其特征在于，在所述第一终端设备确定第二安全保护方式之后，所述方法还包括:

所述第一终端设备向第二终端设备发送所述第二安全保护方式，并接收所述第二终端设备根据所述第二安全保护方式和第三安全保护方式确定的第四安全保护方式；或者

所述第一终端设备接收第二终端设备发送的第三安全保护方式，并根据所述第二安全保护方式和所述第三安全保护方式，确定第四安全保护方式；

其中，所述第四安全保护方式的保护等级不低于所述第二安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；所述第三安全保护方式用于保护所述第二终端设备采用第二通信方式时传输的数据，所述第四安全保护方式用于保护所述第一终端设备与所述第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据。

5、如权利要求 1 所述的方法，其特征在于，所述第一终端设备获取所述第一通信方式的所述安全保护信息，包括:

所述第一终端设备确定从第一通信方式切换到第二通信方式时，获取所述第一通信方式的所述安全保护信息。

6、如权利要求 5 所述的方法，其特征在于，当所述第二通信方式为 Uu 接口通信方式时，所述第一终端设备根据所述安全保护信息，确定所述第二安全保护方式，包括:

所述第一终端设备向网络设备发送所述安全保护信息；并从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据所述安全保护信息确定的；或者

所述第一终端设备向应用服务器发送所述安全保护信息，以及向网络设备发送请求消息；所述第一终端设备从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据从所述应用服务器获取的所述安全保护信息确定的。

7、如权利要求 1 或 5 所述的方法，其特征在于，当所述第二通信方式为 PC5 接口通信方式时，所述第二安全保护方式具体用于保护所述第一终端设备与第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据；

所述第一终端设备根据所述安全保护信息，确定所述第二安全保护方式，包括：

当所述安全保护信息包含所述第一安全保护方式时，所述第一终端设备向第二终端设备发送所述第一安全保护方式，并从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式和第三安全保护方式确定的，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式时，所述第一终端设备从所述第二终端设备接收第三安全保护方式，并根据所述第一安全保护方式和所述第三安全保护方式，确定所述第二安全保护方式；其中，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，所述第一终端设备向所述第二终端设备发送所述第一安全保护方式和所述第一安全策略；所述第一终端设备从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式、所述第一安全策略，第三安全保护方式，以及第二安全策略确定的；当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，所述第一终端设备从所述第二终端设备接收第三安全保护方式和第二安全策略；所述第一终端设备根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式；其中，当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级；

其中，所述第三安全保护方式用于保护所述第二终端设备采用第一通信方式时传输的数据，所述第二安全策略为所述第二终端设备的所述第一通信方式的安全策略。

8、如权利要求 1-7 任一项所述的方法，其特征在于，

所述第一安全策略包含：机密性保护需求，和/或，完整性保护需求；

所述第一安全保护方式、所述第二安全保护方式均包含：机密性保护需求，和/或，完整性保护需求。

9、一种安全保护方式确定装置，所述装置应用于第一终端设备中，其特征在于，包括：

收发器，用于接收和发送数据；

处理器，用于通过所述收发器执行以下步骤：

获取第一通信方式的安全保护信息，其中，所述安全保护信息包含第一安全保护方式，和/或，第一安全策略；所述第一安全保护方式对应所述第一通信方式，用于保护所述第一终端设备采用所述第一通信方式时传输的数据，所述第一安全策略为所述第一终端设备的所述第一通信方式的安全策略；

根据所述安全保护信息，确定第二安全保护方式，所述第二安全保护方式对应第二通信方式，用于保护所述第一终端设备采用第二通信方式时传输的数据。

10、如权利要求 9 所述的装置，其特征在于，当所述安全保护信息为所述第一安全保护方式时，所述处理器在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

确定所述第二安全保护方式与所述第一安全保护方式相同；或者

获取第二安全策略，所述第二安全策略为所述第一终端设备的所述第二通信方式的安全策略；根据所述第二安全策略、所述第一安全保护方式，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全保护方式的保护等级。

11、如权利要求 9 所述的装置，其特征在于，当所述安全保护信息为所述第一安全策略时，所述处理器在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

根据所述第一安全策略，确定所述第二安全保护方式；或者

获取第二安全策略，所述第二安全策略为所述第一终端设备的所述第二通信方式的安全策略；所述第一终端设备根据所述第二安全策略、所述第一安全策略，确定所述第二安全保护方式，其中，所述第二安全保护方式的保护等级不低于所述第二安全策略的保护等级，且不低于所述第一安全策略的保护等级。

12、如权利要求 9-11 任一项所述的装置，其特征在于，所述处理器还用于：

在确定第二安全保护方式之后，通过所述收发器向第二终端设备发送所述第二安全保护方式，并通过所述收发器接收所述第二终端设备根据所述第二安全保护方式和第三安全保护方式确定的第四安全保护方式；或者

在确定第二安全保护方式之后，通过所述收发器接收第二终端设备发送的第三安全保护方式，并根据所述第二安全保护方式和所述第三安全保护方式，确定第四安全保护方式；

其中，所述第四安全保护方式的保护等级不低于所述第二安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；所述第三安全保护方式用于保护所述第二终端设备采用第二通信方式时传输的数据，所述第四安全保护方式用于保护所述第一终端设备与所述第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据。

13、如权利要求 9 所述的装置，其特征在于，所述处理器在获取所述第一通信方式的所述安全保护信息时，具体用于：

确定从第一通信方式切换到第二通信方式时，获取所述第一通信方式的所述安全保护

信息。

14、如权利要求 13 所述的装置，其特征在于，当所述第二通信方式为 Uu 接口通信方式时，所述处理器在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

通过所述收发器向网络设备发送所述安全保护信息；并通过所述收发器从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据所述安全保护信息确定的；或者

通过所述收发器向应用服务器发送所述安全保护信息，以及向网络设备发送请求消息；通过所述收发器从所述网络设备接收所述第二安全保护方式，所述第二安全保护方式为所述网络设备根据从所述应用服务器获取的所述安全保护信息确定的。

15、如权利要求 9 或 13 所述的装置，其特征在于，当所述第二通信方式为 PC5 接口通信方式时，所述第二安全保护方式具体用于保护所述第一终端设备与第二终端设备之间采用所述第二通信方式进行数据传输时传输的数据；

所述处理器在根据所述安全保护信息，确定所述第二安全保护方式时，具体用于：

当所述安全保护信息包含所述第一安全保护方式时，通过所述收发器向第二终端设备发送所述第一安全保护方式，并从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式和第三安全保护方式确定的，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式时，通过所述收发器从所述第二终端设备接收第三安全保护方式，并根据所述第一安全保护方式和所述第三安全保护方式，确定所述第二安全保护方式；其中，所述第二安全保护方式的保护等级不低于所述第一安全保护方式的保护等级，且不低于所述第三安全保护方式的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，通过所述收发器向所述第二终端设备发送所述第一安全保护方式和所述第一安全策略；通过所述收发器从所述第二终端设备接收所述第二安全保护方式；其中，所述第二安全保护方式为所述第二终端设备根据所述第一安全保护方式、所述第一安全策略，第三安全保护方式，以及第二安全策略确定的；当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级；或者

当所述安全保护信息包含所述第一安全保护方式和所述第一安全策略时，通过所述收发器从所述第二终端设备接收第三安全保护方式和第二安全策略；根据所述第一安全保护方式、所述第一安全策略、所述第三安全保护方式，和所述第二安全策略，确定所述第二安全保护方式；其中，当所述第一安全保护方式与所述第三安全保护方式相同时，所述第二安全保护方式与所述第一安全保护方式相同；当所述第一安全保护方式与所述第三安全保护方式不相同时，所述第二安全保护方式的保护等级不低于所述第一安全保护方式和所述第二安全保护方式的保护等级，且不低于所述第一安全策略和所述第二安全策略的保护等级；

其中，所述第三安全保护方式用于保护所述第二终端设备采用第一通信方式时传输的

数据，所述第二安全策略为所述第二终端设备的所述第一通信方式的安全策略。

16、如权利要求 9-15 任一项所述的装置，其特征在于，

所述第一安全策略包含：机密性保护需求，和/或，完整性保护需求；

所述第一安全保护方式、所述第二安全保护方式均包含：机密性保护需求，和/或，完整性保护需求。

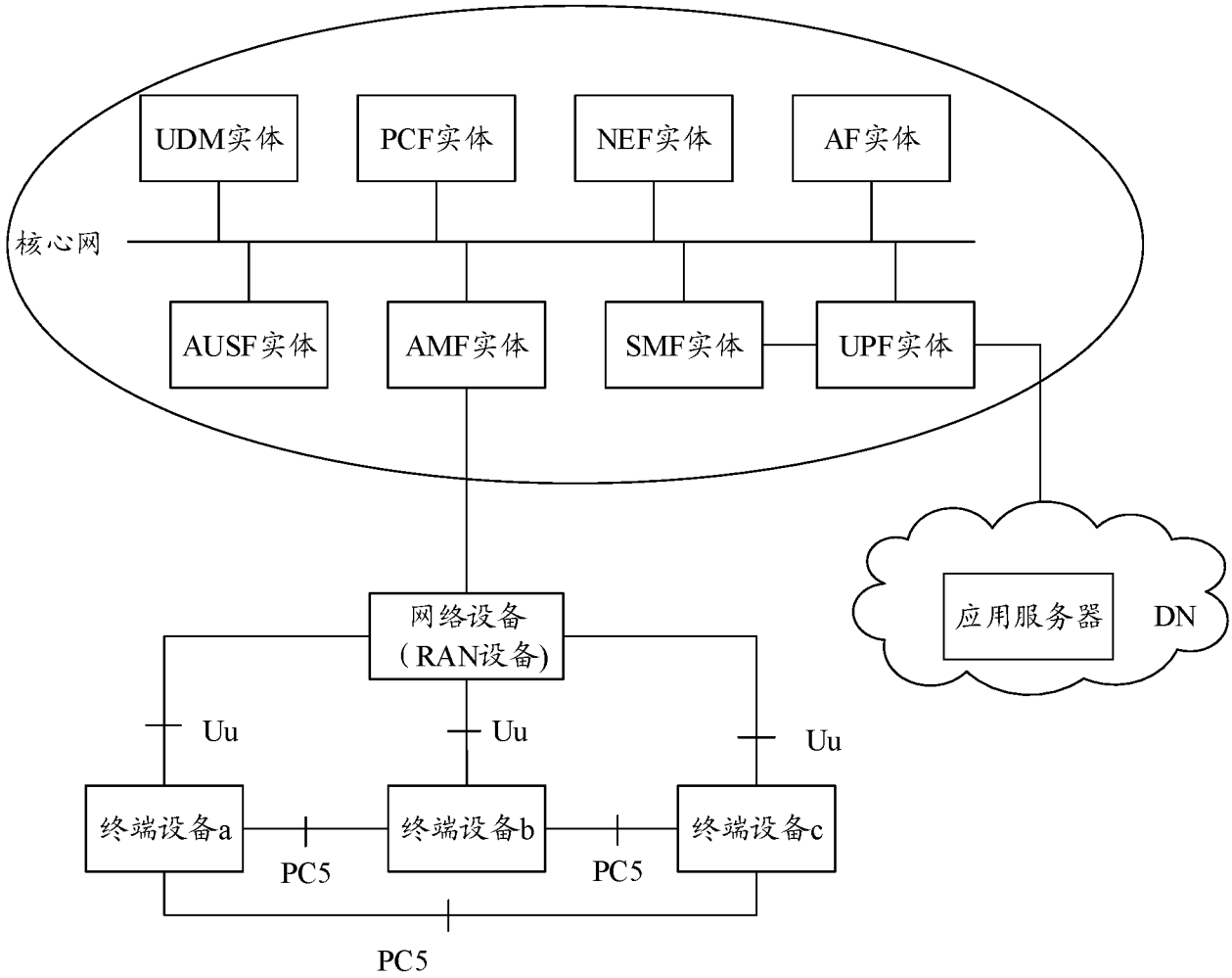
UDM实体
PCF实体
NEF实体
AF实体
核心网
AUSF实体
AMF实体
SMF实体
UPF实体
应用服务器
DN
网络设备
（RAN设备)
Uu
Uu
Uu
终端设备a
终端设备b
终端设备c
PC5
PC5
PC5

图 1

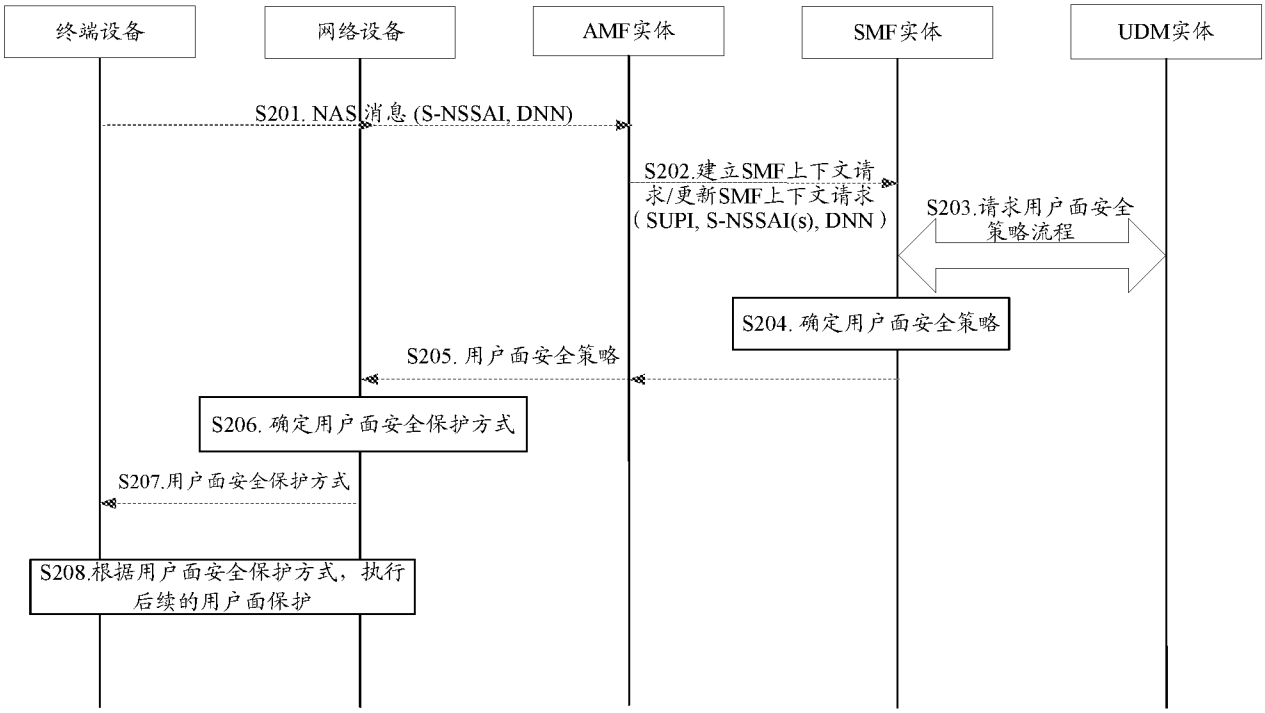
终端设备
网络设备
AMF实体
SMF实体
UDM实体
S201. NAS消息 (S-NSSAI, DNN)
S202.建立SMF上下文请求/更新SMF上下文请求（SUPI, S-NSSAI(s), DNN）
S203.请求用户面安全策略流程
S204. 确定用户面安全策略
S205. 用户面安全策略
S206. 确定用户面安全保护方式
S207.用户面安全保护方式
S208.根据用户面安全保护方式，执行后续的用户面保护

图 2

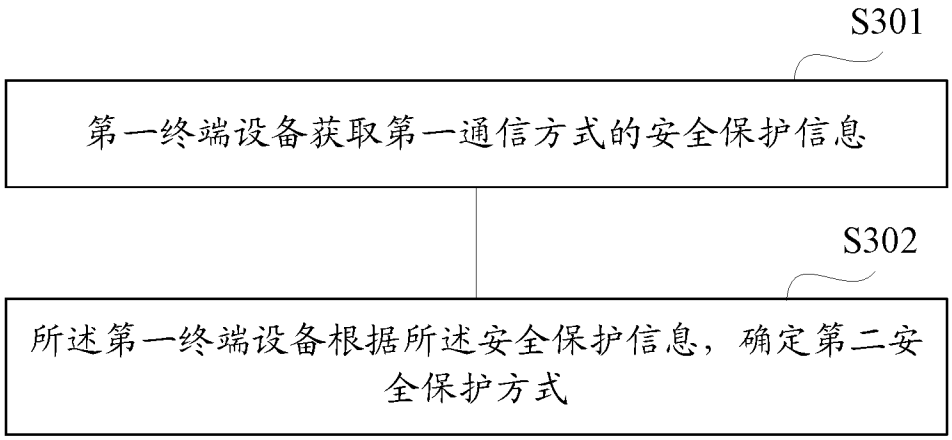
S301
第一终端设备获取第一通信方式的安全保护信息
S302
所述第一终端设备根据所述安全保护信息，确定第二安全保护方式

图 3

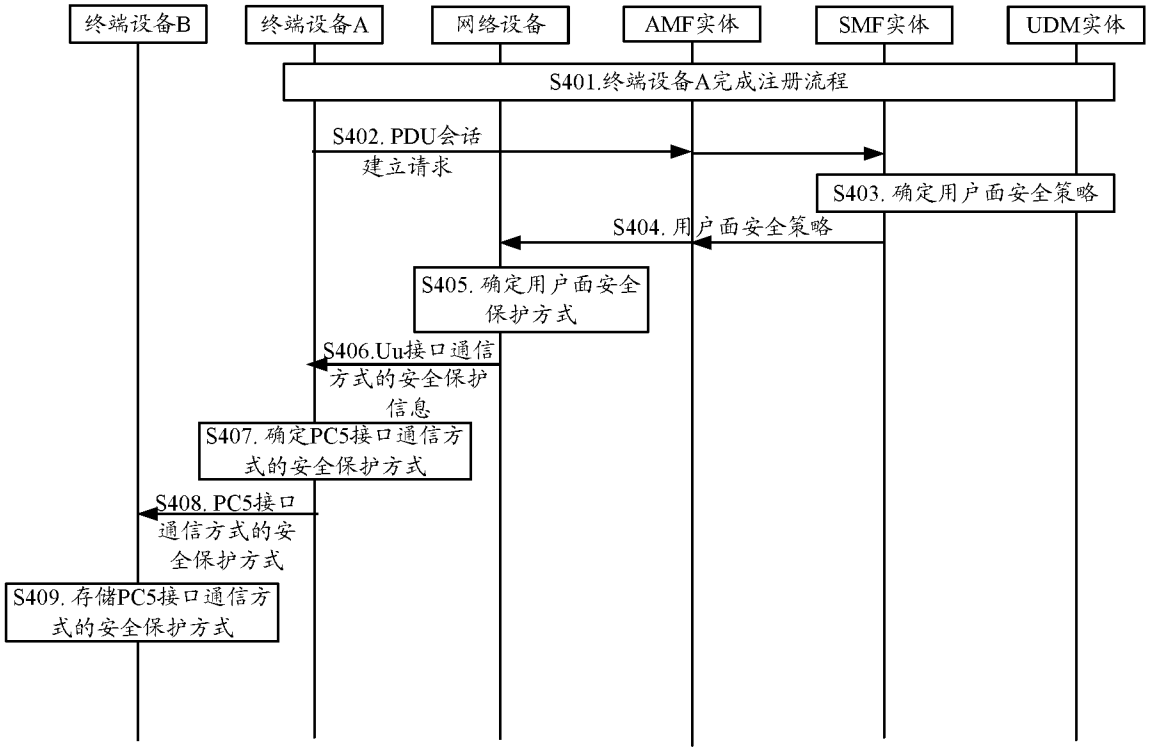
终端设备B
终端设备A
网络设备
AMF实体
SMF实体
UDM实体
S401.终端设备A完成注册流程
S402. PDU会话建立请求
S403. 确定用户面安全策略
S404. 用户面安全策略
S405. 确定用户面安全保护方式
S406.Uu接口通信方式的安全保护信息
S407. 确定PC5接口通信方式的安全保护方式
S408. PC5接口通信方式的安全保护方式
S409. 存储PC5接口通信方式的安全保护方式

图 4

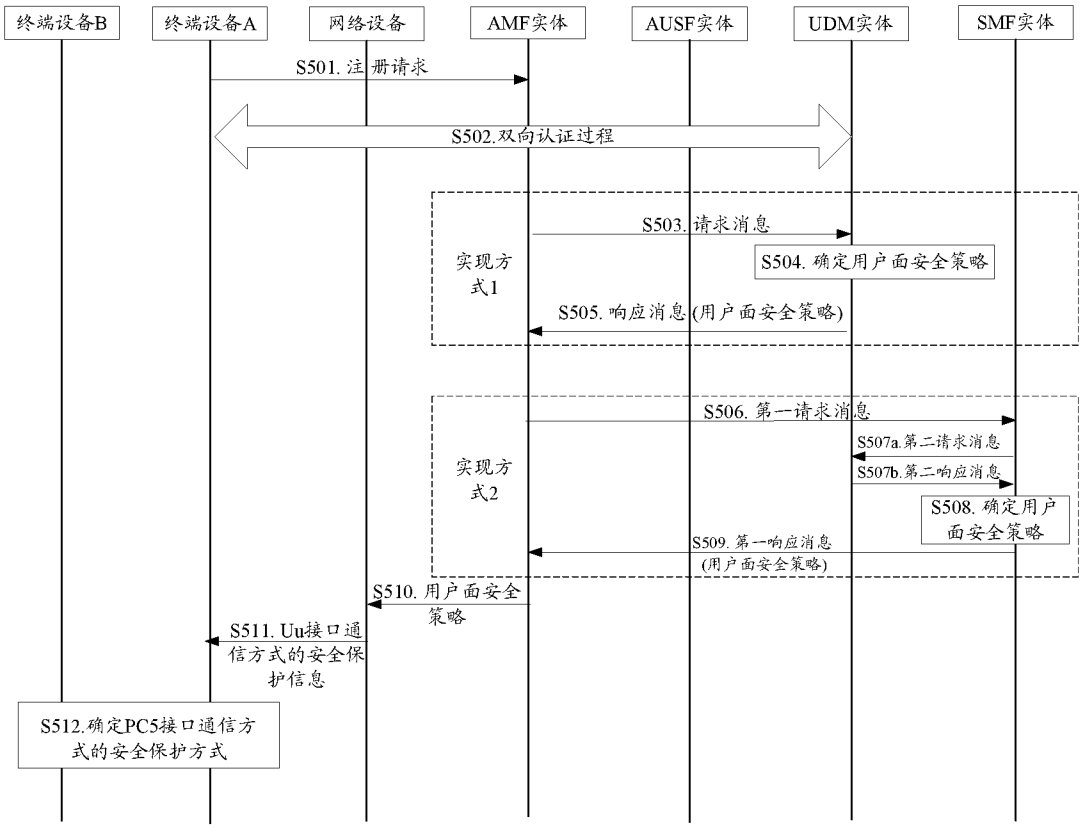
终端设备B
终端设备A
网络设备
AMF实体
AUSF实体
UDM实体
SMF实体
S501. 注册请求
S502.双向认证过程
实现方式1
S503. 请求消息
S504. 确定用户面安全策略
S505. 响应消息 (用户面安全策略)
实现方式2
S506. 第一请求消息
S507a.第二请求消息
S507b.第二响应消息
S508. 确定用户面安全策略
S509. 第一响应消息 (用户面安全策略)
S510. 用户面安全策略
S511. Uu接口通信方式的安全保护信息
S512.确定PC5接口通信方式的安全保护方式

图 5

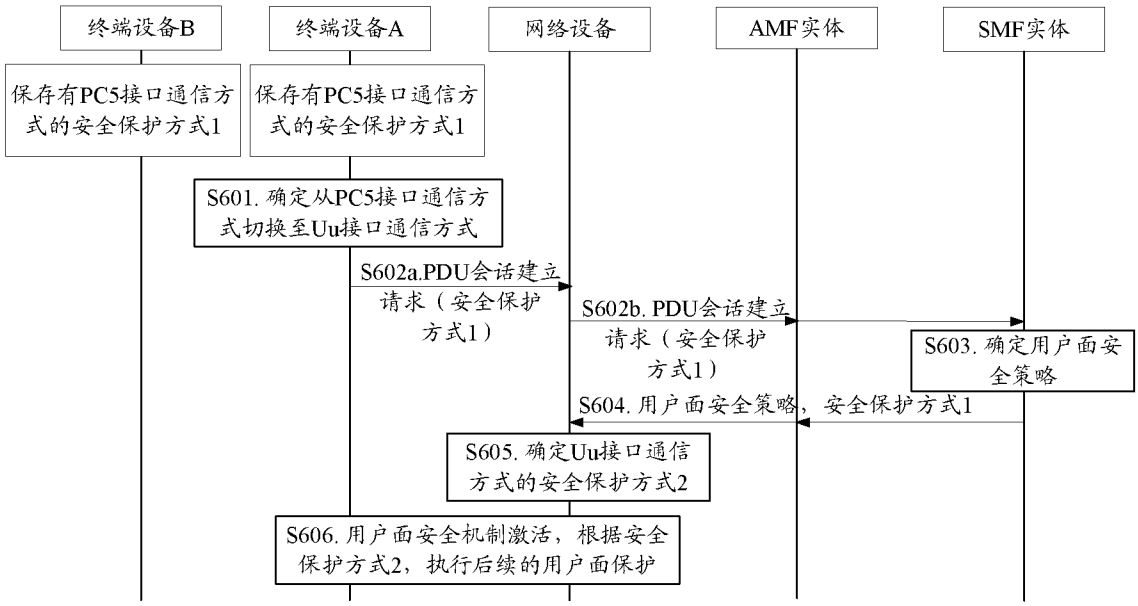
终端设备B
终端设备A
网络设备
AMF实体
SMF实体
保存有PC5接口通信方式的安全保护方式1
保存有PC5接口通信方式的安全保护方式1
S601. 确定从PC5接口通信方式切换至Uu接口通信方式
S602a.PDU会话建立请求（安全保护方式1）
S602b. PDU会话建立请求（安全保护方式1）
S603. 确定用户面安全策略
S604. 用户面安全策略，安全保护方式1
S605. 确定Uu接口通信方式的安全保护方式2
S606. 用户面安全机制激活，根据安全保护方式2，执行后续的用户面保护

图 6

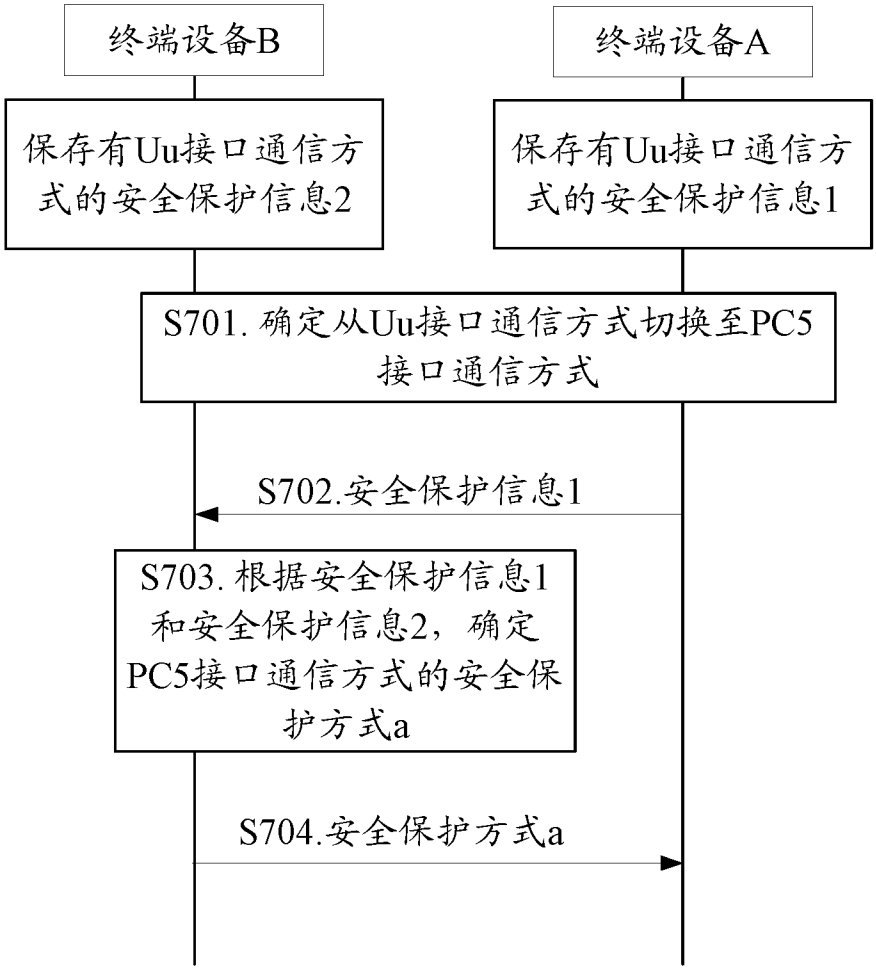
终端设备B
终端设备A
保存有Uu接口通信方式的安全保护信息2
保存有Uu接口通信方式的安全保护信息1
S701. 确定从Uu接口通信方式切换至PC5接口通信方式
S702.安全保护信息1
S703. 根据安全保护信息1和安全保护信息2，确定PC5接口通信方式的安全保护方式a
S704.安全保护方式a

图 7

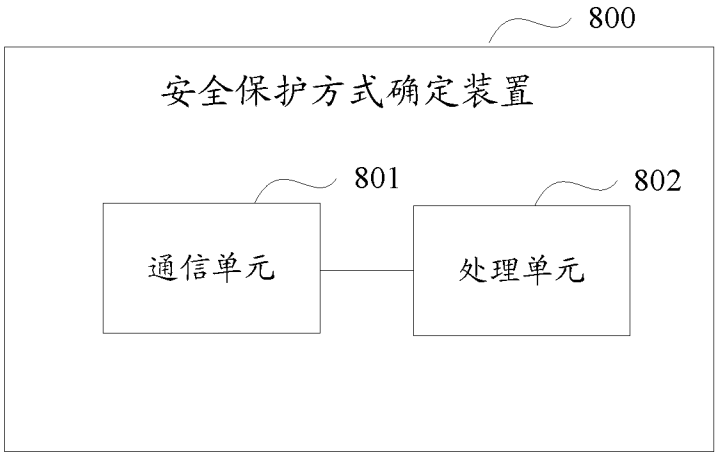
800
安全保护方式确定装置
801
802
通信单元
处理单元

图 8

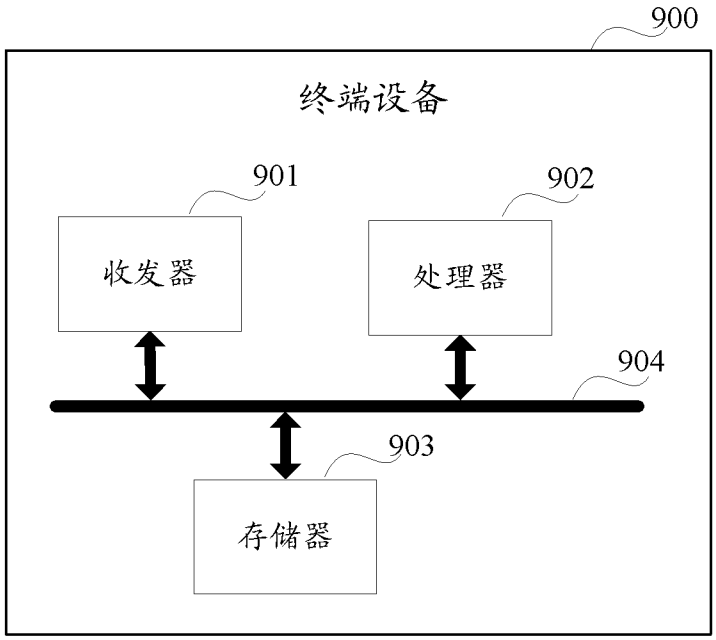
900
终端设备
901
902
收发器
处理器
904
903
存储器

图 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/100310

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/00(2009.01)i; 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)

H04W; H04L

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; VEN; EPTXT; USTXT; WOTXT; CNKI; 3GPP: 安全, 机密, 完整性, 加密, 保护, 设备到设备, 车到车, 上行链路, 直连链路, 旁路, 接口, 策略, 切换, security, integrity, encrypt, protection, D2D, V2V, Uu, PC5, SL, sidelink, interface, policy, handover, switch

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 104737570 A (NOKIA TECHNOLOGY CO., LTD.) 24 June 2015 (2015-06-24) description paragraphs [0078]-[0083], figure 3	1, 8, 9, 16
Y	CN 103297961 A (ALCATEL-LUCENT SHANGHAI BELL CO., LTD.) 11 September 2013 (2013-09-11) description, paragraphs [0038]-[0057]	1, 8, 9, 16
Y	CN 109729524 A (HUAWEI TECHNOLOGIES CO., LTD.) 07 May 2019 (2019-05-07) description, paragraphs [0115]-[0142]	1, 8, 9, 16
A	US 2019223008 A1 (QUALCOMM INCORPORATED) 18 July 2019 (2019-07-18) entire document	1-16
A	CATT. "“Uu and PC5 Availabity”" *3GPP TSG-RAN2 Meeting #106, R2-1905809,* 03 May 2019 (2019-05-03), the main body, pages 1-3	1-16
A	LG ELECTRONICS INC. "“Protection of PC5-RRC Messages”" *3GPP TSG-RAN WG2 #105bis, R2-1905052,* 29 March 2019 (2019-03-29), the main body, pages 1 and 2	1-16

☐ 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
17 August 2020	**27 September 2020**

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

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/100310

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104737570	A	24 June 2015	CN	104737570	B	31 August 2018
				US	2015281953	A1	01 October 2015
				EP	2910044	A1	26 August 2015
				WO	2014059657	A1	24 April 2014
				US	10341859	B2	02 July 2019
CN	103297961	A	11 September 2013	CN	103297961	B	09 March 2018
CN	109729524	A	07 May 2019	WO	2019085908	A1	09 May 2019
US	2019223008	A1	18 July 2019	WO	2019139689	A1	18 July 2019
				AU	2018400748	A1	09 July 2020

国际检索报告

国际申请号
PCT/CN2020/100310

A. 主题的分类

H04W 12/00(2009.01)i; 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)

H04W; H04L

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;VEN;EPTXT;USTXT;WOTXT;CNKI;3GPP：安全，机密，完整性，加密，保护，设备到设备，车到车，上行链路，直连链路，旁路，接口，策略，切换，security，integrity，encrypt，protection，D2D，V2V，Uu，PC5，SL，sidelink，interface，policy，handover，switch

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 104737570 A (诺基亚技术有限公司) 2015年 6月 24日 (2015-06-24) 说明书第[0078]-[0083]段，图3	1、8、9、16
Y	CN 103297961 A (上海贝尔股份有限公司) 2013年 9月 11日 (2013-09-11) 说明书第[0038]-[0057]段	1、8、9、16
Y	CN 109729524 A (华为技术有限公司) 2019年 5月 7日 (2019-05-07) 说明书第[0115]-[0142]段	1、8、9、16
A	US 2019223008 A1 (QUALCOMM INC) 2019年 7月 18日 (2019-07-18) 全文	1-16
A	CATT. "“Uu and PC5 Availabity”" 3GPP TSG-RAN2 Meeting #106, R2-1905809, 2019年 5月 3日 (2019-05-03), 正文第1-3页	1-16
A	LG ELECTRONICS INC. "“Protection of PC5-RRC Messages”" 3GPP TSG-RAN WG2 #105bis, R2-1905052, 2019年 3月 29日 (2019-03-29), 正文第1、2页	1-16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：
“A” 认为不特别相关的表示了现有技术一般状态的文件
“E” 在国际申请日的当天或之后公布的在先申请或专利
“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
“O” 涉及口头公开、使用、展览或其他方式公开的文件
“P” 公布日先于国际申请日但迟于所要求的优先权日的文件
“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 8月 17日	2020年 9月 27日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 贾斌 电话号码 (86-512) 88996134

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/100310

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	104737570	A	2015年 6月 24日	CN	104737570	B	2018年 8月 31日
				US	2015281953	A1	2015年 10月 1日
				EP	2910044	A1	2015年 8月 26日
				WO	2014059657	A1	2014年 4月 24日
				US	10341859	B2	2019年 7月 2日
CN	103297961	A	2013年 9月 11日	CN	103297961	B	2018年 3月 9日
CN	109729524	A	2019年 5月 7日	WO	2019085908	A1	2019年 5月 9日
US	2019223008	A1	2019年 7月 18日	WO	2019139689	A1	2019年 7月 18日
				AU	2018400748	A1	2020年 7月 9日