

(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
2022 年 1 月 27 日 (27.01.2022)



(10) 国际公布号
WO 2022/017158 A1

(51) 国际专利分类号:
H04W 12/04 (2021.01) H04W 12/08 (2021.01)

(21) 国际申请号: PCT/CN2021/104236

(22) 国际申请日: 2021 年 7 月 2 日 (02.07.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202010709512.0 2020 年 7 月 22 日 (22.07.2020) CN

(71) 申请人: 大唐移动通信设备有限公司 (DATANG MOBILE COMMUNICATIONS EQUIPMENT CO., LTD.) [CN/CN]; 中国北京市海淀区上地东路 5 号院 1 号楼 1 层, Beijing 100085 (CN)。

(72) 发明人: 王妍 (WANG, Yan); 中国北京市海淀区上地东路 5 号院 1 号楼 1 层, Beijing 100085 (CN)。
谌丽 (CHEN, Li); 中国北京市海淀区上地东路 5 号院 1 号楼 1 层, Beijing 100085 (CN)。

(74) 代理人: 北京银龙知识产权代理有限公司 (DRAGON INTELLECTUAL PROPERTY LAW

FIRM); 中国北京市海淀区西直门北大街 32 号院枫蓝国际中心 2 号楼 10 层, Beijing 100082 (CN)。

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

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

(54) Title: SECURITY MANAGEMENT METHOD, APPARATUS AND DEVICE BETWEEN USER AND MULTIPLE TERMINALS

(54) 发明名称: 用户与多终端间的安全性管理方法、装置及设备

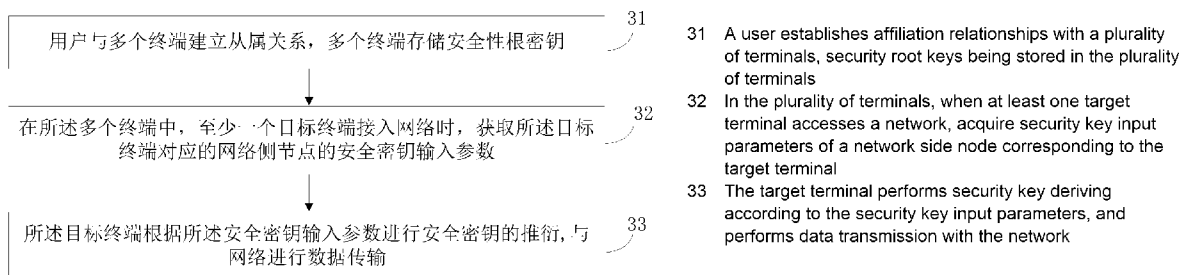


图 3

(57) Abstract: Disclosed in the present disclosure are a security management method, apparatus and device between a user and multiple terminals. The method comprises: the user establishing affiliation relationships with the plurality of terminals, security root keys being stored in the plurality of terminals; in the plurality of terminals, when at least one target terminal accesses a network, acquiring security key input parameters of a network side node corresponding to the target terminal; and the target terminal performing security key deriving according to the security key input parameters, and performing data transmission with the network.

(57) 摘要: 本公开公开了一种用户与多终端间的安全性管理方法、装置及设备。方法包括: 用户与多个终端建立从属关系, 多个终端存储安全性根密钥; 在所述多个终端中, 至少一个目标终端接入网络时, 获取所述目标终端对应的网络侧节点的安全密钥输入参数; 所述目标终端根据所述安全密钥输入参数进行安全密钥的推衍, 与网络进行数据传输。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

用户与多终端间的安全性管理方法、装置及设备

相关申请的交叉引用

本申请主张在 2020 年 7 月 22 日在中国提交的中国专利申请号 No. 202010709512.0 的优先权，其全部内容通过引用包含于此。

技术领域

本公开涉及通信技术领域，尤其涉及一种用户与多终端间的安全性管理方法、装置及设备。

背景技术

在无线通信蜂窝网中，为了保证网络安全，需要对信令 and 用户数据的传输进行加密和完整性保护。在单个用户终端与网络间节点派生相关密钥，共同进行通信过程的安全保障。

(1) 密钥体系

用户终端与网络节点间的密钥如图 1 所示，包括由用户和网络侧签约的长期密钥推导出终端与核心网节点的根密钥 K_{AMF} ，以及由终端和核心网节点从 K_{AMF} 推导出的 NAS 信令密钥 K_{NASint} , K_{NASenc} ，用于 NAS 信令的加密与完整性保护；还包括接入网节点的相关密钥，如由 K_{AMF} 推导的终端与接入节点间的密钥 K_{gNB} ，以及由终端和接入节点从 K_{gNB} 推导出的 AS 信令和传输数据密钥 K_{RRCint} , K_{RRCenc} , K_{UPint} , K_{UPenc} ，用于终端和接入节点间的信令和传输数据的加密和完整性保护。

(2) 双连接的安全机制

无线通信蜂窝网的双连接中，终端可连接至一个 MN (Master Node, 主节点) 以及一个 SN (Secondary Node, 辅节点)。MN 为 MN 和 UE 之间共享的给定 AS 安全上下文首次 SN 与 UE 之间建立安全上下文时，MN 为 SN 生成 K_{SN} 并通过 Xn-C 接口将其发送给 SN。为了生成 K_{SN} ，MN 将称为 SN 计数器的计数器与当前的 AS 安全上下文相关联。当需要生成新的 K_{SN} 时，MN 通过 RRC 信令路径将 SN 计数器的值发送给 UE。 K_{SN} 用于获取在 UE 和 SN

之间使用的进一步的 RRC 和 UP 密钥。

如图 2 所示，为由 MN 发起的 SN 添加/修改流程的安全过程，MN 通过 Xn-C 向 SN 发送 SN 添加/修改请求过程中，将 MN 根据 SN 计数器参数计算的 KSN 以及 UE 安全能力发送给 SN。SN 进行相关配置，并根据 KSN 计算所需的 RRC 和 UP 密钥。MN 在通过向 UE 发送 RRC 链接重配置请求，为其配置新的 DRB 和/或 SRB，且包括 SN 计数器参数。UE 将计算 SN 的 KSN 及相关 DRB 和/或 SRB 所需的 RRC 和 UP 密钥，UE 将重配置完成发送给 MN，并激活 SN 选择的加密和完整性保护密钥。在 SN 接收到 MN 发送的重配置完成后，激活 UE 所选择的加密和完整性保护。以上为 UE 与多个接入节点间的安全过程，仅针对单个终端的由 MN 到 SN 所需密钥的交互。

但在未来移动通信系统中，一个用户可在不同地点拥有多个终端设备，如公司、私家车、家里等地方可使用的多种类型终端设备，这些相互分离的终端设备在与用户建立从属关系后共同为一个用户提供服务。当用户移动时，可激活一个或多个终端设备以供使用。在这种单用户多终端的场景下，针对单个终端的安全性管理方法将不再适用于单用户多终端模式。

蜂窝网中的信息数据传输的安全性是以单个终端为目标的，未来通信系统中，一个用户可以有多个相互分离的从属终端，且多个终端相互关联，为一个用户提供服务，目前相关技术还不能支持单用户多终端场景下的数据传输安全性管理。

发明内容

本公开实施例提供了一种用户与多终端间的安全性管理方法、装置及设备。在用户终端的从属关系生效接入网络时，用户终端与网络侧安全密钥的输入参数通过网络节点进行传递，以保障用户终端与网络连接的安全性。

为解决上述技术问题，本公开的实施例提供如下技术方案：

一种用户与多终端间的安全性管理方法，应用于终端，所述方法包括：

用户与多个终端建立从属关系，多个终端存储安全性根密钥；

在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数；

所述目标终端根据所述安全密钥输入参数进行安全密钥的推衍，与网络进行数据传输。

可选的，存储安全性根密钥，包括：

获取用户的预设参数，所述预设参数包括：用户与网络侧签约的标识和/或用户与网络侧签约的第一密钥；

根据所述预设参数，存储所述安全性根密钥。

可选的，根据所述预设参数，存储安全性根密钥，包括：

所述多个终端与用户建立从属关系的过程中，根据用户与网络侧签约的第一密钥生成安全性根密钥并存储；

或者，

所述多个终端直接从所述用户接收所述第一密钥，并将所述第一密钥作为安全性根密钥进行存储。

可选的，在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应网络侧节点的安全密钥输入参数。

可选的，在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，核心网确定所述第二终端从属于第一终端的用户后，所述第二终端接收核心网发送的非接入NAS层的安全密钥输入参数集合以及接入网节点根密钥的输入参数，以及由所述核心网通知接入网节点进行接入AS层的安全密钥输入参数集合。

可选的，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，

所述核心网通知所述第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述第二接入网节点所发送的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述接入网节点发送的所述接入网节点的安全密钥输入参数。

可选的，在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一个终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，若所述第一终端与所述第二终端接入同一接入网节点，则该接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，触发非接入 NAS 层密钥及接入网节点根密钥输入参数的传递，所述第二终端接收所述接入网节点发送的接入 AS 层安全密钥输入参数以及接收所述核心网发送的安全输入参数。

可选的，根据所述预设参数，存储安全性根密钥，包括：

在用户与多个终端建立从属关系的过程中，根据用户与网络侧签约的第一密钥以及终端与用户建立从属关系时的终端计数值，生成安全性根密钥并存储；

或者，

在用户与多个终端建立从属关系的过程中，用户根据终端计数值，更新用户与网络侧签约的第一密钥，各终端获取与其对应的更新后的第一密钥，作为该终端的安全性根密钥并存储。

可选的，在所述多个终端中的至少一个目标终端接入网络时，获取所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

可选的，所述第二终端接收网络侧节点根据所述目标终端的计数值触发

并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网和接入网节点的根密钥推导参数以及非接入 NAS 层的密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

可选的，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网通知第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及接入网节点 AS 层的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

可选的，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，第二终端向网络侧上报第二终端所对应的终端计数值，接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新；接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，所述核心网通过所述第一终端与所述第二终端的关系，根据第二终端计数值及进行 NAS 或者 AS 根密钥参数的推算更新，第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

可选的，所述目标终端根据所述安全密钥输入参数与网络进行数据传输，包括：

所述第二终端根据所述安全密钥输入参数,激活非接入NAS层以及接入AS层的安全性,与网络进行数据传输。

可选的,当用户与多个终端的从属关系结束时,多个终端删除所存储的第二密钥。

本公开的实施例还提供一种用户与多终端间的安全性管理方法,应用于网络侧,所述方法包括:

从属于同一用户的多个终端中的至少一个目标终端接入网络时,网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数;

根据所述安全密钥输入参数与终端进行数据传输。

可选的,网络侧触发网络侧节点传递所述目标终端对应的接入节点的安全密钥输入参数,包括:

在所述多个终端中,首个与用户建立从属关系的第一终端,与用户的从属关系激活并接入网络后,进行初始认证及密钥协商流程,确定第一终端的第一密钥推衍集合;

在非首个与所述用户建立从属关系的目标终端接入网络时,根据用户与终端的从属关系,触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数。

可选的,根据所述第一终端的第一密钥推衍集合,触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数,包括:

核心网确定所述第二终端从属于第一终端的用户后,向第二终端发送非接入NAS层的安全密钥输入参数集合以及接入网节点根密钥的推衍参数,再由所述核心网通知接入网节点进行接入AS层的安全密钥输入参数集合。

可选的,根据所述第一终端的第一密钥推衍集合,触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数,包括:

若所述第一终端与所述第二终端接入同一接入网节点,则该接入网节点确定所述第一终端和所述第二终端从属于同一用户,并上报核心网,所述核心网触发非接入NAS层密钥及接入网节点根密钥输入参数的传递,接入网节点向所述第二终端发送接入AS层安全密钥输入参数。

可选的,网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的

安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

可选的，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网的非接入 NAS 层的密钥输入参数和接入网节点的根密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

可选的，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，网络侧接收第二终端上报的第二终端所对应的终端计数值，接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新；

所述接入网节点向所述第二终端发送安全密钥输入参数。

本公开的实施例还提供一种终端，包括：收发机，处理器，存储器，所述存储器上存有所述处理器可执行的程序；所述处理器执行所述程序时实现：用户与多个终端建立从属关系，多个终端存储安全性根密钥；在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数；所述目标终端根据所述安全密钥输入参数进行安全密钥的推衍，与网络进行数据传输。

可选的，存储安全性根密钥，包括：

获取用户的预设参数，所述预设参数包括：用户与网络侧签约的标识和/或用户与网络侧签约的第一密钥；

根据所述预设参数，存储所述安全性根密钥。

可选的，根据所述预设参数，存储安全性根密钥，包括：

所述多个终端与用户建立从属关系的过程中，根据用户与网络侧签约的第一密钥生成安全性根密钥并存储；

或者，

所述多个终端直接从所述用户接收所述第一密钥，并将所述第一密钥作为安全性根密钥进行存储。

可选的，在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应网络侧节点的安全密钥输入参数。

可选的，根据所述预设参数，存储安全性根密钥，包括：

在用户与多个终端建立从属关系的过程中，根据用户与网络侧签约的第一密钥以及终端与用户建立从属关系时的终端计数值，生成安全性根密钥并存储；

或者，

在用户与多个终端建立从属关系的过程中，用户根据终端计数值，更新用户与网络侧签约的第一密钥，各终端获取与其对应的更新后的第一密钥，作为该终端的安全性根密钥并存储。

可选的，在所述多个终端中的至少一个目标终端接入网络时，获取所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

本公开的实施例还提供一种用户与多终端间的安全性管理装置，应用于

终端，所述装置包括：

存储模块，用于用户与多个终端建立从属关系，多个终端存储安全性根密钥；

获取模块，用于在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数；

处理模块，用于根据所述安全密钥输入参数进行安全密钥的推衍与网络进行数据传输。

本公开的实施例还提供一种网络侧设备，包括：收发机，处理器，存储器，所述存储器上存有所述处理器可执行的程序；所述处理器执行所述程序时实现：从属于同一用户的多个终端中的至少一个目标终端接入网络时，网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数；根据所述安全密钥输入参数与终端进行数据传输。

本公开的实施例还提供一种用户与多终端间的安全性管理装置，应用于网络侧设备，所述装置包括：

处理模块，用于从属于同一用户的多个终端中的至少一个目标终端接入网络时，网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数；

收发模块，用于根据所述安全密钥输入参数与终端进行数据传输。

本公开的实施例还提供一种处理器可读存储介质，所述处理器可读存储介质存储有处理器可执行指令，所述处理器可执行指令用于使所述处理器执行如上所述的方法。

本公开实施例的有益效果是：

本公开的上述实施例，通过用户与多个终端建立从属关系，多个终端存储安全性根密钥；在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数；所述目标终端根据所述安全密钥输入参数进行安全密钥的推衍，与网络进行数据传输。在用户终端的从属关系生效接入网络时，用户终端与网络侧安全密钥的输入参数通过网络节点进行传递，以保障用户终端与网络连接的安全性。

附图说明

图 1 是密钥体系的示意图；

图 2 是双连接的安全机制示意图；

图 3 是本公开的用户与多终端间的安全性管理方法流程示意图；

图 4 是本公开的实施例中核心网节点触发的多终端安全性管理流程示意图；

图 5 是本公开的实施例中接入网节点触发的多终端安全性管理流程示意图；

图 6 是本公开的实施例中核心网节点触发的多终端安全性管理流程示意图；

图 7 是本公开的实施例中接入网节点触发的多终端安全性管理流程示意图；

图 8 是本公开的实施例终端的架构示意图；

图 9 是本公开的实施例用户与多终端分离架构下的安全性管理装置的模块示意图。

具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

如图 3 所示，本公开的实施例提供一种用户与多终端间的安全性管理方法，应用于终端，所述方法包括：

步骤 31，用户与多个终端建立从属关系，多个终端存储安全性根密钥；

步骤 32，在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数；

步骤 33，所述目标终端根据所述安全密钥输入参数进行安全密钥的推衍，与网络进行数据传输。

本公开的该实施例，用户可与多个终端建立从属关系，并于终端侧存储

用户安全性根密钥。在用户终端的从属关系生效接入网络时，用户终端与网络侧安全密钥的输入参数通过网络节点进行传递，以保障用户终端与网络连接的安全性。

本公开的一可选的实施例中，存储安全性根密钥，包括：

步骤 311，获取用户的预设参数，所述预设参数包括：用户与网络侧签约的标识和/或用户与核心网侧签约的第一密钥；

步骤 312，根据所述预设参数，存储所述安全性根密钥。

可选的，步骤 312 可以包括：

方式一：所述多个终端与用户建立从属关系的过程中，根据用户与网络侧签约的第一密钥生成安全性根密钥并存储；或者，所述多个终端直接从所述用户接收所述第一密钥，并将所述第一密钥作为安全性根密钥进行存储。

方式二：在用户与多个终端建立从属关系的过程中，根据用户与网络侧签约的第一密钥以及终端与用户建立从属关系时的终端计数值，生成安全性根密钥并存储；或者，在用户与多个终端建立从属关系的过程中，用户根据终端计数值，更新用户与网络侧签约的第一密钥，各终端获取与其对应的更新后的第一密钥，作为该终端的安全性根密钥并存储。

这里，用户可与多个终端建立从属关系，即用户在与终端建立从属关系时将特有参数信息传递给终端，如用户签约标识以及用户与核心网侧签约的长期安全性根密钥，并于终端侧进行存储，以确定该终端从属于用户，为其提供服务。

用户与多个终端建立从属关系后，终端侧存储的安全性根密钥形式，采用以下方式之一：

用户具有与核心网侧签约的长期安全性根密钥，在与终端建立从属关系后，将由长期密钥自生成安全性密钥，如加密与完整性根密钥，所有从属于用户的终端具有相同根密钥，并存储于终端内部。或，用户直接将相同的用户长期根密钥传递并存储于从属终端内部。

用户具有的长期安全性根密钥根据 UE COUNT 值进行从属终端安全性密钥的自生成，如加密与完整性根密钥，根据终端建立从属关系的先后顺序于终端侧存储不同的安全性根密钥。或，用户根据 UE COUNT 值更新用户与

网络侧签约的长期安全性根密钥，不同的终端存储与 UE COUNT 值相对应的安全性长期根密钥。

在首个终端与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，根据根密钥等参数进行接入网与核心网的安全密钥参数推衍，保证用户面与控制面的安全性传输。

本公开的一可选的实施例中，基于上述方式一，步骤 32 可以包括：

步骤 321，在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

步骤 322，在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应网络侧节点的安全密钥输入参数。

可选的，由核心网节点触发参数传递：步骤 322 可以包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，核心网确定所述第二终端从属于第一终端的用户后，所述第二终端接收核心网发送的非接入 NAS 层的安全密钥输入参数集合以及接入网节点根密钥的输入参数，以及由核心网通知接入网节点进行接入 AS 层的安全密钥输入参数集合。

基于核心网节点触发参数传递的方式，可选的，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，所述核心网通知所述第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述第二接入网节点所发送的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述接入网节点发送的所述接入网节点的安全密钥输入参数。

也就是说，由核心网节点触发方式中，核心网节点：当第二终端 2（与用户建立从属关系的非首个终端）接入网络后，核心网确定其从属于第一终端（与用户建立从属关系的首个终端）的用户后，将第一终端的核心网及接入网根密钥计算参数、NAS 层的密钥推衍集合（如算法类型、算法标识符）发

送给该用户的第二终端，以进行 NAS 层安全参数的推衍。并通知接入网节点将 AS 层的密钥推衍集合发送给第二终端，以进行 AS 层参数的推衍。

接入网节点：若第一终端（与用户建立从属关系的首个终端）和第二终端（与用户建立从属关系的非首个终端）接入同一接入网节点，则直接由该接入网节点进行 AS 密钥参数推衍集合的传递；若第一终端和第二终端接入不同接入网节点，则由第一终端的第一接入节点将推衍的接入节点密钥参数（如推衍密钥、计数器参数等）通过接口发送给第二终端的第二接入节点，并将计数器参数发送给核心网侧，再由核心网侧转发给第二终端，进行其接入网节点密钥推算，确保第二终端与其接入节点的数据传输安全。

用户从属第二终端：在接收到 NAS 和 AS 层密钥参数推衍集合后，进行相关密钥参数的推算，并激活 NAS 层和 AS 层的安全过程，以保障信令及用户数据传输的安全性。

本公开的一可选的实施例中，基于上述方式一，接入网节点触发参数传递的情况：步骤 322 可以包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，若所述第一终端与所述第二终端接入同一接入网节点，则该接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，触发非接入 NAS 层密钥及接入网节点根密钥输入参数的传递，所述第二终端接收所述接入网节点发送的接入 AS 层安全密钥输入参数以及接收所述核心网发送的安全输入参数。

也就是说，由接入网节点触发的情况下：

接入网节点：第二终端（与用户建立从属关系的非首个终端）接入网络后，若第一终端（与用户建立从属关系的首个终端）与第二终端接入同一接入网节点，则该接入网节点确定两终端从属于同一用户，向第二终端发送 AS 层的密钥推衍集合，并上报核心网两终端关系，触发密钥参数的传递。

核心网节点：由核心网向第二终端（与用户建立从属关系的非首个终端）发送第一终端（与用户建立从属关系的首个终端）的核心网及接入网根密钥计算参数及 NAS 层的密钥推衍集合。

用户从属第二终端：第二终端进行相关密钥参数的推衍以及安全过程的激活，以确保第二终端与网络的数据传输安全性。

若两终端接入不同的接入节点，则由接入网节点将终端信息发送给核心网节点，由核心网侧触发不同接入节点下的安全密钥参数传递过程。

本公开的一可选的实施例中，基于上述方式二，步骤 32 可以包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

基于上述方式二，由核心网节点触发参数传递的方式，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

可选的，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网通知第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及接入网节点 AS 层的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

也就是说，由核心网触发的情况下，在第二当终端（与用户建立从属关

系的非首个终端)接入网络后,向核心网侧上报其对应的 UE COUNT 值,核心网在确定其从属于第一终端(与用户建立从属关系的首个终端)的用户后,根据所存储的第一终端的核心网密钥根据 UE COUNT 值进行第二终端的密钥更新,并将第一终端的核心网及接入网根密钥计算参数、NAS 层的密钥推衍集合发送给第二终端,以进行 NAS 层安全参数的推衍。并通知接入网节点根据 UE COUNT 值将 AS 层的密钥进行更新,将推衍集合发送给第二终端,以进行 AS 层参数的推衍。针对相同或不同的终端节点,采用同方式一相同方法。

本公开的一可选的实施例中,基于上述方式二,由接入网节点触发:所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数,包括:

在非首个与所述用户建立从属关系的第二终端接入网络后,第二终端向网络侧上报第二终端所对应的终端计数值,接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新;接入网节点确定所述第一终端和所述第二终端从属于同一用户,并上报核心网,所述核心网通过所述第一终端与所述第二终端的关系,根据第二终端计数值进行 NAS 或者 AS 根密钥参数的推算更新,第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

也就是说,由接入网节点触发的情况下:第二终端接入网络后,与方式一不同的是,首先第二终端向网络侧上报第二终端所对应的 UE COUNT 参数,网络侧节点根据 UE COUNT 值进行对应密钥参数的更新,再进行第二终端密钥推衍集合的传递。

本公开的一可选的实施例中,步骤 33 可以包括:

所述第二终端根据所述安全密钥输入参数,激活非接入 NAS 层以及接入层的安全性,与网络进行数据传输。

可选的,当用户与多个终端的从属关系结束时,多个终端删除所存储的第二密钥。当用户与终端的从属关系结束时,终端侧删除所存储的用户相关参数信息。

下面结合具体的实例,说明上述方法的具体实现过程:

实施例一：基于上述方式一的情况下，核心网节点触发的多终端安全管理，与用户建立从属关系的两个终端分别接入不同的接入节点：

如图 4 所示，该流程包括：

步骤 0：终端 1（与用户建立从属关系的首个终端）与终端 2（与用户建立从属关系的非首个终端）建立与用户的从属关系，获取相同的用户特有参数信息，如用户签约标识等用户特有标识及与网络侧相对应的安全性密钥等。

所获取的安全性密钥参数如下：

用户直接将其长期安全性根密钥存储于从属终端内部；

或，由用户长期安全性根密钥自生成加密与完整性保护根密钥，存储于终端内部，且各终端的安全性密钥相同。

步骤 1：首个与用户建立从属关系的终端 1 接入网络（接入节点 1 和核心网），完成用户的注册及认证流程，并建立与网络侧的密钥体系。

步骤 2：当用户激活从属终端 2（例如，与用户第二个建立从属关系的终端）后，通过接入节点 2 接入网络，核心网侧根据终端 2 所携带的用户特有标识确定其所从属的用户，并识别用户的所有从属终端。

步骤 3：核心网将终端 1 所对应的核心网及接入网根密钥计算参数、NAS 层密钥推衍集合（如算法类型、算法标识符等）发送给终端 2，使终端进行 NAS 层密钥参数的推衍。

步骤 4：激活终端 2 与核心网侧的安全性，包括信令及用户数据的加密与完整性保护的安全过程。

步骤 5：由核心网侧触发接入节点 1 进行接入网密钥集合的传递，触发消息中包括终端 2 的接入节点信息及相关参数信息。

步骤 6：接入节点 1 根据终端 1 的接入节点根密钥进行接入节点 2 的密钥推衍，将推衍密钥发送给接入节点 2，并于向核心网反馈的消息中，将终端 2 的接入节点的密钥推衍集合发送给核心网侧。

步骤 7：核心网将终端 2 的接入节点密钥推衍集合（如算法类型、算法标识等）转发给终端 2。

步骤 8：终端 2 利用密钥推衍集合参数信息推衍接入节点的相关密钥参数信息，并激活与接入节点 2 的安全性，包括信令及用户数据的加密与完整

性保护的安全过程。

步骤 9：在完成用户从属终端 2 的接入网与核心网的安全激活流程后，终端可与网络侧安全地进行数据信息传递。

实施例 2：核心网节点触发的多终端安全性管理（方式 1），与用户建立从属关系的两个终端分别接入相同的接入节点的实现方式中，与上述实施例 1 的区别在于，将接入节点 1 和接入节点 2 合并为一个接入节点，步骤 6 中：接入节点根据终端 1 的接入节点根密钥进行接入节点的密钥推衍，将推衍密钥向核心网反馈。

实施例 3：基于上述方式一的情况下，接入网节点触发的多终端安全性管理（两终端同一接入节点）：

如图 5 所示，该流程包括：

步骤 0：终端 1 与终端 2 建立与用户的从属关系，获取相同的用户特有参数信息，如用户签约标识等用户特有标识及与网络侧相对应的安全性密钥等。所获取的安全性密钥参数如下：

用户直接将其长期安全性根密钥存储于从属终端内部；

或，由用户长期密钥自生成的加密与完整性保护根密钥，存储于终端内部，且各终端的安全性密钥相同。

步骤 1：用户的首个从属终端 1 接入网络（接入节点和核心网），完成用户的注册及认证流程，并建立与网络侧的密钥体系。

步骤 2：当用户激活从属终端 2 后，通过接入节点接入网络，接入网节点根据终端 2 所携带的用户标识确定其所从属的用户，并识别用户的所有从属终端。

步骤 3：接入节点向核心网侧上报用户从属终端 1 与终端 2 的关系，并指示进行终端 2 的 NAS/AS 密钥参数的传递。

步骤 4：核心网将终端 1 的核心网及接入网根密钥计算参数、NAS 层密钥推衍集合（如算法类型、算法标识等）转发给终端 2。

步骤 5：终端 2 利用核心网及接入网根密钥计算参数推衍其核心网和接入网的根密钥参数，再利用密钥推衍集合参数信息推衍与核心网节点的相关密钥参数，并激活核心网侧的安全性，包括信令及用户数据的加密与完整性

保护的安全过程。

步骤 6: 终端 1 与终端 2 从属于同一接入节点, 则直接由接入节点将终端 1 相关联的 AS 密钥推衍集合 (如算法类型、算法标识等) 发送给终端 2。

步骤 7: 终端 2 利用密钥推衍集合参数信息推衍与接入网节点的相关密钥参数信息, 并激活终端 2 与接入网侧的安全性, 包括信令及用户数据的加密与完整性保护的安全过程。

步骤 8: 在完成用户从属终端 2 的接入网与核心网的安全激活流程后, 终端可与网络侧安全地进行数据信息传递。

实施例 4: 接入网节点触发的多终端安全性管理 (方式 1, 若两终端接入不同的接入节点), 由接入网节点将终端信息发送给核心网节点, 由核心网侧触发不同接入节点下的安全密钥参数传递过程, 可参考实施例 1 中相对应过程。

实施例 5: 基于上述方式二的情况下, 核心网节点触发的多终端安全性管理 (两终端接入不同的接入节点):

如图 6 所示, 该流程包括:

步骤 0: 终端 1 与终端 2 建立与用户的从属关系, 获取用户特有参数信息, 如用户签约标识等用户特定标识及与网络侧相对应的安全性密钥等。所获取的安全性密钥参数如下:

用户根据其长期密钥利用 UE COUNT 值进行从属终端安全性根密钥的更新, 并存储于终端内部。其中用户第一个从属终端所对应的 UE COUNT=0, 具有与用户相同的长期密钥, 之后与用户建立从属关系的终端的 UE COUNT 值递增;

或, 由用户长期密钥利用 UE COUNT 值自生成加密与完整性根密钥, 存储于终端内部, 且各终端的安全性密钥参数不同。

步骤 1: 用户的首个从属终端 1 接入网络 (接入节点 1 和核心网), 完成用户的注册及认证流程, 并建立与网络侧的密钥体系。

步骤 2: 当用户激活从属终端 2 后, 通过接入节点接入网络, 核心网节点根据终端 2 所携带的用户标识确定其所从属的用户, 并识别用户的所有从属终端。

步骤 3: 核心网侧通过用户从属终端 1 与终端 2 的关系, 根据 UE COUNT 值及网络侧的用户长期密钥进行终端 2 的 NAS 根密钥参数的更新。

步骤 4: 核心网将终端 2 所对应的核心网及接入网根密钥计算参数、NAS 层密钥推衍集合 (如算法类型、算法标识符等) 发送给终端 2, 使终端进行 NAS 层密钥参数的推衍。

步骤 5: 激活终端 2 与核心网侧的安全性, 包括信令及用户数据的加密与完整性保护的安全过程。

步骤 6: 由核心网侧触发接入节点 1 进行接入网密钥集合的传递, 触发消息中包括终端 2 的接入节点信息及相关参数信息。

步骤 7: 接入节点 1 根据终端 1 的接入节点根密钥及 UE COUNT 值进行接入节点 2 的密钥推衍, 将推衍密钥发送给接入节点 2, 并于向核心网反馈的消息中将终端 2 接入节点的密钥推衍集合发送给核心网侧。

步骤 8: 核心网将终端 2 的接入节点密钥推衍集合 (如算法类型、算法标识等) 转发给终端 2。

步骤 9: 终端 2 利用密钥推衍集合参数信息推衍接入节点的相关密钥参数信息, 并激活与接入节点 2 的安全性, 包括信令及用户数据的加密与完整性保护的安全过程。

步骤 10: 在完成用户从属终端 2 的接入网与核心网的安全激活流程后, 终端可与网络侧安全地进行数据信息传递。

实施例 6: 核心网节点触发的多终端安全性管理 (方式 2, 两终端接入相同的接入节点), 与上述实施例 5 的区别在于, 将接入节点 1 和接入节点 2 合并为一个接入节点, 步骤 7 中: 接入节点根据终端 1 的接入节点根密钥进行接入节点的密钥推衍, 将推衍密钥向核心网反馈。步骤 8 中, 核心网将接入节点密钥推衍集合 (如算法类型、算法标识等) 转发给终端 2。

实施例 7: 基于上述方式二的情况下, 接入网节点触发的多终端安全性管理 (两终端同一接入节点)

如图 7 所示, 该流程包括:

步骤 0: 终端 1 与终端 2 建立与用户的从属关系, 获取用户特有参数信息, 如用户签约标识等用户特定标识及与网络侧相对应的安全性密钥等。所

获取的安全性密钥参数如下：

用户根据其长期密钥利用 UE COUNT 值进行从属终端安全性根密钥的更新,并存储于终端内部。其中用户第一个从属终端所对应的 UE COUNT=0,具有与用户相同的长期密钥,之后与用户建立从属关系的终端的 UE COUNT 值递增;

或,由用户长期密钥利用 UE COUNT 值自生成加密与完整性保护的根密钥,存储于终端内部,且各终端的安全性密钥参数不同。

步骤 1: 用户的首个从属终端 1 接入网络(接入节点和核心网),完成用户的注册及认证流程,并建立与网络侧的密钥体系。

步骤 2: 当用户激活从属终端 2 后,通过接入节点接入网络,接入网节点根据终端 2 所携带的用户标识确定其所从属的用户,并识别用户的所有从属终端。

步骤 3: 接入节点根据终端 2 的 UE COUNT 值进行接入节点密钥参数的更新。

步骤 4: 接入节点向核心网侧上报用户从属终端 1 与终端 2 的关系,并指示进行终端 2 的 NAS 密钥参数的更新与传递。

步骤 5: 核心网侧通过用户从属终端 1 与终端 2 的关系,根据 UE COUNT 值及终端 1 的长期密钥进行终端 2 的 NAS/AS 根密钥参数的推算更新。

步骤 6: 核心网将终端 1 的核心网及接入网根密钥计算参数、NAS 层密钥推衍集合(如算法类型、算法标识等)发送给终端 2。

步骤 7: 终端 2 利用核心网及接入网根密钥计算参数更新接入网与核心网的根密钥,再根据密钥推衍集合参数信息推衍与核心网节点的相关密钥参数信息,并激活核心网侧的安全性,包括信令及用户数据的加密与完整性保护的安全过程。

步骤 8: 终端 1 与终端 2 从属于同一接入节点,则直接由接入节点将根据 UE COUNT 值更新后 AS 密钥推衍集合(如算法类型、算法标识等)发送给终端 2。

步骤 9: 终端 2 利用密钥推衍集合参数信息推衍与接入网节点的相关密钥参数信息,并激活接入网侧的安全性,包括信令及用户数据的加密与完整

性保护的安全过程。

步骤 10：在完成用户从属终端 2 的接入网与核心网的安全激活流程后，终端可与网络侧安全地进行数据信息传递。

实施例 8：若两终端接入不同的接入节点，则由接入网节点将终端信息发送给核心网节点，由核心网侧触发不同接入节点下的安全密钥参数更新与传递过程，可参考实施例 5 中相对应过程。

通过本公开的上述实施例，可以实现用户多终端场景下，用户在移动过程中激活并使用不同终端时，仍可以保证用户信令及业务数据传输的安全性。

如图 8 所示，本公开的实施例还提供一种终端 80，包括：收发机 81，处理器 82，存储器 83，所述存储器 83 上存有所述处理器 82 可执行的程序；所述处理器 82 执行所述程序时实现：用户与多个终端建立从属关系，多个终端存储安全性根密钥；在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数；所述目标终端根据所述安全密钥输入参数进行安全密钥的推衍，与网络进行数据传输。

可选的，存储安全性根密钥，包括：

获取用户的预设参数，所述预设参数包括：用户与网络侧签约的标识和/或用户与核心网侧相对应网络侧签约的第一安全性根密钥；

根据所述预设参数，存储所述安全性根密钥。

可选的，根据所述预设参数，存储安全性根密钥，包括：

所述多个终端与用户建立从属关系的过程中，根据用户与网络侧签约的第一密钥生成安全性根密钥并存储；

或者，

所述多个终端直接从所述用户接收所述第一密钥，并将所述第一密钥作为安全性根密钥进行存储。

可选的，在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推导集合，通过网络节点触发网络节点传递所述目标终端的对应网络侧节点的安全密钥输入参数。

可选的，在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推导集合，通过网络节点触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，核心网确定所述第二终端从属于第一终端的用户后，所述第二终端接收核心网发送的非接入 NAS 层的安全密钥输入参数集合以及接入网节点根密钥的输入参数，以及由所述核心网通知接入网节点进行接入 AS 层的安全密钥输入参数集合。

可选的，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，所述核心网通知所述第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述第二接入网节点所发送的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述接入网节点发送的所述接入网节点的安全密钥输入参数。

可选的，在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一个终端的第一密钥推导集合，通过网络节点触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，若所述第一终端与所述第二终端接入同一接入网节点，则该接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，触发非接入 NAS 层密钥及接入网节点根密钥输入参数的传递，所述第二终端接收所述接入网节点发送的接入 AS 层安全密钥输入参数以及接收所述核心网发送的安全输入参数。

可选的，根据所述预设参数，存储安全性根密钥，包括：

在用户与多个终端建立从属关系的过程中，根据用户与网络侧签约的第一密钥以及终端与用户建立从属关系时的终端计数值，生成安全性根密钥并存储；

或者，

在用户与多个终端建立从属关系的过程中，用户根据终端计数值，更新用户与网络侧签约的第一密钥，各终端获取与其对应的更新后的第一密钥，作为该终端的安全性根密钥并存储。

可选的，在所述多个终端中的至少一个目标终端接入网络时，获取所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

可选的，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

可选的，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网通知第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及接入网节点 AS 层的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所

述接入网节点的安全密钥输入参数。

可选的，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，第二终端向网络侧上报第二终端所对应的终端计数值，接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新；接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，所述核心网通过所述第一终端与所述第二终端的关系，根据第二终端计数值及进行 NAS 或者 AS 根密钥参数的推算更新，第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

可选的，所述目标终端根据所述安全密钥输入参数与网络进行数据传输，包括：

所述第二终端根据所述安全密钥输入参数，激活非接入 NAS 层以及接入 AS 层的安全性，与网络进行数据传输。

可选的，当用户与多个终端的从属关系结束时，多个终端删除所存储的第二密钥。

需要说明的是，该实施例中的终端是与上述图 3 所示的方法对应的终端，上述各实施例中的实现方式均适用于该实施例中，也能达到相同的技术效果。该终端中，收发机 81 与存储器 83，以及收发机 81 与处理器 82 均可以通过总线接口通讯连接，处理器 82 的功能也可以由收发机 81 实现，收发机 81 的功能也可以由处理器 82 实现。在此需要说明的是，本公开实施例提供的上述通信设备，能够实现上述方法实施例所实现的所有方法步骤，且能够达到相同的技术效果，在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

如图 9 所示，本公开的实施例还提供一种用户与多终端间的安全性管理装置 90，应用于终端，所述装置 90 包括：

存储模块 91，用于用户与多个终端建立从属关系，多个终端存储安全性根密钥；

获取模块 92，用于在所述多个终端中，至少一个目标终端接入网络时，

获取所述目标终端对应的网络侧节点的安全密钥输入参数；

处理模块 93，用于根据所述安全密钥输入参数进行安全密钥的推衍，与网络进行数据传输。

获取用户的预设参数，所述预设参数包括：用户与网络侧签约的标识和/或用户与核心网侧相对应网络侧签约的第一安全性根密钥；

根据所述预设参数，存储所述安全性根密钥。

可选的，根据所述预设参数，存储安全性根密钥，包括：

所述多个终端与用户建立从属关系的过程中，根据用户与网络侧签约的第一密钥生成安全性根密钥并存储；

或者，

所述多个终端直接从所述用户接收所述第一密钥，并将所述第一密钥作为安全性根密钥进行存储。

可选的，在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应网络侧节点的安全密钥输入参数。

可选的，在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，核心网确定所述第二终端从属于第一终端的用户后，所述第二终端接收核心网发送的非接入 NAS 层的安全密钥输入参数集合以及接入网节点根密钥的输入参数，以及由所述核心网通知接入网节点进行接入 AS 层的安全密钥输入参数集合。

可选的，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，

所述核心网通知所述第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述第二接入网节点所发送的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述接入网节点发送的所述接入网节点的安全密钥输入参数。

可选的，在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一个终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，若所述第一终端与所述第二终端接入同一接入网节点，则该接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，触发非接入 NAS 层密钥及接入网节点根密钥输入参数的传递，所述第二终端接收所述接入网节点发送的接入 AS 层安全密钥输入参数以及接收所述核心网发送的安全输入参数。

可选的，根据所述预设参数，存储安全性根密钥，包括：

在用户与多个终端建立从属关系的过程中，根据用户与网络侧签约的第一密钥以及终端与用户建立从属关系时的终端计数值，生成安全性根密钥并存储；

或者，

在用户与多个终端建立从属关系的过程中，用户根据终端计数值，更新用户与网络侧签约的第一密钥，各终端获取与其对应的更新后的第一密钥，作为该终端的安全性根密钥并存储。

可选的，在所述多个终端中的至少一个目标终端接入网络时，获取所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

可选的，所述第二终端接收网络侧节点根据所述目标终端的计数值触发

并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

可选的，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网通知第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及接入网节点 AS 层的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

可选的，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，第二终端向网络侧上报第二终端所对应的终端计数值，接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新；接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，所述核心网通过所述第一终端与所述第二终端的关系，根据第二终端计数值及进行 NAS 或者 AS 根密钥参数的推算更新，第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

可选的，所述目标终端根据所述安全密钥输入参数与网络进行数据传输，包括：

所述第二终端根据所述安全密钥输入参数，激活非接入 NAS 层以及接入 AS 层的安全性，与网络进行数据传输。

可选的，当用户与多个终端的从属关系结束时，多个终端删除所存储的第二密钥。

需要说明的是，该实施例中的装置是与终端侧的方法对应的装置，上述各实施例中的实现方式均适用于该装置的实施例中，也能达到相同的技术效果。在此需要说明的是，本公开实施例提供的上述装置，能够实现上述方法实施例所实现的所有方法步骤，且能够达到相同的技术效果，在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

本公开的实施例还提供一种用户与多终端间的安全性管理方法，应用于网络侧，所述方法包括：

从属于同一用户的多个终端中的至少一个目标终端接入网络时，网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数；

根据所述安全密钥输入参数与终端进行数据传输。

可选的，网络侧触发网络侧节点传递所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推导集合；

在非首个与所述用户建立从属关系的目标终端接入网络时，根据所述第一终端的第一密钥推导集合 用户与终端的从属关系，触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数。

可选的，根据所述第一终端的第一密钥推导集合，触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

核心网确定所述第二终端从属于第一终端的用户后，向第二终端发送非接入 NAS 层的安全密钥输入参数集合以及接入网节点根密钥的输入参数，再由所述核心网通知接入网节点进行接入 AS 层的安全密钥输入参数集合的第一终端的第一密钥推导集合；以及

所述核心网触发接入网节点，进行接入 AS 层的安全密钥输入参数。

可选的，根据所述第一终端的第一密钥推衍集合，触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

若所述第一终端与所述第二终端接入同一接入网节点，则该接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，触发非接入 NAS 层密钥及接入网节点根密钥输入参数的传递，接入网节点向所述第二终端发送接入 AS 层安全密钥输入参数；以及

所述核心网向所述第二终端发送所述第一终端的第一密钥推衍集合。

可选的，网络侧触发网络侧节点传递所述目标终端对应的接入节点 网络侧节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合以及终端计数值，通过网络节点触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数。

可选的，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网的非接入 NAS 层的密钥输入参数和接入网节点的根密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

可选的，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，网络侧接收第二终端上报的第二终端所对应的终端计数值，接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新；

所述接入网节点向所述第二终端发送安全密钥输入参数。

需要说明的是，该网络侧的方法是与上述终端侧的方法对应的流程，上述终端侧的方法的各实施例中的所有实现方式均适用于该网络侧的方法的实现流程中。

本公开的实施例还提供一种网络侧设备，包括：收发机，处理器，存储器，所述存储器上存有所述处理器可执行的程序；所述处理器执行所述程序时实现：从属于同一用户的多个终端中的至少一个目标终端接入网络时，网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数；根据所述安全密钥输入参数与终端进行数据传输。

可选的，网络侧触发网络侧节点传递所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推导集合；

在非首个与所述用户建立从属关系的目标终端接入网络时，根据所述第一终端的第一密钥推导集合用户与终端的从属关系，触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数。

可选的，根据所述第一终端的第一密钥推导集合，触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

核心网确定所述第二终端从属于第一终端的用户后，向第二终端发送非接入 NAS 层的安全密钥输入参数集合以及接入网节点根密钥的输入参数，以及由所述核心网通知接入网节点进行接入 AS 层的安全密钥输入参数集合的第一终端的第一密钥推导集合；以及

所述核心网触发接入网节点，进行接入 AS 层的安全密钥输入参数。

可选的，根据所述第一终端的第一密钥推导集合，触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

若所述第一终端与所述第二终端接入同一接入网节点，则该接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，触发非接入 NAS 层密钥及接入网节点根密钥输入参数的传递，接入网节点向所述第

二终端发送接入 AS 层安全密钥输入参数；以及

所述核心网向所述第二终端发送所述第一终端的第一密钥推衍集合。

可选的，网络侧触发网络侧节点传递所述目标终端对应的接入节点 网络侧节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合以及终端计数值，通过网络节点触发网络侧节点传递所述目标终端的对应的接入节点的安全密钥输入参数。

可选的，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网的非接入 NAS 层的密钥输入参数和接入网节点的根密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

可选的，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，网络侧接收第二终端上报的第二终端所对应的终端计数值，接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新；

所述接入网节点向所述第二终端发送安全密钥输入参数。

需要说明的是，该实施例中的网络设备是与上述网络侧的方法对应的网络设备，上述各实施例中的实现方式均适用于该实施例中，也能达到相同的技术效果。该网络设备中，收发机与存储器，以及收发机与处理器均可以通过总线接口通讯连接，处理器 82 的功能也可以由收发机实现，收发机的功能

也可以由处理器实现。在此需要说明的是，本公开实施例提供的上述网络设备，能够实现上述方法实施例所实现的所有方法步骤，且能够达到相同的技术效果，在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

本公开的实施例还提供一种用户与多终端间的安全性管理装置，应用于网络侧设备，所述装置包括：

处理模块，用于从属于同一用户的多个终端中的至少一个目标终端接入网络时，网络侧触发网络侧节点传递所述目标终端对应的接入节点的安全密钥输入参数；

收发模块，用于根据所述安全密钥输入参数与终端进行数据传输。

可选的，网络侧触发网络侧节点传递所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络时，根据所述第一终端的第一密钥推衍集合 用户与终端的从属关系，触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数。

可选的，根据所述第一终端的第一密钥推衍集合，触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

核心网确定所述第二终端从属于第一终端的用户后，向第二终端发送非接入 NAS 层的安全密钥输入参数集合以及接入网节点根密钥的输入参数，再由所述核心网通知接入网节点进行接入 AS 层的安全密钥输入参数集合的第一终端的第一密钥推衍集合；以及

所述核心网触发接入网节点，进行接入 AS 层的安全密钥输入参数。

可选的，根据所述第一终端的第一密钥推衍集合，触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

若所述第一终端与所述第二终端接入同一接入网节点，则该接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，触发非

接入 NAS 层密钥及接入网节点根密钥输入参数的传递, 接入网节点向所述第二终端发送接入 AS 层安全密钥输入参数; 以及

所述核心网向所述第二终端发送所述第一终端的第一密钥推衍集合。

可选的, 网络侧触发网络侧节点传递所述目标终端对应的接入节点 网络侧节点的安全密钥输入参数, 包括:

在所述多个终端中, 首个与用户建立从属关系的第一终端, 与用户的从属关系激活并接入网络后, 以及在非首个与所述用户建立从属关系的目标终端接入网络后, 将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网, 网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数进行初始认证及密钥协商流程, 确定第一终端的第一密钥推衍集合;

在非首个与所述用户建立从属关系的目标终端接入网络后, 根据所述第一终端的第一密钥推衍集合以及终端计数值, 通过网络节点触发网络侧节点传递所述目标终端的对应的接入节点的安全密钥输入参数。

可选的, 网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数, 包括:

核心网在确定第二终端从属于第一终端的用户后, 根据第二终端的终端计数值更新根密钥, 并向第二终端发送核心网的非接入 NAS 层的密钥输入参数和接入网节点的根密钥输入参数, 核心网触发接入网节点进行 AS 层密钥输入参数的传递。

可选的, 网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数, 包括:

在非首个与所述用户建立从属关系的第二终端接入网络后, 网络侧接收第二终端上报的第二终端所对应的终端计数值, 接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新;

所述接入网节点向所述第二终端发送安全密钥输入参数。

需要说明的是, 该实施例中的装置是与网络侧的方法对应的装置, 上述各实施例中的实现方式均适用于该装置的实施例中, 也能达到相同的技术效果。在此需要说明的是, 本公开实施例提供的上述装置, 能够实现上述方法

实施例所实现的所有方法步骤，且能够达到相同的技术效果，在此不再对本实施例中与方法实施例相同的部分及有益效果进行具体赘述。

本公开的实施例还提供一种处理器可读存储介质，所述处理器可读存储介质存储有处理器可执行指令，所述处理器可执行指令用于使所述处理器执行如上所述的终端侧的方法或者网络侧的方法。上述方法实施例中的所有实现方式均适用于该实施例中，也能达到相同的技术效果。

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

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

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

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

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

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用

时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本公开的技术方案本质上或者说对相关技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备)执行本公开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、ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

此外，需要指出的是，在本公开的装置和方法中，显然，各部件或各步骤是可以分解和/或重新组合的。这些分解和/或重新组合应视为本公开的等效方案。并且，执行上述系列处理的步骤可以自然地按照说明的顺序按时间顺序执行，但是并不需要一定按照时间顺序执行，某些步骤可以并行或彼此独立地执行。对本领域的普通技术人员而言，能够理解本公开的方法和装置的全部或者任何步骤或者部件，可以在任何计算装置(包括处理器、存储介质等)或者计算装置的网络中，以硬件、固件、软件或者它们的组合加以实现，这是本领域普通技术人员在阅读了本公开的说明的情况下运用他们的基本编程技能就能实现的。

因此，本公开的目的还可以通过在任何计算装置上运行一个程序或者一组程序来实现。所述计算装置可以是公知的通用装置。因此，本公开的目的也可以仅仅通过提供包含实现所述方法或者装置的程序代码的程序产品来实现。也就是说，这样的程序产品也构成本公开，并且存储有这样的程序产品的存储介质也构成本公开。显然，所述存储介质可以是任何公知的存储介质或者将来所开发出来的任何存储介质。还需要指出的是，在本公开的装置和方法中，显然，各部件或各步骤是可以分解和/或重新组合的。这些分解和/或重新组合应视为本公开的等效方案。并且，执行上述系列处理的步骤可以自然地按照说明的顺序按时间顺序执行，但是并不需要一定按照时间顺序执行。某些步骤可以并行或彼此独立地执行。

需要说明的是，应理解以上各个模块的划分仅仅是一种逻辑功能的划分，实际实现时可以全部或部分集成到一个物理实体上，也可以物理上分开。且这些模块可以全部以软件通过处理元件调用的形式实现；也可以全部以硬件

的形式实现；还可以部分模块通过处理元件调用软件的形式实现，部分模块通过硬件的形式实现。例如，确定模块可以为单独设立的处理元件，也可以集成在上述装置的某一个芯片中实现，此外，也可以以程序代码的形式存储于上述装置的存储器中，由上述装置的某一个处理元件调用并执行以上确定模块的功能。其它模块的实现与之类似。此外这些模块全部或部分可以集成在一起，也可以独立实现。这里所述的处理元件可以是一种集成电路，具有信号的处理能力。在实现过程中，上述方法的各步骤或以上各个模块可以通过处理器元件中的硬件的集成逻辑电路或者软件形式的指令完成。

例如，各个模块、单元、子单元或子模块可以是被配置成实施以上方法的一个或多个集成电路，例如：一个或多个特定集成电路（Application Specific Integrated Circuit, ASIC），或，一个或多个微处理器（digital signal processor, DSP），或，一个或者多个现场可编程门阵列（Field Programmable Gate Array, FPGA）等。再如，当以上某个模块通过处理元件调度程序代码的形式实现时，该处理元件可以是通用处理器，例如中央处理器（Central Processing Unit, CPU）或其它可以调用程序代码的处理器。再如，这些模块可以集成在一起，以片上系统（system-on-a-chip, SOC）的形式实现。

本公开的说明书和权利要求书中的术语“第一”、“第二”等是用于区别类似的对象，而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换，以便这里描述的本公开的实施例，例如除了在这里图示或描述的那些以外的顺序实施。此外，术语“包括”和“具有”以及他们的任何变形，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、产品或设备不必限于清楚地列出的那些步骤或单元，而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。此外，说明书以及权利要求中使用“和/或”表示所连接对象的至少其中之一，例如 A 和/或 B 和/或 C，表示包含单独 A，单独 B，单独 C，以及 A 和 B 都存在，B 和 C 都存在，A 和 C 都存在，以及 A、B 和 C 都存在的 7 种情况。类似地，本说明书以及权利要求中使用“A 和 B 中的至少一个”应理解为“单独 A，单独 B，或 A 和 B 都存在”。

以上所述的是本公开的可选实施方式，应当指出对于本技术领域的普通

人员来说，在不脱离本公开所述的原理前提下还可以作出若干改进和润饰，这些改进和润饰也在本公开的保护范围内。

权利要求书

1. 一种用户与多终端间的安全性管理方法,应用于终端,所述方法包括:

用户与多个终端建立从属关系,多个终端存储安全性根密钥;

在所述多个终端中,至少一个目标终端接入网络时,获取所述目标终端对应的网络侧节点的安全密钥输入参数;

所述目标终端根据所述安全密钥输入参数进行安全密钥的推衍,与网络进行数据传输。

2. 根据权利要求1所述的用户与多终端间的安全性管理方法,其中,存储安全性根密钥,包括:

获取用户的预设参数,所述预设参数包括:用户与网络侧签约的标识和/或用户与网络侧签约的第一密钥;

根据所述预设参数,存储所述安全性根密钥。

3. 根据权利要求2所述的用户与多终端间的安全性管理方法,其中,根据所述预设参数,存储安全性根密钥,包括:

所述多个终端与用户建立从属关系的过程中,根据用户与网络侧签约的第一密钥生成安全性根密钥并存储;

或者,

所述多个终端直接从所述用户接收所述第一密钥,并将所述第一密钥作为安全性根密钥进行存储。

4. 根据权利要求3所述的用户与多终端间的安全性管理方法,其中,在所述多个终端中,至少一个目标终端接入网络时,获取所述目标终端对应的网络侧节点的安全密钥输入参数,包括:

在所述多个终端中,首个与用户建立从属关系的第一终端,与用户的从属关系激活并接入网络后,进行初始认证及密钥协商流程,确定第一终端的第一密钥推衍集合;

在非首个与所述用户建立从属关系的目标终端接入网络后,根据所述第一终端的第一密钥推衍集合,通过网络节点触发网络节点传递所述目标终端的对应网络侧节点的安全密钥输入参数。

5. 根据权利要求4所述的用户与多终端间的安全性管理方法, 其中, 在非首个与所述用户建立从属关系的目标终端接入网络后, 根据所述第一终端的第一密钥推衍集合, 通过网络节点触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数, 包括:

在非首个与所述用户建立从属关系的第二终端接入网络后, 核心网确定所述第二终端从属于第一终端的用户后, 所述第二终端接收核心网发送的非接入NAS层的安全密钥输入参数集合以及接入网节点根密钥的输入参数, 以及由所述核心网通知接入网节点进行接入AS层的安全密钥输入参数集合。

6. 根据权利要求5所述的用户与多终端间的安全性管理方法, 其中,

若所述第一终端接入第一接入网节点, 所述第二终端接入第二接入网节点, 所述第一接入网节点和所述第二接入网节点是不同的网络节点, 所述核心网通知所述第一接入网节点向所述第二接入网节点发送安全密钥输入参数, 所述第二终端接收所述第二接入网节点所发送的安全密钥输入参数;

若所述第一终端和所述第二终端接入相同的接入网节点, 所述核心网触发所述接入网节点进行安全密钥输入参数的传递, 所述第二终端接收所述接入网节点发送的所述接入网节点的安全密钥输入参数。

7. 根据权利要求4所述的用户与多终端间的安全性管理方法, 其中, 在非首个与所述用户建立从属关系的目标终端接入网络后, 根据所述第一个终端的第一密钥推衍集合, 通过网络节点触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数, 包括:

在非首个与所述用户建立从属关系的第二终端接入网络后, 若所述第一终端与所述第二终端接入同一接入网节点, 则该接入网节点确定所述第一终端和所述第二终端从属于同一用户, 并上报核心网, 触发非接入NAS层密钥及接入网节点根密钥输入参数的传递, 所述第二终端接收所述接入网节点发送的接入AS层安全密钥输入参数以及接收所述核心网发送的安全输入参数。

8. 根据权利要求2所述的用户与多终端间的安全性管理方法, 其中, 根据所述预设参数, 存储安全性根密钥, 包括:

在用户与多个终端建立从属关系的过程中, 根据用户与网络侧签约的第一密钥以及终端与用户建立从属关系时的终端计数值, 生成安全性根密钥并

存储；

或者，

在用户与多个终端建立从属关系的过程中，用户根据终端计数值，更新用户与网络侧签约的第一密钥，各终端获取与其对应的更新后的第一密钥，作为该终端的安全性根密钥并存储。

9. 根据权利要求 8 所述的用户与多终端间的安全性管理方法，其中，在所述多个终端中的至少一个目标终端接入网络时，获取所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

10. 根据权利要求 9 所述的用户与多终端间的安全性管理方法，其中，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网和接入网节点的根密钥推导参数以及非接入 NAS 层的密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

11. 根据权利要求 10 所述的用户与多终端间的安全性管理方法，其中，若所述第一终端接入第一接入网节点，所述第二终端接入第二接入网节点，所述第一接入网节点和所述第二接入网节点是不同的网络节点，所述核心网根据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网通知第一接入网节点向所述第二接入网节点发送安全密钥输入参数，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及接入网节点 AS 层的安全密钥输入参数；

若所述第一终端和所述第二终端接入相同的接入网节点，所述核心网根

据所述第二终端的计数值更新根密钥，并向所述第二终端发送核心网和接入网节点的根密钥输入参数以及非接入 NAS 层的密钥输入参数，核心网触发所述接入网节点进行安全密钥输入参数的传递，所述第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

12. 根据权利要求 9 所述的用户与多终端间的安全性管理方法，其中，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，第二终端向网络侧上报第二终端所对应的终端计数值，接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新；接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，所述核心网通过所述第一终端与所述第二终端的关系，根据第二终端计数值进行 NAS 或者 AS 根密钥参数的推算更新，第二终端接收所述核心网发送的网络节点根密钥输入参数和非接入 NAS 层的安全密钥输入参数及所述接入网节点的安全密钥输入参数。

13. 根据权利要求 4 至 12 任一项所述的用户与多终端间的安全性管理方法，其中，所述目标终端根据所述安全密钥输入参数与网络进行数据传输，包括：

所述第二终端根据所述安全密钥输入参数，激活非接入 NAS 层以及接入 AS 层的安全性，与网络进行数据传输。

14. 根据权利要求 4 至 12 任一项所述的用户与多终端间的安全性管理方法，其中，

当用户与多个终端的从属关系结束时，多个终端删除所存储的第二密钥。

15. 一种用户与多终端间的安全性管理方法，应用于网络侧，所述方法包括：

从属于同一用户的多个终端中的至少一个目标终端接入网络时，网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数；

根据所述安全密钥输入参数与终端进行数据传输。

16. 根据权利要求 15 所述的用户与多终端间的安全性管理方法，其中，

网络侧触发网络侧节点传递所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络时，根据用户与终端的从属关系，触发网络节点传递所述目标终端的对应的网络侧节点的安全密钥输入参数。

17. 根据权利要求 16 所述的用户与多终端间的安全性管理方法，其中，根据所述第一终端的第一密钥推衍集合，触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

核心网确定所述第二终端从属于第一终端的用户后，向第二终端发送非接入 NAS 层的安全密钥输入参数集合以及接入网节点根密钥的推衍参数，再由所述核心网通知接入网节点进行接入 AS 层的安全密钥输入参数集合。

18. 根据权利要求 16 所述的用户与多终端间的安全性管理方法，其中，根据所述第一终端的第一密钥推衍集合，触发网络节点传递所述目标终端的对应的接入节点的安全密钥输入参数，包括：

若所述第一终端与所述第二终端接入同一接入网节点，则该接入网节点确定所述第一终端和所述第二终端从属于同一用户，并上报核心网，所述核心网触发非接入 NAS 层密钥及接入网节点根密钥输入参数的传递，接入网节点向所述第二终端发送接入 AS 层安全密钥输入参数。

19. 根据权利要求 15 所述的用户与多终端间的安全性管理方法，其中，网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

20. 根据权利要求 19 所述的用户与多终端间的安全性管理方法，其中，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

核心网在确定第二终端从属于第一终端的用户后，根据第二终端的终端计数值更新根密钥，并向第二终端发送核心网的非接入 NAS 层的密钥输入参数和接入网节点的根密钥输入参数，核心网触发接入网节点进行 AS 层密钥输入参数的传递。

21. 根据权利要求 19 所述的用户与多终端间的安全性管理方法，其中，网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数，包括：

在非首个与所述用户建立从属关系的第二终端接入网络后，网络侧接收第二终端上报的第二终端所对应的终端计数值，接入网节点根据第二终端的终端计数值进行对应密钥输入参数的更新；

所述接入网节点向所述第二终端发送安全密钥输入参数。

22. 一种终端，包括：收发机，处理器，存储器，所述存储器上存有所述处理器可执行的程序；所述处理器执行所述程序时实现：用户与多个终端建立从属关系，多个终端存储安全性根密钥；在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数；所述目标终端根据所述安全密钥输入参数进行安全密钥的推衍，与网络进行数据传输。

23. 根据权利要求 22 所述的终端，其中，存储安全性根密钥，包括：

获取用户的预设参数，所述预设参数包括：用户与网络侧签约的标识和/或用户与网络侧签约的第一密钥；

根据所述预设参数，存储所述安全性根密钥。

24. 根据权利要求 23 所述的终端，其中，根据所述预设参数，存储安全性根密钥，包括：

所述多个终端与用户建立从属关系的过程中，根据用户与网络侧签约的第一密钥生成安全性根密钥并存储；

或者，

所述多个终端直接从所述用户接收所述第一密钥，并将所述第一密钥作为安全性根密钥进行存储。

25. 根据权利要求 24 所述的终端，其中，在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，进行初始认证及密钥协商流程，确定第一终端的第一密钥推衍集合；

在非首个与所述用户建立从属关系的目标终端接入网络后，根据所述第一终端的第一密钥推衍集合，通过网络节点触发网络节点传递所述目标终端的对应网络侧节点的安全密钥输入参数。

26. 根据权利要求 23 所述的终端，其中，根据所述预设参数，存储安全性根密钥，包括：

在用户与多个终端建立从属关系的过程中，根据用户与网络侧签约的第一密钥以及终端与用户建立从属关系时的终端计数值，生成安全性根密钥并存储；

或者，

在用户与多个终端建立从属关系的过程中，用户根据终端计数值，更新用户与网络侧签约的第一密钥，各终端获取与其对应的更新后的第一密钥，作为该终端的安全性根密钥并存储。

27. 根据权利要求 26 所述的终端，其中，在所述多个终端中的至少一个目标终端接入网络时，获取所述目标终端对应的接入节点的安全密钥输入参数，包括：

在所述多个终端中，首个与用户建立从属关系的第一终端，与用户的从属关系激活并接入网络后，以及在非首个与所述用户建立从属关系的目标终端接入网络后，将所述第一终端和所述目标终端的关系以及所述目标终端的计数值上报核心网，所述第二终端接收网络侧节点根据所述目标终端的计数值触发并传递的安全密钥输入参数。

28. 一种用户与多终端间的安全性管理装置，应用于终端，所述装置包

括：

存储模块，用于用户与多个终端建立从属关系，多个终端存储安全性根密钥；

获取模块，用于在所述多个终端中，至少一个目标终端接入网络时，获取所述目标终端对应的网络侧节点的安全密钥输入参数；

处理模块，用于根据所述安全密钥输入参数进行安全密钥的推衍与网络进行数据传输。

29. 一种网络侧设备，包括：收发机，处理器，存储器，所述存储器上存有所述处理器可执行的程序；所述处理器执行所述程序时实现：从属于同一用户的多个终端中的至少一个目标终端接入网络时，网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数；根据所述安全密钥输入参数与终端进行数据传输。

30. 一种用户与多终端间的安全性管理装置，应用于网络侧设备，所述装置包括：

处理模块，用于从属于同一用户的多个终端中的至少一个目标终端接入网络时，网络侧触发网络侧节点传递所述目标终端对应的网络侧节点的安全密钥输入参数；

收发模块，用于根据所述安全密钥输入参数与终端进行数据传输。

31. 一种处理器可读存储介质，所述处理器可读存储介质存储有处理器可执行指令，所述处理器可执行指令用于使所述处理器执行权利要求 1 至 14 任一项所述的方法或者执行权利要求 15 至 21 任一项所述的方法。

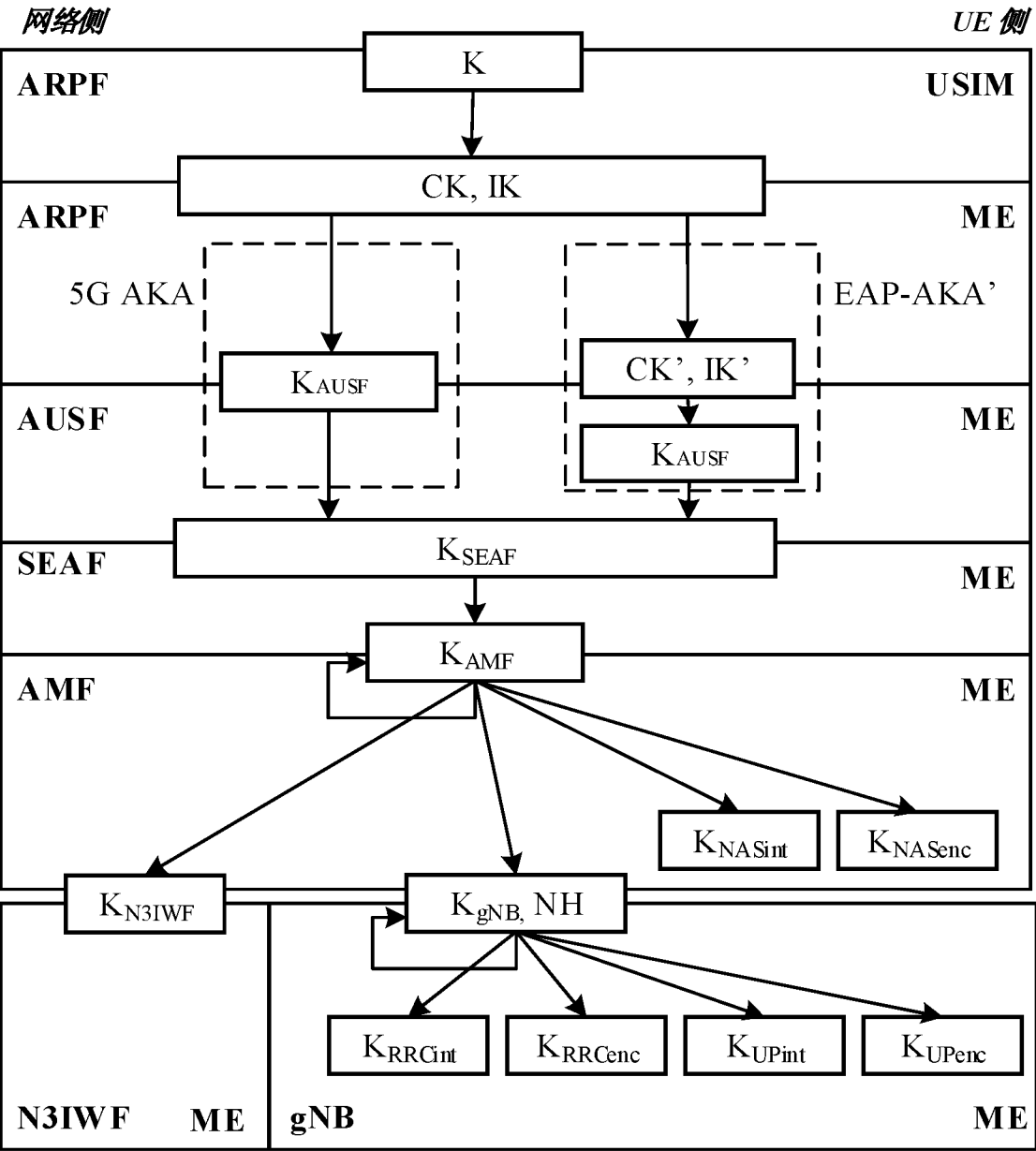


图 1

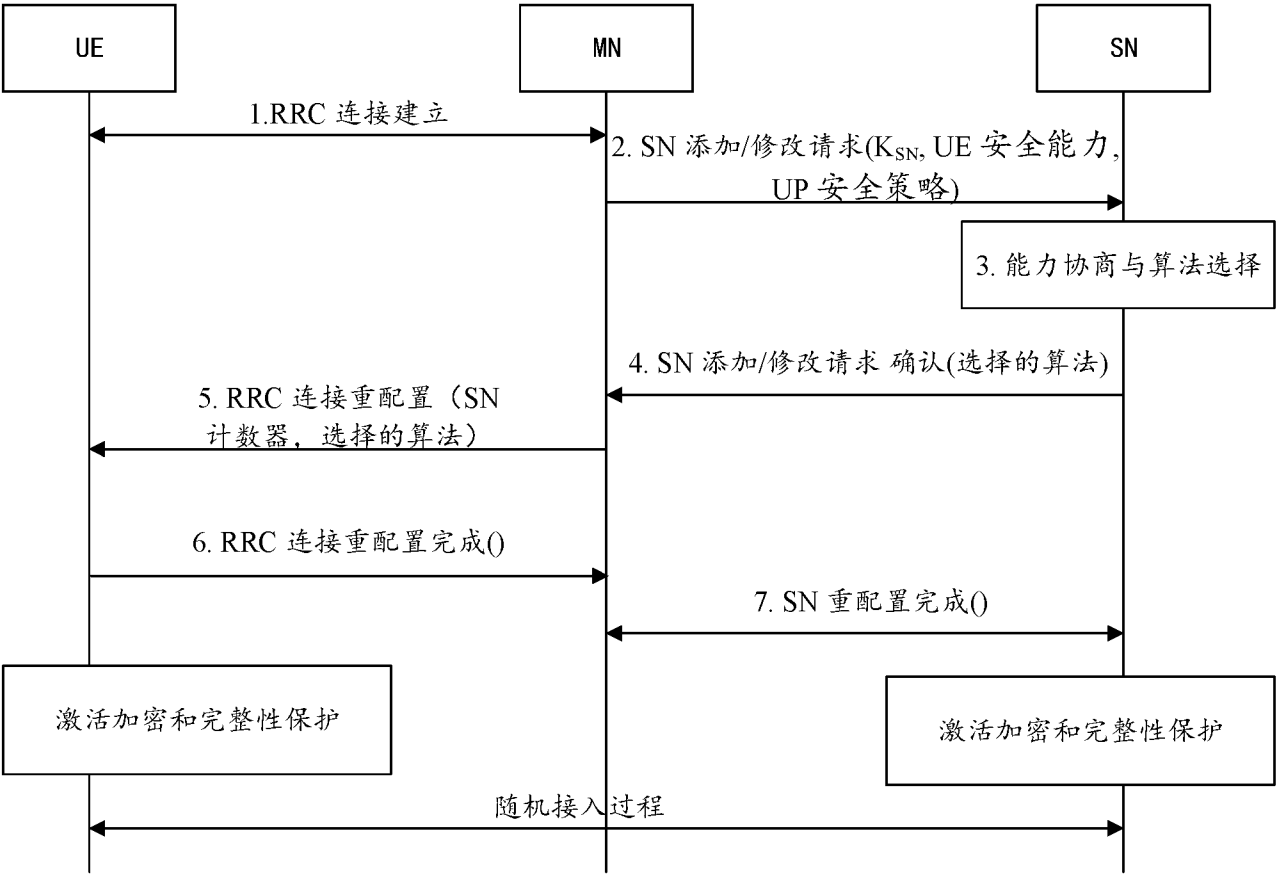


图 2

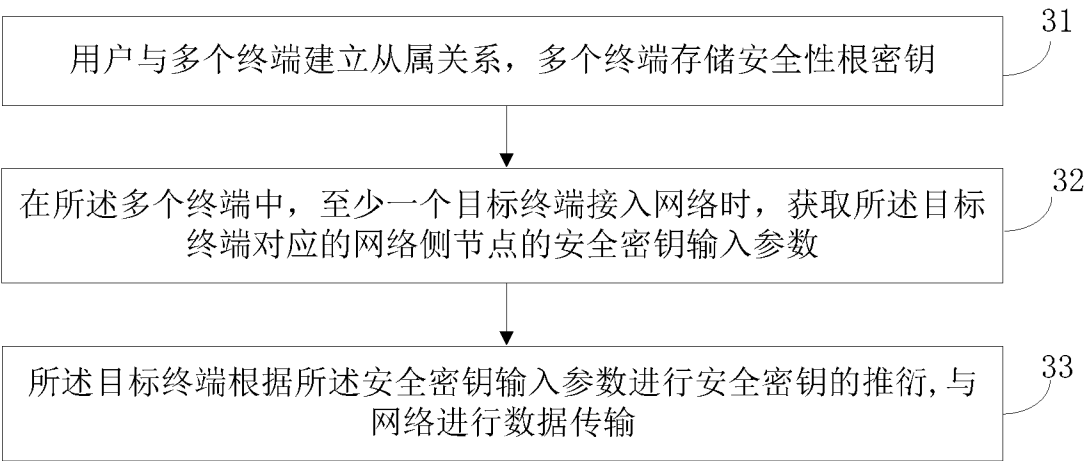


图 3

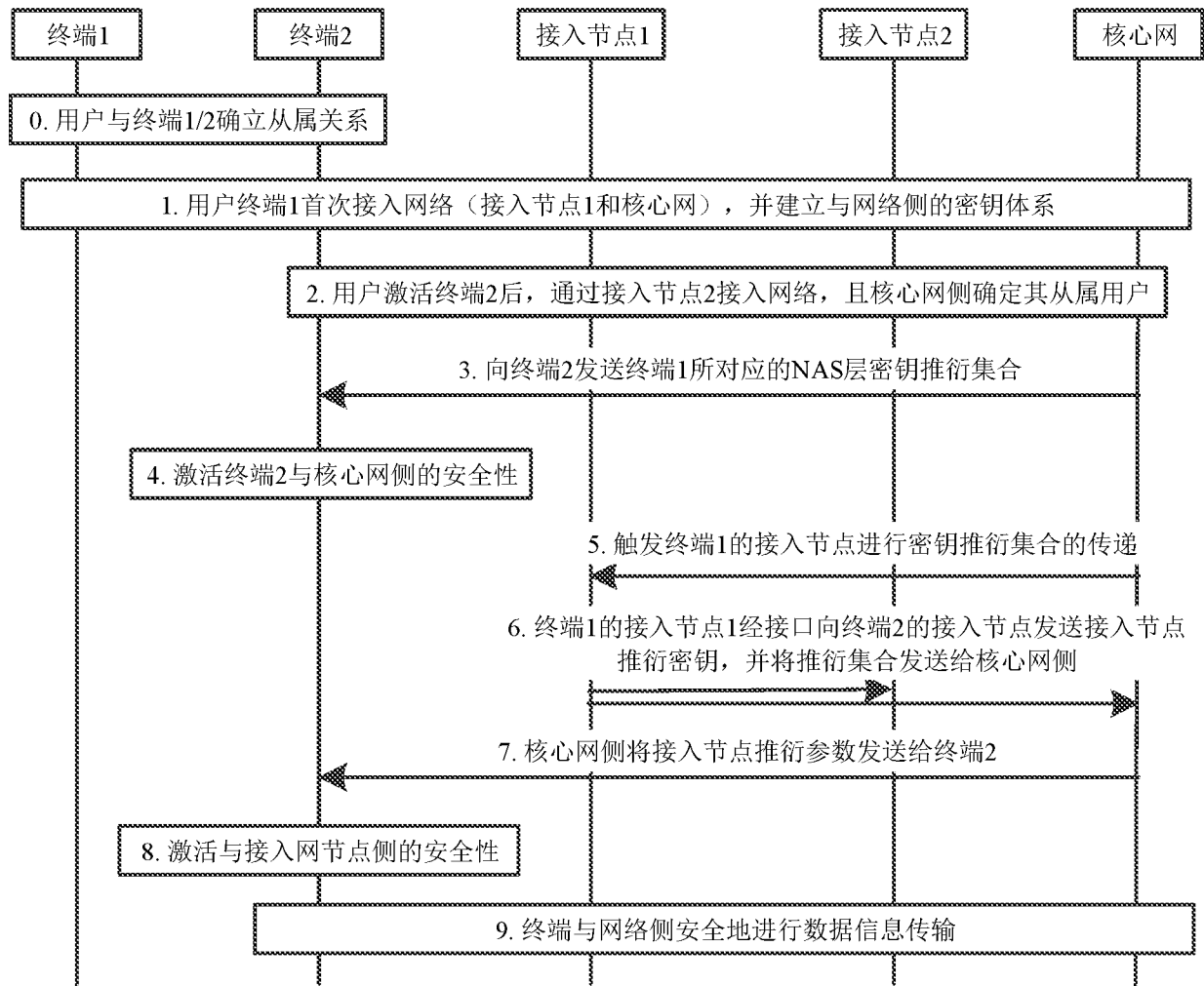


图 4

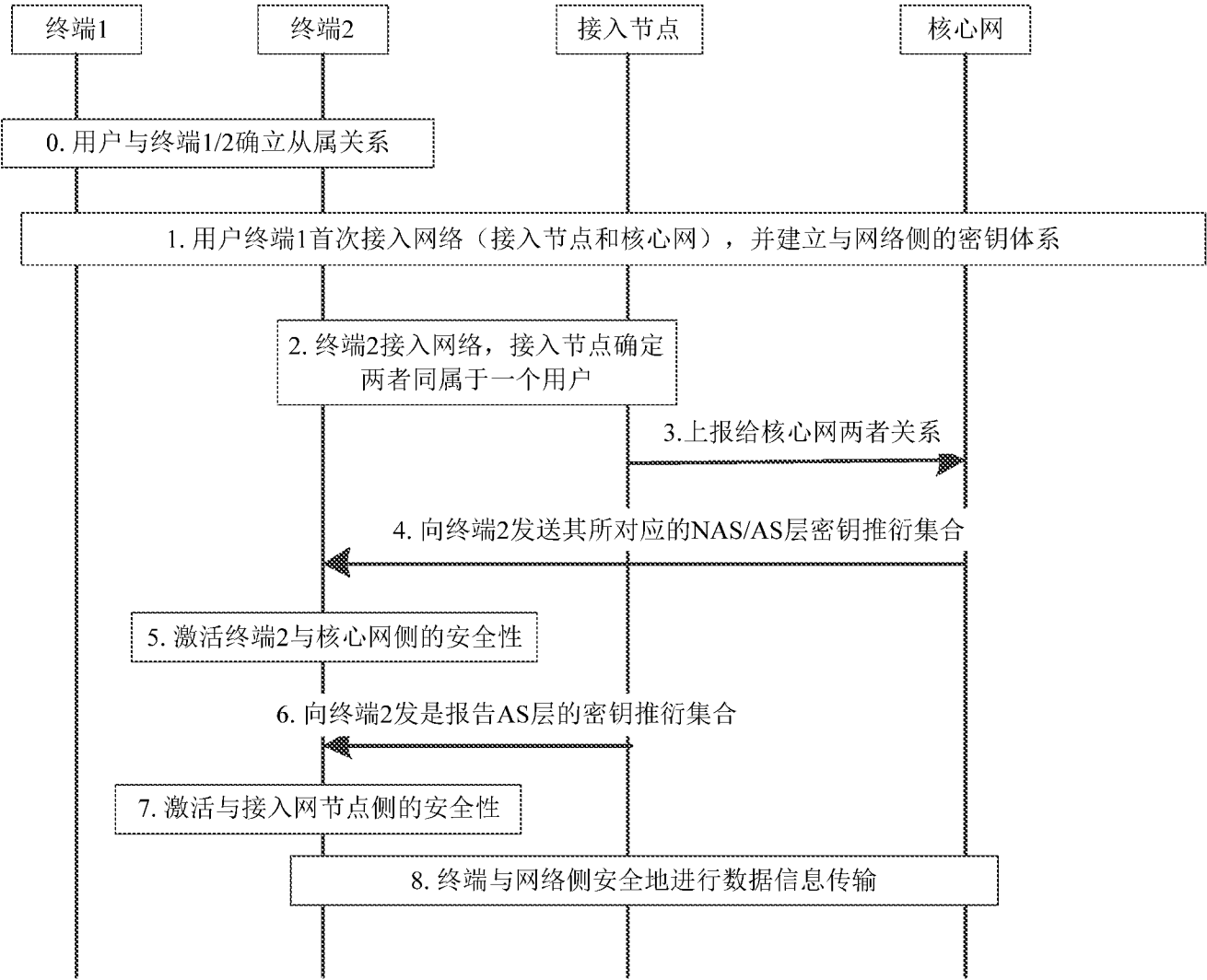


图 5

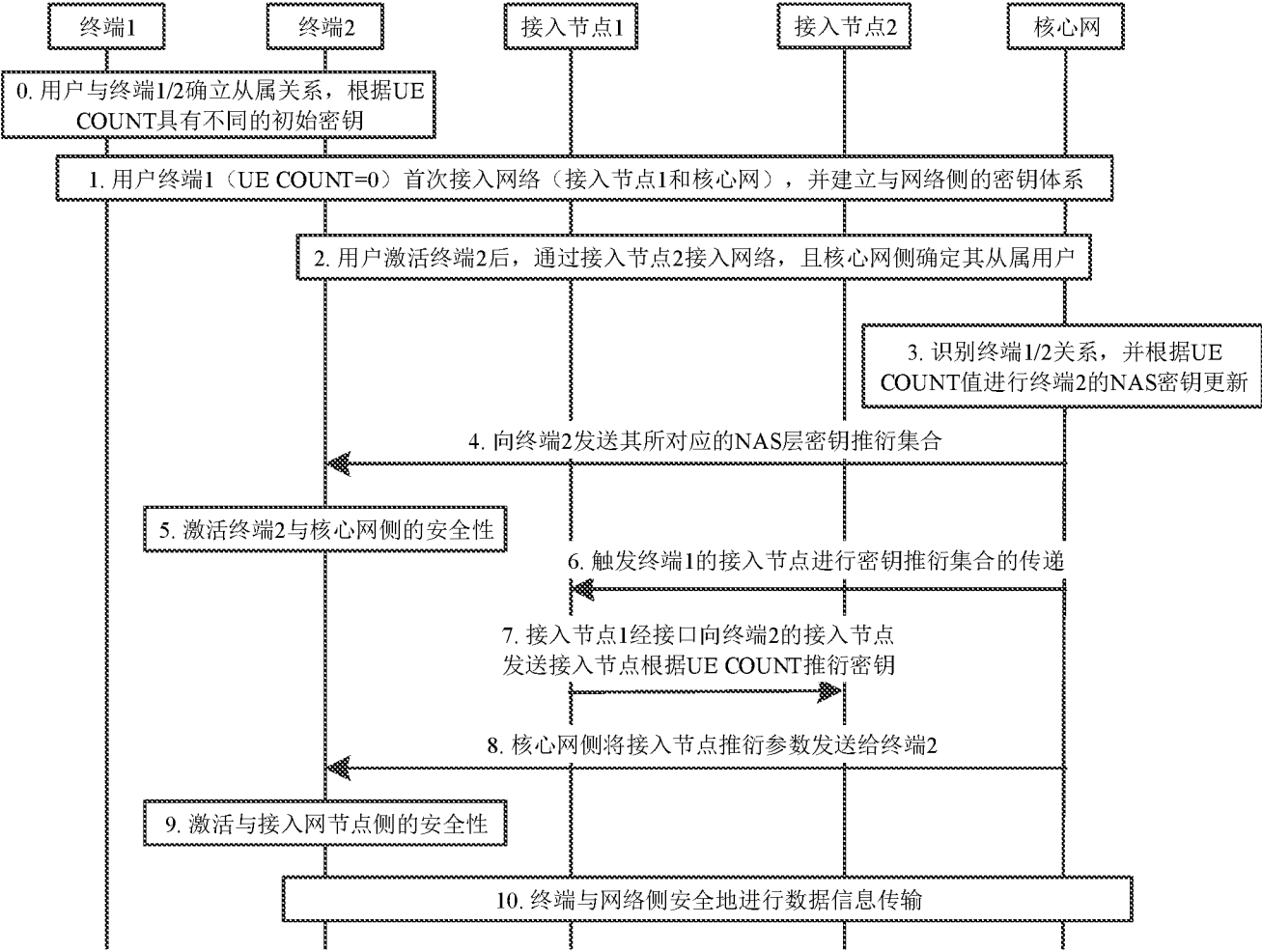


图 6

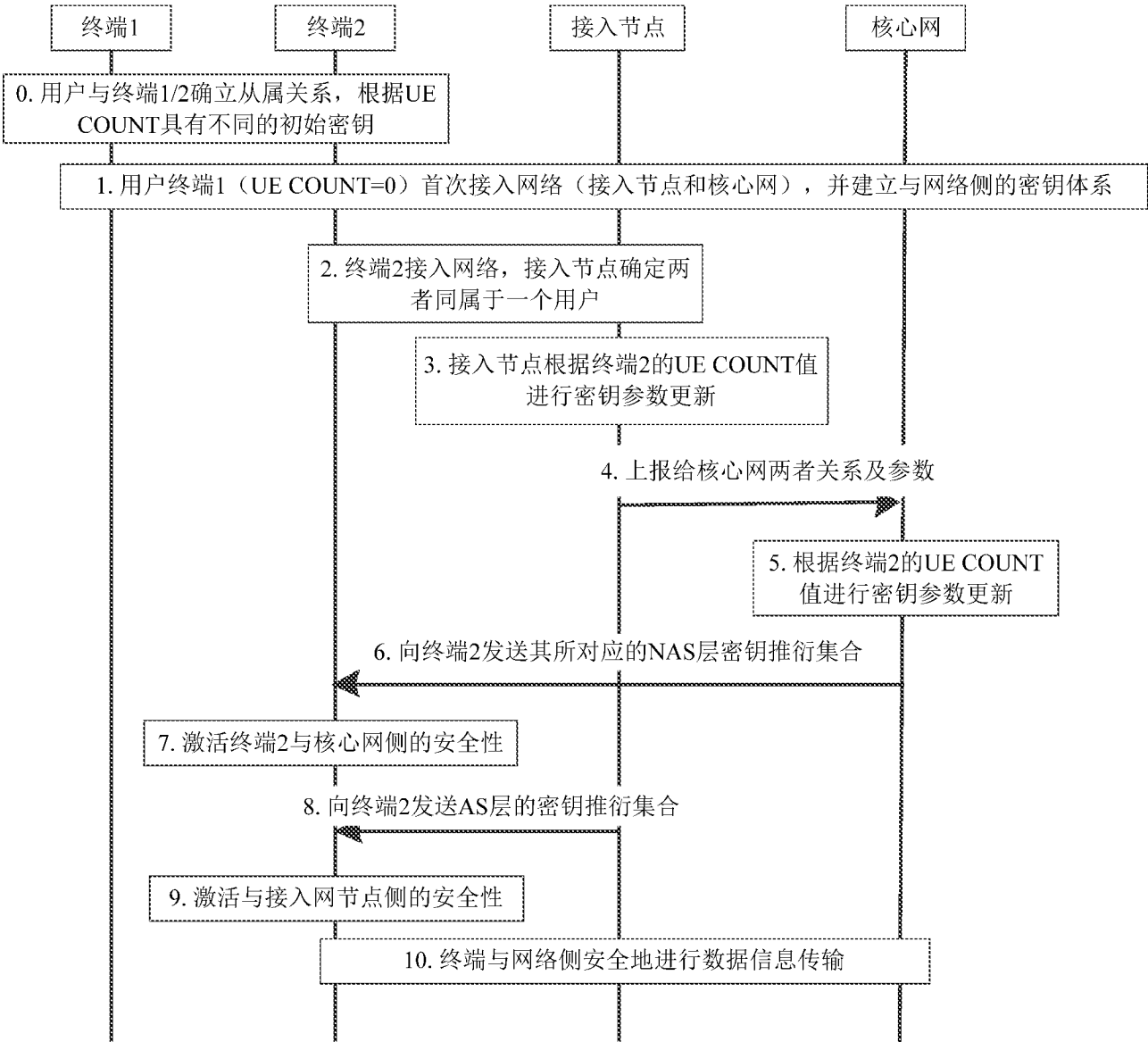


图 7

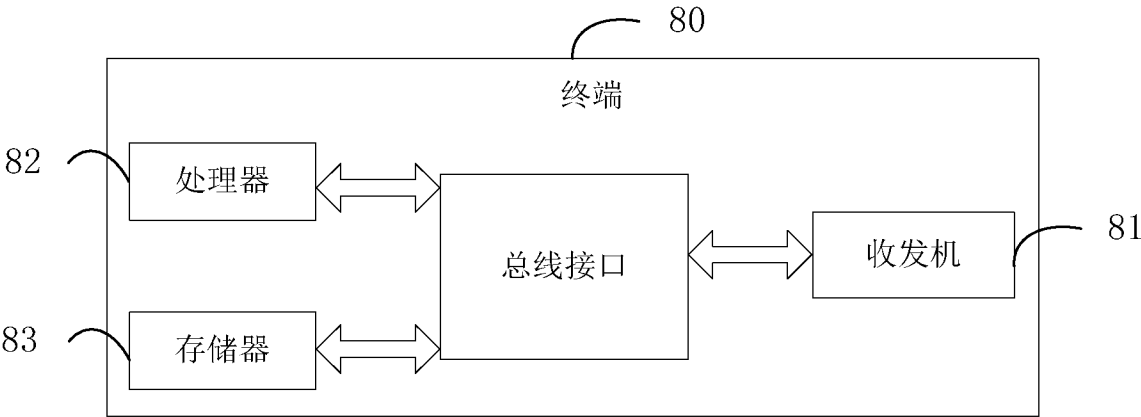


图 8

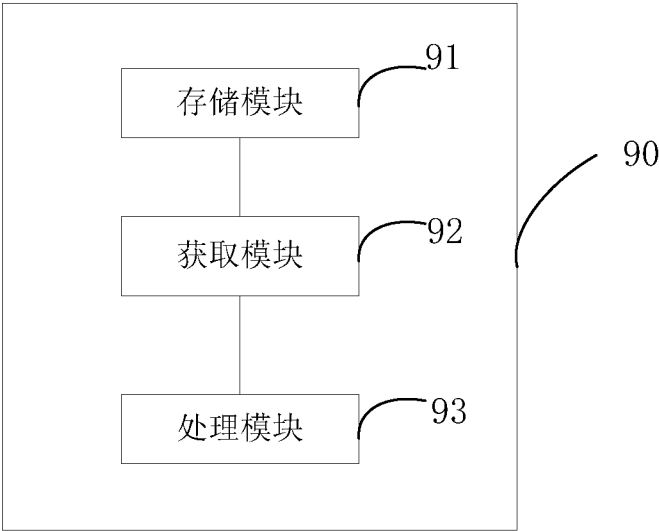


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2021/104236

A. CLASSIFICATION OF SUBJECT MATTER

H04W 12/04(2021.01)i; H04W 12/08(2021.01)i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04W; H04Q; 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, CNKI, WPI, EPODOC, 3GPP: 多, 终端, 安全, 密钥, 输入, 参数, 推衍, multiple, terminal, security, key, input, parameter, derivation

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 111386720 A (NEC CORPORATION) 07 July 2020 (2020-07-07) description, paragraphs [0088]-[0144] and [0259]-[0271]	1-31
X	CN 109644339 A (TELEFONAKTIEBOLAGET LM ERICSSON (PUBL)) 16 April 2019 (2019-04-16) description, paragraphs [0052]-[0073]	1-31
A	CN 1602611 A (ERICSSON TELEFON AB L M PUBL) 30 March 2005 (2005-03-30) entire document	1-31
A	US 2019253888 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 15 August 2019 (2019-08-15) entire document	1-31
A	APPLE. "PCR: KAF refreshment" 3GPP TSG-SA WG3 Meeting #98bis-e S3-200607, 17 April 2020 (2020-04-17), entire document	1-31



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

01 September 2021

Date of mailing of the international search report

28 September 2021

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2021/104236

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	111386720	A	07 July 2020	JP	2021057921	A	08 April 2021
				JP	WO2019065897	A1	06 August 2020
				EP	3691317	A1	05 August 2020
				US	2020280849	A1	03 September 2020
				WO	2019065897	A1	04 April 2019
				IN	202017017663	A	04 September 2020
CN	109644339	A	16 April 2019	MX	2019008770	A	09 September 2019
				AR	110865	A1	08 May 2019
				AU	2018212610	A1	25 July 2019
				EP	3574670	A1	04 December 2019
				CN	109644340	A	16 April 2019
				EP	3574669	A1	04 December 2019
				US	2019141523	A1	09 May 2019
				KR	20190100366	A	28 August 2019
				ZA	201903899	B	23 December 2020
				US	2020120498	A1	16 April 2020
				PH	12019501467	A1	24 February 2020
				US	2020120497	A1	16 April 2020
				JP	2020505866	A	20 February 2020
				AR	110917	A1	15 May 2019
				RU	2719772	C1	23 April 2020
				JP	2020507268	A	05 March 2020
				WO	2018138348	A1	02 August 2018
				WO	2018138347	A1	02 August 2018
				US	2019141584	A1	09 May 2019
				BR	112019015387	A2	17 December 2019
				SG	11201905330	A1	30 July 2019
				IN	201817049813	A	02 August 2019
CN	1602611	A	30 March 2005	WO	03049357	A2	12 June 2003
				US	2005063544	A1	24 March 2005
				EP	1452000	A2	01 September 2004
				AU	2002361050	A1	17 June 2003
US	2019253888	A1	15 August 2019	WO	2018056957	A1	29 March 2018
				EP	3516819	A1	31 July 2019

国际检索报告

国际申请号

PCT/CN2021/104236

A. 主题的分类 H04W 12/04(2021.01)i; H04W 12/08(2021.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类																				
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) H04W; H04Q; 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, CNKI, WPI, EPDOC, 3GPP:多, 终端, 安全, 密钥, 输入, 参数, 推衍, multiple, terminal, security, key, input, parameter, derivation																				
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>X</td> <td>CN 111386720 A (日本电气株式会社) 2020年 7月 7日 (2020 - 07 - 07) 说明书第[0088]-[0144], [0259]-[0271]段</td> <td>1-31</td> </tr> <tr> <td>X</td> <td>CN 109644339 A (瑞典爱立信有限公司) 2019年 4月 16日 (2019 - 04 - 16) 说明书第[0052]-[0073]段</td> <td>1-31</td> </tr> <tr> <td>A</td> <td>CN 1602611 A (艾利森电话股份有限公司) 2005年 3月 30日 (2005 - 03 - 30) 全文</td> <td>1-31</td> </tr> <tr> <td>A</td> <td>US 2019253888 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 2019年 8月 15日 (2019 - 08 - 15) 全文</td> <td>1-31</td> </tr> <tr> <td>A</td> <td>APPLE. "pCR: KAF refreshment" 3GPP TSG-SA WG3 Meeting #98bis-e S3-200607, 2020年 4月 17日 (2020 - 04 - 17), 全文</td> <td>1-31</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	X	CN 111386720 A (日本电气株式会社) 2020年 7月 7日 (2020 - 07 - 07) 说明书第[0088]-[0144], [0259]-[0271]段	1-31	X	CN 109644339 A (瑞典爱立信有限公司) 2019年 4月 16日 (2019 - 04 - 16) 说明书第[0052]-[0073]段	1-31	A	CN 1602611 A (艾利森电话股份有限公司) 2005年 3月 30日 (2005 - 03 - 30) 全文	1-31	A	US 2019253888 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 2019年 8月 15日 (2019 - 08 - 15) 全文	1-31	A	APPLE. "pCR: KAF refreshment" 3GPP TSG-SA WG3 Meeting #98bis-e S3-200607, 2020年 4月 17日 (2020 - 04 - 17), 全文	1-31
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求																		
X	CN 111386720 A (日本电气株式会社) 2020年 7月 7日 (2020 - 07 - 07) 说明书第[0088]-[0144], [0259]-[0271]段	1-31																		
X	CN 109644339 A (瑞典爱立信有限公司) 2019年 4月 16日 (2019 - 04 - 16) 说明书第[0052]-[0073]段	1-31																		
A	CN 1602611 A (艾利森电话股份有限公司) 2005年 3月 30日 (2005 - 03 - 30) 全文	1-31																		
A	US 2019253888 A1 (NOKIA SOLUTIONS AND NETWORKS OY) 2019年 8月 15日 (2019 - 08 - 15) 全文	1-31																		
A	APPLE. "pCR: KAF refreshment" 3GPP TSG-SA WG3 Meeting #98bis-e S3-200607, 2020年 4月 17日 (2020 - 04 - 17), 全文	1-31																		
☐ 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																		
2021年 9月 1日		2021年 9月 28日																		
ISA/CN的名称和邮寄地址		受权官员																		
中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		常交法 电话号码 86-(10)-53961735																		

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2021/104236

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	111386720	A	2020年 7月 7日	JP	2021057921	A	2021年 4月 8日
				JP	W02019065897	A1	2020年 8月 6日
				EP	3691317	A1	2020年 8月 5日
				US	2020280849	A1	2020年 9月 3日
				WO	2019065897	A1	2019年 4月 4日
				IN	202017017663	A	2020年 9月 4日
CN	109644339	A	2019年 4月 16日	MX	2019008770	A	2019年 9月 9日
				AR	110865	A1	2019年 5月 8日
				AU	2018212610	A1	2019年 7月 25日
				EP	3574670	A1	2019年 12月 4日
				CN	109644340	A	2019年 4月 16日
				EP	3574669	A1	2019年 12月 4日
				US	2019141523	A1	2019年 5月 9日
				KR	20190100366	A	2019年 8月 28日
				ZA	201903899	B	2020年 12月 23日
				US	2020120498	A1	2020年 4月 16日
				PH	12019501467	A1	2020年 2月 24日
				US	2020120497	A1	2020年 4月 16日
				JP	2020505866	A	2020年 2月 20日
				AR	110917	A1	2019年 5月 15日
				RU	2719772	C1	2020年 4月 23日
				JP	2020507268	A	2020年 3月 5日
				WO	2018138348	A1	2018年 8月 2日
				WO	2018138347	A1	2018年 8月 2日
				US	2019141584	A1	2019年 5月 9日
				BR	112019015387	A2	2019年 12月 17日
				SG	11201905330	A1	2019年 7月 30日
				IN	201817049813	A	2019年 8月 2日
CN	1602611	A	2005年 3月 30日	WO	03049357	A2	2003年 6月 12日
				US	2005063544	A1	2005年 3月 24日
				EP	1452000	A2	2004年 9月 1日
				AU	2002361050	A1	2003年 6月 17日
US	2019253888	A1	2019年 8月 15日	WO	2018056957	A1	2018年 3月 29日
				EP	3516819	A1	2019年 7月 31日