(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
2017 年 7 月 13 日 (13.07.2017)

WIPO | PCT

(10) 国际公布号
WO 2017/117775 A1

(51) 国际专利分类号:
H04W 12/04 (2009.01)

(21) 国际申请号: PCT/CN2016/070379

(22) 国际申请日: 2016 年 1 月 7 日 (07.01.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(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: **应江威 (YING, Jiangwei)**; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: **深圳市深佳知识产权代理事务所（普通合伙） (SHENPAT INTELLECTUAL PROPERTY AGENCY)**; 中国广东省深圳市国贸大厦 15 楼西座 1521 室, Guangdong 518014 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则 4.17 的声明:
— 关于申请人有权申请并被授予专利(细则 4.17(ii))

本国际公布:
— 包括国际检索报告(条约第 21 条(3))。

(54) **Title**: COMMUNICATION SECURITY PROCESSING METHOD AND SYSTEM AND RELEVANT DEVICE

(54) **发明名称** : 一种通信安全处理方法、系统及相关设备

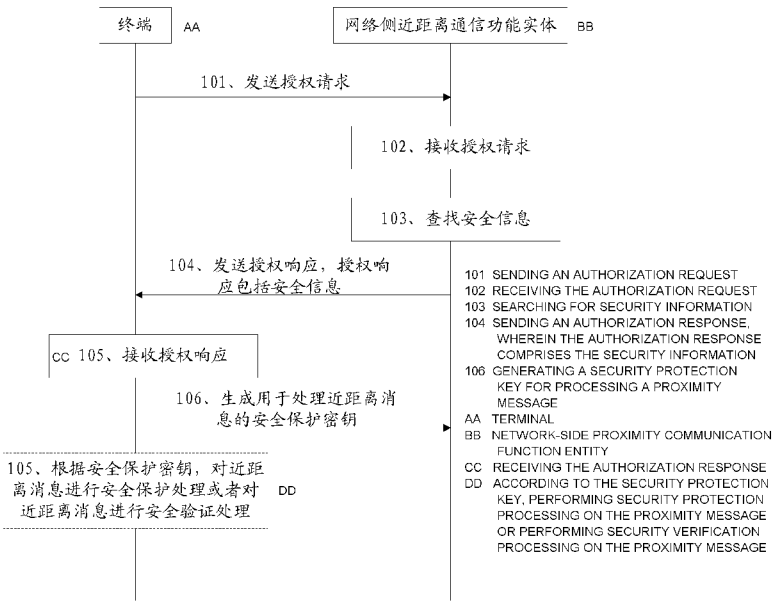

图 1a

(57) **Abstract**: A communication security processing method and system and a relevant device, for improving communication security, and especially for communication security in a talk-around mode. Some method embodiments provided in the present invention can comprise: the terminal sending an authorization request to a network-side proximity communication function entity, wherein the authorization request contains identifier information about the terminal, the authorization request is used to request security information about the terminal from the network-side proximity communication function entity, the security information comprises a group identifier, a group key and a group key identifier, the group identifier is used to indicate a group where the terminal belongs, and the group key identifier is used to indicate the group key; the terminal receiving an authorization response sent by the network-side proximity communication function entity, wherein the authorization response comprises the security information about the terminal; and the terminal generating, according to the security information about the terminal, a security protection key for processing a proximity message.

(57) **摘要**:

[见续页]

WO 2017/117775 A1

一种通信安全处理方法、系统及相关设备，用于提高通信安全，尤其是脱网模式下的通信安全。本发明提供的一些方法实施例，可包括:所述终端向网络侧近距离通信功能实体发送授权请求，所述授权请求包含所述终端的标识信息，所述授权请求用于向所述网络侧近距离通信功能实体请求所述终端的安全信息，所述安全信息包括群组标识、组密钥和组密钥标识，所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥；所述终端接收所述网络侧近距离通信功能实体发送的授权响应，所述授权响应包括所述终端的安全信息；所述终端根据所述终端的安全信息，生成用于处理近距离消息的安全保护密钥。

一种通信安全处理方法、系统及相关设备

技术领域

本发明涉及通信技术领域，具体涉及一种通信安全处理方法、系统及相关设备。

背景技术

随着智能移动终端中社交类应用的推广，近距离服务（Proximity Service）被广泛应用到人们生活和工作中，并给人们生活和工作带来更多便利，例如，通过近距离服务查找附近感兴趣的服务（如住宿、餐馆、运动馆等）。第三代合作伙伴计划（3rd Generation Partnership Project，简称 3GPP）提出的长期演进（Long Term Evolution，简称 LTE）网络架构中引入的设备到设备（Device to Device，简称 D2D）通信是实现近距离服务的一种通信技术。D2D 技术提供了发现和通信两种功能。其中，发现是指网络侧近距离通信功能实体为具有 D2D 能力的用户设备（User Equipment，简称 UE）分配近距离服务码（Proximity Service Code，简称 ProSe Code），广播 UE（Announcing UE，简称 A-UE）通过广播自己的近距离服务码来表明自己的存在，监测 UE（Monitoring UE，简称 M-UE）通过在空口上监听广播 UE 的近距离服务码，从而发现 A-UE，与 A-UE 建立连接，之后 A-UE 与 M-UE 可进行通信。

由于近距离服务码在很长一段时间内都不会改变，攻击者可以截获近距离服务码，并重播携带有该邻近业务码的发现消息来让 M-UE 发现它并与其建立通信，这样，攻击者就可以对接上来的 M-UE 进行伪造信息、非法获取 M-UE 信息等安全攻击，因此，在 D2D 技术中需要一套安全机制来防止这种安全威胁。

一种 D2D 技术的发现和通信方法中通过第一安全密钥来提高其安全性，例如，A-UE 向网络侧临近功能实体申请授权消息，授权消息包括近距离服务码、第一安全密钥、计时器值等，A-UE 根据第一安全密钥生成一个 MIC 验证值，然后基于该 MIC 对发现过程进行完整性保护。比如 A-UE 广播发现消息，在发现消息中携带近距离服务码、MIC 验证值和计时器值。M-UE 接收到发现消息后，将 MIC 验证值和计时器值发送给网络侧临近功能实体，由网络侧临

近功能实体进行MIC验证值的验证，网络侧临近功能实体验证成功后向M-UE返回验证响应，M-UE根据返回的成功验证MIC验证值的验证响应，与A-UE建立通信。

另外，在另一种D2D技术的通信方法中通过组密钥（ Group Keys，简称PGK）来提高通信内容的安全性。例如，UE1向网络侧临近功能实体申请密钥信息，网络侧临近功能实体返回密钥信息，密钥信息携带有PGK，UE1基于PGK广播发现消息和与UE2进行通信。

上述D2D发现和通信方案均在联网模式（运营商网络覆盖）下实现，如果D2D发现和通信是在脱网模式（无运营商网络覆盖）下，UE无法与网络侧临近功能实体进行连接以获得授权消息或密钥信息等，因此，联网模式下的安全机制无法在脱网模式下使用，进而，在脱网模式下D2D发现和通信仍然受到安全威胁。

发明内容

针对上述存在的技术缺陷，本发明实施例提供了一种通信安全处理方法、系统及相关设备，用于解决脱网模式下通信的安全问题。

本发明第一方面提供了一种通信安全处理方法，应用于终端，可包括:

上述终端向网络侧近距离通信功能实体发送授权请求，上述授权请求包含上述终端的标识信息，上述授权请求用于向上述网络侧近距离通信功能实体请求上述终端的安全信息，上述安全信息包括群组标识、组密钥和组密钥标识，上述群组标识用于指示上述终端所属的群组，上述组密钥标识用于指示上述组密钥;

上述终端接收上述网络侧近距离通信功能实体发送的授权响应，上述授权响应包括上述终端的安全信息;

上述终端根据上述终端的安全信息，生成用于处理近距离消息的安全保护密钥。

可以看出，在本发明实施例中终端向网络侧近距离通信功能实体请求到安全信息，那么，在终端不处于运营商的网络覆盖下时，终端还可以根据该安全信息生成安全保护密钥，利用该安全保护密钥对近距离消息进行处理，从而实现脱网模式下的通信安全性。其中，这里的处理包括对近距离消息的安全保护

处理或者安全验证处理。

可选地，上述安全信息还包括第一完整性保护算法标识、第二完整性保护算法标识、加密算法标识中的至少一种。需要说明，在本发明另一些实施例中，第一完整性保护算法标识、第二完整性保护算法标识、加密算法标识还可以由两个终端之间进行协商确定。

可选地，上述安全信息还包括发送终端的身份标识和上述接收终端的身份标识中的至少一种。

在本发明一些实施例中，上述终端根据上述终端的安全信息，生成用于处理近距离消息的安全保护密钥包括：上述终端根据密钥生成功能 KDF 算法、上述群组标识和上述组密钥，生成第一安全密钥；上述终端根据安全保护算法标识、上述 KDF 算法和上述第一安全密钥，生成安全保护密钥。其中，在终端中配置了 KDF 算法，安全信息进一步包括安全保护算法标识，当然，在本发明另一些实施例中，安全保护算法标识也可以由两个终端协商得到。

可选地，安全保护密钥可以是第一完整性保护密钥，或者加密密钥，或者第二完整性保护密钥。

在本发明一些实施例中，上述近距离消息为近距离发现消息，上述安全保护算法标识为第一完整性保护算法标识，上述第一完整性保护算法标识用于标识处理近距离发现消息的第一完整性保护算法；上述终端根据安全保护算法标识、上述 KDF 算法和上述第一安全密钥，生成上述安全保护密钥包括：上述终端根据上述第一完整性保护算法标识、上述 KDF 算法和上述第一安全密钥，生成第一完整性保护密钥，上述第一完整性保护密钥为上述安全保护密钥。可以看出，第一方面的一些实施例中，若近距离消息为近距离发现消息，进一步根据 KDF 算法、第一完整性保护算法标识和第一安全密钥生成了第一完整性保护密钥，从而利用第一完整性保护密钥对近距离发现消息进行完整性保护或者完整性的安全验证，以提高安全性。

在本发明一些实施例中，所述近距离消息为近距离通信消息，所述安全保护算法标识为加密密钥标识，所述加密密钥标识用于标识处理近距离通信消息的加密算法；所述终端根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，生成所述安全保护密钥包括：所述终端根据所述加密算法标识、所述

KDF 算法和所述第一安全密钥，生成加密密钥，所述加密密钥为所述安全保护密钥。可以看出，第一方面的一些实施例中，若近距离消息为近距离通信消息，进一步根据 KDF 算法、第一安全密钥和加密算法标识生成加密密钥，根据加密密钥对近距离通信消息进行加密保护或者解码的安全验证处理，提高安全性。

本发明一些实施例中，所述近距离消息为近距离通信消息，所述安全保护算法标识为第二完整性保护算法标识，所述第二完整性保护算法标识用于标识处理近距离通信消息的第二完整性保护算法；所述终端根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，生成所述安全保护密钥包括：所述终端根据所述第二完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，生成第二完整性保护密钥，所述第二完整性保护密钥为所述安全保护密钥。可以看出，第一方面的一些实施例中，若近距离消息为近距离通信消息，进一步根据 KDF 算法、第一安全密钥和第二完整性保护算法标识生成第二完整性保护密钥，根据第二完整性保护密钥对近距离通信消息进行安全保护处理或者安全验证处理，提高安全性。

在本发明实施例中，上述终端根据上述安全信息生成用于处理近距离消息的安全保护密钥之后包括：上述终端根据上述安全保护密钥，对上述近距离消息进行安全保护处理；或者，上述终端根据上述安全保护密钥，对上述近距离消息进行安全验证处理。

可选地，上述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

本发明第二方面提供了一种通信安全处理方法，应用于网络侧近距离通信功能实体，可包括：

上述网络侧近距离通信功能实体接收终端发送的授权请求，上述授权请求包括上述终端的标识信息；

上述网络侧近距离通信功能实体根据上述终端的标识信息，查找上述终端的安全信息，上述安全信息包括群组标识、组密钥和组密钥标识，上述群组标识用于指示上述终端所属的群组，上述组密钥标识用于指示上述组密钥，上述终端的安全信息用于生成处理近距离消息的安全保护密钥；

上述网络侧近距离通信功能实体向上述终端发送授权响应，上述授权响应包括上述终端的安全信息。

可以看出，在本发明实施例中，网络侧近距离通信功能实体根据终端发送的授权请求，查找到终端的安全信息，然后将安全信息返回给终端，以便终端不处于运营商网络覆盖下，也能完成实现安全通信。

在本发明一些实施例中，上述网络侧近距离通信功能实体根据上述终端的标识信息，查找上述终端的安全信息包括：上述网络侧近距离通信功能实体根据上述终端的标识信息，查找上述终端所属群组的授权信息，上述授权信息中包括上述终端所属群组的群组标识；上述网络侧近距离通信功能实体根据上述终端的标识信息和上述群组标识，查找上述群组标识所指示的群组的安全信息。

可选地，上述终端的安全信息还包括第一完整性保护算法标识、第二完整性保护算法标识和加密算法标识中的至少一种。

可选地，上述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

本发明第三方面提供了一种终端，可包括：

发送器，用于向网络侧近距离通信功能实体发送授权请求，上述授权请求包含上述终端的标识信息，上述授权请求用于向上述网络侧近距离通信功能实体请求上述终端的安全信息，上述安全信息包括群组标识、组密钥和组密钥标识，上述群组标识用于指示上述终端所属的群组，上述组密钥标识用于指示上述组密钥；

接收器，用于接收上述网络侧近距离通信功能实体发送的授权响应，上述授权响应包括上述终端的安全信息；

处理器，用于根据上述终端的安全信息，生成用于处理近距离消息的安全保护密钥。

在本发明一些实施例中，上述处理器具体用于，根据密钥生成功能 KDF 算法、上述群组标识和上述组密钥，生成第一安全密钥；根据安全保护算法标识、上述 KDF 算法和上述第一安全密钥，生成上述安全保护密钥。

在本发明一些实施例中，上述近距离消息为近距离发现消息时，上述安全

保护算法标识为第一完整性保护算法标识，上述第一完整性保护算法标识用于标识处理近距离发现消息的第一完整性保护算法，上述处理器进一步具体用于，根据上述第一完整性保护算法标识、上述 KDF 算法和上述第一安全密钥，生成第一完整性保护密钥，上述第一完整性保护密钥为上述安全保护密钥。

在本发明一些实施例中，上述近距离消息为近距离通信消息时，上述安全保护算法标识为加密密钥标识，上述加密密钥标识用于标识处理近距离通信消息的加密算法，上述处理器进一步具体用于，根据上述加密算法标识、上述 KDF 算法和上述第一安全密钥，生成加密密钥，上述加密密钥为上述安全保护密钥。

在本发明一些实施例中，在上述近距离消息为近距离通信消息，上述安全保护算法标识为第二完整性保护算法标识，上述第二完整性保护算法标识用于标识处理近距离通信消息的第二完整性保护算法，上述处理器进一步具体用于，根据上述第二完整性保护算法标识、上述 KDF 算法和上述第一安全密钥，生成第二完整性保护密钥，上述第二完整性保护密钥为上述安全保护密钥。

在本发明一些实施例中，上述处理器还用于，在根据上述安全信息生成用于处理近距离消息的安全保护密钥之后，根据上述安全保护密钥，对上述近距离消息进行安全保护处理；或者，根据上述安全保护密钥，对上述近距离消息进行安全验证处理。

可选地，上述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

本发明第四方面提供了一种网络侧近距离通信功能实体，可包括:

通信接口，用于接收终端发送的授权请求，上述授权请求包括上述终端的标识信息;

处理器，用于根据上述终端的标识信息，查找上述终端的安全信息，上述终端的安全信息包括群组标识、组密钥和组密钥标识，上述群组标识用于指示上述终端所属的群组，上述组密钥标识用于指示上述组密钥，上述终端的安全信息用于生成处理近距离消息的安全保护密钥;

上述通信接口还用于向上述终端发送授权响应，上述授权响应包括上述终端的安全信息。

在本发明一些实施例中，上述处理器具体用于，根据上述终端的标识信息，查找上述终端所属群组的授权信息，上述授权信息中包括上述终端所属群组的群组标识；根据上述终端的标识信息和上述群组标识，查找上述群组标识所指示的群组的安全信息。

可选地，上述安全信息还包括第一完整性保护算法标识、第二完整性保护算法标识和加密算法标识中的至少一种。

可选地，上述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

本发明第五方面提供了一种通信安全处理系统，可包括：

第三方面提供的终端以及第四方面提供的网络侧近距离功能实体。

附图说明

为了更清楚地说明本发明实施例的技术方案，下面将对实施例描述所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1a 为本发明实施例提供的通信安全处理方法的信令图；

图 1b 为本发明实施例提供的安全保护密钥的生成示意图；

图 2a 为本发明实施例提供的通信安全处理方法的另一信令图；

图 2b 为本发明实施例提供的通信安全处理方法的另一信令图；

图 3a 为本发明实施例提供的通信安全处理方法的另一信令图；

图 3b 为本发明实施例提供的发现密钥的生成示意图；

图 3c 为本发明实施例提供的第一完整性保护密钥的生成示意图；

图 3d 为本发明实施例提供的完整性保护的处理示意图；

图 4 为本发明实施例提供的通信安全处理方法的另一信令图；

图 5a 为本发明实施例提供的通信安全处理方法的另一信令图；

图 5b 为本发明实施例提供的通信密钥的生成示意图；

图 5c 为本发明实施例提供的加密密钥的生成示意图；

图 5d 为本发明另一实施例提供的完整性保护的处理示意图；

图 6 为本发明实施例提供的通信安全处理方法的另一信令图；

图 7 为本发明实施例提供的通信安全处理方法的另一信令图；

图 8 为本发明实施例提供的终端的结构示意图；

图 9 为本发明实施例提供的网络侧近距离功能实体的结构示意图；

图 10 为本发明实施例提供的通信安全处理系统的结构示意图；

图 11 为本发明另一实施例提供的终端的结构示意图。

具体实施方式

本发明实施例提供了一种通信安全处理方法，用于提高脱网模式下，通信的安全性。本发明实施例还提供了一种通信安全处理方法对应的系统、以及终端、网络侧近距离通信功能实体。

为使得本发明的发明目的、特征、优点能够更加的明显和易懂，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行描述，显然，下面所描述的实施例仅仅是本发明一部分实施例，而非全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

本发明的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”“第四”等是用于区别不同的对象，而不是用于描述特定顺序。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

本发明实施例应用于近距离服务中的 D2D 通信系统中，终端（User Equipment，简称 UE）与终端之间可以在处于运营商的网络覆盖下（即联网模式下）建立 D2D 通信，也可以在不处于运营商的网络覆盖下（即脱网模式下）建立 D2D 通信，在 D2D 通信之前，终端与终端可能先进行 D2D 发现过程，然后进行 D2D 通信；也可能终端与终端不发起 D2D 发现过程，而直接进行 D2D 通信。现有技术中，对于处于运营商的网络覆盖下的 D2D 发现和 D2D 通信都提供了安全保护策略，而对于不处于运营商的网络覆盖下的 D2D 发现和 D2D 通信，终端由于处于脱网模式下，无法从网络侧临近功能实体获得相关

信息对 D2D 发现和 D2D 通信进行安全保护，导致不处于运营商的网络覆盖下的 D2D 发现和 D2D 通信存在较大的安全问题。

本发明实施例用于解决终端不处于运营商的网络覆盖下的 D2D 发现和 D2D 通信的安全问题，以提高通信安全，当然，本发明实施例同样可以用在终端处于运营商的网络覆盖下的 D2D 发现和 D2D 通信的安全问题。在 D2D 发现中，终端通过广播发现消息，让同一群组的其它终端发现它，以便有通信需求和终端之间进行 D2D 通信；D2D 通信可能是一对多的通信，也可能是一对一的通信。群组可以是运营商根据业务类型等进行划分。

下面将以具体实施例，对本发明技术方案进行详细介绍。

请参阅图 1a，图 1a 为本发明实施例提供的通信安全处理方法的信令图。如图 1a 所示，一种通信安全处理方法可包括:

101、终端向网络侧近距离通信功能实体发送授权请求，所述授权请求包含所述终端的标识信息;

其中，所述授权请求用于向所述网络侧近距离通信功能实体请求所述终端的安全信息，所述安全信息包括群组标识（ProSe group ID）、组密钥（ProSe group key）和组密钥标识（ProSe group key ID），所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥，所述组密钥是指同一群组中的终端共有的密钥。

在本发明实施例中，终端的标识信息可以是国际移动用户识别码（International Mobile Subscriber Identification Number，简称 IMSI）和/或移动用户号码(Mobile Subscriber International ISDN/PSTN number，简称 MSISDN)。

终端可以包括手机、平板电脑、个人数字助理（Personal Digital Assistant，简称 PDA）、销售终端（Point of Sales，简称 POS）、车载电脑等任意可以进行通信的终端设备。网络侧近距离通信功能实体可以是 ProSe Function 等。

在本发明实施例中，终端向网络侧近距离通信功能实体发送授权请求可能是基于三种情况下：终端在网络运营商中完成签约，在首次通信之前；在终端需要进行公共陆地移动网络（Public Land Mobile Network，简称 PLMN）切换时；终端定时向网络侧近距离通信功能实体请求安全信息。

102、网络侧近距离通信功能实体接收授权请求;

103、网络侧近距离通信功能实体根据所述终端的标识信息，查找所述终端的安全信息；

在本发明一些实施例中，在网络侧近距离通信功能实体中，设置了终端的标识信息、终端所属群组的授权信息和安全信息的对应关系。其中，授权信息中罗列了该终端被授权加入的每一个群组的群组标识，而该终端在每一个群组中都对应着相应的安全信息。举例来说，终端被授权加入的群组包括群组 A、群组 B 和群组 C，其中，授权信息中包括了群组 A、群组 B 和群组 C 的群组标识，根据终端的标识信息和群组 A 的群组标识，则可以找到对应的安全信息 A，根据终端的标识信息和群组 B 的群组标识，则可以找到对应的安全信息 B，根据终端的标识信息和群组 C 的群组标识，则可以找到对应的安全信息 C。也就是说，终端在群组 A 使用安全信息 A，终端在群组 B 中使用安全信息 B，终端在群组 C 中使用安全信息 C。

需要说明，网络侧近距离通信功能实体在每一次收到终端的授权请求时，都会将授权信息中的每一个群组标识所指示的群组的安全信息发送给终端，以上述例子而言，网络侧近距离通信功能实体将会向终端发送三个安全信息，分别为安全信息 A、安全信息 B 和安全信息 C。

104、网络侧近距离通信功能实体向终端发送授权响应，所述授权响应包括所述终端的安全信息；

105、终端接收所述授权响应；

106、终端所述终端的安全信息，生成用于处理近距离消息的安全保护密钥；

在本发明一些实施例中，在终端中配置了密钥生成功能（Key Derivation Function，简称 KDF）算法，步骤 106 具体包括：根据 KDF 算法、群组标识和组密钥，先生成第一安全密钥，然后根据 KDF 算法、第一安全密钥和安全保护算法标识生成安全保护密钥。在该实施例中，终端的安全信息除了包括上述群组标识、组密钥和组密钥标识之外，还可以进一步包括安全保护算法标识。

请参阅图 1b，图 1b 为本发明实施例提供的安全保护密钥的生成示意图。在图 1b 中，使用 2 个 KDF 算法组成两层结构，每一层结构中的 KDF 算法看作一个函数（或者一个算法处理模块），在第一层结构中，群组标识和组密钥

作为输入参数，经过KDF算法后得到输出为第一安全密钥，如图1b中的左边流程所示。第一安全密钥作为第二层结构的输入参数，还有另外一个输入参数为安全保护算法标识，经过KDF算法，输出为安全保护密钥（如图1b中的右边流程所示。

可选地，在本发明一些实施例中，若近距离消息为近距离发现消息，安全保护算法标识可以是第一完整性保护算法标识，第一完整性保护算法标识用于标识处理近距离发现消息的第一完整性保护算法。

可选地，在本发明一些实施例中，若近距离消息为近距离通信消息，安全保护算法标识可以是加密算法标识，加密算法标识用于标识处理近距离通信消息的加密算法。

可选地，在本发明一些实施例中，若近距离消息为近距离通信消息，安全保护算法标识可以是加密算法标识和第二完整性保护算法标识，其中，第二完整性保护算法标识用于标识处理近距离通信消息的第二完整性保护算法。

其中，安全信息可以进一步携带第一完整性保护算法标识、第二完整性保护算法和加密算法标识，当然，在本发明一些实施例中，第一完整性保护算法标识、第二完整性保护算法和加密算法标识还可以由两个互相通信的终端协商得到。

107、终端根据安全保护密钥，对近距离消息进行安全保护处理或者对近距离消息进行安全验证处理。

在本发明实施例中，终端可以发送近距离消息和/或接收近距离消息，若是终端发送近距离消息，在发送之前，终端根据安全保护密钥对近距离进行安全保护处理。若是终端接收到一个近距离消息，在接收近距离消息之后，终端根据安全保护密钥对近距离消息进行安全验证处理，以确保该近距离消息是安全消息。其中，安全保护处理和安全验证处理将会在后续实施例中进行详细说明，在此不再赘述。

需要说明，本发明实施例终端在步骤101~步骤107中均是处于运营商网络覆盖下。当然，还可以是终端在步骤101~步骤105中处于运营商网络覆盖下，而在步骤106与步骤107中不处于运营商网络覆盖，从而能够在终端不处于运营商网络覆盖的时候，也能确保终端的通信安全。

可选地，安全保护密钥可以是第一完整性保护密钥、第二完整性保护密钥和加密密钥中的至少一种。其中，第一完整性保护密钥用于处理近距离发现消息，第二完整性保护密钥用于处理近距离通信消息，加密密钥用于处理近距离通信消息。

请参阅图 2a，图 2 为本发明另一实施例提供的通信安全处理方法的另一信令图；在图 2a 中，一种通信安全处理方法可包括:

201、UE1（发送终端）向其对应的 ProSe Function A 发送第一授权请求，以及 UE2（接收终端）向其对应的 ProSe Function B 发送第二授权请求;

其中，第一授权请求用于 UE1 向 ProSe Function A 请求安全信息，第二授权请求用于 UE2 向 ProSe Function B 请求安全信息。第一授权请求包括 UE1 的标识信息，第二授权请求包括 UE2 的标识信息。在本发明实施例中 UE1 和 UE2 属于同一个群组，UE1 的和 UE2 的安全信息相同，其中，组密钥是指同一群组中的 UE 共有的密钥，在此，是指 UE1 和 UE2 共有的密钥。

可选地，上述安全信息中还可以包括第一完整性保护算法标识、第二完整性保护算法标识、加密算法标识中的至少一种;

进一步地，上述安全信息中还可以包括 UE1 的身份标识和 UE2 的身份标识中的至少一种。

202、ProSe Function A 根据第一授权请求，查找安全信息；ProSe Function B 根据第二授权请求，查找安全信息;

需要说明的是，ProSe Function A 配置了 UE1 的标识信息、授权信息和安全信息的对应关系。ProSe Function A 通过 UE1 查找到 UE1 的授权信息，然后根据 UE1 的授权信息中的群组标识，分别查找到每一个群组标识对应的安全信息。同样，ProSe Function B 中配置了 UE2 的授权信息，然后根据 UE2 的授权信息的群组标识，分别查找到每一个群组标识对应的安全信息。其中，在本发明实施例中 UE1 和 UE2 是互为通信的两端，因此，UE1 的授权信息和 UE2 的授权信息中至少包括一个共同的群组标识，然后根据共同的群组标识查找到公共的安全信息（该安全信息即为本发明实施例中所指示的安全信息），然后 UE1 与 UE2 基于该安全信息，在同一个群组内进行通信。

当然，在本发明实施例中，ProSe Function A 还会将 UE1 所属的其它群组

的安全信息发送给 UE1，ProSe Function B 还会将 UE2 所属的其它群组的安全信息发送给 UE2，在本发明实施例中 UE1 和 UE2 需要进行通信，UE1 和 UE2 都具有至少一个共同的安全信息，然后在一个群组中进行通信，因此，在本发明实施例中仅以 UE1 和 UE2 共同的安全信息为例进行说明。

203、ProSe Function A 向 UE1 发送授权响应，该授权响应中包括该安全信息；ProSe Function B 向 UE2 发送授权响应，该授权响应中包括该安全信息；

204、UE1 接收 ProSe Function A 发送的授权响应；UE2 接收 ProSe Function B 发送的授权响应。

其中，本发明实施例中 UE1 和 UE2 均处于运营商网络覆盖下，完成向 ProSe Function 请求安全信息的操作。

在图 2a 实施例中，在处于运营商网络覆盖下，UE1 通过向 ProSe Function A 发送第一授权请求去请求安全信息。UE2 通过向 ProSe Function B 发送第二授权请求去请求安全信息。

请参阅图 2b，图 2b 为本发明另一实施例提供的通信安全处理方法的另一信令图；如图 2b 所示，一种通信安全处理方法包括步骤：

210、ProSe Function A 查找安全信息；ProSe Function B 查找安全信息；

220~230 与步骤 203~204 相同，在此不再赘述。

其中，图 2b 所示实施例与图 2a 所示实施例的不同点在于，还可以是在 UE1 和 UE2 处于运营商网络覆盖下，ProSe Function A 主动向 UE1 发送安全信息，ProSe Function B 主动向 UE2 发送安全信息，然后 UE1 和 UE2 分别将安全信息保存在内存中。

其中，在本发明一些实施例中，ProSe Function A 和 ProSe Function B 可以是同一个 ProSe Function，意味着 UE1 和 UE2 从属于同一个 ProSe Function，从同一个 ProSe Function 获取安全信息。而在图 2a 和图 2b 中，UE1 和 UE2 从属于不同的 ProSe Function，两个 ProSe Function 需要共享同一个安全信息。

请参阅图 3a，图 3a 为本发明实施例提供的通信安全处理方法的另一信令图。在图 3a 中，UE1 和 UE2 在处于运营商网络覆盖下或不处于运营商网络覆盖下进行近距离发现过程，一种通信安全处理方法可包括：

301、UE1 根据 KDF 算法、安全信息中的群组标识和组密钥，生成发现密

钥;

请参阅图 3b，图 3b 为本发明实施例提供的发现密钥的生成示意图。本发明实施例中发现密钥为图 1b 中的第一安全密钥，图 3b 即为图 1b 左边生成第一安全密钥的实际应用。在图 3b 中，除了群组标识和组密钥，还可以选择 PGK ID、Discovery key ID、UE1 ID、UE2 ID 的至少一种作为 KDF 算法的输入参数。

请结合图 1b，发现密钥的生成公式如下:

Discovery key=KDF(群组 ID, PGK, (PGK ID), (Discovery key ID), (UE1 ID), (UE2 ID))。

其中，Discovery key 用于表示发现密钥，Discovery key ID 用于表示发现密钥标识，PGK ID、Discovery key ID、UE1 ID、UE2 ID 是可选的生成参数。Discovery key ID 可以是 UE1 从 ProSe Function A 获取，也可能是 UE1 生成。如果是 UE1 生成，那么 UE1 需要将 Discovery key ID 携带在发现消息中，以便 UE2 从发现消息中获取到该 Discovery key ID，还用于告诉 UE2 生成发现密钥还需要 Discovery key ID。另外，如果 UE1 ID 和/或 UE2 ID 也作为 Discovery key 的生成参数，则也需要携带在发现消息中，以告诉 UE2 在生成发现密钥时还需要考虑 UE1 ID 和 UE2 ID。

302、UE1 根据 KDF 算法、第一完整性保护算法标识和上述发现密钥生成第一完整性保护密钥;

请参阅图 3c，图 3c 为本发明一些实施例提供的第一完整性保护密钥的生成示意图。图 3c 中第一完整性保护密钥为图 1b 中的安全保护密钥，图 3c 即为图 1b 中的右边生成安全保护密钥的实际应用。在图 3c 中，第一完整性保护算法标识为图 1b 中的安全保护算法标识，在本发明实施例中还可以包括算法类型指示。

第一完整性保护密钥的公式如下:

PIK1=KDF{Discovery key , algorithm identity1 , (algorithm type distinguisher) }。

其中，PIK1 表示第一完整性保护密钥，algorithm identity1 表示第一完整性保护算法标识，algorithm type distinguisher 为算法类型指示（还可以在上述

公式中增加 algorithm type distinguisher，用于指示所采用的算法类型）。

303、UE1 根据第一完整性保护密钥，对近距离发现消息进行完整性保护，得到目标近距离发现消息；

可选地，在本发明实施例中，UE1 中还配置了第一完整性保护算法。

请参阅图 3d，图 3d 为本发明实施例提供的完整性保护的处理示意图；在图 3d 所示的 UE1 中，将第一完整性保护算法看作一个函数（或者一个算法处理模块），将近距离发现消息和第一完整性保护密钥看作第一完整性保护算法的输入参数，经过第一完整性保护算法运算处理后得到一个验证值，验证值携带在近距离发现消息尾部得到目标近距离消息。

304、UE1 向 UE2 发送目标近距离发现消息；

305、UE2 接收目标近距离发现消息；

306、UE2 利用配置的 KDF 算法，根据安全信息生成发现密钥；

其中，在 UE2 中也同样内置了 KDF 算法，以及配置第一完整性保护算法。可选地，UE2 中安全信息还包括第一完整性保护算法标识。进一步地还可以包括 UE1 的身份标识（ID）和/或 UE2 的身份标识（ID）。进一步地，上述安全信息中还包括发现密钥标识。根据图 3b 所示的生成方法生成发现密钥，在此不再赘述。

307、UE2 根据 KDF 算法、根据第一完整性保护算法标识和上述发现密钥生成第一完整性保护密钥；

在 UE1 中根据第一完整性保护密钥对近距离消息进行完整性保护处理，得到目标近距离消息。在 UE2 中根据第一完整性保护密钥对目标近距离消息进行安全验证处理。

308、UE2 根据第一完整性保护密钥确定目标近距离发现消息为安全消息，对目标近距离发现消息进行处理。

请结合图 3d 中的 UE2 端，UE2 根据第一完整性保护算法、第一完整性保护密钥和近距离发现消息生成一个验证值。其中，目标近距离发现消息中包括了一个验证值和近距离发现消息（这里的近距离发现消息也是 UE1 中的近距离发现消息），同样，在 UE2 根据目标近距离发现消息中的近距离发现消息，以及接收终端生成的第一完整性保护密钥生成一个验证值。比较两个验证值，

若两个验证值相同，则说明验证通过，UE2 则可以确认该目标近距离发现消息为安全消息，从而与 UE1 建立通信。若验证值不相同，则说明验证不通过。

请参阅图 4，图 4 为本发明实施例提供的通信安全处理方法的另一信令图；如图 4 所示，一种通信安全处理方法可包括：

401~402；其中，步骤 401~402 与上述步骤 301~302 相同，在此不再赘述。

403、UE1 生成第一安全参数，将第一安全参数携带在近距离发现消息中；

UE1 可以通过随机生成方式生成第一参数。

404~409；其中，步骤 404~409 与上述步骤 301~308 相同，在此不再赘述。

410、UE2 从目标近距离发现消息中，获取第一安全参数；

411、UE2 生成第二安全参数；

UE2 可以通过随机生成方式生成第二参数。

412、UE2 将第二安全参数发送给 UE1；

需要说明，UE1 是在近距离发现消息中将第一安全参数发送给 UE2，那么 UE2 可以通过响应近距离发现消息，然后将第二安全参数发送给 UE1。

413、UE2 将第一安全参数和第二安全参数保存下来；

414、UE1 接收第二安全参数，并和第一安全参数一起保存。

在本发明实施例中，UE1 通过在近距离发现消息中携带第一安全参数，然后 UE2 根据第一安全参数生成第二安全参数，并将第二安全参数发送给 UE1。UE1 和 UE2 同时将第一安全参数和第二安全参数保存下来，在进行 D2D 通信过程中根据第一安全参数、第二安全参数以及安全信息中的组密钥等，作为生成参数生成用于保护近距离通信消息的安全密钥和/或第二完整性保护密钥，从而对近距离通信消息进行安全保护处理。

请参阅图 5a，图 5a 为本发明实施例提供的通信安全处理方法的另一信令图；如图 5a 所示，一种通信安全处理方法可包括：

501、UE1 根据 KDF 算法和安全信息中的群组标识和组密钥，生成通信密钥；

请参阅图 5b，图 5b 为本发明实施例提供的通信密钥的生成示意图。本发明实施例中通信密钥为图 1b 中的第一安全密钥，图 3b 即为图 1b 左边生成第一安全密钥的实际应用。在图 3b 中，除了群组标识和组密钥，还可以选择 PGK

ID、Communication key ID、UE1 ID、UE2 ID 的至少一种作为 KDF 算法的输入参数。

请结合图 1b，在图 5b 中，通信密钥的生成公式如下：

Communication key=KDF(群组 ID、PGK、(PGK ID)、(Communication key ID)、(UE1 ID)、(UE2 ID))。

其中，Communication key 用于表示通信密钥，Communication key ID 用于表示上述通信密钥标识。PGK ID 、Communication key ID、UE1 ID、UE2 ID 是可选的输入参数。Communication key ID 可以是 UE1 从所属 ProSe Function A 获取，也可能是 UE1 生成。若是由 UE1 生成，需要 UE1 将 Communication key ID 携带在通信消息中，以便 UE2 通过通信消息获取到 Communication key ID 和通知生成通信密钥时需要 Communication key ID 作为输入参数。如果 UE1 ID、UE2 ID 作为 Communication key 的生成参数，则也需要携带在通信消息中，以便通知 UE2 知道生成通信密钥时，需要 UE1 ID、UE2 ID 作为输入参数。

502、UE1 根据 KDF 算法、加密算法标识和通信密钥，生成加密密钥；

请参阅图 5c，图 5c 为本发明一些实施例提供的加密密钥的生成示意图。图 5c 中第一完整性保护密钥为图 1b 中的安全保护密钥，图 3c 即为图 1b 中的右边生成安全保护密钥的实际应用。在图 5c 中，加密算法标识为图 1b 中的安全保护算法标识，在本发明实施例中还可以包括算法类型指示。

生成加密密钥的公式如下：

PEK=KDF（Communication key，algorithm identity2、(algorithm type distinguisher)}。

其中，PEK 表示加密密钥，algorithm identity2 表示加密算法标识，algorithm type distinguisher 为算法类型指示（还可以在上述公式中增加 algorithm type distinguisher，用于指示所采用的算法类型）。

503、UE1 根据所述加密密钥，对近距离通信消息进行加密处理，得到目标近距离通信消息；

请参阅图 5d，图 5d 为本发明实施例提供的完整性保护处理的示意图；在图 5d 中的 UE1 中，根据加密算法和加密密钥生成一串密钥流，然后对密钥流和近距离通信消息进行异或运算，得到目标近距离通信消息。当然，在本发明

实施例中，可以将加密算法看作一个函数（或者运算处理模块），加密算法和加密密钥作为函数的输入参数。

504、UE1 向 UE2 发送目标近距离通信消息；

505、UE2 接收目标近距离通信消息；

506、UE2 根据 KDF 算法、群组标识和组密钥，生成通信密钥；

其中，在 UE2 中同样内置了 KDF 算法，以及配置加密算法。可选地，UE2 安全信息中还包括加密算法标识，进一步地还包括 UE1 的身份标识（ID）和/或 UE2 的身份标识（ID）。进一步地，上述安全信息中还包括通信密钥标识。根据图 5b 所示生成通信密钥，在此不再赘述。

507、UE2 根据 KDF 算法、通信密钥和加密算法标识，生成加密密钥；

在 UE1 中根据加密密钥对近距离消息进行加密保护处理，得到目标近距离消息。在 UE2 中根据加密密钥对目标近距离消息进行解密处理。

508、UE2 根据加密密钥，对目标近距离通信消息进行解密，若目标近距离通信消息为安全消息，对目标近距离通信消息进行处理。

请结合图 5d 中的 UE2，UE2 根据加密算法和加密密码，生成密钥流。然后利用该密钥流与接收到的目标近距离通信消息进行异或处理，解密得到近距离通信消息，则验证通过。

需要说明，在本发明实施例中，用于 UE1 和 UE2 在近距离通信消息的安全保护处理和安全验证处理，其中，发现密钥即为本发明实施例提供的第一安全密钥，加密密钥为本发明实施例提供的安全保护密钥，在 UE1 中，UE1 根据加密密钥和加密算法，对近距离通信消息进行安全保护处理，得到目标近距离通信消息。在 UE2 中，UE2 根据加密密钥和加密算法，对目标近距离通信消息进行解密的安全验证处理，从而得到近距离通信消息。

请参阅图 6a，图 6a 为本发明实施例提供的通信安全处理方法的另一信令图；如图 6a 所示，一种通信安全处理方法可包括：

601、UE1 根据 KDF 算法、群组标识和组密钥，生成通信密钥；

请结合图 5b，根据图 5b 所示的通信密钥生成方法，生成通信密钥。

602、UE1 根据 KDF 算法、加密算法标识和通信密钥生成加密密钥；根据第二完整性保护算法标识和通信密钥生成完第二整性保护密钥；

请结合图 5c，根据图 5c 所示的加密密钥生成方法，生成加密密钥，在此不再赘述。第二完整性保护密钥的公式如下:

PIK2=KDF{ Communication key 、algorithm identity3、algorithm type distinguisher}。

其中，PIK2 用于表示第二完整性保护密钥，algorithm identity3 用于表示第二完整性保护算法标识，algorithm type distinguisher 为算法类型指示（还可以在上述公式中增加 algorithm type distinguisher，用于指示所采用的算法类型）。

请结合图 3c，在本发明实施例中可以利用图 3c 所示的生成方法，生成第二完整性保护密钥，但是，在利用 3c 所示的生成方法生成第二完整性保护密钥，需要用 algorithm identity3 替换图 3c 中的 algorithm identity1，用 Communication key 替换 Discovery key，用 algorithm type distinguisher 替换图 3c 中的 algorithm type distinguisher。

603、UE1 利用所述加密密钥对需要发送的近距离通信消息进行加密处理，并利用第二完整性保护密钥对加密后的近距离通信消息进行完整性保护，得到目标近距离通信消息;

其中，UE1 对近距离通信消息进行加密处理，可以参阅上述图 5d 中的发 UE1 所示的流程，在此不再赘述。根据加密密钥对近距离通信消息进行加密处理，得到一个初次的近距离通信消息。

进一步，利用配置的第二完整性保护算法，对第二完整性保护密钥和初次的近距离通信消息进行处理，得到目标近距离通信消息，具体地，该过程与上述图 3d 所示的 UE1 的处理流程相同，只是在该实施例中，采用的是第二完整性保护算法，参数是第二完整性保护密钥和初次的近距离通信消息。其中，目标近距离通信消息中包括了一个验证值和初次的近距离通信消息。

604、UE1 向 UE2 发送目标近距离通信消息;

605、UE2 接收目标近距离通信消息;

606、UE2 根据 KDF 算法、群组标识和组密钥，生成通信密钥;

通信密钥的生成与上述步骤 601 相同，在此不再赘述。

607、UE2 根据通信密钥和第二完整性保护算法标识，生成第二完整性保

护密钥，并根据通信密钥和加密算法标识，生成加密密钥；

其中，加密密钥的生成与上述步骤 602 相同，在此不再赘述。

608、UE2 根据第二完整性保护密钥，验证目标近距离通信消息是否为安全消息，如果是，再对目标近距离通信消息进行解密处理。

其中，请结合图 3d 中的 UE2 端，首先，UE2 根据第二完整性保护算法、第二完整性保护密钥和目标近距离消息，得到一个验证值，该验证值与目标近距离消息中携带的验证值相同时，验证通过。请结合图 5d 中的 UE2，然后根据加密算法和加密密钥生成一串密钥流，对初次的近距离通信消息和密钥流进行异或运算，完成解密。

如果目标近距离通信消息既有完整性保护又有加密保护，则先对目标近距离通信消息进行完整性验证，如果验证通过，再进行解密处理；如果目标近通信距离消息只有完整性保护，则对目标近距离通信消息进行完整性验证；如果目标近通信距离消息只有加密保护，则对目标近距离消息进行解密处理。

请参阅图 7，图 7 为本发明实施例提供的通信安全处理方法的另一信令图；如图 7 所示，一种通信安全处理方法可包括：

701、UE1 读取第一安全参数、第二安全参数以及安全信息的组密钥，根据第一安全参数、第二安全参数和组密钥生成安全保护密钥；

其中，安全保护密钥可以包括加密密钥和/或完整性保护密钥。需要说明，这里的加密密钥与图 5 和图 6 实施例中所提供的加密密钥不同，同样，完整性保护密钥与图 5 和图 6 提供的第二完整性保护密钥不同。

702、UE1 根据安全保护密钥，对近距离通信消息进行安全保护处理，得到目标近距离通信消息；

703、UE1 向 UE2 发送目标近距离通信消息；

704、UE2 接收目标近距离通信消息，读取第一安全参数、第二安全参数以及安全信息的组密钥生成安全验证密钥；

需要说明，这里的安全验证密钥与上述步骤 701 中的安全保护密钥相同，仅用于验证目标近距离通信消息是否安全。

705、UE2 根据安全验证密钥对目标近距离通信消息进行安全验证，在目标近距离通信消息为安全消息时，对目标近距离通信消息进行处理。

在本发明实施例中，UE1 和 UE2 在图 4 所示的实施例的基础上，以获得第一安全参数和第二安全参数，然后根据第一安全参数和第二安全参数，实现对近距离通信消息的安全保护。

请参阅图 8，图 8 为本发明实施例提供的终端的结构示意图；如图 8 所示，一种终端 800 可包括至少一个处理器 810（例如 CPU，Central Processing Unit）、至少一个发送器 820，一个接收器 830 和存储器 840，至少一个网络接口或者其它通信接口，和至少一个通信总线，通信总线用于实现处理器 810、发送器 820，接收器 830 和存储器 840 之间的连接通信。处理器 810 用于执行存储器 840 中存储的可执行模块，例如计算机程序。上述存储器 840 可能包含高速随机存取存储器（RAM，Random Access Memory），也可能还包括非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。通过至少一个网络接口（可以是有线或者无线）实现该系统网关与至少一个其它网元之间的通信连接，可以使用互联网，广域网，本地网，城域网等。

其中，发送器 820，用于向网络侧近距离通信功能实体发送授权请求，所述授权请求包含所述终端的标识信息，所述授权请求用于向所述网络侧近距离通信功能实体请求所述终端的安全信息，所述安全信息包括群组标识、组密钥和组密钥标识，所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥；

接收器 830，用于接收所述网络侧近距离通信功能实体发送的授权响应，所述授权响应包括所述终端的安全信息；

处理器 810，用于根据所述终端的安全信息，生成用于处理近距离消息的安全保护密钥。

可选地，在本发明实施例中，上述处理器 810 具体用于，根据密钥生成功能 KDF 算法、所述群组标识和所述组密钥，生成第一安全密钥；根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，生成所述安全保护密钥。

在本发明一些实施例中，所述近距离消息为近距离发现消息，所述安全保护算法标识为第一完整性保护算法标识，所述第一完整性保护算法标识用于标识处理近距离发现消息的第一完整性保护算法；所述处理器 810 进一步具体用于，根据所述第一完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，

生成第一完整性保护密钥，所述第一完整性保护密钥为所述安全保护密钥。

在本发明一些实施例中，所述近距离消息为近距离通信消息，所述安全保护算法标识为加密密钥标识，所述加密密钥标识用于标识处理近距离通信消息的加密算法；所述处理器 810 进一步具体用于，根据所述加密算法标识、所述 KDF 算法和所述第一安全密钥，生成加密密钥，所述加密密钥为所述安全保护密钥。

在本发明一些实施例中，所述近距离消息为近距离通信消息，所述安全保护算法标识为第二完整性保护算法标识，所述第二完整性保护算法标识用于标识处理近距离通信消息的第二完整性保护算法；所述处理器 810 进一步具体用于，根据所述第二完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，生成第二完整性保护密钥，所述第二完整性保护密钥为所述安全保护密钥。

在本发明一些实施例中，所述处理器 810 还用于，在根据所述安全信息生成用于处理近距离消息的安全保护密钥之后，根据所述安全保护密钥，对所述近距离消息进行安全保护处理；或者，根据所述安全保护密钥，对所述近距离消息进行安全验证处理。

可选地，所述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

请参阅图 9，图 9 为本发明实施例提供的网络侧近距离通信功能实体的结构示意图；如图 9 所示，一种网络侧近距离通信功能实体 900 可包括至少一个处理器 910（例如 CPU，Central Processing Unit）、存储器 920 和至少一个网络接口或者其它通信接口 930，和至少一个通信总线，通信总线用于实现处理器 910、通信接口 930 和存储器 920 之间的连接通信。处理器 910 用于执行存储器 920 中存储的可执行模块，例如计算机程序。上述存储器 910 可能包含高速随机存取存储器（RAM，Random Access Memory），也可能还包括非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。通过至少一个网络接口（可以是有线或者无线）实现该系统网关与至少一个其它网元之间的通信连接，可以使用互联网，广域网，本地网，城域网等。

其中，通信接口 930，用于接收终端发送的授权请求，所述授权请求包括所述终端的标识信息；

处理器 910，用于根据所述终端的标识信息，查找所述终端的安全信息，所述终端的安全信息包括群组标识、组密钥和组密钥标识，所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥，所述终端的安全信息用于生成处理近距离消息的安全保护密钥；

所述通信接口还用于向所述终端发送授权响应，所述授权响应包括所述终端的安全信息。

在本发明一些实施例中，所述处理器 910 具体用于，根据所述终端的标识信息，查找所述终端所属群组的授权信息，所述授权信息中包括所述终端所属群组的群组标识；根据所述终端的标识信息和所述群组标识，查找所述群组标识所指示的群组的安全信息。

可选地，所述安全信息还包括第一完整性保护算法标识、第二完整性保护算法标识和加密算法标识中的至少一种。

可选地，所述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

请参阅图 10，图 10 为本发明实施例提供的通信安全处理系统的结构示意图；如图 10 所示，一种通信安全处理系统可包括：图 8 所示的终端、以及图 9 所示的网络侧近距离功能实体。

对图 8 所示的终端和图 9 所示网络侧近距离功能实体，可以参阅上述方法实施例和装置实施例的说明，在此不再赘述。

本发明实施例还提供了另一种终端的结构示意图，如图 11 所示，为了便于说明，仅示出了与本发明实施例相关的部分，具体技术细节未揭示的，请参照本发明实施例方法部分。以终端为手机为例：

图 11 示出的是与本发明实施例提供的终端相关的手机的部分结构的框图。参考图 11，手机包括：射频（Radio Frequency，RF）电路 1110、存储器 1120、输入单元 1130、显示单元 1140、传感器 1150、音频电路 1160、无线保真（wireless fidelity，WiFi）模块 1170、处理器 1180、以及电源 1190 等部件。本领域技术人员可以理解，图 11 中示出的手机结构并不构成对手机的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

下面结合图 11 对手机的各个构成部件进行具体的介绍：

RF 电路 1110 可用于收发信息或通话过程中，信号的接收和发送，特别地，将基站的下行信息接收后，给处理器 1180 处理；另外，将设计上行的数据发送给基站。通常，RF 电路 1110 包括但不限于天线、至少一个放大器、收发信机、耦合器、低噪声放大器（Low Noise Amplifier，LNA）、双工器等。此外，RF 电路 1110 还可以通过无线通信与网络和其他设备通信。上述无线通信可以使用任一通信标准或协议，包括但不限于全球移动通讯系统（Global System of Mobile communication，GSM）、通用分组无线服务（General Packet Radio Service，GPRS）、码分多址（Code Division Multiple Access，CDMA）、宽带码分多址（Wideband Code Division Multiple Access, WCDMA）、长期演进（Long Term Evolution，LTE）、电子邮件、短消息服务（Short Messaging Service，SMS）等。

存储器 1120 可用于存储软件程序以及模块，处理器 1180 通过运行存储在存储器 1120 的软件程序以及模块，从而执行手机的各种功能应用以及数据处理。存储器 1120 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、至少一个功能所需的应用程序（比如 D2D 通信功能）等；存储数据区可存储根据手机的使用所创建的数据（比如配置的 KDF 算法、第一完整性保护算法、第二完整性保护算法、加密算法和 D2D 通信数据等）等。此外，存储器 1120 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。

输入单元 1130 可用于接收输入的数字或字符信息，以及产生与手机的用户设置以及功能控制有关的键信号输入。具体地，输入单元 1130 可包括触控面板 1131 以及其他输入设备 1132。触控面板 1131，也称为触摸屏，可收集用户在其上或附近的触摸操作（比如用户使用手指、触笔等任何适合的物体或附件在触控面板 1131 上或在触控面板 1131 附近的操作），并根据预先设定的程式驱动相应的连接装置。可选的，触控面板 1131 可包括触摸检测装置和触摸控制器两个部分。其中，触摸检测装置检测用户的触摸方位，并检测触摸操作带来的信号，将信号传送给触摸控制器；触摸控制器从触摸检测装置上接收触摸信息，并将它转换成触点坐标，再送给处理器 1180，并能接收处理器 1180 发来的命令并加以执行。此外，可以采用电阻式、电容式、红外线以及表面声

波等多种类型实现触控面板 1131。除了触控面板 1131，输入单元 1130 还可以包括其他输入设备 1132。具体地，其他输入设备 1132 可以包括但不限于物理键盘、功能键（比如音量控制按键、开关按键等）、轨迹球、鼠标、操作杆等中的一种或多种。

显示单元 1140 可用于显示由用户输入的信息或提供给用户的信息以及手机的各种菜单。显示单元 1140 可包括显示面板 1141，可选的，可以采用液晶显示器（Liquid Crystal Display，LCD）、有机发光二极管（Organic Light-Emitting Diode, OLED）等形式来配置显示面板 1141。进一步的，触控面板 1131 可覆盖显示面板 1141，当触控面板 1131 检测到在其上或附近的触摸操作后，传送给处理器 1180 以确定触摸事件的类型，随后处理器 1180 根据触摸事件的类型在显示面板 1141 上提供相应的视觉输出。虽然在图 11 中，触控面板 1131 与显示面板 1141 是作为两个独立的部件来实现手机的输入和输入功能，但是在某些实施例中，可以将触控面板 1131 与显示面板 1141 集成而实现手机的输入和输出功能。

手机还可包括至少一种传感器 1150，比如光传感器、运动传感器以及其他传感器。具体地，光传感器可包括环境光传感器及接近传感器，其中，环境光传感器可根据环境光线的明暗来调节显示面板 1141 的亮度，接近传感器可在手机移动到耳边时，关闭显示面板 1141 和/或背光。作为运动传感器的一种，加速计传感器可检测各个方向上（一般为三轴）加速度的大小，静止时可检测出重力的大小及方向，可用于识别手机姿态的应用（比如横竖屏切换、相关游戏、磁力计姿态校准）、振动识别相关功能（比如计步器、敲击）等；至于手机还可配置的陀螺仪、气压计、湿度计、温度计、红外线传感器等其他传感器，在此不再赘述。

音频电路 1160、扬声器 1161，传声器 1162 可提供用户与手机之间的音频接口。音频电路 1160 可将接收到的音频数据转换后的电信号，传输到扬声器 1161，由扬声器 1161 转换为声音信号输出；另一方面，传声器 1162 将收集的声音信号转换为电信号，由音频电路 1160 接收后转换为音频数据，再将音频数据输出处理器 1180 处理后，经 RF 电路 1110 以发送给比如另一手机，或者将音频数据输出至存储器 1120 以便进一步处理。

WiFi 属于短距离无线传输技术，手机通过 WiFi 模块 1170 可以帮助用户进行 D2D 发现、D2D 通信、收发电子邮件、浏览网页和访问流式媒体等，它为用户提供了无线的宽带互联网访问。虽然图 11 示出了 WiFi 模块 1170，但是可以理解的是，其并不属于手机的必须构成，完全可以根据需要在不改变发明的本质的范围内而省略。

处理器 1180 是手机的控制中心，利用各种接口和线路连接整个手机的各个部分，通过运行或执行存储在存储器 1120 内的软件程序和/或模块，以及调用存储在存储器 1120 内的数据，执行手机的各种功能和处理数据，从而对手机进行整体监控。可选的，处理器 1180 可包括一个或多个处理单元；优选的，处理器 1180 可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器 1180 中。

手机还包括给各个部件供电的电源 1190（比如电池），优选的，电源可以通过电源管理系统与处理器 1180 逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。

尽管未示出，手机还可以包括摄像头、蓝牙模块等，在此不再赘述。

在本发明实施例中，该终端所包括的处理器 1180 还具有以下功能：向网络侧近距离通信功能实体发送授权请求，所述授权请求包含所述终端的标识信息，所述授权请求用于向所述网络侧近距离通信功能实体请求所述终端的安全信息，所述安全信息包括群组标识、组密钥和组密钥标识，所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥；接收所述网络侧近距离通信功能实体发送的授权响应，所述授权响应包括所述终端的安全信息；根据所述终端的安全信息，生成用于处理近距离消息的安全保护密钥。

在本发明实施例中，该终端所包括的处理器 1180 还具有以下功能：根据密钥生成功能 KDF 算法、所述群组标识和所述组密钥，生成第一安全密钥；根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，生成所述安全保护密钥。

在本发明实施例中，该终端所包括的处理器 1180 还具有以下功能：在所述近距离消息为近距离发现消息时，所述安全保护算法标识为第一完整性保护

算法标识，所述第一完整性保护算法标识用于标识处理近距离发现消息的第一完整性保护算法，根据所述第一完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，生成第一完整性保护密钥，所述第一完整性保护密钥为所述安全保护密钥。

在本发明实施例中，该终端所包括的处理器 1180 还具有以下功能：在所述近距离消息为近距离通信消息，所述安全保护算法标识为加密密钥标识，所述加密密钥标识用于标识处理近距离通信消息的加密算法；根据所述加密算法标识、所述 KDF 算法和所述第一安全密钥，生成加密密钥，所述加密密钥为所述安全保护密钥。

在本发明实施例中，该终端所包括的处理器 1180 还具有以下功能：所述近距离消息为近距离通信消息，所述安全保护算法标识为第二完整性保护算法标识，所述第二完整性保护算法标识用于标识处理近距离通信消息的第二完整性保护算法；根据所述第二完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，生成第二完整性保护密钥，所述第二完整性保护密钥为所述安全保护密钥。

在本发明实施例中，该终端所包括的处理器 1180 还具有以下功能：在根据所述安全信息生成用于处理近距离消息的安全保护密钥之后，根据所述安全保护密钥，对所述近距离消息进行安全保护处理；或者，所述终端根据所述安全保护密钥，对所述近距离消息进行安全验证处理。

在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其他实施例的相关描述。

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

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

接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

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

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用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，本发明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）执行本发明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（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质。

以上对本发明所提供的一种通信安全处理方法、系统及相关设备进行了详细介绍，对于本领域的一般技术人员，依据本发明实施例的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

权 利 要 求

1、一种通信安全处理方法，其特征在于，应用于终端，所述方法包括:

所述终端向网络侧近距离通信功能实体发送授权请求，所述授权请求包含所述终端的标识信息，所述授权请求用于向所述网络侧近距离通信功能实体请求所述终端的安全信息，所述安全信息包括群组标识、组密钥和组密钥标识，所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥;

所述终端接收所述网络侧近距离通信功能实体发送的授权响应，所述授权响应包括所述终端的安全信息;

所述终端根据所述终端的安全信息，生成用于处理近距离消息的安全保护密钥。

2、根据权利要求 1 所述的方法，其特征在于，所述终端根据所述终端的安全信息，生成用于处理近距离消息的安全保护密钥包括:

所述终端根据密钥生成功能 KDF 算法、所述群组标识和所述组密钥，生成第一安全密钥;

所述终端根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，生成所述安全保护密钥。

3、根据权利要求 2 所述的方法，其特征在于，所述近距离消息为近距离发现消息，所述安全保护算法标识为第一完整性保护算法标识，所述第一完整性保护算法标识用于标识处理近距离发现消息的第一完整性保护算法;

所述终端根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，生成所述安全保护密钥包括:

所述终端根据所述第一完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，生成第一完整性保护密钥，所述第一完整性保护密钥为所述安全保护密钥。

4、根据权利要求 2 所述的方法，其特征在于，所述近距离消息为近距离通信消息，所述安全保护算法标识为加密密钥标识，所述加密密钥标识用于标识处理近距离通信消息的加密算法;

所述终端根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，

生成所述安全保护密钥包括:

所述终端根据所述加密算法标识、所述 KDF 算法和所述第一安全密钥，生成加密密钥，所述加密密钥为所述安全保护密钥。

5、根据权利要求 2 所述的方法，其特征在于，所述近距离消息为近距离通信消息，所述安全保护算法标识为第二完整性保护算法标识，所述第二完整性保护算法标识用于标识处理近距离通信消息的第二完整性保护算法;

所述终端根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，生成所述安全保护密钥包括:

所述终端根据所述第二完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，生成第二完整性保护密钥，所述第二完整性保护密钥为所述安全保护密钥。

6、根据权利要求 1~5 任一项所述的方法，其特征在于，所述终端根据所述安全信息生成用于处理近距离消息的安全保护密钥之后包括:

所述终端根据所述安全保护密钥，对所述近距离消息进行安全保护处理;或者，所述终端根据所述安全保护密钥，对所述近距离消息进行安全验证处理。

7、根据权利要求 1~6 任一项所述的方法，其特征在于，所述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

8、一种通信安全处理方法，其特征在于，应用于网络侧近距离通信功能实体，所述方法包括:

所述网络侧近距离通信功能实体接收终端发送的授权请求，所述授权请求包括所述终端的标识信息;

所述网络侧近距离通信功能实体根据所述终端的标识信息，查找所述终端的安全信息，所述安全信息包括群组标识、组密钥和组密钥标识，所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥，所述终端的安全信息用于生成处理近距离消息的安全保护密钥;

所述网络侧近距离通信功能实体向所述终端发送授权响应，所述授权响应包括所述终端的安全信息。

9、根据权利要求 8 所述的方法，其特征在于，所述网络侧近距离通信功能实体根据所述终端的标识信息，查找所述终端的安全信息包括:

所述网络侧近距离通信功能实体根据所述终端的标识信息，查找所述终端所属群组的授权信息，所述授权信息中包括所述终端所属群组的群组标识；

所述网络侧近距离通信功能实体根据所述终端的标识信息和所述群组标识，查找所述群组标识所指示的群组的安全信息。

10、根据权利要求 8 或 9 所述的方法，其特征在于，所述终端的安全信息还包括第一完整性保护算法标识、第二完整性保护算法标识和加密算法标识中的至少一种。

11、根据权利要求 8~10 任一项所述的方法，其特征在于，所述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

12、一种终端，其特征在于，包括：

发送器，用于向网络侧近距离通信功能实体发送授权请求，所述授权请求包含所述终端的标识信息，所述授权请求用于向所述网络侧近距离通信功能实体请求所述终端的安全信息，所述安全信息包括群组标识、组密钥和组密钥标识，所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥；

接收器，用于接收所述网络侧近距离通信功能实体发送的授权响应，所述授权响应包括所述终端的安全信息；

处理器，用于根据所述终端的安全信息，生成用于处理近距离消息的安全保护密钥。

13、根据权利要求 12 所述的终端，其特征在于，

所述处理器具体用于，根据密钥生成功能 KDF 算法、所述群组标识和所述组密钥，生成第一安全密钥；根据安全保护算法标识、所述 KDF 算法和所述第一安全密钥，生成所述安全保护密钥。

14、根据权利要求 13 所述的终端，其特征在于，

所述近距离消息为近距离发现消息时，所述安全保护算法标识为第一完整性保护算法标识，所述第一完整性保护算法标识用于标识处理近距离发现消息的第一完整性保护算法，所述处理器进一步具体用于，根据所述第一完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，生成第一完整性保护密钥，

所述第一完整性保护密钥为所述安全保护密钥。

15、根据权利要求 13 所述的终端，其特征在于，

所述近距离消息为近距离通信消息时，所述安全保护算法标识为加密密钥标识，所述加密密钥标识用于标识处理近距离通信消息的加密算法，所述处理器进一步具体用于，根据所述加密算法标识、所述 KDF 算法和所述第一安全密钥，生成加密密钥，所述加密密钥为所述安全保护密钥。

16、根据权利要求 13 所述的终端，其特征在于，

在所述近距离消息为近距离通信消息，所述安全保护算法标识为第二完整性保护算法标识，所述第二完整性保护算法标识用于标识处理近距离通信消息的第二完整性保护算法，所述处理器进一步具体用于，根据所述第二完整性保护算法标识、所述 KDF 算法和所述第一安全密钥，生成第二完整性保护密钥，所述第二完整性保护密钥为所述安全保护密钥。

17、根据权利要求 12~16 任一项所述的终端，其特征在于，

所述处理器还用于，在根据所述安全信息生成用于处理近距离消息的安全保护密钥之后，根据所述安全保护密钥，对所述近距离消息进行安全保护处理；或者，根据所述安全保护密钥，对所述近距离消息进行安全验证处理。

18、根据权利要求 12~17 任一项所述的终端，其特征在于，

所述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

19、一种网络侧近距离通信功能实体，其特征在于，包括：

通信接口，用于接收终端发送的授权请求，所述授权请求包括所述终端的标识信息；

处理器，用于根据所述终端的标识信息，查找所述终端的安全信息，所述终端的安全信息包括群组标识、组密钥和组密钥标识，所述群组标识用于指示所述终端所属的群组，所述组密钥标识用于指示所述组密钥，所述终端的安全信息用于生成处理近距离消息的安全保护密钥；

所述通信接口还用于向所述终端发送授权响应，所述授权响应包括所述终端的安全信息。

20、根据权利要求 19 所述的网络侧近距离通信功能实体，其特征在于，

所述处理器具体用于，根据所述终端的标识信息，查找所述终端所属群组的授权信息，所述授权信息中包括所述终端所属群组的群组标识；根据所述终端的标识信息和所述群组标识，查找所述群组标识所指示的群组的安全信息。

21、根据权利要求 19 或 20 所述的网络侧近距离通信功能实体，其特征在于，所述安全信息还包括第一完整性保护算法标识、第二完整性保护算法标识和加密算法标识中的至少一种。

22、根据权利要求 19~20 任一项所述的网络侧近距离通信功能实体，其特征在于，所述终端的标识信息包括国际移动用户识别码 IMSI 和移动用户号码 MSISDN 中的至少一种。

23、一种通信安全处理系统，其特征在于，包括：

权利要求 12~18 任一项所述的终端，以及权利要求 19~22 任一项所述的网络侧近距离通信功能实体。

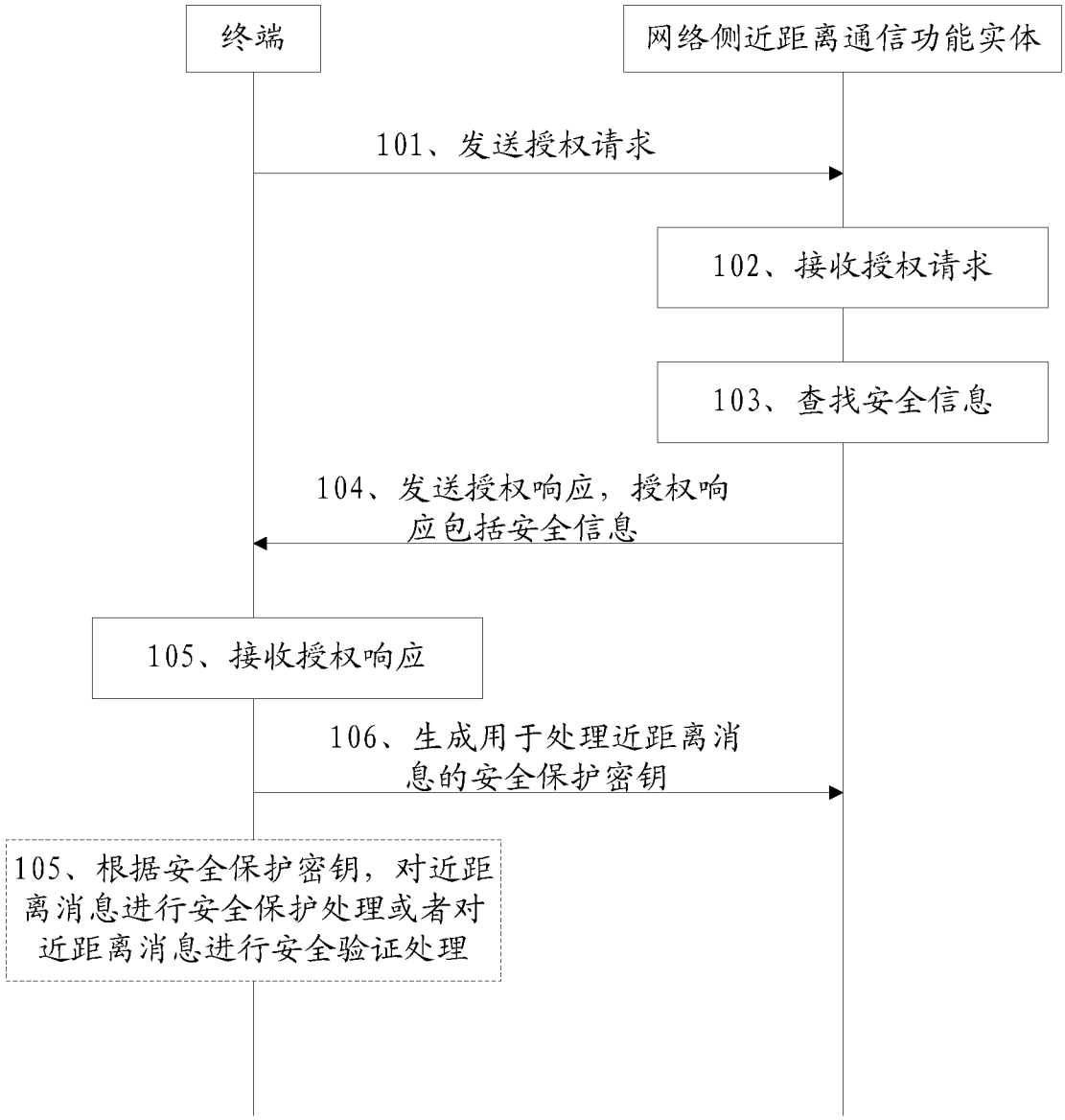
终端
网络侧近距离通信功能实体
101、发送授权请求
102、接收授权请求
103、查找安全信息
104、发送授权响应，授权响应包括安全信息
105、接收授权响应
106、生成用于处理近距离消息的安全保护密钥
105、根据安全保护密钥，对近距离消息进行安全保护处理或者对近距离消息进行安全验证处理

图 1a

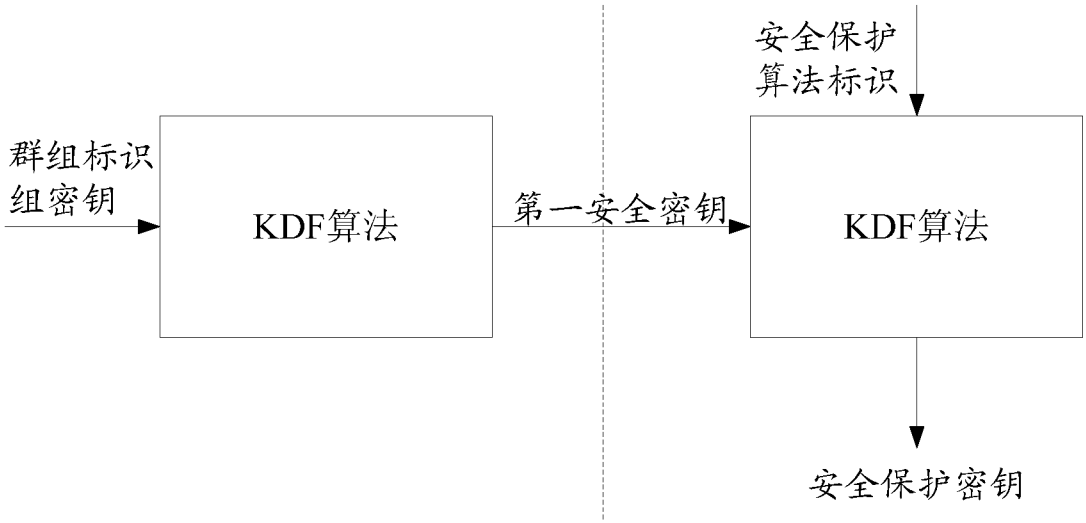
安全保护
算法标识
群组标识
组密钥
KDF算法
第一安全密钥
KDF算法
安全保护密钥

图 1b

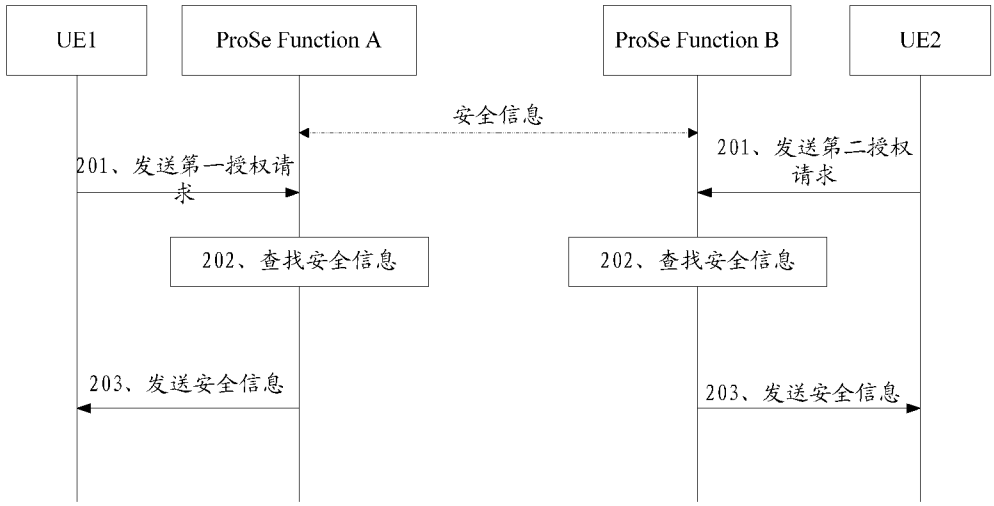
UE1
ProSe Function A
ProSe Function B
UE2
安全信息
201、发送第一授权请求
201、发送第二授权请求
202、查找安全信息
202、查找安全信息
203、发送安全信息
203、发送安全信息

图 2a

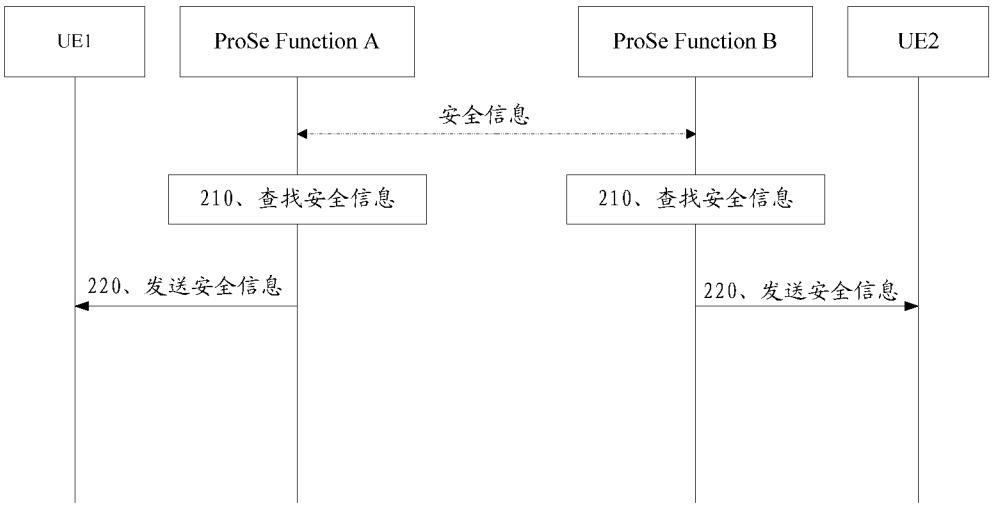
UE1
ProSe Function A
ProSe Function B
UE2
安全信息
210、查找安全信息
210、查找安全信息
220、发送安全信息
220、发送安全信息

图 2b

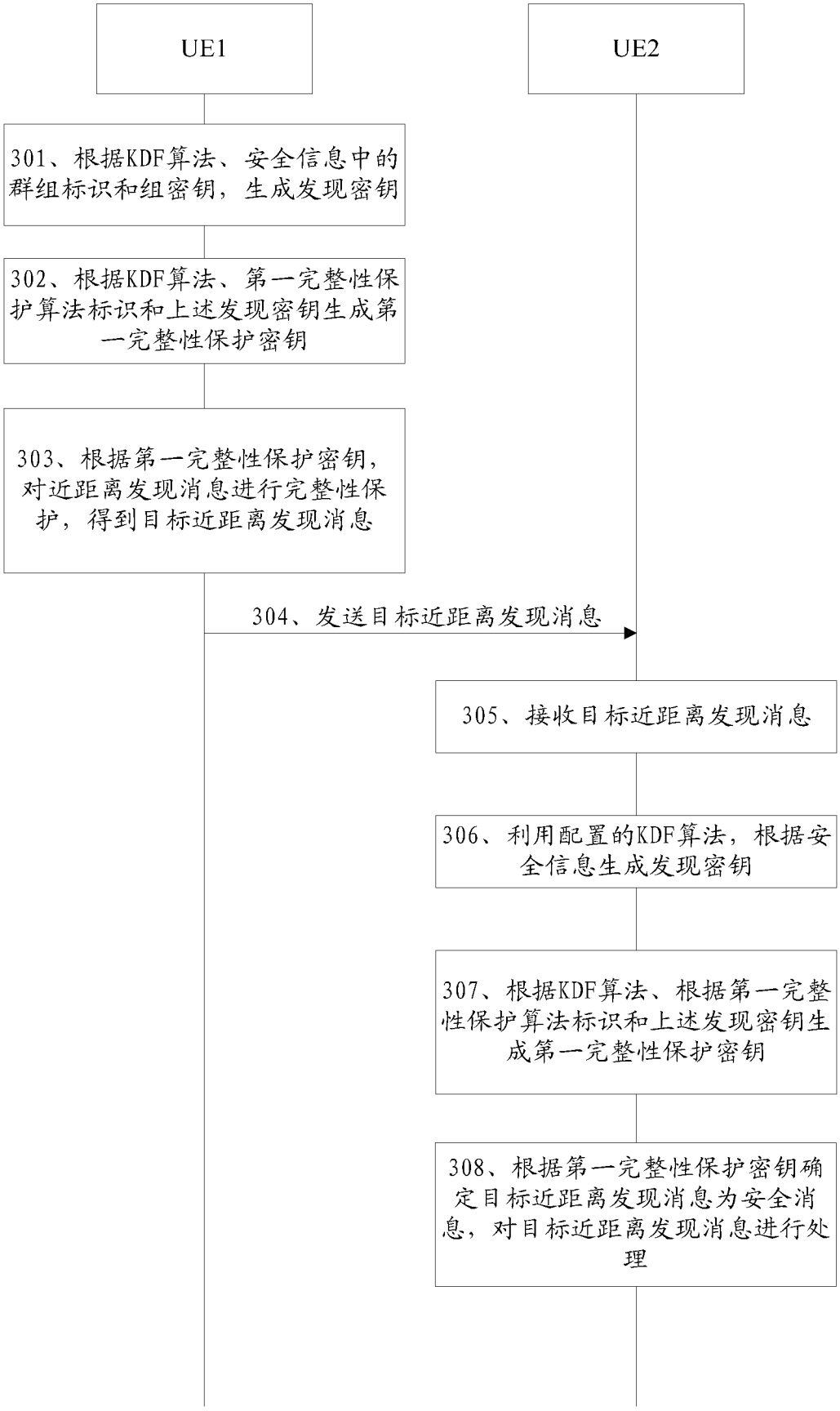
UE1
UE2
301、根据KDF算法、安全信息中的群组标识和组密钥，生成发现密钥
302、根据KDF算法、第一完整性保护算法标识和上述发现密钥生成第一完整性保护密钥
303、根据第一完整性保护密钥，对近距离发现消息进行完整性保护，得到目标近距离发现消息
304、发送目标近距离发现消息
305、接收目标近距离发现消息
306、利用配置的KDF算法，根据安全信息生成发现密钥
307、根据KDF算法、根据第一完整性保护算法标识和上述发现密钥生成第一完整性保护密钥
308、根据第一完整性保护密钥确定目标近距离发现消息为安全消息，对目标近距离发现消息进行处理

图 3a

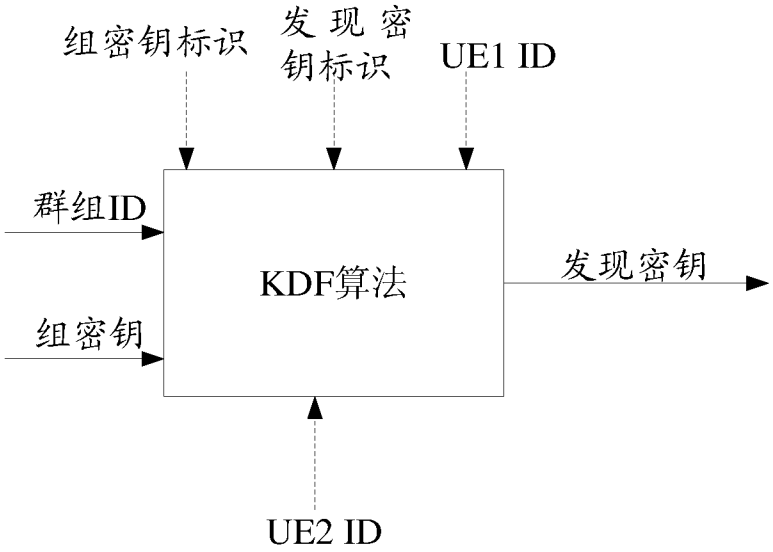
组密钥标识
发现密钥标识
UE1 ID
群组ID
KDF算法
发现密钥
组密钥
UE2 ID

图 3b

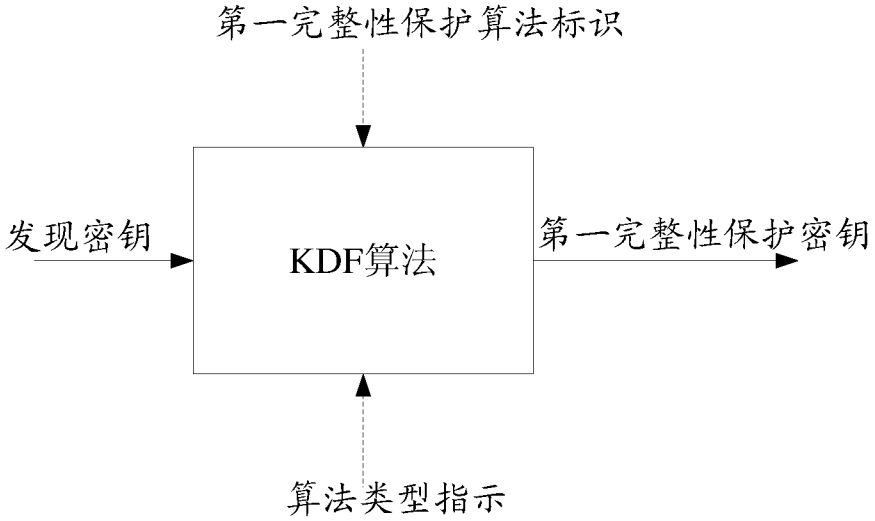
第一完整性保护算法标识
发现密钥
KDF算法
第一完整性保护密钥
算法类型指示

图 3c

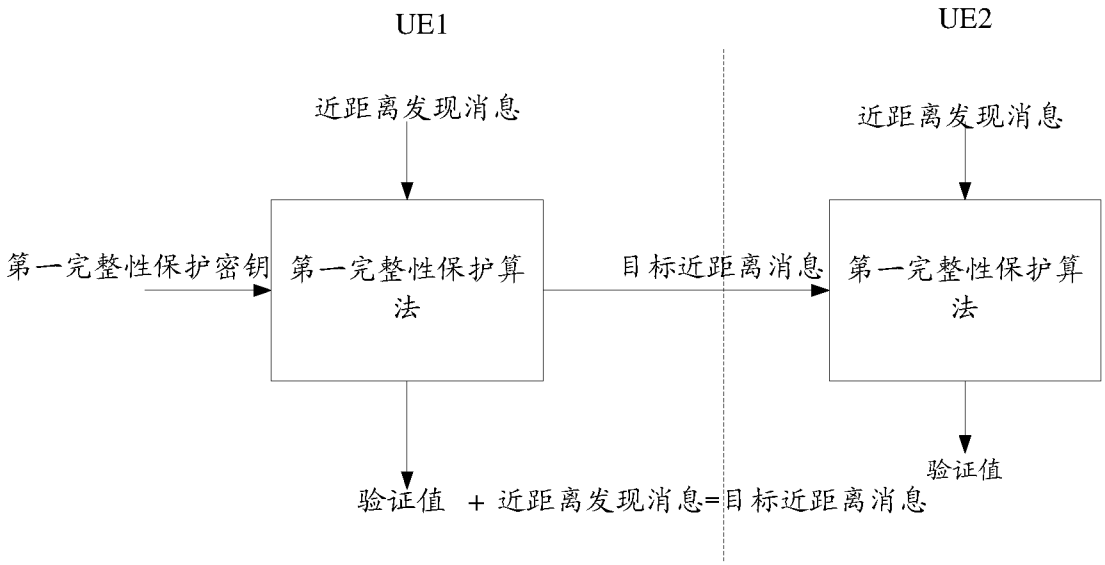
UE1
UE2
近距离发现消息
近距离发现消息
第一完整性保护密钥
第一完整性保护算法
目标近距离消息
第一完整性保护算法
验证值
验证值 + 近距离发现消息=目标近距离消息

图 3d

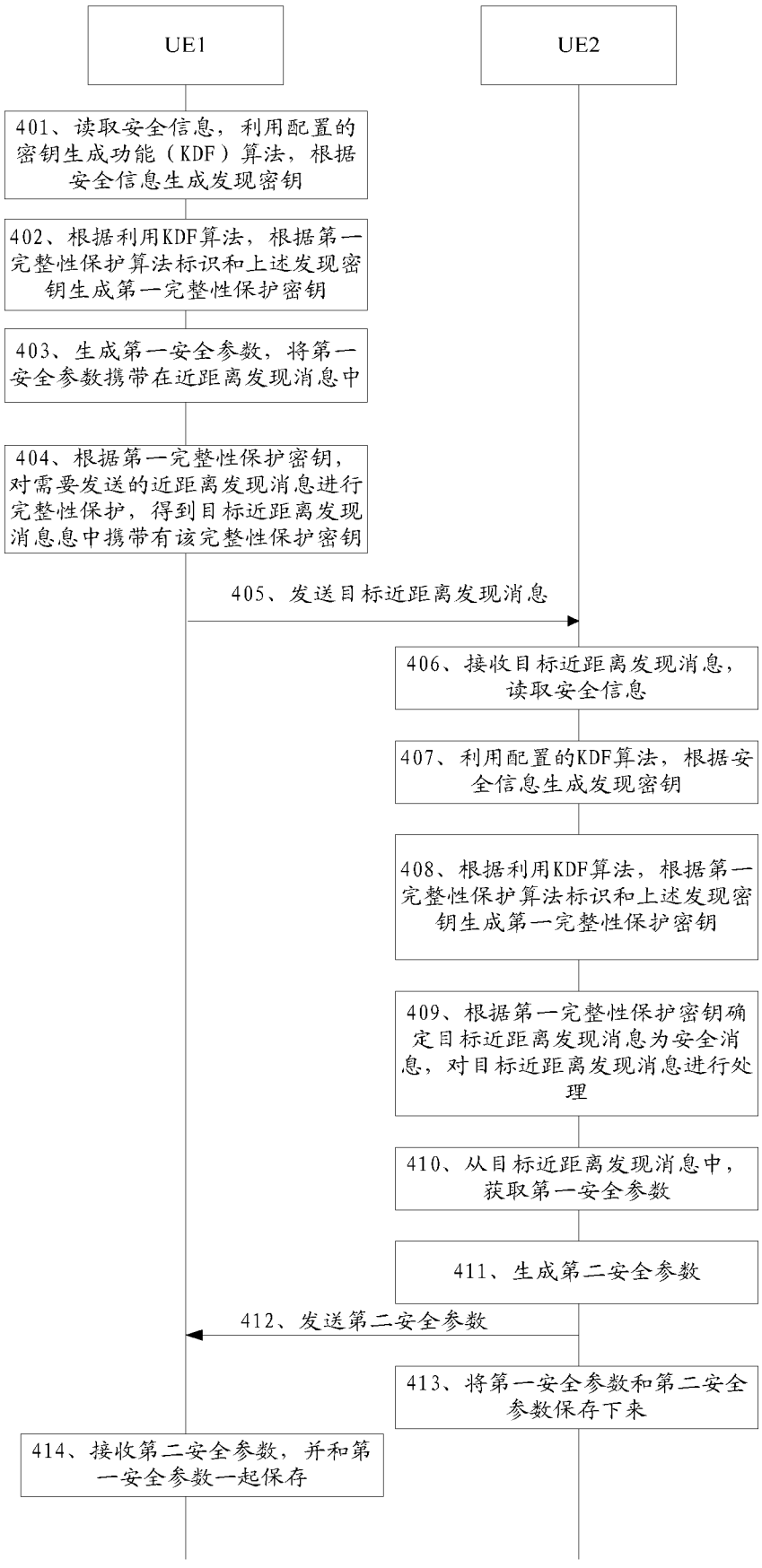
UE1
UE2
401、读取安全信息，利用配置的密钥生成功能（KDF）算法，根据安全信息生成发现密钥
402、根据利用KDF算法，根据第一完整性保护算法标识和上述发现密钥生成第一完整性保护密钥
403、生成第一安全参数，将第一安全参数携带在近距离发现消息中
404、根据第一完整性保护密钥，对需要发送的近距离发现消息进行完整性保护，得到目标近距离发现消息息中携带有该完整性保护密钥
405、发送目标近距离发现消息
406、接收目标近距离发现消息，读取安全信息
407、利用配置的KDF算法，根据安全信息生成发现密钥
408、根据利用KDF算法，根据第一完整性保护算法标识和上述发现密钥生成第一完整性保护密钥
409、根据第一完整性保护密钥确定目标近距离发现消息为安全消息，对目标近距离发现消息进行处理
410、从目标近距离发现消息中，获取第一安全参数
411、生成第二安全参数
412、发送第二安全参数
413、将第一安全参数和第二安全参数保存下来
414、接收第二安全参数，并和第一安全参数一起保存

图 4

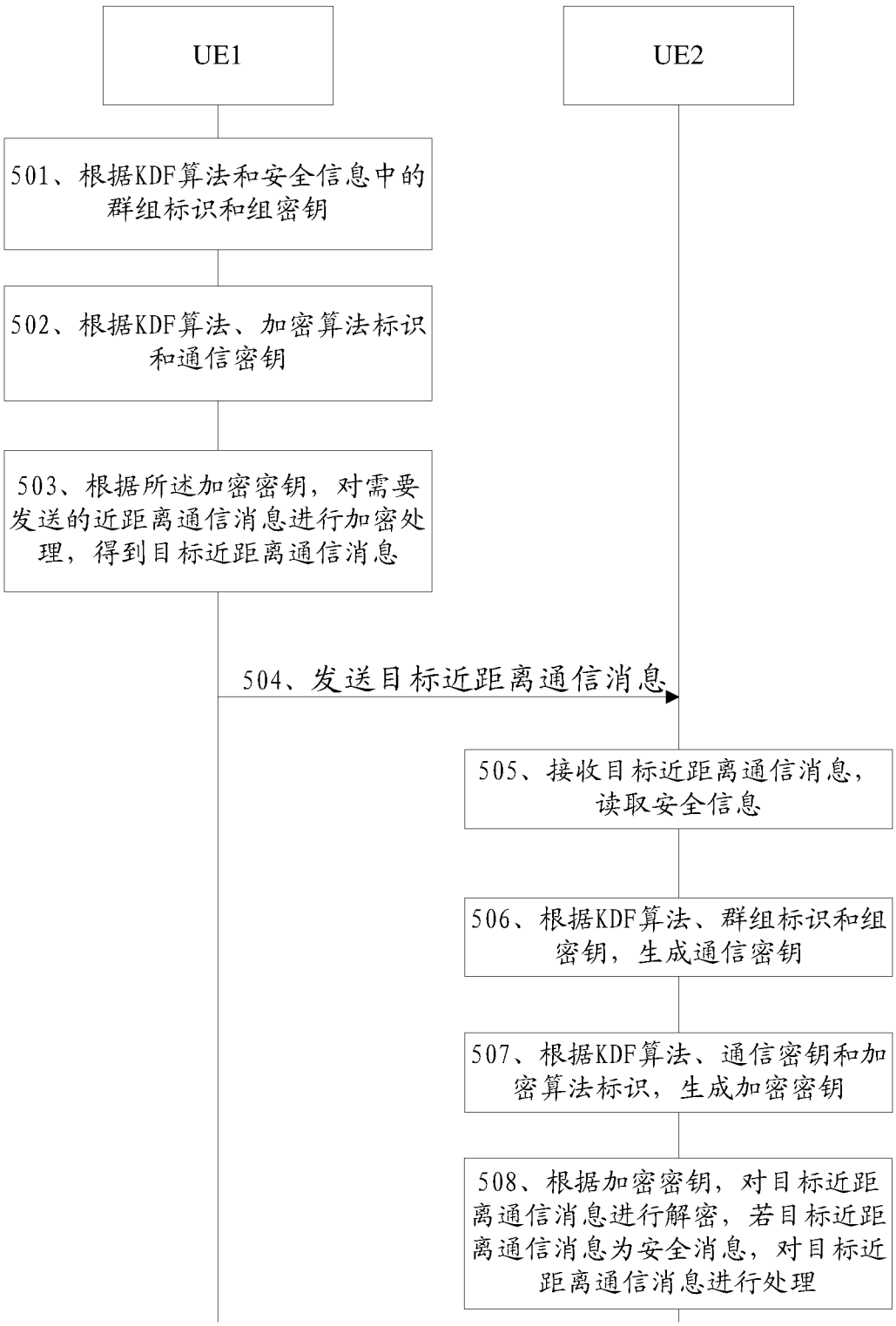
UE1
UE2
501、根据KDF算法和安全信息中的群组标识和组密钥
502、根据KDF算法、加密算法标识和通信密钥
503、根据所述加密密钥，对需要发送的近距离通信消息进行加密处理，得到目标近距离通信消息
504、发送目标近距离通信消息
505、接收目标近距离通信消息，读取安全信息
506、根据KDF算法、群组标识和组密钥，生成通信密钥
507、根据KDF算法、通信密钥和加密算法标识，生成加密密钥
508、根据加密密钥，对目标近距离通信消息进行解密，若目标近距离通信消息为安全消息，对目标近距离通信消息进行处理

图 5a

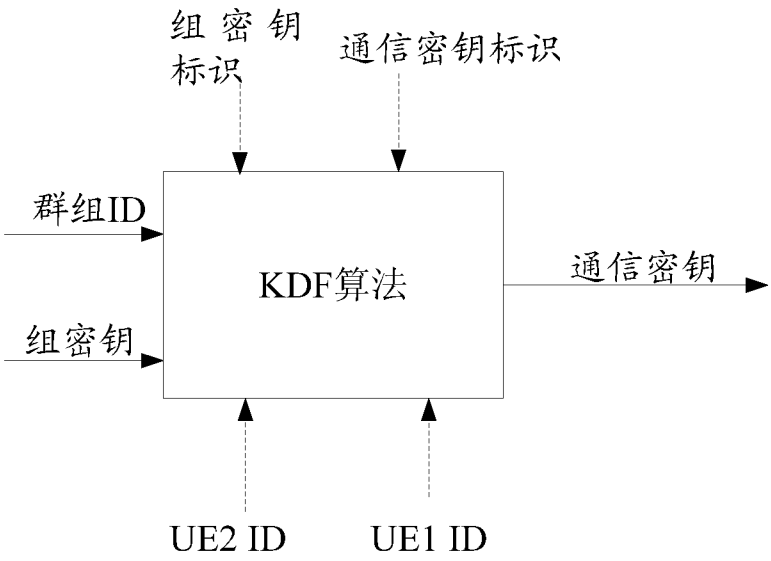
组密钥标识
通信密钥标识
群组ID
KDF算法
通信密钥
组密钥
UE2 ID
UE1 ID

图 5b

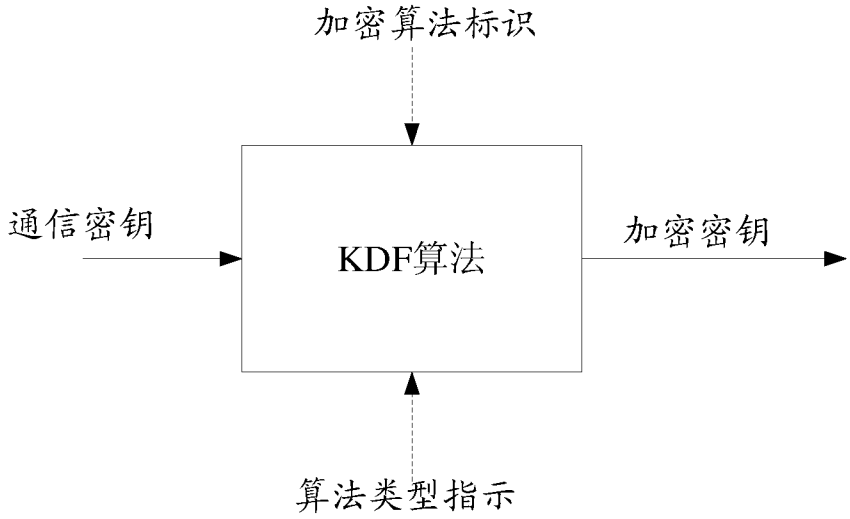
加密算法标识
通信密钥
KDF算法
加密密钥
算法类型指示

图 5c

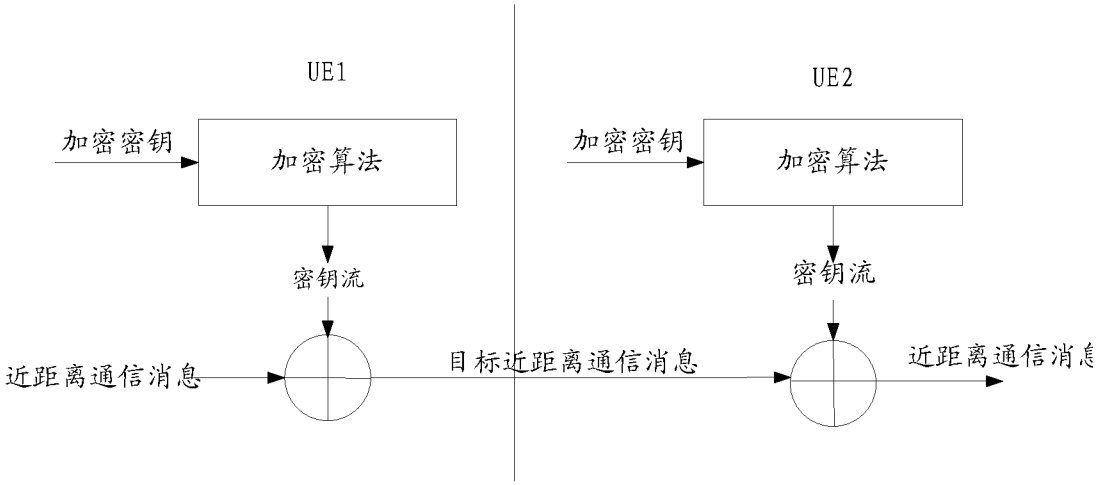
UE1
UE2
加密密钥
加密算法
加密密钥
加密算法
密钥流
密钥流
近距离通信消息
目标近距离通信消息
近距离通信消息

图 5d

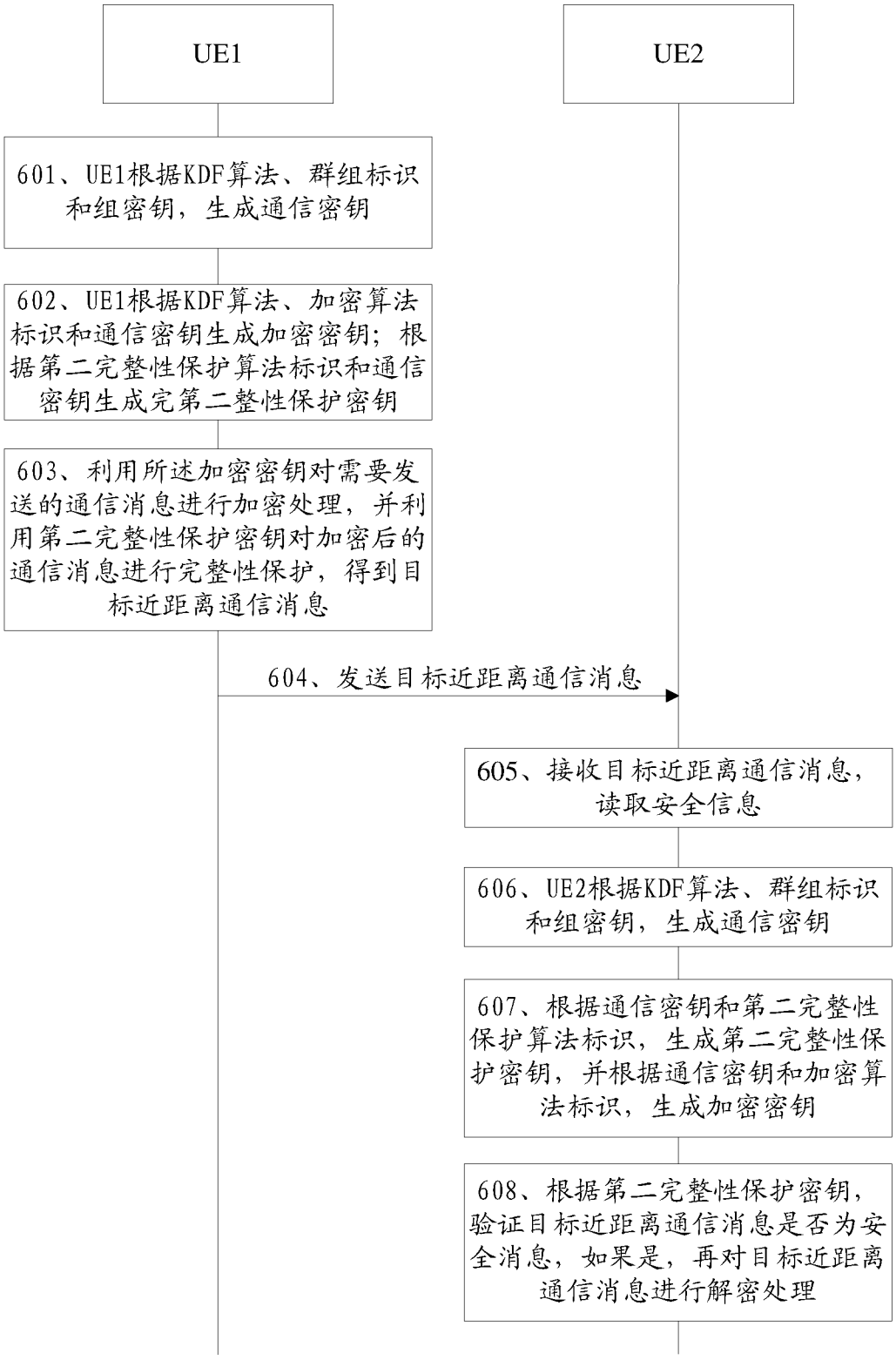
UE1
UE2
601、UE1根据KDF算法、群组标识和组密钥，生成通信密钥
602、UE1根据KDF算法、加密算法标识和通信密钥生成加密密钥；根据第二完整性保护算法标识和通信密钥生成完第二整性保护密钥
603、利用所述加密密钥对需要发送的通信消息进行加密处理，并利用第二完整性保护密钥对加密后的通信消息进行完整性保护，得到目标近距离通信消息
604、发送目标近距离通信消息
605、接收目标近距离通信消息，读取安全信息
606、UE2根据KDF算法、群组标识和组密钥，生成通信密钥
607、根据通信密钥和第二完整性保护算法标识，生成第二完整性保护密钥，并根据通信密钥和加密算法标识，生成加密密钥
608、根据第二完整性保护密钥，验证目标近距离通信消息是否为安全消息，如果是，再对目标近距离通信消息进行解密处理

图 6

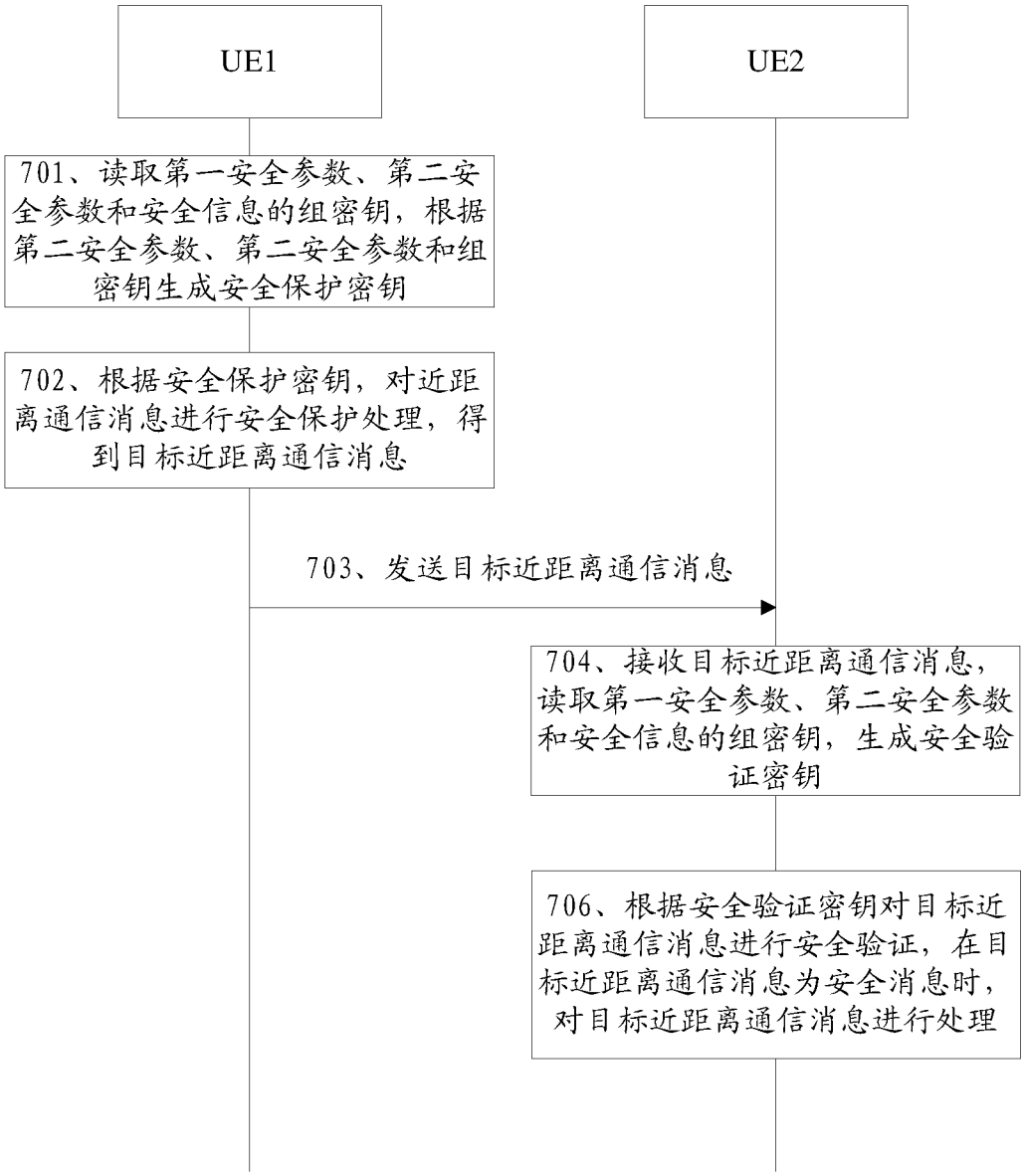
UE1
UE2
701、读取第一安全参数、第二安全参数和安全信息的组密钥，根据第二安全参数、第二安全参数和组密钥生成安全保护密钥
702、根据安全保护密钥，对近距离通信消息进行安全保护处理，得到目标近距离通信消息
703、发送目标近距离通信消息
704、接收目标近距离通信消息，读取第一安全参数、第二安全参数和安全信息的组密钥，生成安全验证密钥
706、根据安全验证密钥对目标近距离通信消息进行安全验证，在目标近距离通信消息为安全消息时，对目标近距离通信消息进行处理

图 7

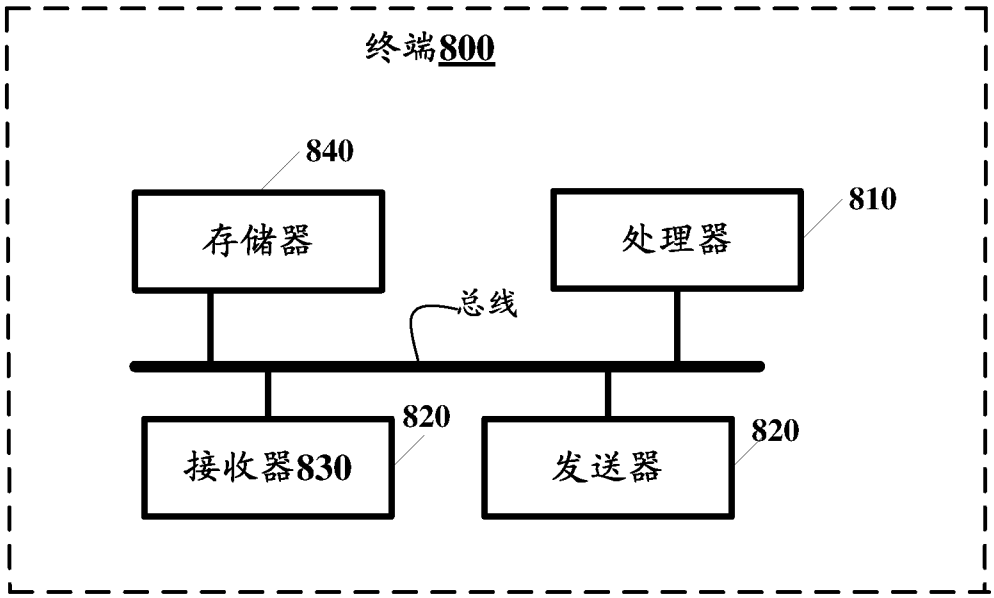
终端800
840
存储器
处理器
810
总线
820
接收器830
820
发送器

图 8

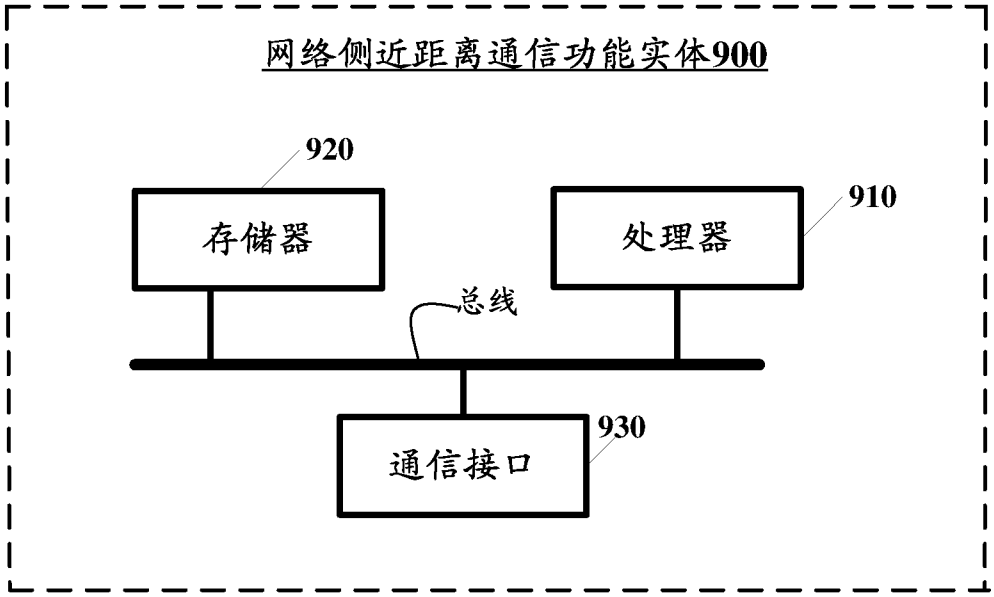
网络侧近距离通信功能实体900
920
存储器
处理器
910
总线
930
通信接口

图 9

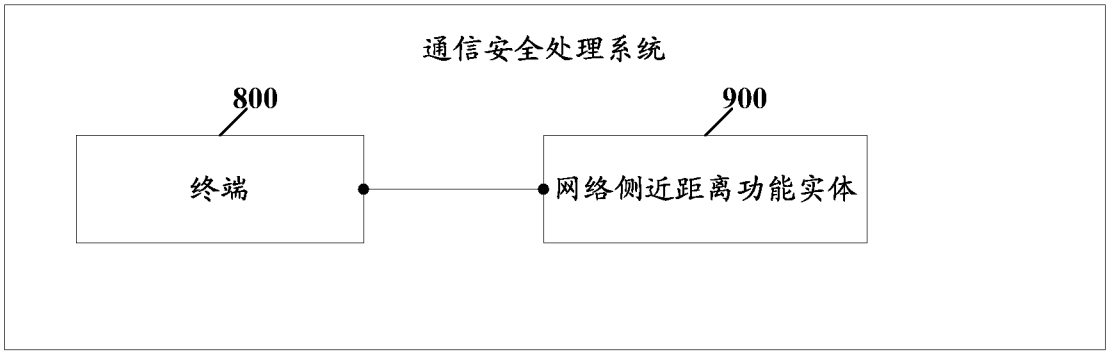
通信安全处理系统
800
900
终端
网络侧近距离功能实体

图 10

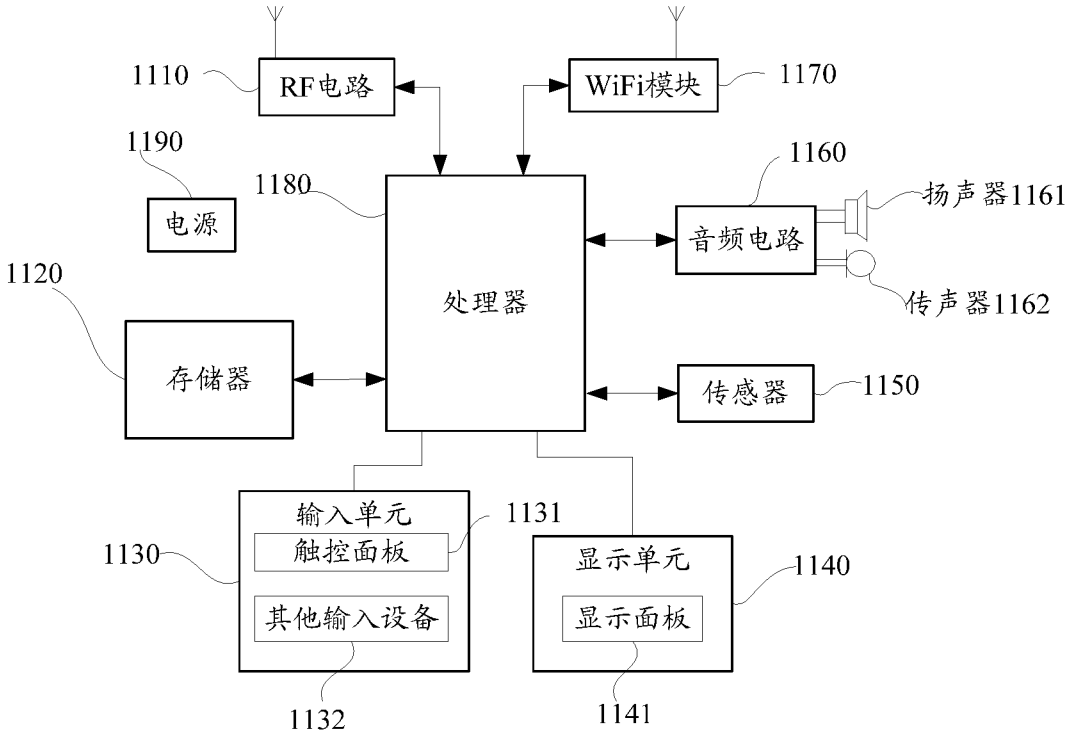
1110
RF电路
WiFi模块
1170
1190
电源
1180
处理器
1160
音频电路
扬声器1161
传声器1162
1120
存储器
传感器
1150
输入单元
1131
触控面板
1130
其他输入设备
显示单元
1140
显示面板
1132
1141

图 11

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/070379

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04 (2009.01) 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)

CNPAT; EPODOC; WPI; 3GPP: KDF, device to device, proximity service, service, D2D, function, proximity, group?, ProSe, key?, request, response

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	SAMSUNG, "Solution for key establishment between the Remote UE and UE-to-Network Relay,", 3GPP TSG SA WG3 (Security) Meeting #79 S3-151398, 24 April 2015 (24.04.2015), section 2	1-23
A	CN 105025478 A (ZTE CORP.), 04 November 2015 (04.11.2015), the whole document	1-23
A	CN 104935426 A (HUAWEI TECHNOLOGIES CO., LTD.), 23 September 2015 (23.09.2015), the whole document	1-23
A	WO 2015105402 A1 (SAMSUNG ELECTRONICS CO., LTD.), 16 July 2015 (16.07.2015), the whole document	1-23

☐ 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
03 August 2016 (03.08.2016)	**27 September 2016 (27.09.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **XU, Hongyan** Telephone No.: (86-10) **62413251**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/070379

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 105025478 A	04 November 2015	WO 2015165149 A1	05 November 2015
CN 104935426 A	23 September 2015	WO 2015139622 A1	24 September 2015
WO 2015105402 A1	16 July 2015	KR 20150084224 A	22 July 2015

国际检索报告

国际申请号
PCT/CN2016/070379

A. 主题的分类

H04W 12/04(2009.01)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）)

CNPAT;EPODOC;WPI;3GPP:密钥，请求，响应，组，群，KDF，设备到设备，device to device，proximity service，service，D2D，function，proximity，group?，ProSe，key?，request，response

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	SAMSUNG, . "Solution for key establishment between the Remote UE and UE-to-Network Relay, " 3GPP TSG SA WG3 (Security) Meeting #79 S3-151398, , 2015年 4月 24日 (2015-04-24), 第2节	1-23
A	CN 105025478 A (中兴通讯股份有限公司) 2015年 11月 4日 (2015-11-04) 全文	1-23
A	CN 104935426 A (华为技术有限公司) 2015年 9月 23日 (2015-09-23) 全文	1-23
A	WO 2015105402 A1 (SAMSUNG ELECTRONICS CO., LTD.) 2015年 7月 16日 (2015-07-16) 全文	1-23

☐ 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
2016年 8月 3日	2016年 9月 27日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 许洪岩 电话号码 (86-10)62413251

表 PCT/ISA/210 (第2页) (2009年7月)

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/070379

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	105025478	A	2015年 11月 4日	WO	2015165149	A1	2015年 11月 5日
CN	104935426	A	2015年 9月 23日	WO	2015139622	A1	2015年 9月 24日
WO	2015105402	A1	2015年 7月 16日	KR	20150084224	A	2015年 7月 22日