

确定用户面安全算法的方法、系统及装置

本申请要求于 2020 年 08 月 06 日提交中国专利局、申请号为 202010785355.1、申请名称为“确定用户面安全算法的方法、系统及装置”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，尤其涉及确定用户面安全算法的方法、系统及装置。

背景技术

终端设备的通信方式可包括 Uu 通信和 PC5 单播通信。Uu 通信，指的是终端设备与基站通过 Uu 接口进行通信的方式。在传统的蜂窝网络通信中，终端设备之间通常不能直接进行通信，终端设备之间发送的任何一条信令经过基站处理后再转发。经过基站处理，表示终端设备与基站通过 Uu 接口进行通信。但是在设备到设备（device-to-device，D2D）和车联网（vehicle-to-everything，V2X）的短距离直连通信需求下，D2D 技术提供了基于终端设备之间短距离直连通信的 PC5 接口。PC5 单播通信，指的是终端设备之间通过 PC5 接口直接进行通信的方式，数据和信令不再经过基站传输。这两种通信方式均涉及控制面安全保护和用户面安全保护。控制面安全保护，指的是控制面完整性保护是否开启以及控制面机密性保护是否开启；用户面安全保护，指的是用户面完整性保护是否开启以及用户面机密性保护是否开启。

目前在定义在 V2X 场景下使用 PC5 通信的 5G V2X 标准中，在控制面安全保护和用户面安全保护均开启的情况下，用户面使用的安全算法与控制面协商的安全算法一致。例如，在控制面完整性保护和控制面机密性保护均开启的情况下，两端终端设备通过协商，确定控制面使用非空值（non-null）的完整性保护算法和非空值的机密性保护算法，若用户面完整性保护和用户面机密性保护均开启，则用户面使用的安全算法与控制面协商的安全算法一致。在控制面完整性保护不开启的情况下，控制面机密性保护和用户面安全保护均不开启，但是在控制面完整性保护开启的情况下，控制面安全保护与用户面安全保护不存在耦合关系。例如在控制面完整性保护开启的情况下，控制面机密性保护可开启或不开启，用户面完整性保护可开启或不开启，用户面机密性保护可开启或不开启。该 PC5 单播连接使用的安全算法在协商控制面安全开启方式的时候协商，而用户面安全开启方式的协商在控制面安全开启方式协商之后执行，那么当控制面安全保护协商结果为控制面机密性保护不开启时，对应选择该 PC5 单播连接的机密性保护算法为空（null）值的算法，可能存在之后用户面安全保护协商结果为机密性保护开启后，两端 UE 无法使用有效的机密性保护算法对用户面数据进行机密性保护的情况。

因此，如何确定有效的用户面机密性保护算法是亟待解决的技术问题。

发明内容

本申请提供一种确定用户面安全算法的方法、系统及装置，可以确定出有效的用户面机密性保护算法，从而对用户面数据进行机密性保护。

本申请第一方面提供一种确定用户面安全算法的方法。该方法可以由第二设备执行，也可以由第二设备中的装置（例如处理器或芯片等）执行。该方法以第二设备为例，包括以下内容。

在第二设备与第一设备之间用户面机密性保护开启且与第一设备之间控制面机密性保护不开启的情况下，第二设备根据第一设备的安全能力和第二设备的安全能力，选择非空值的用户面机密性保护算法，并向第一设备发送第一消息，第一消息包括用于指示用户面机密性保护算法的第一算法指示信息。

本申请第一方面，在第二设备与第一设备之间用户面机密性保护开启且控制面机密性保护不开启的情况下，第二设备根据第一设备和第二设备的安全能力，选择非空值的用户面机密性保护算法，并通过第一算法指示信息告知第一设备，以便第一设备在用户面机密性保护开启的情况下，可以采用该非空值的用户面机密性保护算法对用户面数据进行机密性保护。

在一种可能的实现方式中，上述第一消息还包括用于指示开启第二设备与第一设备之间用户面机密性保护的指示信息，以便第一设备根据该指示信息开启与第二设备之间的用户面机密性保护。

在一种可能的实现方式中，第二设备接收来自第一设备的第二消息，第二消息包括第一设备的用户面安全策略，根据第一设备的用户面安全策略和第二设备自身的用户面安全策略，确定与第一设备之间用户面机密性保护开启。例如，第一设备的用户面安全策略为用户面机密性保护必须开启（required），第二设备的用户面安全策略为用户面机密性保护必须开启（required），则第二设备确定与第一设备之间用户面机密性保护开启；再例如第一设备的用户面安全策略为用户面机密性保护可选开启（preferred），第二设备的用户面安全策略为用户面机密性保护可选开启（preferred），第二设备可以根据预设的策略，例如自身的负荷情况，确定与第一设备之间用户面机密性保护开启。

在一种可能的实现方式中，在第二设备接收来自第一设备的第二消息之前，接收来自第一设备的第三消息，第三消息包括第一设备的控制面安全策略和第一设备的安全能力，第二设备根据第一设备控制面安全策略和第二设备自身的控制面安全策略，确定与第一设备之间控制面机密性保护不开启。例如，第一设备的控制面安全策略为控制面机密性保护必须不开启（not needed），和/或第二设备的用户面安全策略为控制面机密性保护必须不开启（not needed），则第二设备确定与第一设备之间控制面机密性保护不开启；再例如第一设备的用户面安全策略为用户面机密性保护可选开启（preferred），第二设备的用户面安全策略为用户面机密性保护可选开启（preferred），第二设备可以根据预设的策略，例如自身的负荷情况，确定与第一设备之间用户面机密性保护不开启。

在一种可能的实现方式中，第二设备还根据与第一设备之间的控制面机密性保护不开启，选择空值的控制面机密性保护算法，并向第一设备发送第四消息，第四消息包括用于指示空值的控制面机密性保护算法的指示信息，以便第一设备根据该指示信息不开启与第二设备之间的控制面机密性保护。

在一种可能的实现方式中，第二设备在接收到第三消息时，可保存第一设备的安全能力。第二设备在与第一设备之间控制面机密性保护不开启的情况下，保存第一设备的安全能力，以便在协商用户面机密性保护算法时，第一设备无需再次发送第一设备的安全能力，可以节省信令开销。

本申请第二方面提供一种确定用户面安全算法的方法。该方法可以由第一设备执行，也可以由第一设备中的装置（例如处理器或芯片等）执行。该方法以第一设备为例，包括以下内容。

第一设备向第二设备发送第三消息，第三消息包括第一设备的控制面安全策略和第一设备的安全能力；接收来自第二设备的第四消息，第四消息包括用于指示空值的控制面机密性

保护算法的指示信息；向第二设备发送第二消息，第二消息包括第一设备的用户面安全策略；接收来自第二设备的第一消息，第一消息包括用于指示非空值的用户面机密性保护算法的第一算法指示信息；根据第一算法指示信息指示的用户面机密性保护算法，对与第二设备之间的用户面数据进行机密性保护。

本申请第二方面，第一设备根据空值的控制面机密性保护算法，确定与第二设备之间控制面机密性保护不开启；根据第一算法指示信息指示的非空值的用户面机密性保护算法，获得有效的用户面机密性保护算法，从而可以对用户面数据进行机密性保护。

在一种可能的实现方式中，上述第一消息还包括用于指示开启第二设备与第一设备之间用户面机密性保护的指示信息，以便第一设备根据该指示信息开启与第二设备之间的用户面机密性保护。

在一种可能的实现方式中，上述第四消息还包括用于指示控制面完整性保护算法的指示信息，在第一设备根据第一算法指示信息指示的用户面机密性保护算法，对与第二设备之间的用户面数据进行机密性保护之前，根据控制面完整性保护算法的指示信息指示的控制面完整性保护算法，开启与第二设备之间的控制面完整性保护；对第一消息进行完整性验证；在对第一消息验证通过的情况下，第一设备根据第一算法指示信息指示的用户面机密性保护算法，开启与第二设备之间的用户面机密性保护。第一设备对第一消息进行完整性保护验证，可以减少第一消息被篡改的风险。

将第一方面和第二方面提供的方法应用于 PC5 单播通信时，上述第一消息可以是直连通信接受消息，上述第二消息可以是直连安全模式完成消息，上述第三消息可以是直连通信请求消息，上述第四消息可以是直连模式命令消息。

本申请第三方面提供一种确定用户面安全算法的方法，可以应用于 PC5 单播通信等通信场景。该方法可以由第二设备执行，也可以由第二设备中的装置（例如处理器或芯片等）执行。该方法以第二设备为例，包括以下内容。

第二设备在接收到来自第一设备的直连安全命令完成消息的情况下，确定与第一设备之间的用户面安全保护方式包括用户面机密性保护开启；第二设备根据该用户面安全保护方式、第一设备的安全能力和第二设备的安全能力，选择用户面安全算法，并向第一设备发送包括第一算法指示信息的直连通信接受消息，第一算法指示信息用于指示选择的用户面安全算法，该用户面安全算法包括非空值的用户面机密性保护算法。

本申请第一方面，第二设备在确定用户面安全保护方式包括用户面机密性保护开启的情况下，根据该用户面安全保护方式以及第一设备和第二设备的安全能力，选择非空值的用户面机密性保护算法，并通过第一算法指示信息告知第一设备，以便第一设备在用户面机密性保护开启的情况下，可以采用该非空值的用户面机密性保护算法对用户面数据进行机密性保护。

在一种可能的实现方式中，第二设备在用户面安全保护方式与控制面安全保护方式不一致的情况下，根据该用户面安全保护方式以及第一设备和第二设备的安全能力，选择用户面安全算法。这样在用户面安全保护方式与控制面安全保护方式不一致的情况下，第二设备也可以选择出用户面安全算法，以确定出有效的用户面安全算法，从而对用户面数据进行安全保护。

在一种可能的实现方式中，用户面安全保护方式与控制面安全保护方式不一致可以包括控制面完整性保护开启和控制面机密性保护不开启，而用户面安全保护方式包括用户面机密性保护开启。在控制面机密性保护不开启的情况下，也能选择出非空值的用户面机密性保护

算法，从而可以对用户面数据进行机密性保护。

在一种可能的实现方式中，第二设备在确定用户面安全保护方式的情况下，可以进一步根据该用户面安全保护方式，生成用户面安全开启指示信息。该用户面安全开启指示信息用于指示确定的用户面安全保护方式。

进一步的，上述直连通信接受消息还包括用户面安全开启指示信息，以便第一设备可以通过用户面安全开启指示信息获得用户面安全保护方式。

在一种可能的实现方式中，上述直连安全命令完成消息包括第一设备的用户面安全策略，第二设备根据第一设备的用户面安全策略和第二设备的用户面安全策略，确定与第一设备之间的用户面安全保护方式包括用户面机密性保护开启。

在一种可能的实现方式中，上述直连安全命令完成消息还包括第一设备的安全能力，以便第二设备选择用户面安全算法。上述直连安全命令完成消息也可不包括第一设备的安全能力，这样第二设备在需要选择用户面安全算法时，从其存储的信息中提取第一设备的安全能力，根据第一设备和第二设备的安全能力，以及用户面安全保护方式，选择用户面安全算法。

在一种可能的实现方式中，第二设备在控制面安全算法不支持用户面安全保护方式的情况下，根据该用户面安全保护方式以及第一设备和第二设备的安全能力，选择用户面安全算法。这样在控制面安全算法不支持用户面安全保护方式的情况下，第二设备也可以选择出用户面安全算法，以确定出有效的用户面安全算法，从而对用户面数据进行安全保护。

其中，控制面安全算法不支持用户面安全保护方式，例如控制面机密性保护算法为空值，而用户面机密性保护需要开启，那么控制面机密性保护算法不支持用户面机密性保护开启。

在一种可能的实现方式中，第二设备接收来自第一设备的直连安全命令完成消息之前，还协商控制面安全算法，可包括：

接收来自第一设备的直连通信请求消息，该直连通信请求消息包括第一设备的控制面安全策略和第一设备的安全能力；这样第二设备可以根据第一设备的控制面安全策略和第二设备的控制面安全策略，确定与第一设备之间的控制面安全保护方式；进而根据该控制面安全保护方式、第一设备的安全能力和第二设备的安全能力，选择控制面安全算法，并向所述第一设备发送包括第二算法指示信息的直连安全模式命令消息，第二算法指示信息用于指示选择的控制面安全算法。

其中，第二设备在接收到第一设备的安全能力的情况下，可对第一设备的安全能力进行存储，这样第一设备在发送直连安全命令完成消息时，无需在直连安全命令完成消息中携带第一设备的安全能力。

本申请第四方面提供一种确定用户面安全算法的方法，可以应用于 PC5 单播通信等通信场景。该方法可以由第一设备执行，也可以由第一设备中的装置（例如处理器或芯片等）执行。该方法以第一设备为例，包括以下内容。

第一设备接收来自第二设备的直连通信接受消息，该直连通信接受消息包括用户面安全开启指示信息和用于指示用户面安全算法的第一算法指示信息；第一设备根据用户面安全开启指示信息，确定与第二设备之间的用户面安全保护方式；根据用户面安全保护方式和第一算法指示信息指示的用户面安全算法，对与第二设备之间的用户面数据进行用户面安全保护。

本申请第四方面，用户面安全保护方式通过用户面安全开启指示信息进行指示，用户面安全算法通过第一算法指示信息进行指示，从而可以对用户面数据进行安全保护。

在一种可能的实现方式中，第一设备在确定用户面安全算法之前，与第二设备进行控制面协商，以确定控制面安全算法以及控制面安全保护方式。通过接收来自第二设备的直连安

全模式命令消息确定控制面安全算法，该直连安全模式命令消息包括用于指示控制面安全算法的第二算法指示信息。

在一种可能的实现方式中，在控制面完整性保护开启的情况下，第一设备对直连安全模式命令消息进行完整性保护验证，并在直连安全模式命令消息通过完整性保护验证的情况下，第一设备根据第二算法指示信息指示的控制面安全算法，确定与第二设备之间的控制面安全保护方式。

在一种可能的实现方式中，第一设备向第二设备发送直连安全命令完成消息，该直连安全命令完成消息包括第一设备的用户面安全策略，以便第二设备根据第一设备和第二设备的用户面安全策略，确定用户面安全保护方式。

在一种可能的实现方式中，上述直连安全命令完成消息还包括第一设备的安全能力，以便第二设备根据第一设备和第二设备的安全能力，选择控制面安全算法。第二设备可对第一设备的安全能力进行存储，这样第二设备在需要选择用户面安全算法时，可以直接获取第一设备的安全能力，无需第一设备再次发送第一设备的安全能力，节省信令开销。

本申请第五方面提供一种确定用户面安全算法的方法，可以应用于 PC5 单播通信和 Uu 通信等通信场景。该方法可以由第一设备执行，也可以由第一设备中的装置（例如处理器或芯片等）执行。该方法以第一设备为例，包括以下内容。

第一设备接收来自第二设备的直连通信接受消息，该直连通信接受消息包括用于指示用户面安全算法的第一算法指示信息；根据第一算法指示信息所指示的用户面安全算法，确定与第二设备之间的用户面安全保护方式；根据用户面安全保护方式和用户面安全算法，对与第二设备之间的用户面数据进行用户面安全保护。

本申请第五方面，第一算法指示信息既可以指示选择的用户面安全算法，还可以指示用户面安全保护方式，从而可以对用户面数据进行安全保护。

在一种可能的实现方式中，第一设备在确定用户面安全算法之前，与第二设备进行控制面协商，以确定控制面安全算法以及控制面安全保护方式。通过接收来自第二设备的直连安全模式命令消息确定控制面安全算法，该直连安全模式命令消息包括用于指示控制面安全算法的第二算法指示信息。

在一种可能的实现方式中，在控制面完整性保护开启的情况下，第一设备对直连安全模式命令消息进行完整性保护验证，并在直连安全模式命令消息通过完整性保护验证的情况下，第一设备根据第二算法指示信息指示的控制面安全算法，确定与第二设备之间的控制面安全保护方式。

在一种可能的实现方式中，第一设备向第二设备发送直连安全命令完成消息，该直连安全命令完成消息包括第一设备的用户面安全策略，以便第二设备根据第一设备和第二设备的用户面安全策略，确定用户面安全保护方式。

在一种可能的实现方式中，上述直连安全命令完成消息还包括第一设备的安全能力，以便第二设备根据第一设备和第二设备的安全能力，选择控制面安全算法。第二设备可对第一设备的安全能力进行存储，这样第二设备在需要选择用户面安全算法时，可以直接获取第一设备的安全能力，无需第一设备再次发送第一设备的安全能力，节省信令开销。

本申请第六方面提供一种通信装置，该通信装置可以是第二设备，也可以是第二设备中的装置。一种设计中，该装置可以包括执行第一或第三方面中，以及各种可能性实现方式所描述的方法/操作/步骤/动作所对应的模块，该模块可以是硬件电路，也可以是软件，也可以是硬件电路结合软件实现。一种设计中，该装置可以包括处理模块和收发模块。示例性的，

处理模块，用于在第二设备与第一设备之间用户面机密性保护开启且与第一设备之间控制面机密性保护不开启的情况下，根据第一设备的安全能力和第二设备的安全能力，选择非空值的用户面机密性保护算法；

收发模块，用于向第一设备发送第一消息，第一消息包括用于指示用户面机密性保护算法的第一算法指示信息。

本申请第七方面提供一种通信装置，该装置包括处理器，用于实现上述第一或第三方面描述的方法。该装置还可以包括存储器，用于存储指令和数据。该存储器与该处理器耦合，该处理器执行该存储器中存储的指令时，可以使该装置实现上述第一方面以及第一方面的各个可能实现方式，或第三方面以及第三方面的各个可能实现方式提供的方法。该装置还可以包括通信接口，该通信接口用于该装置与其它设备进行通信，示例性的，通信接口可以是收发器、总线等电路硬件模块，其它设备可以为第一设备等。在一种可能的设计中，该装置包括：

存储器，用于存储程序指令；

处理器，用于在第二设备与第一设备之间用户面机密性保护开启且与第一设备之间控制面机密性保护不开启的情况下，根据第一设备的安全能力和第二设备的安全能力，选择非空值的用户面机密性保护算法，并利用通信接口向第一设备发送第一消息，第一消息包括用于指示用户面机密性保护算法的第一算法指示信息。

本申请第八方面提供一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行第一方面以及第一方面的各个可能实现方式，或第三方面以及第三方面的各个可能实现方式提供的方法。

本申请第九方面提供一种芯片系统，该芯片系统包括处理器，还可以包括存储器，用于实现上述第一方面以及第一方面的各个可能实现方式，或第三方面以及第三方面的各个可能实现方式提供的方法。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。

本申请第十方面提供一种通信装置，该通信装置可以是第一设备，也可以是第一设备中的装置。一种设计中，该装置可以包括执行第二方面或第四方面或第五方面中，以及各种可能性实现方式所描述的方法/操作/步骤/动作所对应的模块，该模块可以是硬件电路，也可以是软件，也可以是硬件电路结合软件实现。一种设计中，该装置可以包括处理模块和收发模块。示例性的，

收发模块，用于向第二设备发送第三消息，第三消息包括第一设备的控制面安全策略和第一设备的安全能力；接收来自第二设备的第四消息，第四消息包括用于指示空值的控制面机密性保护算法的指示信息；向第二设备发送第二消息，第二消息包括第一设备的用户面安全策略；接收来自第二设备的第一消息，第一消息包括用于指示非空值的用户面机密性保护算法的第一算法指示信息；

处理模块，用于根据第一算法指示信息指示的用户面机密性保护算法，对与第二设备之间的用户面数据进行机密性保护。

本申请第十一方面提供一种通信装置，该装置包括处理器，用于实现上述第二方面或第三方面描述的方法。该装置还可以包括存储器，用于存储指令和数据。该存储器与该处理器耦合，该处理器执行该存储器中存储的指令时，可以使该装置实现上述第二方面以及第二方面的各个可能实现方式，或第四方面以及第四方面的各个可能实现方式，或第五方面以及第五方面的各个可能实现方式所描述的方法。该装置还可以包括通信接口，该通信接口用于该装置与其它设备进行通信，示例性的，通信接口可以是收发器、总线等电路硬件模块，其它

设备可以为第二设备等。在一种可能的设计中，该装置包括：

存储器，用于存储程序指令；

处理器，用于利用通信接口向第二设备发送第三消息，第三消息包括第一设备的控制面安全策略和第一设备的安全能力；接收来自第二设备的第四消息，第四消息包括用于指示空值的控制面机密性保护算法的指示信息；向第二设备发送第二消息，第二消息包括第一设备的用户面安全策略；接收来自第二设备的第一消息，第一消息包括用于指示非空值的用户面机密性保护算法的第一算法指示信息；根据第一算法指示信息指示的用户面机密性保护算法，对与第二设备之间的用户面数据进行机密性保护。

本申请第十二方面提供一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行第二方面以及第二方面的各个可能实现方式，或第四方面以及第四方面的各个可能实现方式，或第五方面以及第五方面的各个可能实现方式提供的方法。

本申请第十三方面提供一种芯片系统，该芯片系统包括处理器，还可以包括存储器，用于实现上述第二方面以及第二方面的各个可能实现方式，或第四方面以及第四方面的各个可能实现方式，或第五方面以及第五方面的各个可能实现方式提供的方法。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。

本申请第十四方面提供一种通信系统，该通信系统包括第一设备和第二设备；

第二设备，用于在第二设备与第一设备之间用户面机密性保护开启且与第一设备之间控制面机密性保护不开启的情况下，根据第一设备的安全能力和第二设备的安全能力，选择非空值的用户面机密性保护算法；向第一设备发送第一消息，第一消息包括用于指示用户面机密性保护算法的第一算法指示信息；

第一设备，用于接收第一消息。

可以理解的是，第十三方面提供的系统包括第一方面涉及的第一设备和第二方面涉及的第二设备。

附图说明

图 1 为 PC5 单播通信建立过程的流程示意图；

图 2 为 PC5 单播通信中的安全保护的一种示例图；

图 3 为应用本申请实施例的网络架构示意图；

图 4 为本申请实施例一提供的确定用户面安全算法的方法的流程示意图；

图 5 为本申请实施例二提供的确定用户面安全算法的方法的流程示意图；

图 6 为本申请实施例三提供的确定用户面安全算法的方法的流程示意图；

图 7 为本申请实施例提供的一种通信装置的结构示意图；

图 8 为本申请实施例提供的另一种通信装置的结构示意图。

具体实施方式

为了更好地理解本申请实施例提供的技术方案，首先对本申请实施例涉及的技术术语进行介绍。

1、安全策略

安全策略用于描述是否开启安全保护的策略，可分为三种，分别为开启（required）、不开启（not needed）和可选（preferred）。安全策略为 required，表示需要开启安全保护；安全

策略为 not needed, 表示不需要开启安全保护; 安全策略为 preferred, 表示可以开启安全保护也可以不开启安全保护。安全策略在被发送的时候, 一般情况下只会选择三种(required、not needed 和 preferred)中的一种发送, 在某些殊的场景下可能会选择至少 2 种发送, 并且其中一个 preferred。比如, 在发送 not needed 和 preferred 的时候, 代表倾向不开启安全保护; 发送 required 和 preferred, 则是倾向开启安全保护。

安全策略可包括控制面安全策略和用户面安全策略。控制面安全策略用于表示控制面机密性保护和/或控制面完整性保护是否开启的策略。用户面安全策略用于表示用户面机密性保护和/或用户面完整性保护是否开启的策略。其中, 控制面机密性保护的策略、控制面完整性保护的策略、用户面机密性保护的策略和/或用户面完整性保护的策略取值均可以包括开启(required)、不开启(not needed)和可选(preferred)。例如, 如果控制面机密性保护的策略为 not needed, 控制面完整性保护的策略为 required, 则表示控制面机密性保护不需要开启, 控制面完整性保护需要开启。

控制面机密性保护即保护信令在传输过程中的机密性, 控制面机密性保护也可以称为控制面加密保护, 机密性是指无法被直接看出真实内容。控制面完整性保护即保护信令在传输过程中的完整性, 完整性是指与原始的信令一致, 没有被修改。用户面机密性保护即保护用户面数据在传输过程中的机密性, 用户面机密性保护也可以称为用户面加密保护。用户面完整性保护即保护用户面数据在传输过程中的完整性, 完整性是指与原始的用户面数据一致, 没有被修改。

安全策略可用于确定安全保护方式, 例如 PC5 单播通信中, 发起端将其安全策略告知接收端, 接收端根据发起端的安全策略和接收端的安全策略, 可确定与发起端之间的安全保护方式。安全保护方式可包括控制面安全保护方式和用户面安全保护方式。控制面安全保护方式指的是控制面机密性保护是否开启, 和/或控制面完整性保护是否开启, 例如控制面安全保护方式为开启控制面机密性保护和开启控制面完整性保护; 用户面安全保护方式指的是用户面机密性保护是否开启, 和/或用户面完整性保护是否开启, 例如用户面安全保护方式为开启用户面机密性保护和不开启用户面完整性保护。

2、安全算法

安全算法包括: 至少一个机密性保护算法, 和至少一个完整性保护算法。机密性保护算法也可以称为加密算法。

安全算法可以进一步分为控制面安全算法和用户面安全算法。其中控制面安全算法用于保护信令, 包括控制面机密性保护算法和控制面完整性保护算法; 用户面使用的安全算法用于保护用户面数据, 可以包括用户面机密性保护算法和用户面完整性保护算法。

目前, 用户面安全算法与控制面安全算法相同, 但是在本申请实施例中, 用户面安全算法与控制面安全算法可能相同, 也可能不相同。

需要说明的是, 安全算法为空(null)值, 可以表示不开启安全保护。例如, 如果第一设备和第二设备之间协商后的控制面完整性保护算法为空值, 则可以表示第一设备和第二设备之间不开启控制面完整性保护。

3、安全保护和解安全保护

安全保护, 对于执行安全功能的节点而言, 控制面安全算法和控制面安全密钥一起用于保护控制面数据(即信令), 用户面安全算法和用户面安全密钥一起用于保护用户面数据。具体地, 安全保护包括:

(1) 用户面机密性保护: 使用用户面加密密钥和用户面机密性保护算法对用户面数据进行

行加密保护；

(2) 用户面完整性保护：使用用户面完整性保护密钥和用户面完整性保护算法对用户面数据进行完整性保护；

(3) 控制面机密性保护：使用控制面加密密钥和控制面机密性保护算法对控制面数据进行加密保护；

(4) 控制面完整性保护：使用控制面完整性保护密钥和控制面完整性保护算法对控制面数据进行完整性保护。

本申请实施例不限定加密保护和完整性保护的顺序关系，即可以先对用户面/控制面数据进行加密保护，再做完整性保护；也可以先对用户面/控制面进行完整性保护，再对用户面/控制面数据进行加密保护。当然，用户面和控制面可以不使用相同的执行顺序。

解安全保护，对于执行安全功能的节点而言，控制面安全算法和控制面安全密钥一起用于获得原始的控制面数据，用户面安全算法和用户面安全密钥一起用于获得原始的用户面数据。具体地，解安全保护包括：

(1) 用户面解密：使用用户面加密密钥和用户面机密性保护算法对加密的用户面数据进行解密；

(2) 用户面完整性验证：使用用户面完整性保护密钥和用户面完整性保护算法对用户面数据进行完整性保护验证；

(3) 控制面解密：使用控制面加密密钥和控制面机密性保护算法对加密的控制面数据进行解密；

(4) 控制面完整性验证：使用控制面完整性保护密钥和控制面完整性保护算法对控制面数据进行完整性保护验证。

本申请实施例不限定解密和验证完整性保护的顺序。但需要理解的是，如果是用户面/控制面数据先被加密保护，再被完整性保护，则解安全保护是先验证完整性保护、再对加密后的用户面数据进行解密；如果用户面/控制面数据先被完整性保护，再被加密，则解安全保护的顺序为先解密加密后的数据，再进行完整性保护验证。解安全保护与开启安全保护相对，即只有开启安全保护才需要解安全保护。

4、PC5 单播通信中的安全保护

在 PC5 单播通信中，发起端与接收端通过协商，确定 PC5 的安全是否开启，即确定两端之间的安全保护方式。发起端与接收端可通过控制面消息（或称为信令消息（signalling messages））进行协商，例如在 PC5 单播通信建立过程中通过控制面消息进行协商，可参见图 1 所示。图 1 中，发起端为用户设备（user equipment, UE）1，接收端为 UE 2。具体的：

步骤 101，UE 1 向 UE 2 发送直连通信请求（direct communication request, DCR）消息。相应的，UE 2 接收来自 UE 1 的直连通信请求消息。

其中，直连通信请求消息可包括 UE 1 的安全能力（UE 1 security capabilities），UE 1 的控制面安全策略（UE 1 signalling security policy）以及可选的包括 UE 1 生成的随机数 1（nonce_1）。UE 1 的安全能力可以包括 UE 1 支持的安全算法（适用于用户面和/或控制面），UE 1 支持的安全算法可以是 UE 1 在本次 PC5 单播连接中支持的安全算法，也可以是 UE 1 自身支持的安全算法，安全算法包括完整性保护算法和机密性保护算法。UE2 的安全能力的定义类似，后续不再赘述。UE 1 的控制面安全策略即 UE 1 希望在本次 PC5 单播连接中使用的控制面安全策略，包括控制面完整性保护策略和控制面机密性保护策略，例如 UE 1 希望在本次 PC5 单播连接中开启控制面机密性保护，则控制面完整性保护策略为开启（required）。

直连通信请求消息还可包括密钥建立所需信息 (Key_Est_Info)，密钥建立所需信息可以是一个信息容器 (container)，用于携带建立密钥所需的信息。UE 1 和 UE 2 通过交互密钥建立信息可建立 UE 1 与 UE 2 之间的共享密钥。

可选的，直连通信请求消息还可包括根密钥标识 (K_{NRP} ID)， K_{NRP} ID 用于标识根密钥 K_{NRP} ， K_{NRP} 可以是 UE 1 与 UE 2 执行步骤 101 之前互鉴权流程和密钥建立流程建立的共享密钥。若 UE 1 能够感知 UE 2 的身份且 UE 1 保存有与 UE 2 之间的部分上下文信息，则直连通信请求消息包括 K_{NRP} ID。UE 1 能够感知 UE 2 的身份，即能够确定出 UE 2 是哪个用户。UE 1 保存有与 UE 2 之间的部分上下文信息，即 UE 1 与 UE 2 之前进行过通信，UE 1 上保存有与 UE 2 之间的部分上下文信息，该部分上下文信息包括 UE 1 与 UE 2 之间的 K_{NRP} 以及 K_{NRP} ID。

可选的，步骤 101 也可作为 UE 1 向 UE 2 发送的直连密钥更新请求 (direct rekeying request) 消息，相应的，UE 2 接收来自 UE 1 的直连密钥更新请求。此时该消息不包含 UE 1 的控制面安全策略。

步骤 102，UE 2 确定与 UE 1 之间的控制面安全保护方式，即 UE 2 确定针对 UE 2 与 UE 1 之间的信令是否开启控制面完整性保护，以及是否开启控制面机密性保护，并选择安全算法。

UE 2 根据 UE 1 的控制面安全策略和 UE 2 的控制面安全策略，确定与 UE 1 之间的控制面安全保护方式。UE 2 与 UE 1 之间的控制面安全保护方式也可以描述为该 PC5 单播连接使用的控制面安全保护方式。

例如，UE 2 可以按照如下方法确定是否开启控制面完整性保护：

(1) UE 1 的控制面完整性保护策略为 required，UE 2 的控制面完整性保护策略为 preferred 或者 required，则 UE 2 确定开启与 UE 1 之间的控制面完整性保护；

(2) UE 1 的控制面完整性保护策略为 required 或者 preferred，UE 2 的控制面完整性保护策略为 required，则 UE 2 确定开启与 UE 1 之间的控制面完整性保护；

(3) UE 1 的控制面完整性保护策略为 preferred，UE 2 的控制面完整性保护策略为 preferred，则 UE 2 根据自身的策略确定是否开启与 UE 1 之间的控制面完整性保护；例如，可以默认的策略是可以开启与 UE 1 之间的控制面完整性保护，或者是根据 UE 2 的性能情况确定是否开启与 UE 1 之间的控制面完整性保护；具体策略的设置不做限定；

(4) 当 UE 1 的控制面完整性保护策略和 UE 2 的控制面完整性保护策略中任一个是 not needed，且另外一个不是 required 时，UE 2 确定不开启与 UE 1 之间的控制面完整性保护；

(5) 当 UE 1 的控制面完整性保护策略和 UE 2 的控制面完整性保护策略中任一个是 not needed，且另外一个不是 required 时，UE 2 和 UE 1 之间无法建立安全连接。

UE 2 确定是否开启控制面机密性保护的方法与上述确定是否开启控制面完整性保护的方法类似，不再赘述。进一步的，一种可能的实现方式中，如果 UE 2 确定不开启与 UE 1 之间的控制面完整性保护，则 UE 2 确定也不开启与 UE 1 之间的控制面机密性保护；如果 UE 2 确定开启与 UE 1 之间的控制面完整性保护，则 UE 2 确定是否开启与 UE 1 之间的控制面机密性保护的方法与上述确定是否开启控制面完整性保护的方法类似。

进一步的，UE 2 根据与 UE 1 之间确定的控制面安全保护方式，确定安全算法。

具体的，UE 2 可以根据自身的安全能力以及 UE 1 的安全能力，确定 UE 1 和 UE 2 都支持的一个机密性保护算法作为 UE 1 和 UE 2 之间的控制面机密性保护算法，确定 UE 1 和 UE 2 都支持的一个完整性保护算法作为 UE 1 和 UE 2 之间的控制面完整性保护算法。例如，

如果 UE 2 确定需要开启与 UE 1 之间的控制面机密性保护,则 UE 2 根据 UE1 和 UE2 的安全能力选择一个 UE1 和 UE2 都支持的非空 (non-null) 值的机密性保护算法作为 UE 1 和 UE 2 之间执行控制面机密性保护的机密性保护算法。如果 UE 2 确定需要不开启与 UE 1 之间的控制面机密性保护,则 UE 2 确定一个空 (null) 值的算法作为 UE 1 和 UE 2 之间的控制面机密性保护算法。再例如,如果 UE 2 确定需要开启与 UE 1 之间的控制面完整性保护,那么 UE 2 选择一个非空 (non-null) 值的完整性保护算法。如果 UE 2 确定需要不开启与 UE 1 之间的控制面完整性保护,则 UE 2 确定一个空 (null) 值的算法作为 UE 1 和 UE 2 之间的控制面完整性保护算法。

可选的,步骤 103, UE 1 与 UE 2 执行互鉴权流程和密钥建立流程。

在现有技术中,如果 UE 2 确定开启控制面完整性保护,且 UE 1 与 UE 2 之间无现有的共享密钥,则需要触发与 UE 1 之间的互鉴权流程和密钥建立流程。如果 UE 2 确定不开启控制面完整性保护,则不需要执行步骤 103。若直连通信请求消息包括 K_{NRP} ID,那么 UE 2 根据 K_{NRP} ID 确定与 UE 1 之间的共享密钥 K_{NRP} ,从而也可以不执行步骤 103。

步骤 104, UE 2 向 UE 1 发送直连安全模式命令 (direct security mode command) 消息。相应的,UE 1 接收来自 UE 2 的直连安全模式命令消息。如果在步骤 102 中 UE 2 确定控制面完整性保护开启,则 UE 2 对所述直连安全模式命令消息进行完整性保护。

其中,直连安全模式命令消息包括 UE 2 选择的安全算法 (chosen_algs)。选择的安全算法可包括步骤 102 中 UE 2 选择的安全算法。安全算法可以是如下三种中的一种:

(1) 在 UE 2 确定不开启控制面完整性保护的情况下,默认也不开启控制面机密性保护,那么安全算法包括空值的完整性保护算法和空值的机密性保护算法,可以指示 UE 2 与 UE 1 之间不开启控制面完整性保护和不开启控制面机密性保护;

(2) 在 UE 2 确定开启控制面完整性保护和开启控制面机密性保护的情况下,安全算法包括非空值的完整性保护算法和非空值的机密性保护算法,可以指示 UE 2 与 UE 1 之间开启控制面完整性保护和开启控制面机密性保护;

(3) 在 UE 2 确定开启控制面完整性保护和不开启控制面机密性保护的情况下,安全算法包括非空值的完整性保护算法和空值的机密性保护算法,可以指示 UE 2 与 UE 1 之间开启控制面完整性保护和不开启控制面机密性保护。

直连安全模式命令消息还包括 UE 1 的安全能力和 UE 1 的控制面安全策略。UE 1 的安全能力和 UE 1 的控制面安全策略为步骤 101 中 UE 2 从该消息中收到的 UE 1 的安全能力和 UE 1 的控制面安全策略,以防止降低质量攻击 (bidding down attack)。在 UE 2 确定开启控制面完整性保护的情况下,直连安全模式命令消息还包括 UE 2 生成的随机数 2 (nonce_2),由于 UE 2 开启控制面完整性保护,那么 UE 2 可对直连安全模式命令消息进行完整性保护。例如,UE 2 可使用根密钥 K_{NRP} 、随机数 1 和随机数 2 计算出会话密钥 $K_{NRP-sess}$,进一步根据会话密钥 $K_{NRP-sess}$ 推导生成完整性保护密钥 (NRPIK),并使用完整性保护密钥对直连安全模式命令消息进行完整性保护。

可选的,不管是否开启控制面机密性保护,都不对直连安全模式命令消息进行加密。

步骤 105, UE 1 确定与 UE 2 之间的控制面安全保护方式,即 UE 1 确定针对 UE 1 与 UE 2 之间的信令是否开启控制面完整性保护,以及是否开启控制面机密性保护。

UE 1 根据直连安全模式命令消息中所包括的选择的安全算法,确定与 UE 2 之间的控制面安全保护方式。即直连安全模式命令消息所包括的选择的安全算法既用于指示 UE 1 与 UE 2 之间使用的安全算法,又隐式的指示了是否开启相应的控制面安全保护。例如,机密性保

护算法为非空值，则 UE 1 确定开启控制面机密性保护，并使用直连安全模式命令消息中携带机密性保护算法对后续控制面消息进行机密性保护；完整性保护算法为非空值，则 UE 1 确定开启控制面完整性保护，并使用直连安全模式命令消息中携带的控制面完整性保护算法对后续控制面消息进行完整性保护。

在控制面完整性保护开启的情况下，UE 1 使用 K_{NRP} 、随机数 1 和随机数 2 计算出会话密钥 K_{NRP-ss} ，并进一步使用 K_{NRP-ss} 计算得到该 PC5 单播连接中使用的完整性保护密钥（NRPIK）。若还开启了控制面机密性保护，那么 UE 1 进一步使用 K_{NRP-ss} 计算得到该 PC5 单播连接中使用的加密密钥（NRPEK）。

在控制面完整性保护开启的情况下，UE 1 执行以下三种验证过程：

A、UE 1 验证直连安全模式命令消息中的 UE 1 的安全能力是否与其发给 UE 2 的安全能力相同；

B、UE 1 验证直连安全模式命令消息中的 UE 1 的安全策略是否与其发给 UE 2 的安全策略相同；

C、如果开启完整性保护，则对直连安全模式命令消息进行完整性保护验证，如果没有开启完整性保护，则不需要验证完整性。

上述三种验证都通过的情况下，UE 1 激活其与 UE 2 之间的控制面安全，并将 UE 1 的用户面安全策略携带在直连安全模式完成消息中。若上述三种验证中任何一个验证不通过，则 UE 1 释放与 UE 2 之间的连接，并向 UE 2 发送连接建立拒绝消息，连接建立拒绝消息也携带拒绝原因值。需要说明的是，本申请不限定上述三种验证执行的先后顺序。

在控制面完整性保护不开启的情况下，UE 1 执行上述验证过程 A 和 B，若这两种验证过程都通过，那么 UE 1 将其用户面安全策略携带在直连安全模式完成消息中。

步骤 106，UE 1 向 UE 2 发送直连安全模式完成（direct security mode complete）消息。相应的，UE 2 接收来自 UE 1 的直连安全模式完成消息。

其中，直连安全模式完成消息携带 UE 1 的用户面安全策略，用于与 UE 2 协商以确定用户面安全保护方式。

可选的，在 UE 1 与 UE 2 之间的控制面完整性保护开启的情况下，UE 1 对直连安全模式完成消息进行完整性保护。如果 UE 1 和 UE 2 之间还开启了控制面机密性保护，则 UE 1 对直连安全模式完成消息进行机密性保护。

步骤 107，UE 2 确定与 UE 1 之间的用户面安全保护方式，即 UE 2 确定针对 UE 2 与 UE 1 之间的用户面数据是否开启用户面完整性保护，以及是否开启用户面机密性保护。

UE 2 在接收到直连安全模式完成消息时，可根据 UE 1 的用户面安全策略和 UE 2 的用户面安全策略确定与 UE 1 之间的用户面安全保护方式。UE 2 确定用户面安全保护方式的过程与 UE 2 确定控制面安全保护方式的过程类似，在此不再赘述。

步骤 108，UE 2 向 UE 1 发送直连通信接受（direct communication accept）消息。相应的，UE 1 接收来自 UE 2 的直连通信接受消息。

其中，直连通信接受消息可包括用户面安全配置（user plane security configuration），用户面安全配置用于指示用户面完整性保护是否开启以及用户面机密性保护是否开启。用户面安全配置可以理解作为一种指示信息，该指示信息用于指示用户面完整性保护是否开启以及用户面机密性保护是否开启。

UE 1 在接收到直连通信接受消息的情况下，根据用户面安全配置开启相应的安全保护。

在控制面完整性保护和用户面完整性保护均开启的情况下，控制面和用户面使用相同的

非空值的完整性保护算法；在控制面机密性保护和用户面机密性保护均开启的情况下，控制面和用户面使用相同的非空值的机密性保护算法。

在控制面完整保护不开启的情况下，默认控制面机密性保护不开启，用户面完整性保护和用户面机密性保护均不开启，即完整性保护算法为空值，机密性保护算法为空值。但是，在控制面完整保护开启的情况下，控制面机密性保护可开启或不开启，用户面完整性保护可开启或不开启，用户面加密可开启或不开启，后三者的开启与否相互独立。由于 PC5 单播连接使用的安全算法在协商控制面安全开启方式的时候协商，而用户面安全开启方式的协商在控制面安全开启方式协商之后执行，那么当控制面安全保护协商结果为控制面机密性保护不开启时，对应选择该 PC5 单播连接的机密性保护算法为空值的算法，可能存在之后用户面安全保护协商结果为机密性保护开启后，两端 UE 无法使用有效的机密性保护算法对用户面数据进行机密性保护的情况。

示例性的，可参见图 2 所示，图 2 与图 1 相同的部分可参见图 1 的描述。图 2 中，UE 2 在步骤 102a 中确定控制面完整性保护开启和控制面机密性保护不开启，那么步骤 104a 的直连安全模式命令消息携带的安全算法包括非空值的完整性保护算法和空值的机密性保护算法，以指示 UE 1 开启控制面完整性保护和不开启控制面机密性保护。但是 UE 2 在步骤 107a 确定用户面机密性保护开启，直连通信接受消息中的用户面安全配置指示开启用户面机密性保护，而 UE 1 从步骤 104a 的安全算法中获取到空值的机密性保护算法，空值的机密性保护算法无法对用户面数据进行有效的机密性保护。

可选的，步骤 108 也可作为 UE 2 向 UE 1 发送的直连密钥更新回复 (direct rekeying Response) 消息，相应的，UE 1 接收来自 UE 2 的直连密钥更新请求。

可选的，步骤 108 也可作为 UE 2 向 UE 1 发送的 RRC 连接重配置 (RRC connection reconfiguration) 消息，相应的，UE 1 接收来自 UE 2 的 RRC 连接重配置消息。

5、Uu 通信中的安全保护

基站与终端设备之间通信的 Uu 接口的安全保护方式为先开启无线资源控制 (radio resource control, RRC) 层安全保护，再开启用户面安全保护。其中 RRC 层安全保护可以理解为控制面安全保护。RRC 层安全保护方式为强制开启完整性保护和可选的开启机密性保护，基站在发送给终端设备的接入层 (access stratum, AS) 安全模式命令 (security mode command, SMC) 消息中携带安全算法，安全算法包括完整性保护算法和机密性保护算法。基站在确定用户面安全保护方式的情况下，通过 RRC 连接重配置 (RRC connection reconfiguration) 消息携带的安全开启指示信息，指示终端设备是否开启用户面完整性保护以及是否开启用户面机密性保护。如果开启用户面完整性保护，终端设备可使用 AS SMC 消息携带的完整性保护算法对用户面数据进行完整性保护；如果开启用户面机密性保护，终端设备可使用 AS SMC 消息携带的机密性保护算法对用户面数据进行机密性保护。

Uu 通信中，也可能会存在用户面机密性保护开启，但无法使用有效的机密性保护算法对用户面数据进行机密性保护的情况。

PC5 通信中的安全保护与 Uu 通信中的安全保护，可参见下表 1 所示。

	PC5 通信	Uu 通信
控制面安全保护方式	由选择的安全算法指示，空值算法表示不开启，非空值算法表示开启	强制开启控制面完整性保护，可选开启控制面机密性保护 (或预配置控制面安全保护方式)

控制面安全算法	根据选择的安全算法中的完整性保护算法的标识以及机密性保护算法的标识确定	根据安全算法中的完整性保护算法的标识以及机密性保护算法的标识确定
触发激活控制面安全保护的消息	直连安全模式命令消息	接入层安全模式命令消息
用户面安全保护方式	由用户面安全配置指示	由安全开启指示信息指示
用户面安全算法	遵循控制面协商的安全算法	遵循控制面协商的接入层安全算法
触发激活用户面安全保护的消息	直连通信接受消息	RRC 连接重配置消息

表 1

由表 1 可知，PC5 通信和 Uu 通信的安全保护中，均存在如下问题：在控制面完整性保护开启，控制面机密性保护不开启的情况下，在需要开启用户面机密性保护时，无法使用有效的机密性保护算法对用户面数据进行机密性保护。

鉴于此，本申请实施例提供一种确定用户面安全算法的方法、系统及装置，可以确定出有效的用户面安全算法，从而对用户面数据进行安全保护。进一步的，可以确定出有效的用户面机密性保护算法，从而对用户面数据进行机密性保护。

在本申请实施例中的附图中，各个实施例所示的步骤，以及步骤之间的先后顺序用于举例，并不构成对本申请实施例的限定。应理解，执行图示中的部分步骤或调整步骤的顺序进行具体实施，均落在本申请的保护范围内。

本申请实施例描述的技术可用于各种通信系统，例如第四代（4th generation，4G）通信系统，4.5G 通信系统，5G 通信系统，多种通信系统融合的系统，或者未来演进的通信系统。

本申请实施例涉及的设备可以是终端设备（也可称为终端），终端设备可以是一种具有无线收发功能的设备，可以部署在陆地上，包括室内或室外、手持或车载；也可以部署在水面上（如轮船等）；还可以部署在空中（例如飞机、气球和人造卫星上等）。终端设备可以是 UE，UE 包括具有无线通信功能的手持式设备、车载设备、穿戴式设备或计算设备。示例性地，UE 可以是手机（mobile phone）、平板电脑或带无线收发功能的电脑。终端设备还可以是虚拟现实（virtual reality，VR）终端设备、增强现实（augmented reality，AR）终端设备、智能汽车（smart vehicle）终端设备、工业控制中的无线终端、无人驾驶中的无线终端、无人机、无人机控制器、远程医疗中的无线终端、智能电网中的无线终端、智慧城市（smart city）中的无线终端、智慧家庭（smart home）中的无线终端、等等。本申请实施例中，用于实现终端设备的功能的装置可以是终端设备；也可以是能够支持终端设备实现该功能的装置，例如芯片系统，该装置可以被安装在终端设备中或者和终端设备匹配使用，例如处理器。

本申请实施例涉及的设备也可以是接入网设备，可以包括基站（base station，BS），可以是一种部署在无线接入网络中能够和终端设备进行无线通信的设备。其中，基站可能有多种形式，比如宏基站、微基站、中继站和接入点等。示例性地，本申请实施例涉及到的接入网设备可以是 5G 中的基站或长期演进（long term evolution，LTE）中的基站，其中，5G 中的基站还可以称为发送接收点（transmission reception point，TRP）或下一代基站节点（next generation Node B，gNB）。本申请实施例中，用于实现接入网设备的功能的装置可以是接入网设备；也可以是能够支持接入网设备实现该功能的装置，例如芯片系统，该装置可以被安装在接入网设备中或者和接入网设备匹配使用，例如处理器。本申请实施例中，芯片系统可

可以由芯片构成，也可以包括芯片和其他分立器件。

本申请实施例涉及的设备也可以是核心网设备，可以包括用于移动性管理和接入管理的接入和移动管理网元（access and mobile management function, AMF）、用于会话管理等的会话管理网元（session management function, SMF）和用于终端设备中用户数据的转发和接收的用户面网元（user plane function, UPF）。

在本申请实施例提供的技术方案中，以用于实现终端设备的功能的装置是终端设备为例，描述本申请实施例提供的技术方案。在本申请中，终端设备可以是 D2D 通信系统中的终端设备，也可以是 V2X 通信系统中的终端设备、车到车（vehicle to vehicle, V2V）通信系统中的车载终端等、无人机系统（unmanned aerial system, UAS）中的无人机和无人机控制器等，还可以是其他短距离直连通信系统中的终端设备。

请参见图 3，为应用本申请实施例的网络架构示意图。图 3 包括第一设备 301 和第二设备 302。

设备可以是终端设备，也可以是接入网设备，也可以是核心网设备。接入网设备例如可以是各种通信系统中的基站，核心网设备例如可以是用户面功能（user plane function, UPF），接入和移动性管理（access and mobility management function, AMF），或多接入边缘计算（multi-access edge computing, MEC）设备等。第一设备 301 与第二设备 302 可以是同类型的设备，例如均为 UE，也可以是不同类型的设备，例如第一设备 301 为终端设备，第二设备 302 为接入网设备或 AMF 网元。

应用在本申请中，第一设备 301 与第二设备 302 之间协商用户面安全算法可包括以下三种方式，这三种方式以第一设备 301 向第二设备 302 发起 PC5 单播连接为例。

方式一，第一设备 301 与第二设备 302 在控制面协商，由第二设备 302 确定出控制面安全保护方式、控制面安全算法和第二算法指示信息。第二算法指示信息包括控制面安全算法，第二算法指示信息既可用于指示控制面安全保护方式，又可以用于指示控制面安全算法。需要说明的是，第二算法指示信息指示的算法也可用作用户面安全保护算法。第一设备 301 与第二设备 302 在控制面协商，该协商在确定出控制面安全保护方式和控制面安全算法之后，由第二设备 302 确定用户面安全保护方式，生成用户面安全开启指示信息。

第二设备 302 确定第二算法指示信息中指示的安全算法不支持用户面安全保护方式，例如在控制面协商时第二设备 302 确定机密性保护不开启，第二算法指示信息中包括空值的机密性保护算法，而在用户面协商时第二设备 302 确定用户面机密性保护开启，此时第二算法指示信息中空值的机密性保护算法不支持用户面机密性保护开启；或者第二设备 302 确定出用户面安全保护方式与控制面安全保护方式不一致，例如控制面完整性保护开启和机密性保护不开启，用户面机密性保护开启；那么第二设备 302 根据用户面安全保护方式以及第一设备 301 和第二设备 302 的安全能力，选择用户面安全算法，并通过第一算法指示信息对用户面安全算法进行指示。例如第二设备 302 确定控制面完整性保护开启、控制面机密性保护不开启和用户面机密性保护开启，第一算法指示信息包括非空值的机密性保护算法标识，用于指示用户面机密性保护算法。

方式一中，第二算法指示信息既可用于指示控制面安全保护方式，又可以用于指示控制面安全算法；用户面安全开启指示信息用于指示用户面安全保护方式，第一算法指示信息用于指示用户面安全算法。该方案由于额外发送用于指示用户面安全保护的第一算法指示信息，保证了两端设备可以获取支持用户面安全保护开启的安全保护算法。方式一中，可选的，第二设备 302 无论用户面和控制面安全保护方式是否不一致，或无论控制面安全算法是否支持

用户面安全保护方式，均根据用户面安全保护方式以及第一设备 301 和第二设备 302 的安全能力，选择用户面安全算法，并通过第一算法指示信息对用户面安全算法进行指示，以简化设备的处理逻辑从而提高处理效率。

方式二，第一设备 301 与第二设备 302 在控制面协商，由第二设备 302 确定出控制面安全保护方式、控制面安全算法和第二算法指示信息。第二算法指示信息包括控制面安全算法，第二算法指示信息既可用于指示控制面安全保护方式，又可以用于指示控制面安全算法。需要说明的是，第二算法指示信息指示的算法也可作用用户面安全保护算法。第一设备 301 与第二设备 302 在控制面协商，该协商在确定出控制面安全保护方式和控制面安全算法之后，由第二设备 302 确定用户面安全保护方式。

第二设备 302 确定第二算法指示信息中指示的安全算法不支持用户面安全保护方式，例如控制面机密性保护算法为空值，用户面机密性保护开启，空值的机密性保护算法不支持用户面机密性保护开启；或第二设备 302 确定出用户面安全保护方式与控制面安全保护方式不一致，例如控制面完整性保护开启和机密性保护不开启，用户面机密性保护开启；那么第二设备 302 根据用户面安全保护方式以及第一设备 301 和第二设备 302 的安全能力，选择用户面安全算法，并通过第一算法指示信息对用户面安全算法进行指示。第一算法指示信息还可以指示用户面安全保护方式。例如第二设备 302 确定控制面完整性保护开启、机密性保护不开启和用户面机密性保护开启，第一算法指示信息包括空值的完整性保护算法标识和非空值的机密性保护算法标识，用于指示用户面完整性保护算法和用户面完整性保护不开启，以及指示用户面机密性保护算法和用户面机密性保护开启。

方式二中，第二算法指示信息既可用于指示控制面安全保护方式，又可以用于指示控制面安全算法；第一算法指示信息既可用于指示用户面安全保护方式，又可以用于指示用户面安全算法。该方案由于额外发送用于指示用户面安全保护的第一算法指示信息，保证了两端设备可以获取支持用户面安全保护开启的安全保护算法，同时使用第一算法指示信息指示用户面安全开启方式，减小了消息长度。

方式二中，可选的，第二设备 302 无论用户面和控制面安全保护方式是否不一致，或无论控制面安全算法是否支持用户面安全保护方式，均根据用户面安全保护方式以及第一设备 301 和第二设备 302 的安全能力，选择用户面安全算法，并通过第一算法指示信息对用户面安全算法和用户面安全开启方式进行指示，以简化设备的处理逻辑从而提高处理效率。

方式三，第一设备 301 与第二设备 302 在控制面协商，由第二设备 302 确定出控制面安全保护方式，并基于安全保护开启，根据第一设备 301 与第二设备 302 的安全能力选择安全算法，选择的安全算法通过第三算法指示信息进行指示。第三算法指示信息指示非空值的完整性保护算法和非空值的机密性保护算法。控制面安全保护方式通过控制面安全开启指示信息进行指示，第一设备 301 根据控制面安全保护方式和第三算法指示信息，确定控制面安全保护算法。用户面安全保护方式通过用户面安全开启指示信息进行指示，第一设备 301 根据用户面安全保护方式和第三算法指示信息，确定用户面安全保护算法，具体的，如果安全保护开启则使用第三算法指示信息中指示的非空安全保护算法进行安全保护，如果安全保护不开启则默认使用空值的安全保护算法，或不执行任何算法以节省计算资源。

方式三中，控制面安全开启指示信息用于指示控制面安全保护方式，用户面安全开启指示信息用于指示用户面安全保护方式，第三算法指示信息用于指示非空值的完整性保护算法和非空值的机密性保护算法，其中，第三算法指示信息中指示的非空完整性保护算法用于在完整性保护开启情况下使用，第三算法指示信息中的非空机密性保护算法用于在机密性保护

开启情况下使用。如果安全保护不开启则默认使用空值的安全保护算法，或不执行任何算法以节省计算资源。该方案在第三算法指示信息中指示非空值的机密性保护算法和非空值的完整性保护算法，保证了两端设备可以获取支持用户面安全保护开启的安全保护算法，同时在用户面安全协商中只使用安全开启指示信息指示用户面安全开启方式，减小了消息长度。

采用上述三种方式中的任意一种，可以在控制面完整性保护开启和机密性保护不开启，且用户面机密性保护开启的情况下，确定出有效的机密性保护算法，从而对用户面数据进行机密性保护。

下面将对本申请实施例提供的确定用户面安全算法的方法进行具体阐述，第一设备以 UE 1 为例，第二设备以 UE 2 为例。需要说明的是，本申请下述实施例中各个网元之间的消息名字或消息中各参数的名字等只是一个示例，具体实现中也可以是其他的名字，本申请实施例对此不作具体限定。

请参见图 4，为本申请实施例一提供的确定用户面安全算法的方法的流程示意图，该流程可包括但不限于如下步骤：

步骤 401，UE 1 向 UE 2 发送直连通信请求消息。相应的，UE 2 接收来自 UE 1 的直连通信请求消息。

可选的，步骤 401 也可作为 UE 1 向 UE 2 发送的直连密钥更新请求 (direct rekeying request) 消息，相应的，UE 2 接收来自 UE 1 的直连密钥更新请求。此时该消息不包含 UE 1 的控制面安全策略。

UE 1 在决定与 UE 2 建立 PC5 单播通信时，向 UE 2 发送直连通信请求消息。

其中，直连通信请求消息可包括 UE 1 的控制面安全策略，用于与 UE 2 协商，以确定是否开启控制面完整性保护以及是否开启控制面机密性保护。UE 1 的安全策略可以是核心网设备为其配置的，并告知 UE 1，例如 5G 核心网中的策略控制功能 (policy control function, PCF) 网元为 UE 1 配置安全策略，并告知 UE；也可以是应用功能 (application function, AF) 网元为其配置的，并告知 UE 1；还可以是 AF 网元为其配置的，通过 PCF 网元告知 UE 1；还可以是由核心网设备从统一存储功能 (unified data management, UDM) 网元中获取并发送给 UE；还可以是由网络运营商预配置在 UE 上。本申请对于 UE 如何获得各自的控制面安全策略不做限定。

直连通信请求消息还可包括 UE 1 的安全能力，UE 1 的安全能力可包括 UE 1 在该 PC5 单播连接中支持的安全算法列表。安全算法列表包括完整性保护算法列表和机密性保护算法列表。完整性保护算法列表包括一个或多个非空值和/或空值的完整性保护算法，机密性保护算法列表包括一个或多个非空值和/或空值的机密性保护算法。

可选的，直连通信请求消息还可以包括 UE 1 生成的随机数 1，随机数 1 可用于生成会话密钥 $K_{NRP- sess}$ 。

步骤 402，UE 2 确定与 UE 1 之间的控制面安全保护方式，并选择安全算法。

UE 2 根据 UE 1 的控制面安全策略和 UE 2 的控制面安全策略，确定与 UE 1 之间的控制面安全保护方式，即确定针对该 PC5 单播连接的控制面安全保护方式。UE 2 确定是否开启控制面完整性保护，以及是否开启控制面机密性保护的过程可参考图 1 中相关步骤的具体描述，在此不再赘述。本申请中，不开启控制面完整性保护时，默认也不开启控制面机密性保护，也不开启用户面安全保护。

为了解决控制面机密性保护不开启，而用户面机密性保护开启的情况下，无法使用有效的机密性保护算法进行用户面机密性保护的问题，本申请中，UE 2 确定的控制面安全保护方

式为开启控制面完整性保护和不开启控制面机密性保护。

进一步的，UE 2 根据确定的控制面安全保护方式，UE 1 的安全能力以及 UE 2 的安全能力，选择安全算法。UE 2 选择安全算法的过程可参考图 1 中相关步骤的具体描述，在此不再赘述。例如，控制面安全保护方式为开启控制面完整性保护和不开启控制面机密性保护，那么 UE 2 根据两端 UE 的安全能力，选择一个非空值的完整性保护算法和一个空值的机密性保护算法。

可选的，UE 2 存储 UE 1 的安全能力。如果 UE 2 确定开启控制面完整性保护而不开启控制面机密性保护，那么 UE 2 存储 UE 1 的安全能力，以便 UE 2 在确定开启用户面机密性保护时，可以根据存储的 UE 1 的安全能力选择非空值的机密性保护算法。如果 UE 2 确定开启控制面机密性保护，那么 UE 2 可以存储 UE 1 的安全能力，也可以不存储 UE 1 的安全能力。如果 UE 2 存储了 UE 1 的安全能力，可以保证在用户面和控制面安全均开启且可使用不同的安全保护算法时，UE 2 还可以根据提前存储的 UE 1 的安全能力选择使用的安全保护算法，防止再次在信令消息中发送 UE 1 的安全能力，如果 UE 2 步存储 UE 1 的安全能力，可以减小 UE 2 的存储负担。

可选的，UE 2 在确定控制面完整性开启的情况下，强制开启控制面机密性保护；或在确定控制面机密性保护开启的情况下，强制开启控制面完整性保护；并根据 UE 1 的安全能力以及 UE 2 的安全能力选择安全算法选择非空值的完整性保护算法和非空值的机密性保护算法。例如 UE 2 决策开启控制面完整性保护，则 UE 2 强制开启控制面机密性保护并选择非空值的完整性保护算法和非空值的机密性保护算法。该方案使 UE 1 和 UE 2 均在控制面协商阶段选择了非空值的安全保护算法，保证了两端设备可以获取支持用户面安全保护开启的安全保护算法。

可选的，UE 2 在确定控制面完整保护开启且控制面机密性保护不开启并根据 UE 1 的安全能力以及 UE 2 的安全能力选择空值的机密性保护算法时，额外根据 UE 1 的安全能力以及 UE 2 的安全能力选择额外的非空值的机密性保护算法。保证了两端设备可以获取支持用户面安全保护开启的安全保护算法。

可选的，步骤 403，UE 1 和 UE 2 获取共享密钥。共享密钥即 K_{NRP} 。

其中，共享密钥是指 UE 1 和 UE 2 都知晓并使用的密钥。例如，可以与现有技术中 UE 2 确定需要开启与 UE 1 之间的控制面完整性保护的情况下，执行互鉴权，进而建立密钥的方法相同，即参考上述图 1 实施例的步骤 103。UE 2 可触发步骤 403。

若直连通信请求消息包括 K_{NRP} ID，那么 UE 2 根据 K_{NRP} ID 确定与 UE 1 之间的共享密钥 K_{NRP} ，从而也可以不执行步骤 403。

不管是否开启控制面完整性保护，UE 2 都可以执行步骤 403。例如，运营商可以选择每次都执行步骤 403。再例如，UE 1 与 UE 2 后续流程中，消息没有完整性保护的情况下，都需要获取共享密钥以便于对这个没有完整性保护的消息进行安全保护。

本申请中，不限定 UE 1 和 UE 2 获取共享密钥的具体实现方式。示例性的，UE 1 和 UE 2 获取共享密钥可以包括以下四种方式：

方式一，UE 2 触发与 UE 1 之间的互鉴权流程，并在互鉴权之后与 UE 1 执行密钥建立流程。互鉴权流程用于验证双方的身份，即 UE 2 验证 UE 1 是否为合法用户，UE 1 验证 UE 2 是否为合法用户。在双方均为合法用户时，执行密钥建立流程，以使得双方都可以获得共享密钥。

方式二，UE 1 和 UE 2 上预配置有两者之间的共享密钥，两端可以在需要共享密钥时从

预配置中获取。

方式三，UE 1 和 UE 2 上预配置有公私钥和证书，两端可以在需要共享密钥时，根据公私钥和证书生成共享密钥。

其中 UE 1 上配置有 UE 1 的公钥、UE 1 的私钥和 UE 1 的证书，UE 1 的证书中包含 UE 1 的公钥；UE 2 上配置 UE 2 的公钥、UE 2 的私钥和 UE 2 的证书，UE 2 的证书中包含 UE 2 的公钥。使用公私钥和证书生成共享密钥的流程可以是：以 UE 2 发起建立共享密钥流程为例，UE 2 将自己的证书发送给 UE 1，UE 1 验证 UE 2 证书合法性后使用 UE 2 的公钥加密 UE 1 提供的共享信息 1 后，UE 1 将 UE 1 的证书和加密后的共享信息 1 发送给 UE 2。UE 2 收到后，验证 UE 1 证书的合法性后，使用 UE 2 的私钥解密加密后的共享信息 1 得到共享信息 1，并使用解密得到的共享信息 1 和自己生成的共享信息 2 生成共享密钥。之后 UE 2 使用 UE 1 公钥加密共享信息 2 后，UE 2 将 UE 2 的证书和加密后的共享信息 2 发送给 UE 1，后续 UE 1 解密后获取共享信息 2 并连同共享信息 1 一起生成共享密钥。

方式四，UE 1 和 UE 2 上保存有部分上下文信息，那么 UE 1 和 UE 2 可以直接从部分上下文信息中获取共享密钥。

在 UE 1 首次接入 UE 2 的情况下，UE 1 与 UE 2 执行互鉴权流程和密钥建立流程，以获得共享密钥。UE 1 和 UE 2 可根据共享密钥 K_{NRP} 、随机数 1 和随机数 2 生成的会话密钥 $K_{NRP-sess}$ ，进而使用会话密钥 $K_{NRP-sess}$ 继续推演生成加密密钥 NRPEK 和/或完整性保护密钥 NRPIK。UE 1 和 UE 2 根据确定的安全保护方式采用相应的密钥进行安全保护。在 UE 1 与 UE 2 断开之后，删除 NRPEK 和 NRPIK，例如删除上下文信息时便删除了 NRPEK 和 NRPIK。当 UE 1 再次接入 UE 2 时，UE 1 和 UE 2 需获取上下文信息中的共享密钥，以生成 NRPEK 和/或 NRPIK。

步骤 404，UE 2 向 UE 1 发送直连安全模式命令消息。相应的，UE 1 接收来自 UE 2 的直连安全模式命令消息。

其中，直连安全模式命令消息包括第二算法指示信息，第二算法指示信息用于指示控制面安全算法，即指示步骤 402 中选择的安全算法。

在选择的安全算法包括非空值的完整性保护算法和空值的机密性保护算法的情况下，第二算法指示信息可包括非空值的完整性保护算法的算法标识和空值的机密性保护算法的算法标识。例如，第二算法指示信息可表示为{非空值的完整性保护算法的算法标识,空值的机密性保护算法的算法标识}。再例如，第二算法指示信息可表示为{[非空值的完整性保护算法,算法标识],[空值的机密性保护算法,算法标识]}。具体第二算法指示信息的表现形式在本申请中不作限定。

可选的，如果 UE 2 在确定控制面完整性开启的情况下，强制开启控制面机密性保护；或在确定控制面机密性保护开启的情况下，强制开启控制面完整性保护；并根据 UE 1 的安全能力以及 UE 2 的安全能力，选择非空值的完整性保护算法和非空值的机密性保护算法，则第二算法指示信息包括选择的非空值的完整性保护算法和非空值的机密性保护算法，以使得在控制面安全算法协商阶段获得非空值的安全保护算法，在用户面需要开启安全保护时可以直接使用控制面安全算法协商阶段获得的非空值的安全保护算法。例如 UE 2 决策开启控制面完整性保护，则 UE 2 强制开启控制面机密性保护并选择非空值的完整性保护算法和非空值的机密性保护算法，此时第二算法指示信息可表示为{非空值的完整性保护算法的算法标识,非空值的机密性保护算法的算法标识}。

可选的，如果 UE 2 在确定控制面完整保护开启且控制面机密性保护不开启并根据 UE 1 的安全能力以及 UE 2 的安全能力选择空值的机密性保护算法时，额外根据 UE 1 的安全能力

以及 UE 2 的安全能力选择额外的非空值的机密性保护算法,则此时第二算法指示信息包括该额外的非空值的机密性保护算法的算法标识,以使得在控制面安全算法协商阶段获得非空值的安全保护算法,在用户面需要开启安全保护时可以直接使用控制面安全算法协商阶段获得的非空值的安全保护算法。例如 UE 2 决策开启控制面完整性保护且不开启控制面机密性保护,则此时 UE 2 选择非空值的完整性保护算法和空值的机密性保护算法,同时额外根据 UE 1 的安全能力和 UE 2 的安全能力选择额外的非空值的机密性保护算法,此时第二算法指示信息可表示为{非空值的完整性保护算法的算法标识,空值的机密性保护算法的算法标识,额外的非空值的机密性保护算法的算法标识}。

可选的,直连安全模式命令消息还可包括 UE 2 生成的随机数 2,随机数 2 可用于生成完整性保护密钥和/或机密性保护密钥。

进一步的,UE 2 确定保护密钥,保护密钥用于对直连安全模式消息所携带的部分信息或全部信息进行保护。保护密钥可以是 UE 2 与 UE 1 之间的共享密钥 K_{NRP} ,也可以是根据共享密钥 K_{NRP} 生成的会话密钥 $K_{NRP-secs}$ 。保护密钥还可以是根据会话密钥 $K_{NRP-secs}$ 生成的完整性保护密钥 (NRPIK) 和/或机密性保护密钥 (NRPEK)。

在控制面完整性保护开启和控制面机密性保护不开启的情况下,UE 2 生成完整性保护密钥,不生成机密性保护密钥。完整性保护密钥用于对直连安全模式消息所携带的部分信息或全部信息进行完整性保护,例如采用完整性保护密钥对第二算法指示信息进行完整性保护。

步骤 405,UE 1 根据第二算法指示信息确定与 UE 2 之间的控制面安全保护方式。

可选的,如果 UE 1 获取的第二算法指示信息包括额外的非空值的机密性保护算法标识,UE 1 存储该非空值的机密性保护算法标识指示的机密性保护算法。

基于控制面完整性保护开启的前提,UE 1 在接收到直连安全模式命令消息的情况下,根据步骤 103 获取的共享密钥,对直连安全模式命令消息进行完整性保护验证。

UE 1 与 UE 2 可协商或预配置采用哪种保护密钥,若保护密钥是共享密钥 K_{NRP} ,那么 UE 1 采用共享密钥对直连安全模式命令消息进行完整性保护验证;若保护密钥是会话密钥 $K_{NRP-secs}$,那么 UE 1 根据共享密钥 K_{NRP} 生成会话密钥 $K_{NRP-secs}$,并采用会话密钥 $K_{NRP-secs}$ 对直连安全模式命令消息进行完整性保护验证;若保护密钥是完整性保护密钥 (NRPIK),那么 UE 1 根据随机数 1、随机数 2 和共享密钥 K_{NRP} 推演会话密钥 $K_{NRP-secs}$,并继续使用会话密钥推演的完整性保护密钥 (NRPIK),并采用完整性保护密钥 (NRPIK) 对直连安全模式命令消息进行完整性保护验证。

在直连安全模式命令消息通过完整性保护验证的情况下,UE 1 根据第二算法指示信息确定与 UE 2 之间的控制面安全保护方式,并执行后续流程以建立与 UE 2 之间的 PC5 单播连接。可选的,在直连安全模式命令消息未通过完整性保护验证的情况下,UE 1 向 UE 2 发送连接建立拒绝消息。相应的,UE 2 接收来自 UE 1 的连接建立拒绝消息。连接建立拒绝消息用于指示 UE 2 拒绝与 UE 1 建立 PC5 单播连接。

UE 1 根据第二算法指示信息确定开启控制面完整性保护和不开启控制面机密性保护,那么 UE 1 不生成机密性保护密钥 (NRPEK)。

步骤 406,UE 1 向 UE 2 发送直连安全模式完成消息。相应的,UE 2 接收来自 UE 1 的直连安全模式完成消息。

其中,直连安全命令完成消息包括 UE 1 的用户面安全策略,以便 UE 2 结合 UE 1 和 UE 2 的用户面安全策略确定与 UE 1 之间的用户面安全保护方式。

可选的,直连安全命令完成消息还包括 UE 1 的安全能力,以便 UE 2 结合 UE 1 和 UE 2

的安全能力，以及用户面安全保护方式，选择用户面安全算法。若步骤 402 中，UE 2 执行了存储 UE 1 的安全能力的步骤，那么 UE 1 可不在直连安全命令完成消息中携带 UE 1 的安全能力。若步骤 402 中，UE 2 未执行存储 UE 1 的安全能力的步骤，那么 UE 1 可在直连安全命令完成消息中携带 UE 1 的安全能力。

UE1 在直连安全命令完成消息中携带 UE1 的安全能力，可以在 UE 1 确定控制面机密性保护不开启而控制面完整性保护开启的情况下携带，也可以不在任何前提条件限制下携带。

步骤 407，UE 2 确定与 UE 1 之间的用户面安全保护方式包括用户面机密性保护开启，并生成用户面安全开启指示信息。

在一种实现方式中，UE 2 在接收到直连安全模式完成消息时，根据 UE 1 和 UE 2 的用户面安全策略，确定出与 UE 1 之间的用户面安全保护方式包括用户面机密性保护开启。UE 2 与 UE 1 之间的用户面安全保护方式，即针对本次 PC5 单播连接的用户面安全保护方式。UE 2 根据两端 UE 的用户面安全策略确定用户面安全保护方式，可参考图 1 中根据两端 UE 的控制面安全策略确定控制面安全保护方式的相应描述，在此不再赘述。

在另一种实现方式中，UE 2 在接收到直连安全模式完成消息时，如果此时控制面机密性保护不开启，则不管两端 UE 的用户面安全策略，默认确定与 UE 1 之间的用户面安全保护方式包括用户面机密性保护不开启，即默认不开启用户面机密性保护。以防止因在控制面安全算法协商阶段未获得非空值的机密性保护算法，而导致用户面需要机密性保护时没有协商过的非空值的机密性保护算法的情况。

在另一种实现方式中，UE 2 在接收到直连安全模式完成消息时，不管两端 UE 的用户面机密性和/或完整性保护的策略，默认确定与 UE 1 之间的用户面机密性和/或完整性保护方式与控制面机密性和/或完整性保护方式一致，即默认用户面机密性保护和/或用户面完整性保护方式同控制面一致，以防止因在控制面安全算法协商阶段未获得非空值的安全保护算法，而导致用户面需要安全保护开启时没有协商过的非空值的安全保护算法的情况，同时简化了 UE 在用户面策略协商的逻辑以提高处理效率。其中可以是不管两端 UE 的用户面机密性保护的策略，默认确定与 UE 1 之间的用户面机密性保护方式与控制面机密性保护方式一致，或可以是不管两端 UE 的用户面完整性保护的策略，默认确定与 UE 1 之间的用户面完整性保护方式与控制面完整性保护方式一致，或可以是不管两端 UE 的用户面机密性和完整性保护的策略，默认确定与 UE 1 之间的用户面机密性和完整性保护方式与控制面机密性和完整性保护方式均一致。例如，控制面完整性保护开启且控制面机密性保护不开启，那么用户面完整性保护也开启且用户面机密性保护也不开启。再例如，控制面完整性保护开启且控制面机密性保护不开启，UE 2 只决策用户面机密性保护也不开启，而用户面完整性保护根据两端用户面完整性保护策略确定。

在 UE 2 确定出用户面安全保护方式的情况下，生成用户面安全开启指示信息，用于指示是否开启用户面完整性保护以及是否开启用户面机密性保护。例如，用户面安全保护方式为用户面完整性保护开启和用户面机密性保护开启，那么生成的用户面安全开启指示信息用于指示开启用户面完整性保护和开启用户面机密性保护。再例如，用户面安全保护方式为用户面完整性保护不开启和用户面机密性保护开启，那么生成的用户面安全开启指示信息用于指示不开启用户面完整性保护和开启用户面机密性保护。

步骤 408，UE 2 在用户面安全保护方式与控制面安全保护方式不一致的情况下，根据用户面安全保护方式、UE 1 的安全能力和 UE 2 的安全能力，选择用户面安全算法。

其中此时 UE 1 的安全能力可以是步骤 402 中 UE 2 存储的 UE 1 的安全能力，也可以是

在步骤 406 中由 UE 1 发送给 UE 2。

其中，用户面安全保护方式与控制面安全保护方式不一致，可以包括以下任一种情况：

(1) 控制面完整性保护开启方式与用户面完整性保护开启方式一致，控制面机密性保护开启方式与用户面机密性保护开启方式不一致。例如，控制面完整性保护开启且控制面机密性保护不开启，用户面完整性保护开启且用户面机密性保护开启。

(2) 控制面完整性保护开启方式与用户面完整性保护开启方式不一致，控制面机密性保护开启方式与用户面机密性保护开启方式一致。例如，控制面完整性保护开启且控制面机密性保护开启，用户面完整性保护不开启且用户面机密性保护开启。

(3) 控制面完整性保护开启方式与用户面完整性保护开启方式不一致，控制面机密性保护开启方式与用户面机密性保护开启方式不一致。例如，控制面完整性保护开启且控制面机密性保护开启，用户面完整性保护不开启且用户面机密性保护不开启。

应用在本申请中，用户面安全保护方式与控制面安全保护方式不一致可以包括：用户面安全保护方式包括用户面机密性保护开启，而控制面安全保护方式为控制面完整性保护开启且控制面机密性保护不开启。示例性的，可参见下表 2 所示。

编号	控制面安全保护方式		用户面安全保护方式	
	完整性保护	机密性保护	完整性保护	机密性保护
1	开	不开	开	开
2			不开	开

表 2

表 2 中，编号 1 表示的不一致，指的是用户面机密性保护开启与控制面机密性保护不开启不一致；编号 2 表示的不一致，指的是用户面机密性保护开启与控制面机密性保护不开启不一致，且用户面完整性保护不开启与控制面完整性保护开启不一致。

对于编号 1，UE 2 根据用户面安全保护方式、UE 1 的安全能力和 UE 2 的安全能力，选择非空值的完整性保护算法作为用户面完整性保护算法，选择非空值的机密性保护算法作为用户面机密性保护算法。需要说明的是，步骤 408 中选择的非空值的完整性保护算法与步骤 402 中选择的非空值的完整性保护算法，可以相同，也可以不相同。相同的情况下，可以直接使用控制面使用的完整性保护算法而省去选择步骤，以节省 UE 2 选择完整性保护算法的耗时和简化 UE 2 的处理逻辑以提高终端性能；不相同，可以提高安全性。

对于编号 2，UE 2 根据用户面安全保护方式、UE 1 的安全能力和 UE 2 的安全能力，选择非空值的机密性保护算法作为用户面机密性保护算法。

进一步的，UE 2 在选择非空值的机密性保护算法的情况下，生成机密性保护密钥（NRPEK）。若还选择非空值的完整性保护算法，那么还可以生成完整性保护密钥（NRPIK），或获取控制面协商时生成的完整性保护密钥。

可选的，在控制面完整性保护开启的情况下，用户面安全保护方式与控制面安全保护方式不一致还可以包括如表 3 所示的几种情况。

编号	控制面安全保护方式		用户面安全保护方式	
	完整性保护	机密性保护	完整性保护	机密性保护
3	开	不开	不开	不开

4	开	开	不开	开
5			开	不开
6			不开	不开

表 3

对于编号 3 和 6, UE 2 选择空值的机密性保护算法和空值的完整性保护算法作为用户面机密性保护算法和用户面完整性保护算法。或 UE 2 不选择安全算法, 以简化 UE 2 的处理逻辑从而提高终端性能。

对于编号 4, UE 2 选择非空值的机密性保护算法作为用户面机密性保护算法。用户面机密性保护算法与控制面机密性保护算法可以相同, 也可以不相同。相同的情况下, 可以直接使用控制面使用的机密性保护算法而省去选择步骤以节省 UE 2 选择机密性保护算法的耗时和简化 UE 2 的处理逻辑以提高终端性能。

对于编号 5, UE 2 选择非空值的完整性保护算法作为用户面完整性保护算法。用户面完整性保护算法与控制面完整性保护算法可以相同, 也可以不相同。相同的情况下, 可以直接使用控制面使用的完整性保护算法而省去选择步骤以节省 UE 2 选择完整性保护算法的耗时和简化 UE 2 的处理逻辑以提高终端性能。

在一种实现方式中, 不管用户面安全保护方式如何, UE 2 默认选择非空值的机密性保护算法, 以便 UE 1 在确定用户面机密性保护开启的情况下, 可根据该机密性保护算法进行机密性保护。可选的, UE 2 默认选择非空值的完整性保护算法, 以便 UE 1 在确定用户面完整性保护开启的情况下, 可根据该完整性保护算法进行完整性保护。在此种实现方式中, 如果安全保护不开启则默认选择空值的安全保护算法, 或不选择安全算法, 以简化 UE 2 的处理逻辑从而提高终端性能。

在另一种实现方式中, 如果 UE 2 根据控制面机密性保护不开启, 默认确定不开启用户面机密性保护, 则 UE 2 选择空值的机密性保护算法作为用户面机密性保护算法, 或不选择安全算法, 以简化 UE 2 的处理逻辑从而提高终端性能。

在另一种实现方式中, 如果 UE 2 默认确定与 UE 1 之间的用户面机密性和/或完整性保护方式与控制面机密性和/或完整性保护方式一致, 如果 UE 2 根据控制面机密性保护开启确定用户面机密性保护方式为机密性保护开启, 则选择的用户面机密性保护算法可以和控制面一致, 也可以是不同的非空值机密性保护算法; 如果 UE 2 根据控制面完整性保护开启确定用户面完整性保护方式为完整性保护开启, 则选择的用户面完整性保护算法可以和控制面一致, 也可以是不同的非空值完整性保护算法。如果 UE 2 确定的用户面安全保护方式不开启, 则选择空值的安全保护算法, 或不选择安全保护算法以简化 UE 2 的处理逻辑从而提高终端性能。

可选的, UE 2 在用户面安全保护方式与控制面安全保护方式一致的情况下, 根据用户面安全保护方式、UE 1 的安全能力和 UE 2 的安全能力, 选择用户面安全算法, 其中选择的用户面安全算法可以和控制面安全算法一致, 也可以和控制面安全算法不一致。

步骤 409, UE 2 向 UE 1 发送直连通信接受消息。相应的, UE 1 接收来自 UE 2 的直连通信接受消息。

可选的, 步骤 409 也可作为 UE 2 向 UE 1 发送的直连密钥更新回复(direct rekeying Response)消息, 相应的, UE 1 接收来自 UE 2 的直连密钥更新请求。

可选的, 步骤 409 也可作为 UE 2 向 UE 1 发送的 RRC 连接重配置消息, 相应的, UE 1 接收来自 UE 2 的 RRC 连接重配置消息。

其中，直连通信接受消息包括用户面安全开启指示信息和用于指示用户面安全算法的第一算法指示信息。用户面安全开启指示信息用于指示是否开启用户面完整性保护以及是否开启用户面机密性保护。第一算法指示信息即指示步骤 408 中选择的安全算法。可选的，第一算法标识也可只在用户面安全保护方式与控制面安全保护方式不一致时携带，也可无此限制条件。

对于编号 1，UE 1 根据用户面安全开启指示信息确定开启用户面机密性保护和用户面完整性保护。第一算法指示信息包括非空值的机密性保护算法的算法标识，用于指示选择的非空值的机密性保护算法。若非空值的控制面完整性保护算法与用户面完整性保护算法相同，那么第一算法指示信息可包括或不包括非空值的完整性保护算法，在不包括非空值的完整性保护算法的情况下，UE 1 在根据用户面安全开启指示信息确定开启用户面完整性保护的情况下，默认将控制面完整性保护算法作为用户面完整性保护算法；在包括非空值的完整性保护算法的情况下，UE 1 在根据用户面安全开启指示信息确定开启用户面完整性保护的情况下，根据第一算法指示信息中非空值的用户面完整性保护算法的算法标识确定用户面完整性保护算法。若控制面完整性保护算法与用户面完整性保护算法不相同，那么第一算法指示信息包括非空值的完整性保护算法，该完整性保护算法与控制面完整性保护算法不同。

对于编号 2，UE 1 根据用户面安全开启指示信息确定不开启用户面完整性保护而开启用户面机密性保护。第一算法指示信息包括非空值的机密性保护算法的算法标识和空值的完整性保护算法的算法标识，或第一算法指示信息不包括完整性保护算法的算法标识。非空值的机密性保护算法的算法标识，用于指示选择的非空值的机密性保护算法；空值的完整性保护算法的算法标识，用于指示选择的空值的完整性保护算法。可选的，第一算法指示信息包括非空值的机密性保护算法的算法标识而不包括完整性保护算法的算法标识，UE 1 在根据用户面安全开启指示信息确定不开启用户面完整性保护的情况下，默认不进行用户面完整性保护，或默认使用空值的完整性保护算法。

对于编号 3，UE 1 根据用户面安全开启指示信息确定不开启用户面完整性保护和用户面机密性保护。第一算法指示信息用于指示空值的机密性保护算法和空值的完整性保护算法，或第一算法指示信息不包括完整性保护算法的算法标识，或第一算法指示信息不包括机密性保护算法的算法标识，或均不携带。可选的，可不携带第一算法指示信息。

对于编号 4，UE 1 根据用户面安全开启指示信息确定不开启用户面完整性保护而开启用户面机密性保护。第一算法指示信息包括非空值的机密性保护算法的算法标识和空值的完整性保护算法的算法标识，或第一算法指示信息不包括完整性保护算法的算法标识，或第一算法指示信息不包括机密性保护算法的算法标识，或均不携带。非空值的机密性保护算法可以与控制面机密性保护算法相同或不相同。若相同，第一算法指示信息可不携带非空值的机密性保护算法的算法标识，UE 1 在根据用户面安全开启指示信息确定开启用户面机密性保护的情况下，默认使用控制面机密性保护算法。若不相同，第一算法指示信息包括非空值的机密性保护算法的算法标识，该机密性保护算法与控制面机密性保护算法不同，以提高安全性。可选的，可不携带第一算法指示信息。

对于编号 5，UE 1 根据用户面安全开启指示信息确定开启用户面完整性保护而不开启用户面机密性保护。第一算法指示信息包括非空值的完整性保护算法的算法标识和空值的机密性保护算法的算法标识，或第一算法指示信息不包括机密性保护算法的算法标识，或第一算法指示信息不包括完整性保护算法的算法标识，或均不携带。非空值的完整性保护算法与控制面完整性保护算法可以相同或不相同。若相同，第一算法指示信息可不携带非空值的完

完整性保护算法的算法标识, UE 1 在根据用户面安全开启指示信息确定开启用户面完整性保护的情况下, 默认使用控制面完整性保护算法, 以减少消息长度。若不相同, 第一算法指示信息包括非空值的完整性保护算法的算法标识, 该完整性保护算法与控制面完整性保护算法不同, 以提高安全性。可选的, 可不携带第一算法指示信息。

对于编号 6, UE 1 根据用户面安全开启指示信息确定不开启用户面完整性保护和用户面机密性保护。第一算法指示信息用于指示空值的机密性保护算法和空值的完整性保护算法, 或不携带机密性保护算法的算法标识, 或不携带完整性保护算法的算法标识, 或均不携带。可选的, 可不携带第一算法指示信息。

在一种实现方式中, 不管用户面安全保护方式如何, 第一算法指示信息默认用于指示非空值的机密性保护算法, 以便 UE 1 在确定用户面机密性保护开启的情况下, 可根据该机密性保护算法进行机密性保护。可选的, 第一算法指示信息还默认用于指示非空值的完整性保护算法, 以便 UE 1 在确定用户面完整性保护开启的情况下, 可根据该完整性保护算法进行完整性保护。

在另一种实现方式中, 如果 UE 2 根据控制面机密性保护不开启, 默认选择空值的机密性保护算法, 则第一算法指示信息包括空值的机密性保护算法。可选的, 不携带第一算法指示信息。

在另一种实现方式中, 如果 UE 2 默认确定用户面安全保护方式和控制面一致, 且选择的用户面机密性和完整性保护算法和控制面相同, 则第一算法指示信息和第二算法指示信息一致。可选的, 也可不携带第一算法指示信息。UE 2 默认确定用户面安全保护方式和控制面一致, 且选择的用户面非空值保护算法和控制面不同, 则第一算法指示信息包含与控制面不同的非空值机密性和/或完整性保护算法的算法标识。如果 UE 2 默认确定只有用户面机密性保护方式和控制面机密性保护方式一致, 且选择的用户面机密性保护算法和控制面相同, 则第一算法指示信息包括与控制面相同的机密性保护算法的算法标识。可选的, 第一算法指示信息也可不包括与控制面相同的机密性保护算法的算法标识。如果 UE 2 默认确定只有用户面完整性保护方式和控制面完整性保护方式一致, 且选择的用户面完整性保护算法和控制面相同, 则第一算法指示信息包括与控制面相同的完整性保护算法的算法标识。可选的, 第一算法指示信息也可不包括与控制面相同的完整性保护算法的算法标识。

可选的, UE 2 在用户面安全保护方式与控制面安全保护方式一致的情况下, 步骤 409 中选择用户面安全算法, UE 2 选择的用户面安全算法可以和控制面安全算法一致, 也可以和控制面安全算法不一致。如果选择的算法一致, 可以携带第一算法指示信息, 其中包括选择的用户面机密性保护算法的算法标识和完整性保护算法的算法标识, 也可以不携带第一算法指示信息。如果选择的用户面安全算法和控制面安全算法不一致, 则需携带第一算法指示信息包括用户面机密性保护算法的算法标识和用户面完整性保护算法的算法标识。

可选的, 如果 UE 2 在确定控制面完整保护开启且控制面机密性保护不开启并根据 UE 1 的安全能力以及 UE 2 的安全能力选择空值的机密性保护算法时, 额外根据 UE 1 的安全能力以及 UE 2 的安全能力选择额外的非空值的机密性保护算法, 则此时可不携带第一算法标识。

步骤 410, UE 1 根据用户面安全开启指示信息确定与 UE 2 之间的用户面安全保护方式, 根据第一算法指示信息确定用户面保护算法。

UE 1 在接收到直连通信接受消息的情况下, 根据用户面安全开启指示信息, 确定与 UE 2 之间的用户面安全保护方式; 如果直连通信接受消息中携带第一算法指示信息, 则根据第一算法指示信息确定用户面保护算法。如果直连通信接受消息中不携带第一算法指示信息, 则

使用与控制面使用的安全算法相同的安全算法。

例如，用户面安全保护方式为用户面完整性保护开启和用户面机密性保护开启，第一算法指示信息用于指示非空值的完整性保护算法和非空值的机密性保护算法，那么 UE 1 采用非空值的完整性保护算法和完整性保护密钥对第一用户面数据进行完整性保护，采用非空值的机密性保护算法和机密性保护密钥对第一用户面数据进行机密性保护，从而实现对用户面数据的安全保护。这里的第一用户面数据指的是 UE 1 向 UE 2 发送的用户面数据，对于 UE 2 向 UE 1 发送的第二用户面数据，UE 1 可采用非空值的完整性保护算法和完整性保护密钥对第二用户面数据进行完整性保护验证，采用非空值的机密性保护算法和机密性保护密钥对第二用户面数据进行解密。

再例如，用户面安全保护方式为用户面完整性保护不开启和用户面机密性保护开启，第一算法指示信息用于指示空值的完整性保护算法和非空值的机密性保护算法，那么 UE 1 不对第一用户面数据进行完整性保护，采用非空值的机密性保护算法和机密性保护密钥对第一用户面数据进行机密性保护，从而实现对用户面数据的机密性保护。

可选的，如果 UE 1 接收到的第二算法指示信息包括额外的非空值机密性保护算法，且 UE 1 根据安全开启指示信息确定用户面机密性保护开启，则确定使用第二算法指示信息中包括的额外的非空值机密性保护算法作为用户面机密性保护算法。

其中，UE 1 可在确定出用户面机密性保护开启的情况下，生成机密性保护密钥；若确定出用户面机密性保护不开启，则不生成机密性保护密钥，可选的，不执行对应的空值机密性保护算法以节省计算资源。UE 1 在确定用户面完整性保护开启的情况下，生成完整性保护密钥；若确定出用户面完整性保护不开启，则不生成完整性保护密钥，可选的，不执行对应的空值完整性保护算法以节省计算资源。

在图 4 所示的实施例中，第二算法指示信息既用于指示控制面安全算法，又用于指示控制面安全保护方式；第一算法指示信息用于指示用户面安全算法，用户面安全开启指示信息用于指示用户面安全保护方式。通过第一算法指示信息指示用户面采用何种机密性保护算法，以有效的对用户面数据进行机密性保护。

请参见图 5，为本申请实施例二提供的确定用户面安全算法的方法的流程示意图。图 5 所示流程中与图 4 相同或类似部分，可参见图 4 所示实施例中相应的描述，该流程可包括但不限于如下步骤：

步骤 501，UE 1 向 UE 2 发送直连通信请求消息。相应的，UE 2 接收来自 UE 1 的直连通信请求消息。

可选的，步骤 501 也可作为 UE 1 向 UE 2 发送的直连密钥更新请求 (direct rekeying request) 消息，相应的，UE 2 接收来自 UE 1 的直连密钥更新请求。此时该消息不包含 UE 1 的控制面安全策略。

步骤 502，UE 2 确定与 UE 1 之间的控制面安全保护方式，并选择安全算法。

可选的，步骤 503，UE 1 和 UE 2 获取共享密钥。共享密钥即 K_{NRP} 。

步骤 504，UE 2 向 UE 1 发送直连安全模式命令消息。相应的，UE 1 接收来自 UE 2 的直连安全模式命令消息。

步骤 505，UE 1 根据第二算法指示信息确定与 UE 2 之间的控制面安全保护方式。

步骤 506，UE 1 向 UE 2 发送直连安全模式完成消息。相应的，UE 2 接收来自 UE 1 的直连安全模式完成消息。

步骤 501-步骤 506 的具体实现过程，可参见图 4 所示实施例中步骤 401-步骤 406 的具体

描述，在此不再赘述。

步骤 507，UE 2 确定与 UE 1 之间的用户面安全保护方式包括用户面机密性保护开启，并选择用户面安全算法。

在一种实现方式中，UE 2 在接收到直连安全模式完成消息时，根据 UE 1 和 UE 2 的用户面安全策略，确定出与 UE 1 之间的用户面安全保护方式包括用户面机密性保护开启。

在另一种实现方式中，UE 2 在接收到直连安全模式完成消息时，如果此时控制面机密性保护不开启，则不管两端 UE 的用户面安全策略，默认确定与 UE 1 之间的用户面安全保护方式包括用户面机密性保护不开启，即默认不开启用户面机密性保护。

在另一种实现方式中，UE 2 在接收到直连安全模式完成消息时，不管两端 UE 的用户面安全策略，默认确定出与 UE 1 之间的用户面安全保护方式与控制面安全保护方式一致，即默认用户面机密性保护和用户面完整性保护方式同控制面一致。

在 UE 2 确定出用户面安全保护方式的情况下，根据用户面安全保护方式选择用户面安全算法。

在用户面完整性保护不开启的情况下，用户面完整性保护算法是空值的完整性保护算法。在用户面机密性保护不开启的情况下，用户面机密性保护算法是空值的机密性保护算法。

在控制面完整性保护开启且用户面完整性保护也开启的情况下，用户面完整性保护算法与控制面完整性保护算法可以是相同的非空值完整性保护算法，也可为不同的非空值完整性保护算法。如果要求控制面和用户面使用相同的非空值完整性保护算法，则 UE 2 可执行也可不执行算法选择步骤，不执行算法选择步骤以节省 UE 2 的处理资源。如果不要求控制面和用户面使用相同的非空值完整性保护算法，则 UE 2 选择非空值的完整性保护算法，该非空值完整性保护算法可以与控制面的非空值完整性保护算法不同也可以相同，如果保护算法相同可简化 UE 的处理逻辑，如果保护算法不相同则可提高安全性。

在控制面机密性保护开启且用户面机密性保护也开启的情况下，用户面机密性保护算法与控制面机密性保护算法可以是相同的非空值机密性保护算法，也可为不同的非空值机密性保护算法。如果要求控制面和用户面使用相同的非空值机密性保护算法，则 UE 2 可执行也可不执行算法选择步骤。如果不要求控制面和用户面使用相同的非空值机密性保护算法，则 UE 2 选择非空值的机密性保护算法，该非空值机密性保护算法可以与控制面的非空值机密性保护算法不同也可以相同。

示例 1，用户面安全保护方式为用户面完整性保护开启和用户面机密性保护开启，那么 UE 2 根据两端 UE 的安全能力，从支持的完整性保护算法列表选择一个非空值的完整性保护算法作为用户面完整性保护算法；从支持的机密性保护算法列表选择一个非空值的机密性保护算法作为用户面机密性保护算法。

在控制面完整性保护开启和控制面机密性保护不开启的情况下，用户面完整性保护算法与控制面完整性保护算法可以相同或不相同。在控制面完整性保护开启和控制面机密性保护开启的情况下，用户面完整性保护算法与控制面完整性保护算法可以相同或不相同，用户面机密性保护算法与控制面机密性保护算法可以相同或不相同。

示例 2，用户面安全保护方式为用户面完整性保护不开启和用户面机密性保护开启，那么 UE 2 根据两端 UE 的安全能力，从支持的机密性保护算法列表选择一个非空值的机密性保护算法作为用户面机密性保护算法，不选择完整性保护算法或默认完整性保护算法为空值。

在控制面完整性保护开启和控制面机密性保护开启的情况下，用户面机密性保护算法与控制面机密性保护算法可以相同或不相同。

步骤 508, UE 2 向 UE 1 发送直连通信接受消息。相应的, UE 1 接收来自 UE 2 的直连通信接受消息。

可选的, 步骤 508 也可作为 UE 2 向 UE 1 发送的直连密钥更新回复(direct rekeying Response)消息, 相应的, UE 1 接收来自 UE 2 的直连密钥更新请求。

可选的, 步骤 508 也可作为 UE 2 向 UE 1 发送的 RRC 连接重配置消息, 相应的, UE 1 接收来自 UE 2 的 RRC 连接重配置消息。

其中, 直连通信接受消息包括第一算法指示信息, 用于指示步骤 507 选择的用户面安全算法, 第一算法指示消息也用来指示用户面安全保护方式。

在一种实现方式中, 如果用户面机密性保护方式与控制面机密性保护方式不同, 则第一算法指示信息包括用户面机密性保护算法的算法标识, 否则第一算法指示信息不包括用户面机密性保护算法的算法标识。如果用户面完整性保护方式与控制面完整性保护方式不同, 则第一算法指示信息包括用户面完整性保护算法的算法标识, 否则第一算法指示信息不包括用户面完整性保护算法的算法标识。可选的, 如果用户面安全保护方式和控制面安全保护方式一致, 则不携带第一算法指示信息, 也可携带空值的第一算法指示信息。

在此种实现方式中, 如果第一算法指示信息只携带用户面机密性保护算法的算法标识, 则 UE 1 默认用户面完整性保护方式与控制面完整性保护方式一致, UE 1 默认用户面完整性保护算法与控制面完整性保护算法一致。如果第一算法指示信息只携带用户面完整性保护算法的算法标识, 则 UE 1 默认用户面机密性保护方式与控制面机密性保护方式一致, UE 1 默认用户面机密性保护算法与控制面机密性保护算法一致。如果第一算法指示信息携带非空值的用户面完整性保护算法的算法标识, 则 UE 1 开启用户面完整性保护并使用该算法标识所标识的完整性保护算法对用户面进行完整性保护。如果第一算法指示信息携带空值的用户面完整性保护算法的算法标识, 则 UE 1 不开启用户面完整性保护, 可选的, UE 1 不执行该空值的用户面完整性保护算法以节省计算资源。如果第一算法指示信息携带非空值的用户面机密性保护算法的算法标识, 则 UE 1 开启用户面机密性保护并使用该算法标识所标识的机密性保护算法对用户面进行机密性保护。如果第一算法指示信息携带空值的用户面机密性保护算法的算法标识, 则 UE 1 不开启用户面机密性保护, 可选的, UE 1 不执行该空值的用户面机密性保护算法以节省计算资源。

在另一种实现方式中, 第一算法指示信息默认包括用户面机密性保护算法的算法标识和用户面完整性保护算法的算法标识。

在此种实现方式中, 如果第一算法指示信息携带非空值的用户面完整性保护算法的算法标识, 则 UE 1 开启用户面完整性保护并使用该算法标识所标识的完整性保护算法对用户面进行完整性保护。如果第一算法指示信息携带空值的用户面完整性保护算法的算法标识, 则 UE 1 不开启用户面完整性保护, 可选的, UE 1 不执行该空值的用户面完整性保护算法以节省计算资源。如果第一算法指示信息携带非空值的用户面机密性保护算法的算法标识, 则 UE 1 开启用户面机密性保护并使用该算法标识所标识的机密性保护算法对用户面进行机密性保护。如果第一算法指示信息携带空值的用户面机密性保护算法的算法标识, 则 UE 1 不开启用户面机密性保护, 可选的, UE 1 不执行该空值的用户面机密性保护算法以节省计算资源。

在另一种实现方式中, 第一算法指示信息只在用户面机密性保护开启情况下包括非空值的用户面机密性保护算法的算法标识。第一算法指示信息只在用户面完整性保护开启情况下包括非空值的用户面完整性保护算法的算法标识。

在此种实现方式中, 如果第一算法指示信息只携带用户面机密性保护算法的算法标识,

则 UE 1 默认用户面完整性保护不开启，UE 1 默认用户面机密性保护开启并使用该算法标识所标识的机密性保护算法对用户面进行机密性保护。如果第一算法指示信息只携带用户面完整性保护算法的算法标识，则 UE 1 默认用户面机密性保护不开启，UE 1 默认用户面完整性保护开启并使用该算法标识所标识的完整性保护算法对用户面进行完整性保护。

对于上述示例 1，在用户面完整性保护开启和用户面机密性保护开启的情况下，第一算法指示信息可包括非空值的完整性保护算法的算法标识和非空值的机密性保护算法的算法标识。

对于上述示例 1，在用户面完整性保护和用户面机密性保护均开启，且控制面完整性保护开启和控制面机密性保护不开启的情况下，可选的，第一算法指示信息包括非空值的机密性保护算法的算法标识，不包括非空值的完整性保护算法的算法标识。UE 1 在接收到该第一算法指示信息时，默认用户面完整性保护开启方式与控制面完整性保护开启方式一致，即开启用户面完整性保护并将控制面完整性保护算法作为用户面完整性保护算法。若选择的用户面完整性保护算法与控制面完整性保护算法不同，那么第一算法指示信息包括非空值的完整性保护算法的算法标识和非空值的机密性保护算法的算法标识，该完整性保护算法与控制面完整性保护算法不同。

在控制面完整性保护开启和控制面机密性保护开启的情况下，若用户面完整性保护算法与控制面完整性保护算法不相同，那么第一算法指示信息用于指示非空值的用户面完整性保护算法；若用户面机密性保护算法与控制面机密性保护算法不相同，那么第一算法指示信息用于指示非空值的用户面机密性保护算法；若用户面完整性保护算法与控制面完整性保护算法不相同且用户面机密性保护算法与控制面机密性保护算法不相同，那么第一算法指示信息用于指示非空值的用户面完整性保护算法和非空值的用户面机密性保护算法。

对于上述示例 2，在用户面完整性保护不开启和用户面机密性保护开启的情况下，第一算法指示信息包括空值的完整性保护算法的算法标识和非空值的机密性保护算法的算法标识。

可选的，第一算法指示信息包括非空值的机密性保护算法的算法标识，UE 1 在接收到该第一算法指示信息的情况下，默认用户面完整性保护不开启，不对用户面数据进行完整性保护。

在控制面完整性保护开启和控制面机密性保护开启的情况下，若用户面机密性保护算法与控制面机密性保护算法不相同，那么第一算法指示信息用于指示非空值的用户面机密性保护算法。

步骤 509，UE 1 根据第一算法指示信息确定用户面安全算法，并确定与 UE 2 之间的用户面安全保护方式。

在一种实现方式中，UE 1 确定的第一算法指示信息包含用户面安全保护方式与控制面机密性保护方式不同的安全算法的算法标识。

在此种实现方式中，如果第一算法指示信息只携带用户面机密性保护算法的算法标识，则 UE 1 默认用户面完整性保护方式与控制面完整性保护方式一致，UE 1 默认用户面完整性保护算法与控制面完整性保护算法一致。如果第一算法指示信息只携带用户面完整性保护算法的算法标识，则 UE 1 默认用户面机密性保护方式与控制面机密性保护方式一致，UE 1 默认用户面机密性保护算法与控制面机密性保护算法一致。如果第一算法指示信息携带非空值的用户面完整性保护算法的算法标识，则 UE 1 开启用户面完整性保护并使用该非空值用户面完整性保护算法标识的完整性保护算法对用户面进行完整性保护。如果第一算法指示信息携

带空值的用户面完整性保护算法的算法标识, 则 UE 1 不开启用户面完整性保护, 可选的, UE 1 不执行该空值的用户面完整性保护算法以节省计算资源。如果第一算法指示信息携带非空值的用户面机密性保护算法的算法标识, 则 UE 1 开启用户面机密性保护并使用该算法标识所标识的机密性保护算法对用户面进行机密性保护。如果第一算法指示信息携带空值的用户面机密性保护算法的算法标识, 则 UE 1 不开启用户面机密性保护, 可选的, UE 1 不执行该空值的用户面机密性保护算法以节省计算资源。

在另一种实现方式中, 第一算法指示信息默认包括用户面机密性保护算法的算法标识和用户面完整性保护算法的算法标识。

在此种实现方式中, 如果第一算法指示信息携带非空值的用户面完整性保护算法的算法标识, 则 UE 1 开启用户面完整性保护并使用该算法标识所标识的完整性保护算法对用户面进行完整性保护。如果第一算法指示信息携带空值的用户面完整性保护算法的算法标识, 则 UE 1 不开启用户面完整性保护, 可选的, UE 1 不执行该空值的用户面完整性保护算法以节省计算资源。如果第一算法指示信息携带非空值的用户面机密性保护算法的算法标识, 则 UE 1 开启用户面机密性保护并使用该算法标识所标识的机密性保护算法对用户面进行机密性保护。如果第一算法指示信息携带空值的用户面机密性保护算法的算法标识, 则 UE 1 不开启用户面机密性保护, 可选的, UE 1 不执行该空值的用户面机密性保护算法以节省计算资源。

在另一种实现方式中, 第一算法指示信息只在用户面机密性保护开启情况下包括非空值的用户面机密性保护算法的算法标识。第一算法指示信息只在用户面完整性保护开启情况下包括非空值的用户面完整性保护算法的算法标识。

在此种实现方式中, 如果第一算法指示信息只携带用户面机密性保护算法的算法标识, 则 UE 1 默认用户面完整性保护不开启, UE 1 默认用户面机密性保护开启并使用该算法标识所标识的机密性保护算法对用户面进行机密性保护。如果第一算法指示信息只携带用户面完整性保护算法的算法标识, 则 UE 1 默认用户面机密性保护不开启, UE 1 默认用户面完整性保护开启并使用该算法标识所标识的完整性保护算法对用户面进行完整性保护。

在此种实现方式中, 如果第一算法指示信息只携带用户面机密性保护算法的算法标识, 则 UE 1 默认用户面完整性保护不开启, UE 1 默认用户面机密性保护开启并使用该算法标识所标识的机密性保护算法对用户面进行机密性保护。如果第一算法指示信息只携带用户面完整性保护算法的算法标识, 则 UE 1 默认用户面机密性保护不开启, UE 1 默认用户面完整性保护开启并使用该算法标识所标识的完整性保护算法对用户面进行完整性保护。

进一步的, UE 1 可在确定出用户面机密性保护开启的情况下, 生成机密性保护密钥; 若确定出用户面机密性保护不开启, 则不生成机密性保护密钥, 可选的, 不执行对应的空值机密性保护算法以节省计算资源。UE 1 在确定用户面完整性保护开启的情况下, 生成完整性保护密钥; 若确定出用户面完整性保护不开启, 则不生成完整性保护密钥, 可选的, 不执行对应的空值完整性保护算法以节省计算资源。

UE 1 在确定用户面安全算法以及用户面安全保护方式的情况下, 根据机密性保护密钥和/或完整性保护密钥, 对第一用户面数据进行安全保护, 对第二用户面数据进行解安全保护。第一用户面数据指的是 UE 1 向 UE 2 发送的用户面数据, 第二用户面数据指的是 UE 2 向 UE 1 发送的用户面数据。

在图 5 所示的实施例中, 第二算法指示信息既用于指示控制面安全算法, 又用于指示控制面安全保护方式; 第一算法指示信息既用于指示用户面安全算法, 又用于指示用户面安全保护方式。通过第一算法指示信息指示用户面采用何种机密性保护算法, 并指示用户面安全

保护方式，在节省信令开销的同时，可以有效的对用户面数据进行机密性保护。

请参见图 6，为本申请实施例三提供的确定用户面安全算法的方法的流程示意图，图 6 所示流程中与图 4 或图 5 相同或类似部分，可参见图 4 和图 5 所示实施例中相应的描述，该流程可包括但不限于如下步骤：

步骤 601，UE 1 向 UE 2 发送直连通信请求消息。相应的，UE 2 接收来自 UE 1 的直连通信请求消息。

可选的，步骤 601 也可作为 UE 1 向 UE 2 发送的直连密钥更新请求 (direct rekeying request) 消息，相应的，UE 2 接收来自 UE 1 的直连密钥更新请求。此时该消息不包含 UE 1 的控制面安全策略。

步骤 601 的具体实现过程可参见图 4 所示实施例中步骤 401 的具体描述，在此不再赘述。

步骤 602，UE 2 确定与 UE 1 之间的控制面安全保护方式，并生成控制面安全开启指示信息。

步骤 602 与步骤 402 的不同之处在于，步骤 602 在确定控制面安全保护方式的情况下，生成与控制面安全保护方式匹配的控制面安全开启指示信息，用于指示 UE 1 是否开启控制面完整性保护以及是否开启控制面机密性保护。

例如，控制面安全保护方式为控制面完整性保护开启和控制面机密性保护不开启，那么控制面安全开启指示信息用于指示 UE 1 开启控制面完整性保护和不开启控制面机密性保护。

步骤 603，UE 2 选择安全算法，完整性保护算法和机密性保护算法均为非空值。

UE 2 根据 UE 1 和 UE 2 的安全能力，从支持的完整性保护算法列表选择一个非空值的完整性保护算法，从支持的机密性保护算法列表选择一个非空值的机密性保护算法。

需要说明的是，步骤 603 选择完整性保护算法是基于完整性保护开启，选择机密性保护算法是基于机密性保护开启，与步骤 602 确定的控制面安全保护方式无关。

本申请不限定步骤 602 与步骤 603 执行的先后顺序，可以同时执行，也可以先执行步骤 602 再执行步骤 603，或先执行步骤 603 再执行步骤 602。

可选的，步骤 604，UE 1 和 UE 2 获取共享密钥。共享密钥即 K_{NRP} 。

步骤 604 的具体实现过程可参见图 4 所示实施例中步骤 403 的具体描述，在此不再赘述。

步骤 605，UE 2 向 UE 1 发送直连安全模式命令消息。相应的，UE 1 接收来自 UE 2 的直连安全模式命令消息。

其中，直连安全模式命令消息包括控制面安全开启指示信息和第三算法指示信息，第三算法指示信息用于指示步骤 603 选择的安全算法，包括非空值的完整性保护算法的算法标识以及非空值的机密性保护算法的算法标识。

其中，如果控制面安全开启指示信息指示控制面完整性和/或机密性保护不开启，则默认选择空值的完整性算法和/或空值的机密性保护算法，可选的，也可不选择和执行完整性保护算法和/或机密性保护算法。第三算法指示信息中包括的非空值完整性保护算法的算法标识用于指示在控制面和/或用户面完整性保护开启时使用的完整性保护算法。非空值机密性保护算法的算法标识用于在指示在控制面和/或用户面完整性保护开启时使用的完整性保护算法。

可选的，直连安全模式命令消息还包括 UE 2 生成的随机数 2，随机数 2 可用于生成完整性保护密钥和/或机密性保护密钥。

可选的，UE 2 存储第三算法指示信息。

步骤 606，UE 1 根据控制面安全开启指示信息确定与 UE 2 之间的控制面安全保护方式。基于控制面完整性保护开启的前提，UE 1 在接收到直连安全模式命令消息的情况下，根

据步骤 604 获取的共享密钥，对直连安全模式命令消息进行完整性保护验证。

在直连安全模式命令消息通过完整性保护验证的情况下，UE 1 根据控制面安全开启指示信息确定与 UE 2 之间的控制面安全保护方式，并根据第三算法指示信息进行控制面安全保护。具体的，如果 UE 1 接收到的控制面安全开启指示信息指示控制面完整性和/或机密性保护不开启，则默认选择空值的完整性算法和/或空值的机密性保护算法作为控制面完整性和/或控制面机密性保护算法，可选的，也可不选择和执行完整性保护算法和/或机密性保护算法。如果控制面安全开启指示信息指示控制面完整性保护开启，则使用第三算法指示信息中包括的非空值完整性保护算法的算法标识指示的完整性保护算法作为控制面完整性保护算法，对控制面进行完整性保护；如果控制面安全开启指示信息指示控制面机密性保护开启，则使用第三算法指示信息中包括的非空值机密性保护算法的算法标识指示的机密性保护算法作为控制面机密性保护算法，对控制面进行机密性保护。

例如，控制面安全开启指示信息用于指示开启控制面完整性保护和不开启控制面机密性保护，那么控制面安全保护方式为控制面完整性保护开启和控制面机密性保护不开启。UE 1 根据第三算法指示信息，采用非空值的完整性保护算法对信令进行完整性保护，默认采用空值的机密性保护算法，或不执行任何算法，不对信令进行机密性保护以节省计算资源。

再例如，控制面安全开启指示信息用于指示开启控制面完整性保护和开启控制面机密性保护，那么控制面安全保护方式为控制面完整性保护开启和控制面机密性保护开启。UE 1 根据第三算法指示信息，采用非空值的完整性保护算法对信令进行完整性保护，采用非空值的机密性保护算法对信令进行机密性保护。

可选的，UE 1 存储第三算法指示信息。

步骤 607，UE 1 向 UE 2 发送直连安全模式接受消息。相应的，UE 2 接收来自 UE 1 的直连安全模式接受消息。

其中，直连安全模式接受消息可包括 UE 1 的用户面安全策略，可以不包括 UE 1 的安全能力。

步骤 608，UE 2 确定与 UE 1 之间的用户面安全保护方式包括用户面机密性保护开启，并生成用户面安全开启指示信息。

步骤 608 的具体实现过程可参见图 4 所示实施例中步骤 407 的具体描述，在此不再赘述。

步骤 609，UE 2 向 UE 1 发送直连通信接受消息。相应的，UE 1 接收来自 UE 2 的直连通信接受消息。

可选的，步骤 609 也可作为 UE 2 向 UE 1 发送的直连密钥更新回复(direct rekeying Response)消息，相应的，UE 1 接收来自 UE 2 的直连密钥更新请求。

可选的，步骤 609 也可作为 UE 2 向 UE 1 发送的 RRC 连接重配置(RRC connection reconfiguration)消息，相应的，UE 1 接收来自 UE 2 的 RRC 连接重配置消息。

其中，直连通信接受消息包括用户面安全开启指示信息，用于指示 UE 1 是否开启用户面完整性保护以及是否开启用户面机密性保护。

步骤 610，UE 1 根据用户面安全开启指示信息确定与 UE 2 之间的用户面安全保护方式，根据第三算法指示信息确定用户面保护算法。

UE 1 在接收到直连通信接受消息的情况下，根据用户面安全开启指示信息，确定与 UE 2 之间的用户面安全保护方式；根据第三算法指示信息确定用户面保护算法。

具体的，如果 UE 1 接收到的用户面安全开启指示信息指示用户面完整性和/或机密性保护不开启，则默认选择空值的完整性保护算法和/或空值的机密性保护算法作为用户面完整性

和/或用户面机密性保护算法，可选的，也可不选择和执行完整性保护算法和/或机密性保护算法。如果用户面安全开启指示信息指示用户面完整性保护开启，则使用第三算法指示信息中包括的非空值完整性保护算法的算法标识指示的完整性保护算法作为用户面完整性保护算法，对用户面进行完整性保护；如果用户面安全开启指示信息指示用户面保护开启，则使用第三算法指示信息中包括的非空值机密性保护算法的算法标识指示的机密性保护算法作为用户面机密性保护算法，对用户面进行机密性保护。

例如，用户面安全保护方式为用户面完整性保护开启和用户面机密性保护开启，UE 1 根据第三算法指示信息所指示的非空值的完整性保护算法和非空值的机密性保护算法，对第一用户面数据进行完整性保护和机密性保护，从而实现对用户面数据的安全保护。

再例如，用户面安全保护方式为用户面完整性保护不开启和用户面机密性保护开启，UE 1 根据第三算法指示信息所指示的非空值的机密性保护算法，对第一用户面数据进行机密性保护，从而实现对用户面数据的安全保护。此时，可以不对第一用户面数据进行完整性保护，或默认使用空值的完整性保护算法进行完整性保护。

在图 6 所示的实施例，控制面安全开启指示信息用于指示控制面安全保护方式，用户面安全开启指示信息用于指示用户面安全保护方式，在完整性保护和/或机密性保护开启的情况下，根据第三算法指示信息选择相应的非空值的安全算法进行相应的安全保护，从而可以实现控制面安全保护和用户面安全保护。

图 4-图 6 所示的实施例以 PC5 通信建立流程为例进行介绍，本申请也可以应用于 PC5 通信直连密钥更新流程。在 PC5 通信直连密钥更新流程中，直连通信请求消息可替换为直连密钥更新请求消息，直连通信接受消息可替换为直连密钥更新回复消息。

本申请也可以应用于 Uu 通信。在应用于 Uu 通信时，图 4-图 6 中的 UE 2 可替换为接入网设备或基站，直连通信请求消息可替换为连接建立请求消息，直连安全模式命令消息可替换为接入层安全模式命令消息，直连安全模式完成消息可替换为接入层安全模式完成消息，直连通信接受消息可替换为 RRC 连接重配置消息。

本申请还可以应用于非接入层（non access stratum，NAS）安全保护的流程，例如 UE 与 AMF 网元之间的安全保护。在应用于 NAS 安全保护的流程时，图 4-图 6 中的 UE2 可替换为核心网设备，直连通信请求消息可替换为连接建立请求消息，直连安全模式命令消息可以替换为非接入层安全模式命令消息，直连安全模式完成消息可替换为非接入层安全模式完成消息，直连通信接受消息可替换为 RRC 连接重配置消息。

相应于上述方法实施例给出的方法，本申请实施例还提供了相应的装置，包括用于执行上述实施例相应的模块。所述模块可以是软件，也可以是硬件，或者是软件和硬件结合。

请参见图 7，为本申请提供的一种通信装置的结构示意图。

请参见图 7，为本申请提供的一种通信装置的结构示意图。图 7 所示的通信装置 700 包括收发模块 701 和处理模块 702。

在一种设计中，装置 700 为第二设备：

示例性的，处理模块 702，用于在第二设备与第一设备之间用户面机密性保护开启且与第一设备之间控制面机密性保护不开启的情况下，根据第一设备的安全能力和第二设备的安全能力，选择非空值的用户面机密性保护算法；

收发模块 701，用于向第一设备发送第一消息，第一消息包括用于指示用户面机密性保护算法的第一算法指示信息。

该示例用于实现图 4-图 6 所示实施例中 UE 2 的功能。

在一种设计中，装置 700 为第一设备：

示例性的，收发模块 701，用于向第二设备发送第三消息，第三消息包括第一设备的控制面安全策略和第一设备的安全能力；接收来自第二设备的第四消息，第四消息包括用于指示空值的控制面机密性保护算法的指示信息；向第二设备发送第二消息，第二消息包括第一设备的用户面安全策略；接收来自第二设备的第一消息，第一消息包括用于指示非空值的用户面机密性保护算法的第一算法指示信息；

处理模块 702，用于根据第一算法指示信息指示的用户面机密性保护算法，对与第二设备之间的用户面数据进行机密性保护。

该示例用于实现图 4-图 6 所示实施例 UE 1 的功能。

请参见图 8，为本申请提供的另一种通信装置的结构示意图。图 8 所示的通信装置 800 包括至少一个处理器 801、存储器 802，可选的，还可包括通信接口 803。

存储器 802 可以是易失性存储器，例如随机存取存储器；存储器也可以是非易失性存储器，例如只读存储器，快闪存储器，硬盘（hard disk drive，HDD）或固态硬盘（solid-state drive，SSD）、或者存储器 802 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其他介质，但不限于此。存储器 802 可以是上述存储器的组合。

本申请实施例中不限定上述处理器 801 以及存储器 802 之间的具体连接介质。本申请实施例在图中以存储器 802 和处理器 801 之间通过总线 804 连接，总线 804 在图中以粗线表示，其它部件之间的连接方式，仅是进行示意性说明，并不引以为限。该总线 804 可以分为地址总线、数据总线、控制总线等。为便于表示，图 8 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。

处理器 801 可以具有数据收发功能，能够与其他设备进行通信，在如图 8 装置中，也可以设置独立的数据收发模块，例如通信接口 803，用于收发数据；处理器 801 在与其他设备进行通信时，可以通过通信接口 803 进行数据传输。

一种示例中，当第二设备采用图 8 所示的形式时，图 8 中的处理器可以通过调用存储器 802 中存储的计算机执行指令，使得 UE 1 执行上述任一方法实施例中的 UE 2 执行的方法。

一种示例中，当第一设备采用图 8 所示的形式时，图 8 中的处理器可以通过调用存储器 802 中存储的计算机执行指令，使得 UE 1 执行上述任一方法实施例中的 UE 1 执行的方法。

具体的，图 7 的处理模块和收发模块的功能/实现过程均可以通过图 8 中的处理器 801 调用存储器 802 中存储的计算机执行指令来实现。或者，图 7 的处理模块的功能/实现过程可以通过图 8 中的处理器 801 调用存储器 802 中存储的计算机执行指令来实现，图 7 的收发模块的功能/实现过程可以通过图 8 中的通信接口 803 来实现。

本申请实施例还提供一种通信系统，该系统可以包括图 4-图 6 中的 UE 1 和 UE 2。

可以理解的是，本申请实施例的一些可选的特征，在某些场景下，可以不依赖于其他特征，比如其当前所基于的方案，而独立实施，解决相应的技术问题，达到相应的效果，也可以在某些场景下，依据需求与其他特征进行结合。相应的，本申请实施例中给出的装置也可以相应的实现这些特征或功能，在此不予赘述。

本领域技术人员还可以理解到本申请实施例列出的各种说明性逻辑块（illustrative logical block）和步骤（step）可以通过电子硬件、电脑软件，或两者的结合进行实现。这样的功能是通过硬件还是软件来实现取决于特定的应用和整个系统的设计要求。本领域技术人员对于相应的应用，可以使用各种方法实现所述的功能，但这种实现不应被理解为超出本申请实施例保护的范围。

本申请所描述的方案可通过各种方式来实现。例如，这些技术可以用硬件、软件或者硬件结合的方式来实现。对于硬件实现，用于在通信装置（例如，基站，终端、网络实体、核心网网元或芯片）处执行这些技术的处理单元，可以实现在一个或多个通用处理器、数字信号处理器(digital signal processor, DSP)、数字信号处理器件、专用集成电路(application specific integrated circuit, ASIC)、可编程逻辑器件、现场可编程门阵列(field programmable gate array, FPGA)、或其它可编程逻辑装置，离散门或晶体管逻辑，离散硬件部件，或上述任何组合中。通用处理器可以为微处理器，可选地，该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现，例如数字信号处理器和微处理器，多个微处理器，一个或多个微处理器联合一个数字信号处理器核，或任何其它类似的配置来实现。

可以理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器(read-only memory, ROM)、可编程只读存储器(programmable ROM, PROM)、可擦除可编程只读存储器(erasable PROM, EPROM)、电可擦除可编程只读存储器(electrically EPROM, EEPROM)或闪存。易失性存储器可以是随机存取存储器(random access memory, RAM)，其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的RAM可用，例如静态随机存取存储器(static RAM, SRAM)、动态随机存取存储器(dynamic RAM, DRAM)、同步动态随机存取存储器(synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器(double data rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器(enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器(synchlink DRAM, SLD RAM)和直接内存总线随机存取存储器(direct rambus RAM, DR RAM)。应注意，本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

本申请还提供了一种计算机可读介质，其上存储有计算机程序，该计算机程序被计算机执行时实现上述任一方法实施例的功能。

本申请还提供了一种计算机程序产品，该计算机程序产品被计算机执行时实现上述任一方法实施例的功能。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机指令时，全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一个计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线(digital subscriber line, DSL)）或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质（例如，软盘、硬盘、磁带）、光介质（例如，高密度数字视频光盘(digital video disc, DVD)）、或者半导体介质（例如，固态硬盘(solid state disk, SSD)）等。

可以理解，说明书通篇中提到的“实施例”意味着与实施例有关的特定特征、结构或特性包括在本申请的至少一个实施例中。因此，在整个说明书各个实施例未必一定指相同的实施例。此外，这些特定的特征、结构或特性可以任意适合的方式结合在一个或多个实施例中。

可以理解，在本申请的各种实施例中，上述各过程的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

可以理解，在本申请中，“当...时”、“若”以及“如果”均指在某种客观情况下装置会做出相应的处理，并非是限定时间，且也不要求装置实现时一定要有所判断的动作，也不意味着存在其它限定。

本申请中对于使用单数表示的元素旨在用于表示“一个或多个”，而并非表示“一个且仅一个”，除非有特别说明。本申请中，在没有特别说明的情况下，“至少一个”旨在用于表示“一个或者多个”，“多个”旨在用于表示“两个或两个以上”。

另外，本文中术语“系统”和“网络”在本文中常被可互换使用。本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况，其中 A 可以是单数或者复数，B 可以是单数或者复数。

本申请中的预定义可以理解为定义、预先定义、存储、预存储、预协商、预配置、固化、或预烧制。

本领域普通技术人员可以理解，为描述的方便和简洁，上述描述的系统、装置和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

本申请中各个实施例之间相同或相似的部分可以互相参考。在本申请中各个实施例、以及各实施例中的各个实施方式/实施方法/实现方法中，如果没有特殊说明以及逻辑冲突，不同的实施例之间、以及各实施例中的各个实施方式/实施方法/实现方法之间的术语和/或描述具有一致性、且可以相互引用，不同的实施例、以及各实施例中的各个实施方式/实施方法/实现方法中的技术特征根据其内在的逻辑关系可以组合形成新的实施例、实施方式、实施方法、或实现方法。以上所述的本申请实施方式并不构成对本申请保护范围的限定。

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

权 利 要 求 书

1.一种确定用户面安全算法的方法，其特征在于，包括：

第二终端 UE 2 接收来自第一终端 UE 1 的直连通信请求消息，其中，所述直连通信请求消息包括所述 UE1 的安全能力和所述 UE1 的控制面安全策略；

所述 UE2 根据所述 UE 1 的控制面安全策略和所述 UE 2 的控制面安全策略，确定与 UE 1 之间的控制面安全保护方式；

在所述控制面安全保护方式为控制面完整性保护开启且控制面机密性保护不开启的情况下，所述 UE2 向所述 UE1 发送直连安全模式命令消息，且在所述 UE2 接收来自所述 UE1 的携带所述 UE1 的用户面安全策略的直连安全模式完成消息时，则所述 UE2 不管所述 UE1 的用户面安全策略和所述 UE2 的用户面安全策略，确定与所述 UE1 之间的用户面机密性保护不开启；

其中，所述直连安全模式命令消息包括非空值的完整性保护算法和空值的机密性保护算法。

2.根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述 UE2 根据所述 UE2 的安全能力和所述 UE1 的安全能力，选择所述非空值的完整性保护算法和所述空值的机密性保护算法。

3.一种确定用户面安全算法的方法，其特征在于，包括：

第一终端 UE 1 向第二终端 UE 2 发送直连通信请求消息，其中，所述直连通信请求消息包括所述 UE1 的安全能力和所述 UE1 的控制面安全策略；

所述 UE1 接收来自所述 UE2 的直连安全模式命令消息，所述直连安全模式命令消息包括非空值的完整性保护算法和空值的机密性保护算法；

所述直连安全模式命令消息是所述 UE2 根据所述 UE1 的控制面安全策略和所述 UE2 的控制面安全策略，确定控制面安全保护方式为控制面完整性保护开启且控制面机密性保护不开启的情况下发送的；

所述 UE1 根据所述非空值的完整性保护算法和空值的机密性保护算法，向所述 UE2 发送携带所述 UE1 的用户面安全策略的直连安全模式完成消息，其中，所述直连安全模式完成消息包括所述 UE1 的用户面安全策略。

4.一种确定用户面安全算法的方法，其特征在于，包括：

在第二设备与第一设备之间用户面机密性保护开启且与所述第一设备之间控制面机密性保护不开启的情况下，所述第二设备根据所述第一设备的安全能力和所述第二设备的安全能力，选择非空值的用户面机密性保护算法；

所述第二设备向所述第一设备发送第一消息，所述第一消息包括用于指示所述用户面机密性保护算法的第一算法指示信息。

5.根据权利要求 4 所述的方法，其特征在于，所述第一消息还包括用于指示开启所述第二设备与所述第一设备之间用户面机密性保护的指示信息。

6.根据权利要求 4 或 5 所述的方法，其特征在于，所述方法还包括：

所述第二设备接收来自所述第一设备的第二消息，所述第二消息包括所述第一设备的用户面安全策略；

所述第二设备根据所述第一设备的用户面安全策略和所述第二设备的用户面安全策略，确定与所述第一设备之间用户面机密性保护开启。

7.根据权利要求 6 所述的方法，其特征在于，在所述第二设备接收来自所述第一设备的第二消息之前，所述方法还包括：

所述第二设备接收来自所述第一设备的第三消息，所述第三消息包括所述第一设备的控制面安全策略和所述第一设备的安全能力；

所述第二设备根据所述第一设备的控制面安全策略和所述第二设备的控制面安全策略，确定与所述第一设备之间控制面机密性保护不开启。

8.根据权利要求 7 所述的方法，其特征在于，所述方法还包括：

所述第二设备向所述第一设备发送第四消息，所述第四消息包括用于指示空值的控制面机密性保护算法的指示信息。

9.根据权利要求 7 或 8 所述的方法，其特征在于，所述方法还包括：

所述第二设备保存所述第一设备的安全能力。

10.一种确定用户面安全算法的方法，其特征在于，包括：

第一设备向第二设备发送第三消息，所述第三消息包括所述第一设备的控制面安全策略和所述第一设备的安全能力；

所述第一设备接收来自所述第二设备的第四消息，所述第四消息包括用于指示空值的控制面机密性保护算法的指示信息；

所述第一设备向所述第二设备发送第二消息，所述第二消息包括所述第一设备的用户面安全策略；

所述第一设备接收来自所述第二设备的第一消息，所述第一消息包括用于指示非空值的用户面机密性保护算法的第一算法指示信息；

所述第一设备根据所述第一算法指示信息指示的所述用户面机密性保护算法，对与所述第二设备之间的用户面数据进行机密性保护。

11.根据权利要求 10 所述的方法，其特征在于，所述第一消息还包括用于指示开启所述第二设备与所述第一设备之间用户面机密性保护的指示信息。

12.根据权利要求 10 或 11 所述的方法，其特征在于，所述第四消息还包括用于指示控制面完整性保护算法的指示信息；

在所述第一设备根据所述第一算法指示信息指示的所述用户面机密性保护算法，对与所述第二设备之间的用户面数据进行机密性保护之前，所述方法还包括：

所述第一设备根据控制面完整性保护算法的指示信息指示的控制面完整性保护算法，开启与所述第二设备之间的控制面完整性保护；

所述第一设备对所述第一消息进行完整性验证；

在对所述第一消息验证通过的情况下，所述第一设备根据所述第一算法指示信息指示的所述用户面机密性保护算法，开启与所述第二设备之间的用户面机密性保护。

13.一种通信装置，其特征在于，包括：

收发模块，用于接收来自第一终端 UE 1 的直连通信请求消息，其中，所述直连通信请求消息包括所述 UE1 的安全能力和所述 UE1 的控制面安全策略；

处理模块，用于根据所述 UE 1 的控制面安全策略和所述通信装置的控制面安全策略，确定与 UE 1 之间的控制面安全保护方式；

所述收发模块，还用于在所述控制面安全保护方式为控制面完整性保护开启且控制面机密性保护不开启的情况下，向所述 UE1 发送直连安全模式命令消息，且在所述收发模块接收来自所述 UE1 的携带所述 UE1 的用户面安全策略的直连安全模式完成消息时，所述处理模块还用于不管所述 UE1 的用户面安全策略和所述通信装置的用户面安全策略，确定与所述 UE1 之间的用户面机密性保护不开启；

其中，所述直连安全模式命令消息包括非空值的完整性保护算法和空值的机密性保护算法。

14.根据权利要求 13 所述的通信装置，其特征在于，

所述处理模块，还用于根据所述通信装置的安全能力和所述 UE1 的安全能力，选择所述非空值的完整性保护算法和所述空值的机密性保护算法。

15.一种通信装置，其特征在于，包括：

收发模块，用于向第二终端 UE 2 发送直连通信请求消息，其中，所述直连通信请求消息包括所述通信装置的安全能力和所述通信装置的控制面安全策略；

所述收发模块，还用于接收来自所述 UE2 的直连安全模式命令消息，所述直连安全模式命令消息包括非空值的完整性保护算法和空值的机密性保护算法；

所述直连安全模式命令消息是所述 UE2 根据所述通信装置的控制面安全策略和所述 UE2 的控制面安全策略，确定控制面安全保护方式为控制面完整性保护开启且控制面机密性保护不开启的情况下发送的；

所述收发模块，还用于根据所述非空值的完整性保护算法和空值的机密性保护算法，向所述 UE2 发送携带所述通信装置的用户面安全策略的直连安全模式完成消息，其中，所述直连安全模式完成消息包括所述通信装置的用户面安全策略。

16.一种通信装置，其特征在于，所述装置包括处理模块和收发模块；

所述处理模块，用于在通信装置与第一设备之间用户面机密性保护开启且与所述第一设备之间控制面机密性保护不开启的情况下，所述通信装置根据所述第一设备的安全能力和所述通信装置的安全能力，选择非空值的用户面机密性保护算法；

所述收发模块，用于向所述第一设备发送第一消息，所述第一消息包括用于指示所述用户面机密性保护算法的第一算法指示信息。

17.根据权利要求 16 所述的通信装置，其特征在于，所述第一消息还包括用于指示开启

所述通信装置与所述第一设备之间用户面机密性保护的指示信息。

18.根据权利要求 16 或 17 所述的通信装置，其特征在于，

所述收发模块，还用于接收来自所述第一设备的第二消息，所述第二消息包括所述第一设备的用户面安全策略；

所述处理模块，还用于根据所述第一设备的用户面安全策略和所述通信装置的用户面安全策略，确定与所述第一设备之间用户面机密性保护开启。

19.根据权利要求 18 所述的通信装置，其特征在于，

所述收发模块，还用于在所述通信装置接收来自所述第一设备的第二消息之前，接收来自所述第一设备的第三消息，所述第三消息包括所述第一设备的控制面安全策略和所述第一设备的安全能力；

所述处理模块，还用于根据所述第一设备的控制面安全策略和所述通信装置的控制面安全策略，确定与所述第一设备之间控制面机密性保护不开启。

20.根据权利要求 19 所述的通信装置，其特征在于，

所述收发模块，还用于向所述第一设备发送第四消息，所述第四消息包括用于指示空值的控制面机密性保护算法的指示信息。

21.根据权利要求 19 或 20 所述的通信装置，其特征在于，

所述处理模块，还用于保存所述第一设备的安全能力。

22.一种通信装置，其特征在于，包括处理模块和收发模块；

所述收发模块，用于向第二设备发送第三消息，所述第三消息包括所述通信装置的控制面安全策略和所述通信装置的安全能力；

所述收发模块，还用于接收来自所述第二设备的第四消息，所述第四消息包括用于指示空值的控制面机密性保护算法的指示信息；

所述收发模块，还用于向所述第二设备发送第二消息，所述第二消息包括所述通信装置的用户面安全策略；

所述收发模块，还用于接收来自所述第二设备的第一消息，所述第一消息包括用于指示非空值的用户面机密性保护算法的第一算法指示信息；

所述处理模块，用于根据所述第一算法指示信息指示的所述用户面机密性保护算法，对与所述第二设备之间的用户面数据进行机密性保护。

23.根据权利要求 22 所述的通信装置，其特征在于，所述第一消息还包括用于指示开启所述第二设备与所述通信装置之间用户面机密性保护的指示信息。

24.根据权利要求 22 或 23 所述的通信装置，其特征在于，所述第四消息还包括用于指示控制面完整性保护算法的指示信息；

所述处理模块，还用于在根据所述第一算法指示信息指示的所述用户面机密性保护算法，对与所述第二设备之间的用户面数据进行机密性保护之前，根据控制面完整性保护算法的指

示信息指示的控制面完整性保护算法，开启与所述第二设备之间的控制面完整性保护；

所述处理模块，还用于对所述第一消息进行完整性验证；

所述处理模块，还用于在对所述第一消息验证通过的情况下，根据所述第一算法指示信息指示的所述用户面机密性保护算法，开启与所述第二设备之间的用户面机密性保护。

25.一种通信装置，其特征在于，包括：处理器，所述处理器与存储器耦合，所述存储器用于存储程序或指令，当所述程序或指令被所述处理器执行时，使得所述装置执行如权利要求 1 至 12 中任一项所述的方法。

26.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，所述计算机程序被执行时使得计算机执行如权利要求 1 至 12 中任一项所述的方法。

27.一种通信系统，其特征在于，包括第一设备和第二设备；

所述第二设备，用于在所述第二设备与所述第一设备之间用户面机密性保护开启且与所述第一设备之间控制面机密性保护不开启的情况下，根据所述第一设备的安全能力和所述第二设备的安全能力，选择非空值的用户面机密性保护算法；向所述第一设备发送第一消息，所述第一消息包括用于指示所述用户面机密性保护算法的第一算法指示信息；

所述第一设备，用于接收所述第一消息。

28.根据权利要求 27 所述的系统，其特征在于，所述第一消息还包括用于指示开启所述第二设备与所述第一设备之间用户面机密性保护的指示信息。

29.根据权利要求 27 或 28 所述的系统，其特征在于，

所述第一设备，还用于向所述第二设备发送第二消息，所述第二消息包括所述第一设备的用户面安全策略；

所述第二设备，还用于根据所述第一设备的用户面安全策略和所述第二设备的用户面安全策略，确定与所述第一设备之间用户面机密性保护开启。

30.根据权利要求 27 所述的系统，其特征在于，

所述第一设备，还用于向所述第二设备发送第三消息，所述第三消息包括所述第一设备的控制面安全策略和所述第一设备的安全能力；

所述第二设备，还用于根据所述第一设备的控制面安全策略和所述第二设备的控制面安全策略，确定与所述第一设备之间控制面机密性保护不开启；向所述第一设备发送第四消息，所述第四消息包括用于指示空值的控制面机密性保护算法的指示信息。

31.根据权利要求 29 所述的系统，其特征在于，

所述第二设备，还用于保存所述第一设备的安全能力。

32.根据权利要求 29 所述的系统，其特征在于，所述第四消息还包括用于指示控制面完整性保护算法的指示信息；

所述第一设备，还用于根据控制面完整性保护算法的指示信息指示的控制面完整性保护

算法，开启与所述第二设备之间的控制面完整性保护；对所述第一消息进行完整性验证；在对所述第一消息验证通过的情况下，根据所述第一算法指示信息指示的所述用户面机密性保护算法，开启与所述第二设备之间的用户面机密性保护。

33.一种通信系统，其特征在于，包括第一终端 UE 1 和第二终端 UE 2：

所述 UE 1，用于向所述 UE 2 发送直连通信请求消息，其中，所述直连通信请求消息包括所述 UE1 的安全能力和所述 UE1 的控制面安全策略；

所述 UE 2，用于接收所述直连通信请求消息；

所述 UE 2，还用于根据所述 UE 1 的控制面安全策略和所述 UE 2 的控制面安全策略，确定与 UE 1 之间的控制面安全保护方式；以及，在所述控制面安全保护方式为控制面完整性保护开启且控制面机密性保护不开启的情况下，向所述 UE 1 发送直连安全模式命令消息；

其中，所述直连安全模式命令消息包括非空值的完整性保护算法和空值的机密性保护算法；

所述 UE 1，还用于接收所述直连安全模式命令消息，以及，根据所述非空值的完整性保护算法和空值的机密性保护算法，向所述 UE 2 发送携带所述 UE 1 的用户面安全策略的直连安全模式完成消息，其中，所述直连安全模式完成消息包括所述 UE 1 的用户面安全策略；

所述 UE 2，还用于在接收来自所述 UE 1 的携带所述 UE 1 的用户面安全策略的直连安全模式完成消息时，不管所述 UE 1 的用户面安全策略和所述 UE 2 的用户面安全策略，确定与所述 UE 1 之间的用户面机密性保护不开启。

34.根据权利要求 33 所述的系统，其特征在于，

所述 UE 2，还用于根据所述 UE 2 的安全能力和所述 UE 1 的安全能力，选择所述非空值的完整性保护算法和所述空值的机密性保护算法。