(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
2018 年 8 月 2 日 (02.08.2018)

WIPO | PCT

(10) 国际公布号
WO 2018/137351 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2017/102864

(22) 国际申请日: 2017 年 9 月 22 日 (22.09.2017)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710064224.2 2017年1月25日 (25.01.2017) CN

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

(72) 发明人: 雷中定 (LEI, Zhongding); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 李漓春 (LI, Lichun); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 张博 (ZHANG, Bo); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 刘斐 (LIU, Fei); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 王海光 (WANG, Haiguang); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 康鑫 (KANG, Xin); 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

(54) **Title:** METHOD, RELEVANT DEVICE AND SYSTEM FOR PROCESSING NETWORK KEY

(54) **发明名称**: 一种网络密钥处理的方法、相关设备及系统

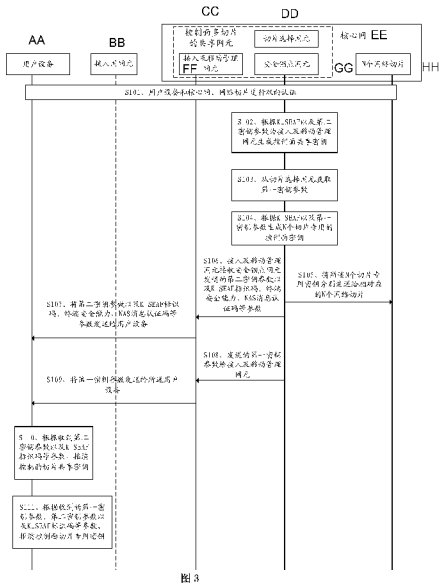

图 3

S101 A user equipment, a core network and a network slice carry out bidirectional authentication
S102 Generate, according to a K-SEAF and a second key parameter, a shared key of a control plane for an access and mobility management network element
S103 Obtain a first key parameter from a slice selection network element
S104 Generate, according to the K-SEAF and the first key parameter, special control plane keys for N slices
S105 Send the special keys for N slices to corresponding N network splices respectively
S106 The access and mobility management network element receives the second key parameter, and parameters, such as a K-SEAF identification code, a security capability of a terminal, and an NAS message authentication code, which are sent by a secure anchor network element
S107 Send the second key parameter, and the parameters, such as the K-SEAF identification code, the security capability of a terminal, and the NAS message authentication code, to the user equipment
S108 Send the first key parameter to the access and mobility management network element
S109 Send the first key parameter to the user equipment
S110 Deduce, according to the received second key parameter, and the parameters, such as the K-SEAF identification code, the shared key of control plane slice
S111 Deduce, according to the received first key parameter, second key parameter, and parameters, such as the K-SEAF identification code, a special key for the control plane slice
AA User equipment
BB Access network element
CC Shared network element of multiple control plane slices
DD Slice selection network element
EE Core network
FF Access and mobility management network element
GG Secure anchor network element
HH N network slices

(57) **Abstract:** Disclosed is a system for processing a network key. The system comprises: a user equipment, a secure anchor network element and an access and mobility management network element, wherein the secure anchor network element is used for obtaining a first key parameter from a slicing selection network element, wherein the first key parameter comprises identifier information about N network slices, and for generating special keys for N slices according to the first key parameter, and sending the special keys for N slices to the corresponding N network slices respectively; the access and mobility management network element is used for obtaining the first

[见续页]

WO 2018/137351 A1

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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

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

本国际公布：
— 包括国际检索报告(条约第21条(3))。

key parameter and sending the first key parameter to the user equipment; and the user equipment is used for generating, according to the first key parameter, special keys for N slices of the N network slices, and accessing the N network slices according to the generated special keys for N splices. In this way, different special keys are set for different network splices, thereby reducing the security risks when a shared key is used for signalling interaction.

(57) 摘要：本申请实施例公开了一种网络密钥处理的系统，包括：用户设备、安全锚点网元、接入及移动管理网元，其中：安全锚点网元用于从切片选择网元获取第一密钥参数，第一密钥参数包括N个网络切片的标识信息，并根据第一密钥参数生成N个切片专用密钥，并将N个切片专用密钥分别发送给相对应的N个网络切片；接入及移动管理网元用于获取第一密钥参数，并将第一密钥参数发送给用户设备；用户设备用于根据第一密钥参数生成N个网络切片的N个切片专用密钥，并根据所生成的N个切片专用密钥访问N个网络切片。这样，针对不同的网络切片设置了不同的专用密钥，从而降低了使用共享密钥进行信令交互时的安全隐患。

一种网络密钥处理的方法、相关设备及系统

本申请要求于 2017 年 1 月 25 日提交中国专利局、申请号为 201710064224.2、发明名称为“一种网络密钥处理的方法、相关设备及系统”的中国专利申请的优先权。

技术领域

本申请涉及移动通信网络的网络安全技术领域，尤其涉及一种网络密钥处理的方法、相关设备及系统。

背景技术

当前移动通信网络（如 3G/LTE）主要提供了三个层面的安全：终端和网络之间的双向认证、NAS (Non Access Stratum，非接入层) 安全、AS（Access Stratum，接入层）安全。终端和网络首先是经过双向认证来确认彼此身份的真实性，并生成可以用来建立 NAS 安全及 AS 安全的根密钥（K_ASME)。NAS 层位于 3GPP EPS（Evolved Packet System，演进分组系统）协议栈中控制面的最高层，它是用来传递终端与核心网之间的非无线接入相关的信令，主要包括了用于移动性管理（MM，Mobility Management）和会话管理（SM，Session Management）的信令协议及流程。而 AS 层主要是用于终端和基站之间交互的无线接入协议栈。NAS 安全和 AS 安全所需要的密钥都是从 K_ASME 派生而来的。

在 3GPP 下一代无线通信网络架构中，引入了网络切片（Network Slicing）的架构。一个网络切片是一种虚拟化的逻辑专网，可以根据不同业务需求而定制。为了更好的支持网络切片的定制化，首先需要将当前的网元进行细化。当前 LTE 核心网中的 MME（Mobility Management Entity，移动性管理网元）的功能网元，在下一代网络中将会被细化为多个功能。比如在 3GPP SA2 TR 23.799 V14.0.0 (2016-12)的技术报告中， MME 功能被分解为接入及移动管理功能（AMF，Access and Mobility Management Function)、安全锚点功能（SEAF)、会话管理功能（SMF）等网络功能。

当一个终端接入网络时，网络会根据某些方法选择一个或多个切片给这个终端，当一个终端同时接入多个切片时，终端与切片之间的信令交互都是经过 AMF，AMF 为 NAS 信令的加解密终结点，AMF 属于多切片共享功能，上述第一点说明，当一个终端同时接入多个切片时，AMF 是一个交汇点。这一限制是来源于终端移动性和对网络架构的复杂性的考虑。一方面，终端不管接入几个切片，它的移动性是一致的或唯一的；另一方面，如果允许一个 UE 同时接入多个 AMF，会显著增加网络功能或网元间链接、接口的数目及复杂性。

切片在同终端交互 NAS 信令时，如切片 1（或切片 2）发送 NAS 信息给终端，NAS 信息对于 AMF 来说是没有加密的明文。当攻击者入侵了 AMF 时，它可以轻易获得 SMF 发出的信息，从而容易造成了切片的 NAS 信息泄露。

发明内容

本申请实施例提供了一种网络密钥处理的方法、相关设备及系统，用于提高网络信令交互的安全性。

本申请第一方面提供一种网络密钥处理的系统，包括：用户设备、安全锚点网元、接入及移动管理网元，其中：

所述安全锚点网元用于从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N

个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片，并根据所述第一密钥参数生成 N 个切片专用密钥；其中，N 为大于或等于 1 的整数，N 个网络切片为用户设备在与核心网进行双向认证时核心网所选择给用户设备的一个或多个网络切片。或者由用户设备先发送需要接入的网络切片的标识给核心网，再由核心网中的网元，比如切片选择功能的网元根据用户设备发送的网络切片的标识确定所对应的网络切片，其中，该切片选择功能的网元还可以先判断该标识所对应的网络切片是否可以分配给该用户设备，若可以，则将其分配给用户设备，若不可以，则不将其分配给所述用户设备。

所述安全锚点网元还用于将所述 N 个切片专用密钥分别发送给相对应的所述 N 个网络切片；安全锚点网元可以根据 N 个网络切片的标识信息将所生成的 N 个专用密钥分别发送给所对应的N个网络切片，每个网络切片接收到与其标识对应的专用密钥，若接收成功，则可以向安全锚点网元发送接收成功的确认信息。

所述接入及移动管理网元用于从所述切片选择网元或者所述安全锚点网元获取所述第一密钥参数，并将所述第一密钥参数发送给所述用户设备；第一密钥参数包括N个网络切片的标识信息，核心网中的切片选择网元与安全锚点网元均已获得该标识信息，所以可以由安全锚点将该标识信息发送给接入及移动管理网元，或者由切片选择网元将该标识信息发送给接入及移动管理网元。

所述用户设备用于根据所述第一密钥参数生成所述N个网络切片的N个切片专用密钥，并根据所生成的所述 N 个切片专用密钥访问所述 N 个网络切片。用户设备与安全锚点网元预先约定使用相同的密钥生成规则进行专用密钥的生成，当用户设备与安全锚点网元均使用同样的第一密钥参数进行专用密钥生成时，那么用户设备所生成的 N 个切片专用密钥则与安全锚点网元所生成的 N 个切片专用密钥是相同的，从而使得用户设备能够根据 N 个切片专用密钥去依次访问该 N 个网络切片。这样，在本申请中，针对不同的网络切片设置了不同的专用密钥，并且用户设备能够生产相同的网络切片的专用密钥，使得用户设备能够与网络切片进行信令交互，从而降低了使用共享密钥进行信令交互时的安全隐患。

一种可能的实现方式中，所述安全锚点网元还用于根据第二密钥参数为所述接入及移动管理网元生成共享密钥，并将所述第二密钥参数发送给所述接入及移动管理网元，所述共享密钥用于所述N个网络切片的共享网络功能使用；

所述接入及移动管理网元还用于接收所述安全锚点网元发送的所述第二密钥参数；

所述用户设备还用于从所述接入及移动管理网元接收到所述第二密钥参数后，并生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。由于在实际应用中，不同的网络切片也可能会存在相同的网络功能，比如一些普遍的基础功能一般均设置为共享网络功能，这类的功能一般每个用户设备在接入时都具备，从而这些网络功能不必要设置在网络切片内被网络切片进行专用保护，从而可以通过设置共享密钥的方式进行与所有合法用户设备进行信令交互。

另一种可能的实现方式中，所述接入及移动管理网元还用于：

在将所述第一密钥参数发送给所述用户设备之前，通过所述共享密钥为所述第一密钥

参数进行加密；

所述接入及移动管理网元具体用于：

所述接入及移动管理网元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备；

所述用户设备具体用于接收所述接入及移动管理网元通过切片安全模式命令发送的进行加密后的所述第一密钥参数。

由于在接入及移动管理网元发送第一密钥参数给用户设备的过程中，可能会导致数据包被拦截，从而使得攻击者获取该数据包中第一密钥参数的内容信息，由于该第一密钥参数包含所述用户设备所接入的网络切片的标识信息，从而获知所述用户设备所接入的网络切片的类型，则可能导致所述用户设备的个人信息泄露，甚至可能造成攻击者直接通过该第一密钥参数接入所对应的网络切片，从而进行不法行为的操作。因此，在本申请中，在接入及移动管理网元发送第一密钥给用户设备之前，还可以对该第一密钥进行加密，具体可以通过共享密钥对该第一密钥进行加密，用户设备在接收到共享密钥的密钥参数后，则能够推演解析出加密数据包的内容，从而获取第一密钥参数。这样，提高了网络通信的安全性。

另一种可能的实现方式中，所述系统还包括网络切片，其中：

所述网络切片用于接收所述安全锚点网元发送的专用密钥；

所述网络切片还用于根据加密参数对 M 个网络功能进行加密，所述加密参数包括所述专用密钥以及所述 M 个网络功能的功能标识；

所述网络切片还用于将所述加密参数发送给所述接入及移动管理网元；

所述接入及移动管理网元还用于将所述加密参数发送给用户设备；

所述用户设备还用于接收所述加密参数，并能够根据所述加密参数访问所述网络切片的所述 M 个网络功能。

每个网络切片可能包含多个网络功能，不同的网络功能的重要性程度不一样，更重要的网络功能应该设置更复杂的加密方法，在本申请中，可以通过对每个网络切片中的各个网络功能进行加密，从而提高不同网络功能的安全性。具体的，每个网络功能的加密算法可以相同，也可以不同，加密后，将加密的参数发送给用户设备，从而使得用户设备能够根据加密的参数访问该加密后的网络功能。

本申请第第二方面提供一种安全锚点网元，所述网元包括：

获取单元，用于从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；

生成单元，用于根据所述第一密钥参数生成 N 个专用密钥；

发送单元，用于将所述 N 个切片专用密钥分别发送给相对应的所述 N 个网络切片，以使得用户设备从接入及移动管理网元接收到所述第一密钥参数后，生成相同的所述 N 个切片专用密钥从而能够访问所述 N 个网络切片。

一种可能的实现方式中，所述发送单元还用于：

将所述第一密钥参数发送给接入及移动管理网元，用于所述接入及移动管理网元发送所述第一密钥参数至用户设备。

另一种可能的实现方式中，所述生成单元还用于：

根据第二密钥参数为所述接入及移动管理网元生成共享密钥，并将所述第二密钥参数发送给所述接入及移动管理网元，所述共享密钥用于所述 N 个网络切片的共享网络功能使用，以使得所述用户设备从所述接入及移动管理网元接收到所述第二密钥参数后，生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

本申请第三方面提供一种接入及移动管理网元，所述网元包括：

获取单元，用于从切片选择网元或者安全锚点网元获取所述第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述 N 个切片专用密钥发送给相对应的所述 N 个网络切片。

发送单元，用于将所述第一密钥参数发送给所述用户设备，以使得所述用户设备根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访问所述 N 个网络切片。

一种可能的实现方式中，所述网元还包括：

接收单元，用于接收所述安全锚点网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述发送单元还用于，将所述第二密钥参数发送给所述用户设备，以使得所述用户设备根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

另一种可能的实现方式中，所述网元还包括：

加密单元，在所述发送单元通过切片安全模式命令将所述第一密钥参数发送给所述用户设备之前，用于所述接入及移动管理网元通过所述共享密钥为所述第一密钥参数进行加密；

所述发送单元具体还用于：

通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备。

另一种可能的实现方式中，所述所述接收单元还用于：

在所述发送单元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备之前，接收所述 N 个网络切片发送的加密参数，所述加密参数为所述N个网络切片中每个网络切片为 M 个网络功能进行加密所使用的参数；

所述发送单元还用于：

通过切片安全模式命令将将进行加密后的所述第一密钥参数以及所述加密参数发送给所述用户设备，以使得所述用户设备根据所述加密参数访问所述 N 个网络切片的所述 M 个网络功能。

本申请第四方面提供一种网络切片，所述网络切片包括：

接收单元，用于接收安全锚点网元发送的专用密钥；

加密单元，用于根据加密参数对 M 个网络功能进行加密，所述加密参数包括所述专用密钥以及所述 M 个网络功能的功能标识；

发送单元，用于将所述加密参数发送给接入及移动管理网元，以使得所述接入及移动管理网元将所述加密参数发送给用户设备，使得所述用户设备根据所述加密参数访问所述网络切片的所述 M 个网络功能。

本申请第五方面提供一种用户设备，所述用户设备包括：

接收单元，用于接收所述接入及移动管理网元发送的第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述 N 个切片专用密钥发送给相对应的所述 N 个网络切片；

生成单元，用于根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访问所述 N 个网络切片。

一种可能的实现方式中，所述接收单元还用于：

接收所述接入及移动管理网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述用户设备还包括：

生成单元，用于根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

另一种可能的实现方式中，所述接收单元具体还用于：

接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数。

另一种可能的实现方式中，所述接收单元具体还用于：

接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数以及加密参数，所述加密参数为所述N个网络切片中每个网络切片为 M 个网络功能进行加密所使用的参数；

所述用户设备还包括：

访问单元，用于根据所述加密参数访问所述 N 个网络切片的所述 M 个网络功能。

本申请第六方面提供一种网络密钥处理的方法，应用于安全锚点网元侧，所述方法包括：

安全锚点网元从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；

所述安全锚点网元根据所述第一密钥参数生成 N 个专用密钥；

所述安全锚点网元将所述 N 个切片专用密钥分别发送给相对应的所述 N 个网络切片，以使得用户设备从接入及移动管理网元接收到所述第一密钥参数后，生成相同的所述 N 个切片专用密钥从而能够访问所述 N 个网络切片。

一种可能的实现方式中，所述方法还包括：

所述安全锚点网元将所述第一密钥参数发送给接入及移动管理网元，用于所述接入及移动管理网元发送所述第一密钥参数至用户设备。

另一种可能的实现方式中，所述方法还包括：

所述安全锚点网元根据第二密钥参数为所述接入及移动管理网元生成共享密钥，并将所述第二密钥参数发送给所述接入及移动管理网元，所述共享密钥用于所述 N 个网络切片的共享网络功能使用，以使得所述用户设备从所述接入及移动管理网元接收到所述第二密钥参数后，生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

本申请第七方面提供一种网络密钥处理的方法，应用于接入及移动管理网元侧，所述方法包括：

接入及移动管理网元从切片选择网元或者安全锚点网元获取所述第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所选择的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述 N 个切片专用密钥发送给相对应的所述 N 个网络切片。

所述接入及移动管理网元将所述第一密钥参数发送给所述用户设备，以使得所述用户设备根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访问所述 N 个网络切片。

一种可能的实现方式中，所述方法还包括：

所述接入及移动管理网元接收所述安全锚点网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述接入及移动管理网元将所述第二密钥参数发送给所述用户设备，以使得所述用户设备根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

另一种可能的实现方式中，所述接入及移动管理网元将所述第二密钥参数发送给所述用户设备，包括：

所述接入及移动管理网元通过所述切片安全模式命令将所述第二密钥参数发送给所述用户设备。

另一种可能的实现方式中，在所述接入及移动管理网元通过切片安全模式命令将所述第一密钥参数发送给所述用户设备之前，所述方法还包括：

所述接入及移动管理网元通过所述共享密钥为所述第一密钥参数进行加密；

所述接入及移动管理网元通过切片安全模式命令将所述第一密钥参数发送给所述用户设备，包括：

所述接入及移动管理网元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备。

另一种可能的实现方式中，在所述接入及移动管理网元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备之前，所述方法还包括：

接收所述 N 个网络切片发送的加密参数，所述加密参数为所述N个网络切片中每个网

络切片为 M 个网络功能进行加密所使用的参数；

所述接入及移动管理网元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备，包括：

所述接入及移动管理网元通过切片安全模式命令将将进行加密后的所述第一密钥参数以及所述加密参数发送给所述用户设备，以使得所述用户设备根据所述加密参数访问所述 N 个网络切片的所述 M 个网络功能。

本申请第八方面提供一种网络密钥处理的方法，应用网络切片侧，所述方法包括：

所述网络切片接收安全锚点网元发送的专用密钥；

所述网络切片根据加密参数对 M 个网络功能进行加密，所述加密参数包括所述专用密钥以及所述 M 个网络功能的功能标识；

所述网络切片将所述加密参数发送给接入及移动管理网元，以使得所述接入及移动管理网元将所述加密参数发送给用户设备，使得所述用户设备根据所述加密参数访问所述网络切片的所述 M 个网络功能。

本申请第九方面提供一种网络密钥处理的方法，应用于用户设备侧，所述方法包括：

所述用户设备接收所述接入及移动管理网元发送的第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述 N 个切片专用密钥发送给相对应的所述 N 个网络切片；

所述用户设备根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访问所述 N 个网络切片。

一种可能的实现方式中，所述方法还包括：

所述用户设备接收所述接入及移动管理网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述用户设备根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

另一种可能的实现方式中，所述用户设备接收所述接入及移动管理网元发送的第二密钥参数，包括：

所述用户设备接收所述接入及移动管理网元通过所述切片安全模式命令发送的所述第二密钥参数。

另一种可能的实现方式中，所述用户设备接收所述接入及移动管理网元通过所述切片安全模式命令发送的所述第二密钥参数，包括：

所述用户设备接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数。

另一种可能的实现方式中，所述用户设备接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数，包括：

所述用户设备接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共

享密钥进行加密后的所述第一密钥参数以及加密参数，所述加密参数为所述N个网络切片中每个网络切片为M个网络功能进行加密所使用的参数；

所述用户设备根据所述加密参数访问所述N个网络切片的所述M个网络功能。

本申请第十方面提供一种安全锚点设备，所述安全锚点设备包括收发器、处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第六方面的任意实现方式描述的网络密钥处理的方法。

本申请第十一方面提供一种接入及移动管理设备，所述接入及移动管理设备包括收发器、处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第七方面的任意实现方式描述的网络密钥处理的方法。

本申请第十二方面提供一种网络切片设备，所述网络切片设备包括收发器、处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第 八方面的任意实现方式描述的网络密钥处理的方法。

本申请第十三方面提供一种用户设备，所述用户设备包括收发器、处理器和存储器，所述存储器用于存储程序和数据；所述处理器调用所述存储器中的程序用于执行第 九方面的任意实现方式描述的网络密钥处理的方法。

本申请第十四方面提供了一种计算机可读存储介质，所述计算机可读存储介质中存储有指令，当其在计算机上运行时，使得计算机执行上述各方面所述的方法。

本申请第十五方面提供了一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述各方面所述的方法。

从以上技术方案可以看出，本申请实施例具有以下优点：

在本申请中，针对不同的网络切片设置了不同的专用密钥，并且用户设备能够生产相同的网络切片的专用密钥，使得用户设备能够与网络切片进行信令交互，从而降低了使用共享密钥进行信令交互时的安全隐患。

附图说明

图1为本申请实施例中提供的网络密钥处理的架构示意图；

图 2 为本申请实施例中提供的用户设备 10、安全锚点设备 30、接入及移动管理设备 40 及网络切片 50 对应的结构示意图；

图3为本申请实施例中提供的网络密钥处理的方法的第一个实施例的流程示意图；

图4为本申请实施例中提供的网络密钥处理的方法的第二个实施例的流程示意图；

图5为本申请实施例中提供的网络密钥处理的方法的第三个实施例的流程示意图；

图6为本申请实施例中提供的网络密钥处理的方法的第四个实施例的流程示意图；

图7为本申请实施例中提供的网络密钥处理的方法的第五个实施例的流程示意图；

图8为本申请实施例中提供的一个密钥架构的示意图；

图9为本申请实施例中提供的另一个密钥架构的示意图；

图 10 为本申请实施例中提供的网络密钥处理的系统及网络密钥处理的系统中相关网元的结构示意图；

图11A-图11F为本申请实施例中提供的第一设备进行密钥推演的六种示意图；

图 12 为本申请实施例中提供的第一设备进行密钥生成与分发的一个流程示意图；

图 13 为本申请实施例中提供的总体密钥架构示意图。

具体实施方式

本申请实施例提供了一种网络密钥处理的方法、相关设备及系统，用于提高网络信令交互的安全性。

本申请的实施方式部分使用的术语仅用于对本申请的具体实施例进行解释，而非旨在限定本申请。

网络切片是一种虚拟化的逻辑专网，可以根据不同业务需求而定制。网络切片的运营、管理方式是多样的。MNO (Mobile network operator, 移动网络运营商) 可以自行运营、管理切片，一个切片可以由不同用户共享。当然，为了配合垂直行业的发展，MNO 的一个或多个网络切片也可以出租给垂直行业，由其自行运营、管理、认证用户设备（移动终端或 IoT 设备等）。对于接入切片的用户设备，首先用户设备需要通过 MNO 的服务去接入切片，然后由切片对用户设备进行管理。也就是说，用户设备既要和 MNO 网络交互，也要和网络切片有交互。

为了更好的支持网络切片的定制化，首先会将当前的网络功能进行细化。比如在 3GPP SA2 TR 23.799 V14.0.0 (2016-12)的技术报告中，MME 功能被分解为 AMF、SEAF、SMF）等网络功能。需要指出的是，本申请中所述的各个网络功能，如 AMF（Access and Mobility Management Function，接入及移动管理功能）、SMF（Session Management Function，会话管理功能）、SEAF（Security Anchor Function，安全锚点功能）等，是目前 3GPP SA2 和 SA3 标准工作组的文稿及技术报告（TR）中所采用的名称。这些名称还有可能更改，如更名、网络功能合并、分拆等，本申请并不局限于这些网络功能的名称及其位置（设在或合设于哪个网元中，比如，在 4G 网络中，MMF 和 SEAF 是合设在一起的，即 MME）。在后续通信标准的制定中，上述功能网元的划分方式可能发生变化，这种变化不影响本申请实施例的实施。

图 1 是本发明实施例提供的一种网络密钥处理的架构示意图。如图 1 所示，网络密钥处理的系统 100 可包括：用户设备 10、接入网网元 20、安全锚点网元 30 以、接入及移动管理网元 40 以及网络切片 50。其中：

接入网网元 20 可用于为用户设备 10 提供网络接入服务。具体实现中，接入网网元 20 可包括基站（NodeB）、基站控制器（Radio Network Controller，RNC）或接入网关等。具体实现中，用户设备 10 可以包括手机、平板电脑、笔记本电脑、移动互联网设备（Mobile Internet Device，MID）、可穿戴设备（例如智能手表、智能手环、计步器等）等用户终端，也可以包括 IoT 设备，还可以包括其他可接入 MNO 网络的通信设备。

安全锚点网元 30 可用于为所有接入网络的 UE 提供网络认证、密钥生成等服务，具体可包括配置在核心网 CN 中的 SEAF 等网络功能。

本发明实施例中，安全锚点网元 30 用于为接入及移动管理网元生成共享密钥，还用于为用户设备 10 所接入的多个网络切片 50 生成专用密钥。

接入及移动管理网元 40 用于将安全锚点网元 30 生成共享密钥的参数以及生成专用密

钥的参数发送给用户设备 10，用户设备则能够推演出网络切片的专用密钥，从而能够访问所接入的网络切片。这样，每个网络切片都设置有专用密钥，使得用户设备与网络切片所交互的 NAS 信令不易被获取，提高了网络通信的安全性。

应理解的，当接入网网元 20 只包括一个网络实体（例如基站）时，后续描述到的接入网网元 20 所执行的操作均由该一个网络实体完成。当接入网网元 20 包括多个网络实体（例如基站和基站控制器）时，后续描述到的接入网网元 20 所执行的操作由所述多个网络实体协作完成。

应理解的，当安全锚点网元 30 只包括一个网络实体（例如 SEAF）时，后续描述到的安全锚点网元 30 所执行的操作均由该一个网络实体完成。当该安全锚点网元 30 包括多个网络实体（例如 SEAF 和 AMF）时，后续描述到的安全锚点网元 30 所执行的操作由所述多个网络实体协作完成。

应理解的，当接入及移动管理网元 40 只包括一个网络实体（例如 AMF）时，后续描述到的接入及移动管理网元 40 所执行的操作均由该一个网络实体完成。当该接入及移动管理网元 40 包括多个网络实体（例如 SEAF 和 AMF）时，后续描述到的接入及移动管理网元 40 所执行的操作所述多个网络实体协作完成。

这里，所述协作完成是指多个网络实体各执行一些操作，执行操作所产生的数据、参数均可以根据需要在这多个网络实体各之间传输。

需要说明的是，不限于图 1 所示，安全锚点网元 30 还可包括更多或更少网络功能，接入及移动管理网元 40 还可包括更多或更少切片网络功能。

需要说明的是，本申请中的所描述的安全锚点网元、接入及移动管理网元、接入网网元等名称在实际应用中可能为其它的名称，这些网元名称并不能对本申请构成限定，只要是具备本申请实施例中所描述的功能和作用，均属于本申请所保护的范围。

图 2 是本发明实施例提供的通信装置示意图。图 1 中的用户设备 10 或者安全锚点设备 30 或者接入及移动管理设备 40 或者网络切片 50 可以通过图 2 所示的通信装置(或系统)200 来实现。

如图 2 所示，通信装置(或系统)200 可包括至少一个处理器 401，存储器 403 以及至少一个通信接口 404。这些部件可在一个或多个通信总线 402 上通信。

需要说明的，图 2 仅仅是本发明实施例的一种实现方式，实际应用中，通信装置 200 还可以包括更多或更少的部件，这里不作限制。

通信接口 404 用于接收和发送射频信号，耦合于通信装置 200 的接收器和发射器。通信接口 404 通过射频信号与通信网络和其他通信设备通信，如以太网（Ethernet），无线接入网(Radio Access Technology， RAN)，无线局域网 Wireless Local Area Networks，WLAN)等。具体实现中，通信接口 404 支持的通信协议可包括但不限于：2G/3G、LTE、Wi-Fi、5G New Radio (NR) 等等。

存储器 403 与处理器 401 耦合，用于存储各种软件程序和/或多组指令。具体实现中，存储器 403 可包括高速随机存取的存储器，并且也可包括非易失性存储器，例如一个或多个磁盘存储设备、闪存设备或其他非易失性固态存储设备。存储器 403 可以存储操作系统

（下述简称系统），例如 ANDROID，IOS，WINDOWS，或者 LINUX 等嵌入式操作系统。存储器 403 可用于存储本发明实施例的实现程序。存储器 403 还可以存储网络通信程序，该网络通信程序可用于与一个或多个附加设备，一个或多个终端设备，一个或多个网络设备进行通信。

处理器 401 可以是一个通用中央处理器(Central Processing Unit，CPU)，微处理器，特定应用集成电路(Application-Specific Integrated Circuit，ASIC)，或一个或多个用于控制本发明方案程序执行的集成电路。

在一些实施例中，通信装置 200 还可以包括输出设备 405 和输入设备 406。输出设备 405 和处理器 401 通信，可以以多种方式来显示信息。例如，输出设备 405 可以是液晶显示器(Liquid Crystal Display，LCD)，发光二级管(Light Emitting Diode，LED)显示设备，阴极射线管(Cathode Ray Tube，CRT) 显示设备，或投影仪(projector)等。输入设备 406 和处理器 401 通信，可以以多种方式接受用户的输入。例如，输入设备 406 可以是鼠标、键盘、触摸屏设备或传感设备等。为了便于输出设备 405 和输入设备 406 的用户使用，在一些实施例中，存储器 202 还可以存储用户接口程序，该用户接口程序可以通过图形化的操作界面将应用程序的内容形象逼真的显示出来，并通过菜单、对话框以及按键等输入控件接收用户对应用程序的控制操作。

当图 2 所示的通信装置 200 实现为图 1 所示的用户设备 10 时，通信装置 200 的存储器中可以存储了一个或多个软件模块，可用于提供接入请求、用户认证响应等功能，具体可参考后续方法实施例。当图 2 所示的通信装置 200 实现为图 1 所示的安全锚点设备 30 时，通信装置 200 的存储器中可以存储了一个或多个软件模块，可用于提供生成密钥等功能，具体可参考后续方法实施例。当图 2 所示的通信装置 200 实现为图 1 所示的接入及移动管理设备 40 时，通信装置 200 的存储器中可以存储了一个或多个软件模块，可用于提供对密钥参数进行加密的功能，具体可参考后续方法实施例。当图 2 所示的通信装置 200 实现为图 1 所示的网络切片 50 时，通信装置 200 的存储器中可以存储了一个或多个软件模块，可用于提供对网络功能进行加密的功能，具体可参考后续方法实施例。

下面结合图 3-7 的几个实施例详细描述本发明实施例提供的网络密钥处理的方法。

图 3 是本发明实施例提供的网络密钥处理的方法的第一实施例的流程示意图。图 3 实施例中，安全锚点网元生成了切片专用控制面密钥，下面展开描述：

S101、用户设备和核心网（SEAF）、网络切片进行双向认证。

具体的，用户设备进行认证时，核心网生成根密 K_SEAF。核心网中的切片选择网元（如 NSSF）为用户设备选择了 N 个网络切片（如确定了切片 ID）Slc-ID1…Slc-IDN。即切片选择网元获取了所确定的 N 个网络切片的标识信息。

S102、所述安全锚点网元根据 K_SEAF 以及第二密钥参数为接入及移动管理网元生成共享密钥，所述共享密钥为控制面共享密钥。

其中，所述控制面共享密钥用于所述 N 个网络切片的控制面的共享网络功能使用，所述第二密钥参数包括密钥算法类型区分码（Algorithm Distinguisher）、密钥算法 ID（Algorithm ID）等信息。

S103、所述安全锚点网元从切片选择网元获取第一密钥参数，所述第一密钥参数包括N个网络切片的标识信息。

S104、所述安全锚点网元根据K_SEAF以及所述第一密钥参数生成N个切片专用密钥，所述专用密钥为控制面专用密钥。

其中，第一密钥参数可以包括网络切片ID：Slc-ID1…Slc-IDN，分别为网络切片n=1…N生成切片专用的控制面根密钥（KCP-S1… KCP-SN）。

需要说明的是，安全锚点网元在为每个网络切片生成专用密钥时，还可以根据第二密钥参数包括密钥算法类型区分码、密钥算法ID等作为密钥参数进行生成。其中，密钥算法类型区分码需要设定为切片专用的控制面密钥算法所对应的值。

S105、所述安全锚点网元于将所述N个切片专用密钥分别发送给相对应的所述N个网络切片。

需要说明的是，网络切片在接收到专用控制面密钥后也可以分别回复接收成功的消息给安全锚点网元。

S106、所述接入及移动管理网元接收所述安全锚点网元发送的第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数。

S107、所述接入及移动管理网元将所述第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数发送给用户设备。

S108、所述安全锚点网元发送的所述第一密钥参数给所述接入及移动管理网元。

需要说明的是，第一密钥参数也可以由切片选择网元（如NSSF）发送给接入及移动管理网元。

S109、所述接入及移动管理网元将所述第一密钥参数发送给所述用户设备。

第一密钥参数可以包括（如切片ID： Slc-ID1…Slc-IDN） 和密钥算法类型区分码设定为切片专用的控制面密钥算法（NAS-Slc）所对应的值等信息，由于其中包含切片的标识信息，现有的发送命令无法携带该标识信息，因此本申请所定义的发送命令为切片安全模式命令SSMC（Slice Security Mode Command），通过该SSMC来发送所述第一密钥给用户设备。

S110、用户设备根据收到第二密钥参数以及K_SEAF标识码等参数，推演控制面切片共享密钥（AMF或CCNF）。

S111、用户设备根据收到的第一密钥参数、第二密钥参数（其中，密钥算法类型区分码需要设定为切片专用的控制面密钥算法所对应的值）以及K_SEAF标识码等参数，推演控制面切片专用密钥。

如，生成第N个切片的密钥的生成函数KDF的参数为：KDF(K_SEAF,Slc-ID1, NAS-Slc, Alg-ID)，其中，KDF 为安全锚点网元为每个网络切片生成专用密钥所使用的生成函数，NAS-Slc 为密钥算法类型区分码参数设定为切片专用的控制面密钥算法所对应的值，Alg-ID 为密钥算法ID)。

这样，用户设备获取到安全锚点网元为每个网络切片所生成专用控制面密钥的密钥参数，则能够根据该密钥参数生成相应的密钥并访问所接入的每个网络切片，即提高了网络

通信的安全性，又保证了用户设备的正常通信。

图 4 是本发明实施例提供的网络密钥处理的方法的第二实施例的流程示意图。图 4 实施例中，进一步对生成切片专用的控制面密钥的参数在发送给用户设备之前进行加密，下面展开描述：

S201、用户设备和核心网（SEAF）、网络切片进行双向认证。

S202、所述安全锚点网元根据 K_SEAF 以及第二密钥参数为接入及移动管理网元生成控制面共享密钥。

S203、所述安全锚点网元从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息。

S204、所述安全锚点网元根据 K_SEAF 以及所述第一密钥参数生成 N 个切片专用的控制面密钥。

S205、所述安全锚点网元于将所述 N 个切片专用的控制面密钥分别发送给相对应的所述 N 个网络切片。

S206、所述接入及移动管理网元接收所述安全锚点网元发送的第二密钥参数以及 K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数。

S207、所述接入及移动管理网元将所述第二密钥参数以及 K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数发送给用户设备。

S208、所述安全锚点网元发送的所述第一密钥参数给所述接入及移动管理网元。

S209、所述接入及移动管理网元使用所述共享密钥为所述第一密钥参数进行加密。

由于第一密钥参数中包含了用户设备所接入的网络切片的标识信息，在实际应用中，网络切片的标识信息具有一定私密性，当攻击者获取到了用户设备所接入的网络切片的标识，从而则可能获取该用户设备所接入的网络切片的类型，从而展开其它攻击，对该用户设备造成一定的安全隐患。因此在传输该第一密钥参数之前，对该第一密钥参数进行加密处理。

需要说明的是，在对该第一密钥参数进行加密时，还需进行加密完整性保护，即可通过生成一段数据添加到加密后的数据包中，从而让接收端判断该数据包是否被修改。

S210、所述接入及移动管理网元将加密后的第一密钥参数嵌入 SSMC 命令，通过接入网网元发给所述用户设备。

S211、用户设备根据收到第二密钥参数以及 K_SEAF 标识码等参数，推演控制面切片共享密钥（AMF 或 CCNF）。

S212、用户设备根据所述推演得到的控制面切片共享密钥对第一密钥参数进行解密，根据解密得到的第一密钥参数以及第二密钥参数（其中，密钥算法类型区分码需要设定为切片专用的控制面密钥算法所对应的值）、K_SEAF 标识码等参数推演控制面切片专用密钥。

图 5 是本发明实施例提供的网络密钥处理的方法的第三实施例的流程示意图。图 5 实施例中，用于优化、减少信令传送的个数，通过发送一个 SSMC 信令来传送切片控制面共享密钥的参数和切片专用的控制面密钥的参数，从而达到节省空口资源的目的，下面展开描述：

S301、用户设备和核心网（SEAF）、网络切片进行双向认证。

S302、所述安全锚点网元根据 K_SEAF 以及第二密钥参数为接入及移动管理网元生成共享密钥。

S303、所述安全锚点网元从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息。

S304、所述安全锚点网元根据所述第一密钥参数 K_SEAF 以及生成 N 个切片专用密钥。

S305、所述安全锚点网元于将所述 N 个切片专用的控制面密钥分别发送给相对应的所述 N 个网络切片。

S306、所述接入及移动管理网元接收所述安全锚点网元发送的第二密钥参数以及 K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数。

S307、所述安全锚点网元发送所述第一密钥参数以及 K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数给所述接入及移动管理网元。

S308、所述接入及移动管理网元将所述第二密钥参数、K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数以及第一密钥参数通过 SSMC 发送给用户设备。

这样，通过发送一个 SSMC 信令来传送切片控制面共享密钥的参数和切片专用的控制面密钥的参数，从而达到节省空口资源的目的。

S309、用户设备根据收到第二密钥参数以及 K_SEAF 标识码等参数，推演控制面切片共享密钥（AMF 或 CCNF）。

S310、用户设备根据收到的第一密钥参数、第二密钥参数（其中，密钥算法类型区分码需要设定为切片专用的控制面密钥算法所对应的值）以及 K_SEAF 标识码等参数，推演控制面切片专用密钥。

图 6 是本发明实施例提供的网络密钥处理的方法的第四实施例的流程示意图。图 6 实施例中，用于优化、减少信令传送的个数，通过发送一个 SSMC 信令来传送切片共享密钥的参数和切片专用密钥的参数，从而达到节省空口资源的目的，并在发送 SSMC 之前，对切片专用密钥的参数进行加密处理，下面展开描述：

S401、用户设备和核心网（SEAF）、网络切片进行双向认证。

S402、所述安全锚点网元根据 K_SEAF 以及第二密钥参数为接入及移动管理网元生成切片控制面共享密钥。

S403、所述安全锚点网元从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息。

S404、所述安全锚点网元根据所述 K_SEAF 以及第一密钥参数生成 N 个切片专用的控制面密钥。

S405、所述安全锚点网元于将所述 N 个切片专用的控制面密钥分别发送给相对应的所述 N 个网络切片。

S406、所述接入及移动管理网元接收所述安全锚点网元发送的第二密钥参数以及 K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数。

S407、所述安全锚点网元发送的所述第一密钥参数以及 K_SEAF 标识码、终端安全能力、

NAS 消息认证码等参数给所述接入及移动管理网元。

S408、所述接入及移动管理网元通过所述切片控制面共享密钥为所述第一密钥参数进行加密。

S409、所述接入及移动管理网元将所述第二密钥参数、K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数以及进行加密后的第一密钥参数通过 SSMC 发送给用户设备。

S410、用户设备根据收到第二密钥参数以及 K_SEAF 标识码等参数，推演控制面切片共享密钥（AMF 或 CCNF）。

S411、用户设备根据所述推演得到的控制面切片共享密钥对第一密钥参数进行解密，根据解密得到的第一密钥参数以及第二密钥参数（其中，密钥算法类型区分码需要设定为切片专用的控制面密钥算法所对应的值）、K_SEAF 标识码等参数推演控制面切片专用密钥。

图 7 是本发明实施例提供的网络密钥处理的方法的第五实施例的流程示意图。图 7 实施例中，用于优化、减少信令传送的个数，通过发送一个 SSMC 信令来传送切片共享密钥的参数和切片专用密钥的参数，从而达到节省空口资源的目的，并在发送 SSMC 之前，对切片专用密钥的参数进行加密处理，并且，针对每个切片内包含多个控制面网络功能的情况，进行网元粒度的加密（及密钥生成、分发），下面展开描述：

S501、用户设备和核心网（SEAF）、网络切片进行双向认证。

S502、所述安全锚点网元根据 K_SEAF 以及第二密钥参数为接入及移动管理网元生成切片控制面共享密钥。

S503、所述安全锚点网元从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息。

S504、所述安全锚点网元根据所述 K_SEAF 以及第一密钥参数生成 N 个切片专用密钥。

S505、所述安全锚点网元于将所述 N 个切片专用的控制面密钥分别发送给相对应的所述 N 个网络切片。

S506、所述 N 个网络切片根据所述 N 个切片控制面专用密钥以及切片中的 M 个网络功能的 ID：NF-ID1…NF-IDM 推演出每个切片内 M 个网元功能的控制面密钥。比如，推演函数可以是 KDF(KCP-sn,NF-IDm, Slc-NF, Alg-ID)。然后，用每个切片专用的控制面密钥来加密用于生成网元功能密钥的加密参数，所述加密参数包括所述 M 个网络功能的功能标识。比如 enc(KCP-sn,NF-IDm)，其中，KCP-sn 为该网络切片的控制面专用密钥，NF-IDm 为第 m 个网络功能的功能标识。

S507、所述网络切片将所述加密后的网元密钥生成参数以及其他生成参数如 Slc-NF 和 Alg-ID 等发送给接入及移动管理网元。

S508、所述接入及移动管理网元接收所述安全锚点网元发送的第二密钥参数以及 K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数。

S509、所述安全锚点网元发送的所述第一密钥参数以及 K_SEAF 标识码、终端安全能力、NAS 消息认证码等参数给所述接入及移动管理网元。

S510、所述接入及移动管理网元通过所述切片控制面共享密钥为所述第一密钥参数进行加密。

S511、所述接入及移动管理网元将所述加密后的网元密钥生成参数以及其他生成参数如 Slc-NF 和 Alg-ID 等参数、第二密钥参数以及进行加密后的第一密钥参数通过 SSMC 发送给用户设备。

S512、用户设备根据收到的第二密钥参数以及 K_SEAF 标识码等参数，推演控制面切片共享密钥（AMF 或 CCNF）。

S513、用户设备根据所述推演的控制面切片共享密钥对加密的第一密钥参数进行解密，根据解密的第一密钥参数以及第二密钥参数、K_SEAF 标识码等参数推演控制面切片专用密钥。根据所述推演得到的控制面切片专用密钥，对所述切片内加密的网络功能生成参数进行解密并继续推演出控制面切片内网络功能的专用密钥。对每个切片 n：用密钥生成函数生成第 m 个网络功能的密钥 KDF(KCP-sn,NF-ID1, Slc-NF, Alg-ID)。

在本申请中，通过密钥的推演，最终得到的密钥及其相互推演关系，可以用一个树状的结构图（即密钥架构）来表示。图 8 中是第一至第四个实施例所对应的切片密钥架构（同样的），而图 9 是第五个实施例所对应的切片密钥架构。其中，enc 代表加密密钥，int 代表完整性保护密钥（即生成消息认证码 MAC 所需密钥），“CP”是指控制面。Kcp-c 表示控制面共享密钥，Kcp-s1 表示切片 1 的控制面专用密钥，Kcp-c-NF1-enc 表示控制面共享网络功能 1 的加密密钥，Kcp-c-NF1-int 表示控制面共享网络功能 1 的完整性保护密钥，Kcp-s1-NF1-enc 表示切片 1 的控制面专用网络功能 1 的加密密钥，Kcp-s1-NF1-enc 表示切片 1 的控制面专用网络功能 1 的完整性保护密钥。

图 10 是本发明实施例提供的网络认证系统以及所述网络认证系统中的相关网元的结构示意图。如图 10 所示，网络密钥处理的系统 300 可包括：安全锚点网元 301、接入及移动管理网元 302、网络切片 303、用户设备 304 以及接入网网元 305。下面展开描述。

如图 10 所示，安全锚点网元 301 可以包括获取单元 3011、生成单元 3012 和发送单元 3013，其中：

获取单元 3011，用于从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；

生成单元 3012，用于根据所述第一密钥参数生成 N 个专用密钥；

发送单元 3013,用于将所述 N 个切片专用密钥分别发送给相对应的所述 N 个网络切片，以使得用户设备从接入及移动管理网元接收到所述第一密钥参数后，生成相同的所述 N 个切片专用密钥从而能够访问所述 N 个网络切片。

可选的，所述发送单元 3013 还用于：

将所述第一密钥参数发送给接入及移动管理网元，用于所述接入及移动管理网元发送所述第一密钥参数至用户设备。

可选的，所述生成单元 3012 还用于：

根据第二密钥参数为所述接入及移动管理网元生成共享密钥，并将所述第二密钥参数发送给所述接入及移动管理网元，所述共享密钥用于所述 N 个网络切片的共享网络功能使用，以使得所述用户设备从所述接入及移动管理网元接收到所述第二密钥参数后，生成相

同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

如图 10 所示，接入及移动管理网元 302 可以包括获取单元 3021、发送单元 3022、接收单元 3023 以及加密单元 3024，其中：

获取单元 3021，用于从切片选择网元或者安全锚点网元获取所述第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述 N 个切片专用密钥发送给相对应的所述 N 个网络切片。

发送单元 3022，用于将所述第一密钥参数发送给所述用户设备，以使得所述用户设备根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访问所述 N 个网络切片。

可选的，所述发送单元 3022 具体用于：

通过切片安全模式命令将所述第一密钥参数发送给所述用户设备。

可选的，所述接收单元 3023，用于接收所述安全锚点网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述发送单元 3022 还用于，将所述第二密钥参数发送给所述用户设备，以使得所述用户设备根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

可选的，所述发送单元 3022 具体还用于：

通过所述切片安全模式命令将所述第二密钥参数发送给所述用户设备。

可选的，所述加密单元 3024，在所述发送单元 3022 通过切片安全模式命令将所述第一密钥参数发送给所述用户设备之前，用于所述接入及移动管理网元通过所述共享密钥为所述第一密钥参数进行加密；

所述发送单元 3022 具体还用于：

通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备。

可选的，所述所述接收单元 3023 还用于：

在所述发送单元 3022 通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备之前，接收所述 N 个网络切片发送的加密参数，所述加密参数为所述N个网络切片中每个网络切片为 M 个网络功能进行加密所使用的参数；

所述发送单元 3022 还用于：

通过切片安全模式命令将将进行加密后的所述第一密钥参数以及所述加密参数发送给所述用户设备，以使得所述用户设备根据所述加密参数访问所述 N 个网络切片的所述 M 个网络功能。

如图10所示，网络切片 303 可以包括接收单元 3031、加密单元 3032 以及发送单元 3033，其中：

接收单元 3031，用于接收安全锚点网元发送的专用密钥；

加密单元 3032，用于根据加密参数对 M 个网络功能进行加密，所述加密参数包括所述

专用密钥以及所述 M 个网络功能的功能标识；

发送单元 3033，用于将所述加密参数发送给接入及移动管理网元，以使得所述接入及移动管理网元将所述加密参数发送给用户设备，使得所述用户设备根据所述加密参数访问所述网络切片的所述 M 个网络功能。

如图 10 所示，用户设备 304 可以包括接收单元 3041、生成单元 3042 以及访问单元 3043，其中：

接收单元 3041，用于接收所述接入及移动管理网元发送的第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述 N 个切片专用密钥发送给相对应的所述 N 个网络切片；

生成单元 3042，用于根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访问所述 N 个网络切片。

可选的，所述接收单元 3041 具体用于：

接收所述接入及移动管理网元通过切片安全模式命令发送的所述第一密钥参数。

可选的，所述接收单元 3041 还用于：

接收所述接入及移动管理网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

生成单元 3042，用于根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

可选的，所述接收单元 3041 具体还用于：

接收所述接入及移动管理网元通过所述切片安全模式命令发送的所述第二密钥参数。

可选的，所述接收单元 3041 具体还用于：

接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数。

可选的，所述接收单元 3041 具体还用于：

接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数以及加密参数，所述加密参数为所述 N 个网络切片中每个网络切片为 M 个网络功能进行加密所使用的参数；

可选的，访问单元 3043，用于根据所述加密参数访问所述 N 个网络切片的所述 M 个网络功能。

需要说明的，安全锚点网元 301、接入及移动管理网元 302、网络切片 303 及用户设备 304 中各个功能单元的具体实现还可参考图 3-7 分别对应实施例中所述网络密钥的处理方法所对应的描述，这里不再赘述。

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。

下面结合图 11A 至图 11F 说明本发明实施例提供的几种第一设备根据中间密钥推衍出至少一个密钥的实施方式。

在第一种实施方式中，如图 11A 所示，假设本实施方式的应用场景为包括 S1~Sn 个切片，每个切片包括 H1~Hm 个会话，则第一设备可以根据中间密钥为每个切片的每个会话生成一组用户平面密钥，每组用户平面密钥包括用户面加密性密钥 Kij-Uenc、用户面完整性密钥 Kij-Uint、其中，i 表示切片的序号，j 表示会话在切片中的序号。第一设备可以根据中间密钥为每个切片生成一组控制面密钥，每组控制面密钥包括控制面加密性密钥 Ki-Cenc 以及控制面完整性密钥 Ki-Uint，其中，i 表示切片的序号。例如，第一设备可以根据中间密钥 Kan 为第一切片的第一会话生成用户面加密性密钥 K11-Uenc 以及用户面完整性密钥 K11-Uint，第一设备可以根据中间密钥 Kan 为第一切片的第二会话生成用户面加密性密钥 K12-Uenc 以及用户面完整性密钥 K12-Uint，依次类推，第一设备可以根据中间密钥 Kan 为第 n 切片的第 m 会话生成用户面加密性密钥 Knm-Uenc 以及用户面完整性密钥 Knm-Uint。第一设备可以根据中间密钥 Kan 为第一切片生成控制面加密性密钥 K1-Cenc 以及控制面完整性密钥 K1-Cint，第一设备可以根据中间密钥 Kan 为第二切片生成控制面加密性密钥 K2-Cenc 以及控制面完整性密钥 K2-Cint，依次类推，第一设备可以根据中间密钥 Kan 为第 n 切片生成控制面加密性密钥 Kn-Cenc 以及控制面完整性密钥 Kn-Cint。

在第二种实施方式中，如图 11B 所示，假设本实施方式的应用场景为包括切片 S1~Sn，每个切片包括 H1~Hm 个会话，则第一设备可以根据中间密钥为每个切片的每个会话生产一组用户平面密钥，每组用户平面密钥包括用户面加密性密钥 Kij-Uenc、用户面完整性密钥 Kij-Uint、其中，i 表示切片的序号，j 表示会话在切片的序号。第一设备可以根据中间密钥为生成一组控制面密钥，该组控制面密钥包括控制面加密性密钥 KCenc 以及控制面完整性密钥 KCint。该组控制面密钥用于对切片 S1~ Sn 的控制面数据进行安全性保护，即，每个切片的控制面数据使用相同的控制面密钥进行安全性保护。例如，第一设备可以根据中间密钥 Kan 为第一切片的第一会话生成用户面加密性密钥 K11-Uenc 以及用户面完整性密钥 K11-Uint，第一设备可以根据中间密钥 Kan 为第一切片的第二会话生成用户面加密性密钥 K12-Uenc 以及用户面完整性密钥 K12-Uint，依次类推，第一设备可以根据中间密钥 Kan 为第 n 切片的第 m 会话生成用户面加密性密钥 Knm-Uenc 以及用户面完整性密钥 Knm-Uint。第一设备可以根据中间密钥 Kan 为生成控制面加密性密钥 KCenc 以及控制面完整性密钥 KCint。

在第三种实施方式中，如图 11C 所示，假设本实施方式的应用场景为包括 S1~Sn 个切片，每个切片包括 H1~Hm 个会话，则第一设备可以根据中间密钥为每个切片的生产一组用户平面密钥，每组用户平面密钥包括用户面加密性密钥 Ki-Uenc、用户面完整性密钥 Ki-Uint、其中，i 表示切片的序号。每组用户平面密钥用于对对应切片的每个会话进行安全性保护，即，同一切片内的会话使用相同的用户平面密钥进行安全性保护。第一设备可以根据中间密钥为每个切片生成一组控制面密钥，每组控制面密钥包括控制面加密性密钥 Ki-Cenc 以及控制面完整性密钥 Ki-Uint，其中，i 表示切片的序号。例如，第一设备可以根据中间密钥 Kan 为第一切片生成用户面加密性密钥 K1-Uenc 以及用户面完整性密钥

K1-Uint，第一设备可以根据中间密钥 Kan 为第二切片生成用户面加密性密钥 K2-Uenc 以及用户面完整性密钥 K2-Uint，依次类推，第一设备可以根据中间密钥 Kan 为第 n 切片生成用户面加密性密钥 Kn-Uenc 以及用户面完整性密钥 Kn-Uint。第一设备可以根据中间密钥 Kan 为第一切片生成控制面加密性密钥 K1-Cenc 以及控制面完整性密钥 K1-Cint，第一设备可以根据中间密钥 Kan 为第二切片生成控制面加密性密钥 K2-Cenc 以及控制面完整性密钥 K2-Cint，依次类推，第一设备可以根据中间密钥 Kan 为第 n 切片生成控制面加密性密钥 Kn-Cenc 以及控制面完整性密钥 Kn-Cint。

在第四种实施方式中，如图 11D 所示，假设本实施方式的应用场景为包括切片 S1~ Sn，每个切片包括 H1~Hm 个会话，则第一设备可以根据中间密钥为每个切片的生成一组用户平面密钥，每组用户平面密钥包括用户面加密性密钥 Ki-Uenc、用户面完整性密钥 Ki-Uint、其中，i 表示切片的序号。每组用户平面密钥用于对对应切片的每个会话进行安全性保护，即，同一切片内的会话使用相同的用户平面密钥进行安全性保护。第一设备可以根据中间密钥为生成一组控制面密钥，该组控制面密钥包括控制面加密性密钥 KCenc 以及控制面完整性密钥 KCint。该组控制面密钥用于对切片 S1~ Sn 的控制面数据进行安全性保护，即，每个切片的控制面数据使用相同的控制面密钥进行安全性保护。例如，第一设备可以根据中间密钥 Kan 为第一切片生成用户面加密性密钥 K1-Uenc 以及用户面完整性密钥 K1-Uint，第一设备可以根据中间密钥 Kan 为第二切片生成用户面加密性密钥 K2-Uenc 以及用户面完整性密钥 K2-Uint，依次类推，第一设备可以根据中间密钥 Kan 为第 n 切片生成用户面加密性密钥 Kn-Uenc 以及用户面完整性密钥 Kn-Uint。第一设备可以根据中间密钥 Kan 为生成控制面加密性密钥 KCenc 以及控制面完整性密钥 KCint。

在第五种实施方式中，如图 11E 所示，假设本实施方式的应用场景为包括切片 S1~ Sn，每个切片包括 H1~Hm 个会话，则第一设备可以根据中间密钥为每个切片生成一个切片根密钥 Ki-root，其中，i 表示切片的序号。第一设备根据切片 i 的根密钥 Ki-root 为切片 i 中的每个会话生成一个用户面密钥 ij-root，其中，i 表示切片的序号，j 为会话在切片中的序号。第一设备再根据每个会话的用户面密钥 ij-root 为每个会话生成用户面加密性密钥 Kij-Uenc 以及用户面完整性密钥 Kij-Uint。第一设备可以根据切片根密钥 Ki-root 为每个切片生成一组控制面密钥，每组控制面密钥包括控制面加密性密钥 Ki-Cenc 以及控制面完整性密钥 Ki-Uint，其中，i 表示切片的序号。即，每个切片的每个会话的用户面控制密钥 ij-root 以及切片的控制面密钥都是根据切片的根密钥生成的。

在第六种实施方式中，如图 11F 所示，本实施例主要是用来补充描述多切片、多会话（切片内）场景下的密钥生成方法及流程。本实施例的核心思想是由 K_SEAF 推衍生成不同切片的会话根密钥，并进一步推衍对应于加密终结点在 UP-GW 的会话密钥，生成的密钥架构如下图所示。其中，“sn”用来标识第 n 个切片，“UP-GWm”用来标识切片中的第 m 个会话。为了简单起见，假设每个切片有同样个数的（m 个）会话。实际当中，不同切片可以有不同数量的会话。

参照图 12 所示，图 11F 的密钥生成与分发的具体步骤如下所述：

801、UE 和核心网（如，认证网元（SEAF）和/或切片认证网元）进行双向认证，并生

成根密钥 K_SEAF。核心网为 UE 确定切片，切片的 ID 可以表示为 Slc-ID1…Slc-IDN。

802、在会话建立过程，核心网内通过会话安全策略的协商，确定需要生成终结点在 UP-GW 的用户面密钥。

803、核心网（如 SEAF）生成每个切片的根密钥 K_UP-s1… K_UP-sn，并分别发送给各个切片（只发送每个切片所对应的密钥，如发送 K_UP-sn 给切片 n）。基于切片根密钥，每个切片推衍所有会话密钥（如：第 n 个切片的 m 个会话密钥为 KUP-Sn-GWm(-enc, -int)，“enc”代表加解密密密钥，“int”代表完整性保护密钥）。加解密和完整性保护密钥的生成函数分别为 KDF(UP-GW-enc-alg, Bearerm, SliceIDn…) 和 KDF(UP-GW-int-alg, Bearerm, SliceIDn…)。其中 KDF 代表密钥生成函数，Bearerm 和 SliceIDn 分别为承载 ID 和切片 ID 作为 KDF 的输入。其他输入包括 UP-GW-enc-alg 和 UP-GW-int-alg，分别代表加密和完保所使用的算法。

804、每个切片给 UP-GW 发送生成的密钥。

805、 UP-GW 收到后应答。

806、每个切片把密钥生成所需输入参数发送给 CCNF（AMF）。

807、AMF 将上述参数通过 SSMC 经过 AN 发送给 UE。

808、UE 根据收到的参数，生成所有密钥（类似第 803 步骤的生成方法）。

参照图 13 所示，图 13 为本申请实施例中所提供的总体密钥架构示意图，其中，核心网控制面密钥架构部分如图 9 实施例所示，核心网用户面密钥架构部分如图 11F 实施例所示，接入网密钥架构部分如图 11A 至图 11E 实施例所示，此处不做赘述。

可以理解的是，为了陈述简便，上述例子中是以每个切片具有的会话的数量相等来进行描述的，在实际应用中，每个切片具有的会话的数量可以均不相等，或者，至少两个切片具有的会话数量相等，本申请不作具体的限定。

在本申请所提供的几个实施例中，应该理解到，所揭露的系统，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，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

所述集成的单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的全部或部分可以以软件产品的形式体现出

来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（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。

在上述实施例中，可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时，可以全部或部分地以计算机程序产品的形式实现。

所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时，全部或部分地产生按照本发明实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中，或者从一个计算机可读存储介质向另一计算机可读存储介质传输，例如，所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线（例如同轴电缆、光纤、数字用户线（DSL））或无线（例如红外、无线、微波等）方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存储的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。所述可用介质可以是磁性介质，（例如，软盘、硬盘、磁带）、光介质（例如，DVD）、或者半导体介质（例如固态硬盘 Solid State Disk(SSD)）等。

权 利 要 求

1、一种网络密钥处理的系统，其特征在于，包括：用户设备、安全锚点网元、接入及移动管理网元，其中：

所述安全锚点网元用于从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片，并根据所述第一密钥参数生成 N 个切片专用密钥；

所述安全锚点网元还用于将所述 N 个切片专用密钥分别发送给相对应的所述 N 个网络切片；

所述接入及移动管理网元用于从所述切片选择网元或者所述安全锚点网元获取所述第一密钥参数，并将所述第一密钥参数发送给所述用户设备；

所述用户设备用于根据所述第一密钥参数生成所述 N 个网络切片的 N 个切片专用密钥，并根据所生成的所述 N 个切片专用密钥访问所述 N 个网络切片。

2、根据权利要求 1 所述的系统，其特征在于，所述安全锚点网元还用于根据第二密钥参数为所述接入及移动管理网元生成共享密钥，并将所述第二密钥参数发送给所述接入及移动管理网元，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述接入及移动管理网元还用于接收所述安全锚点网元发送的所述第二密钥参数；

所述用户设备还用于从所述接入及移动管理网元接收到所述第二密钥参数后，并生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

3、根据权利要求 2 所述的系统，其特征在于，所述接入及移动管理网元还用于：

在将所述第一密钥参数发送给所述用户设备之前，通过所述共享密钥为所述第一密钥参数进行加密；

所述接入及移动管理网元具体用于：

所述接入及移动管理网元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备；

所述用户设备具体用于接收所述接入及移动管理网元通过切片安全模式命令发送的进行加密后的所述第一密钥参数。

4、根据权利要求 1 至 3 其中任意一项所述的系统，其特征在于，所述系统还包括网络切片，其中：

所述网络切片用于接收所述安全锚点网元发送的专用密钥；

所述网络切片还用于根据加密参数对 M 个网络功能进行加密，所述加密参数包括所述专用密钥以及所述 M 个网络功能的功能标识；

所述网络切片还用于将所述加密参数发送给所述接入及移动管理网元；

所述接入及移动管理网元还用于将所述加密参数发送给用户设备；

所述用户设备还用于接收所述加密参数，并能够根据所述加密参数访问所述网络切片的所述 M 个网络功能。

5、一种安全锚点网元，其特征在于，所述网元包括：

获取单元，用于从切片选择网元获取第一密钥参数，所述第一密钥参数包括 N 个网络

切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；

生成单元，用于根据所述第一密钥参数生成 N 个专用密钥；

发送单元，用于将所述 N 个切片专用密钥分别发送给相对应的所述 N 个网络切片，以使得用户设备从接入及移动管理网元接收到所述第一密钥参数后，生成相同的所述 N 个切片专用密钥从而能够访问所述 N 个网络切片。

6、根据权利要求 5 所述的网元，其特征在于，所述发送单元还用于：

将所述第一密钥参数发送给接入及移动管理网元，用于所述接入及移动管理网元发送所述第一密钥参数至用户设备。

7、根据权利要求 5 或 6 所述的网元，其特征在于，所述生成单元还用于：

根据第二密钥参数为所述接入及移动管理网元生成共享密钥，并将所述第二密钥参数发送给所述接入及移动管理网元，所述共享密钥用于所述 N 个网络切片的共享网络功能使用，以使得所述用户设备从所述接入及移动管理网元接收到所述第二密钥参数后，生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

8、一种接入及移动管理网元，其特征在于，所述网元包括：

获取单元，用于从切片选择网元或者安全锚点网元获取所述第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述 N 个切片专用密钥发送给相对应的所述 N 个网络切片；

发送单元，用于将所述第一密钥参数发送给所述用户设备，以使得所述用户设备根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访问所述 N 个网络切片。

9、根据权利要求 8 所述的网元，其特征在于，所述发送单元具体用于：

通过切片安全模式命令将所述第一密钥参数发送给所述用户设备。

10、根据权利要求 9 所述的网元，其特征在于，所述网元还包括：

接收单元，用于接收所述安全锚点网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述发送单元还用于，将所述第二密钥参数发送给所述用户设备，以使得所述用户设备根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

11、根据权利要求 10 所述的网元，其特征在于，所述发送单元具体还用于：

通过所述切片安全模式命令将所述第二密钥参数发送给所述用户设备。

12、根据权利要求 11 所述的网元，其特征在于，所述网元还包括：

加密单元，在所述发送单元通过切片安全模式命令将所述第一密钥参数发送给所述用户设备之前，用于所述接入及移动管理网元通过所述共享密钥为所述第一密钥参数进行加密；

所述发送单元具体还用于：

通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备。

13、根据权利要求 12 所述的网元，其特征在于，所述所述接收单元还用于：

在所述发送单元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备之前，接收所述 N 个网络切片发送的加密参数，所述加密参数为所述N个网络切片中每个网络切片为 M 个网络功能进行加密所使用的参数；

所述发送单元还用于：

通过切片安全模式命令将将进行加密后的所述第一密钥参数以及所述加密参数发送给所述用户设备，以使得所述用户设备根据所述加密参数访问所述 N 个网络切片的所述 M 个网络功能。

14、一种网络切片，其特征在于，所述网络切片包括：

接收单元，用于接收安全锚点网元发送的专用密钥；

加密单元，用于根据加密参数对 M 个网络功能进行加密，所述加密参数包括所述专用密钥以及所述 M 个网络功能的功能标识；

发送单元，用于将所述加密参数发送给接入及移动管理网元，以使得所述接入及移动管理网元将所述加密参数发送给用户设备，使得所述用户设备根据所述加密参数访问所述网络切片的所述 M 个网络功能。

15、一种用户设备，其特征在于，所述用户设备包括：

接收单元，用于接收所述接入及移动管理网元发送的第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述 N 个切片专用密钥发送给相对应的所述 N 个网络切片；

生成单元，用于根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访问所述 N 个网络切片。

16、根据权利要求 15 所述的用户设备，其特征在于，所述接收单元具体用于：

接收所述接入及移动管理网元通过切片安全模式命令发送的所述第一密钥参数。

17、根据权利要求 16 所述的用户设备，其特征在于，所述接收单元还用于：

接收所述接入及移动管理网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述生成单元还用于，用于根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

18、根据权利要求 17 所述的用户设备，其特征在于，所述接收单元具体还用于：

接收所述接入及移动管理网元通过所述切片安全模式命令发送的所述第二密钥参数。

19、根据权利要求 18 所述的用户设备，其特征在于，所述接收单元具体还用于：

接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数。

20、根据权利要求 19 所述的用户设备，其特征在于，所述接收单元具体还用于：

接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数以及加密参数，所述加密参数为所述N个网络切片中每个网络切片为M个网络功能进行加密所使用的参数；

所述用户设备还包括：

访问单元，用于根据所述加密参数访问所述N个网络切片的所述M个网络功能。

21、一种网络密钥处理的方法，应用于安全锚点网元侧，其特征在于，所述方法包括：

安全锚点网元从切片选择网元获取第一密钥参数，所述第一密钥参数包括N个网络切片的标识信息，所述N个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；

所述安全锚点网元根据所述第一密钥参数生成N个专用密钥；

所述安全锚点网元将所述N个切片专用密钥分别发送给相对应的所述N个网络切片，以使得用户设备从接入及移动管理网元接收到所述第一密钥参数后，生成相同的所述N个切片专用密钥从而能够访问所述N个网络切片。

22、根据权利要求21所述的方法，其特征在于，所述方法还包括：

所述安全锚点网元将所述第一密钥参数发送给接入及移动管理网元，用于所述接入及移动管理网元发送所述第一密钥参数至用户设备。

23、根据权利要求21或22所述的方法，其特征在于，所述方法还包括：

所述安全锚点网元根据第二密钥参数为所述接入及移动管理网元生成共享密钥，并将所述第二密钥参数发送给所述接入及移动管理网元，所述共享密钥用于所述N个网络切片的共享网络功能使用，以使得所述用户设备从所述接入及移动管理网元接收到所述第二密钥参数后，生成相同的所述共享密钥从而能够访问所述N个网络切片的共享网络功能。

24、一种网络密钥处理的方法，应用于接入及移动管理网元侧，其特征在于，所述方法包括：

接入及移动管理网元从切片选择网元或者安全锚点网元获取所述第一密钥参数，所述第一密钥参数包括N个网络切片的标识信息，所述N个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成N个切片专用密钥，并将所述N个切片专用密钥发送给相对应的所述N个网络切片；

所述接入及移动管理网元将所述第一密钥参数发送给所述用户设备，以使得所述用户设备根据所述第一密钥参数生成相同的所述N个切片专用密钥，从而能够访问所述N个网络切片。

25、根据权利要求24所述的方法，其特征在于，所述接入及移动管理网元将所述第一密钥参数发送给所述用户设备，包括：

所述接入及移动管理网元通过切片安全模式命令将所述第一密钥参数发送给所述用户设备。

26、根据权利要求25所述的方法，其特征在于，所述方法还包括：

所述接入及移动管理网元接收所述安全锚点网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述N个网络切片的共享网络功能使用；

所述接入及移动管理网元将所述第二密钥参数发送给所述用户设备，以使得所述用户设备根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

27、根据权利要求 26 所述的方法，其特征在于，所述接入及移动管理网元将所述第二密钥参数发送给所述用户设备，包括：

所述接入及移动管理网元通过所述切片安全模式命令将所述第二密钥参数发送给所述用户设备。

28、根据权利要求 27 所述的方法，其特征在于，在所述接入及移动管理网元通过切片安全模式命令将所述第一密钥参数发送给所述用户设备之前，所述方法还包括：

所述接入及移动管理网元通过所述共享密钥为所述第一密钥参数进行加密；

所述接入及移动管理网元通过切片安全模式命令将所述第一密钥参数发送给所述用户设备，包括：

所述接入及移动管理网元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备。

29、根据权利要求 28 所述的方法，其特征在于，在所述接入及移动管理网元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备之前，所述方法还包括：

接收所述 N 个网络切片发送的加密参数，所述加密参数为所述N个网络切片中每个网络切片为 M 个网络功能进行加密所使用的参数；

所述接入及移动管理网元通过切片安全模式命令将进行加密后的所述第一密钥参数发送给所述用户设备，包括：

所述接入及移动管理网元通过切片安全模式命令将将进行加密后的所述第一密钥参数以及所述加密参数发送给所述用户设备，以使得所述用户设备根据所述加密参数访问所述N个网络切片的所述 M 个网络功能。

30、一种网络密钥处理的方法，应用于网络切片侧，其特征在于，所述方法包括：

所述网络切片接收安全锚点网元发送的专用密钥；

所述网络切片根据加密参数对 M 个网络功能进行加密，所述加密参数包括所述专用密钥以及所述 M 个网络功能的功能标识；

所述网络切片将所述加密参数发送给接入及移动管理网元，以使得所述接入及移动管理网元将所述加密参数发送给用户设备，使得所述用户设备根据所述加密参数访问所述网络切片的所述 M 个网络功能。

31、一种网络密钥处理的方法，应用于用户设备侧，其特征在于，所述方法包括：

所述用户设备接收所述接入及移动管理网元发送的第一密钥参数，所述第一密钥参数包括 N 个网络切片的标识信息，所述 N 个网络切片为所述切片选择网元为所述用户设备所确定的网络切片；所述第一密钥参数用于安全锚点网元生成 N 个切片专用密钥，并将所述N个切片专用密钥发送给相对应的所述 N 个网络切片；

所述用户设备根据所述第一密钥参数生成相同的所述 N 个切片专用密钥，从而能够访

问所述 N 个网络切片。

32、根据权利要求 31 所述的方法，其特征在于，所述用户设备接收所述接入及移动管理网元发送的第一密钥参数，包括：

所述用户设备接收所述接入及移动管理网元通过切片安全模式命令发送的所述第一密钥参数。

33、根据权利要求 32 所述的方法，其特征在于，所述方法还包括：

所述用户设备接收所述接入及移动管理网元发送的第二密钥参数，所述第二密钥参数用于所述安全锚点网元为所述接入及移动管理网元生成共享密钥，所述共享密钥用于所述 N 个网络切片的共享网络功能使用；

所述用户设备根据所述第二密钥参数生成相同的所述共享密钥从而能够访问所述 N 个网络切片的共享网络功能。

34、根据权利要求 33 所述的方法，其特征在于，所述用户设备接收所述接入及移动管理网元发送的第二密钥参数，包括：

所述用户设备接收所述接入及移动管理网元通过所述切片安全模式命令发送的所述第二密钥参数。

35、根据权利要求 34 所述的方法，其特征在于，所述用户设备接收所述接入及移动管理网元通过所述切片安全模式命令发送的所述第二密钥参数，包括：

所述用户设备接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数。

36、根据权利要求 35 所述的方法，其特征在于，所述用户设备接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数，包括：

所述用户设备接收所述接入及移动管理网元通过切片安全模式命令发送的根据所述共享密钥进行加密后的所述第一密钥参数以及加密参数，所述加密参数为所述 N 个网络切片中每个网络切片为 M 个网络功能进行加密所使用的参数；

所述用户设备根据所述加密参数访问所述 N 个网络切片的所述 M 个网络功能。

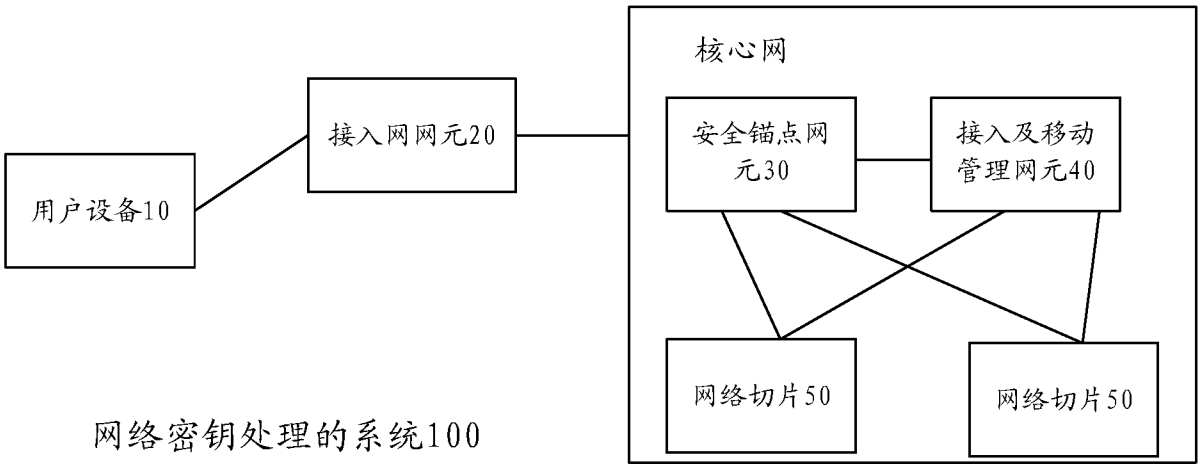
核心网
接入网网元20
用户设备10
安全锚点网元30
接入及移动管理网元40
网络切片50
网络切片50
网络密钥处理的系统100

图 1

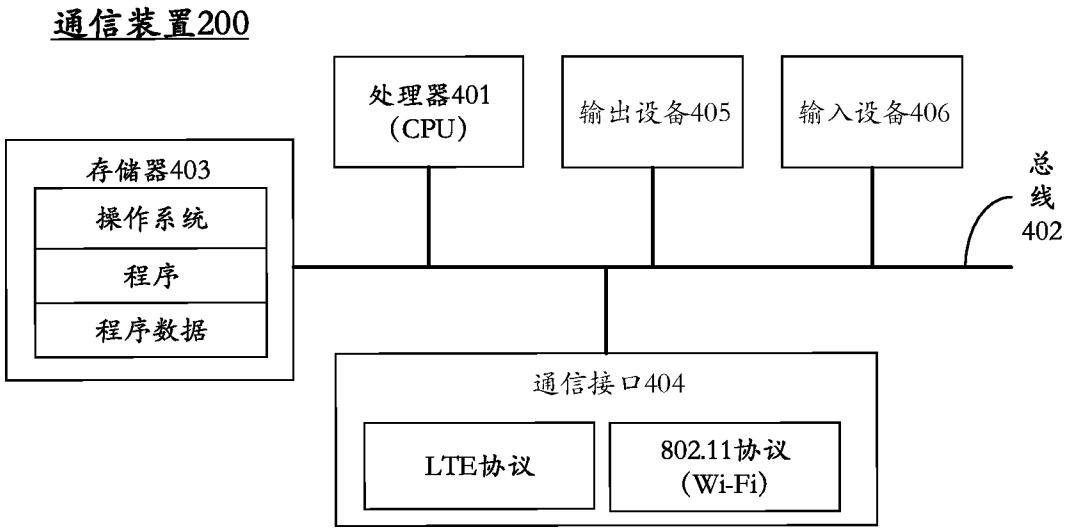
通信装置200
处理器401 (CPU)
输出设备405
输入设备406
总线402
存储器403
操作系统
程序
程序数据
通信接口404
LTE协议
802.11协议 (Wi-Fi)

图 2

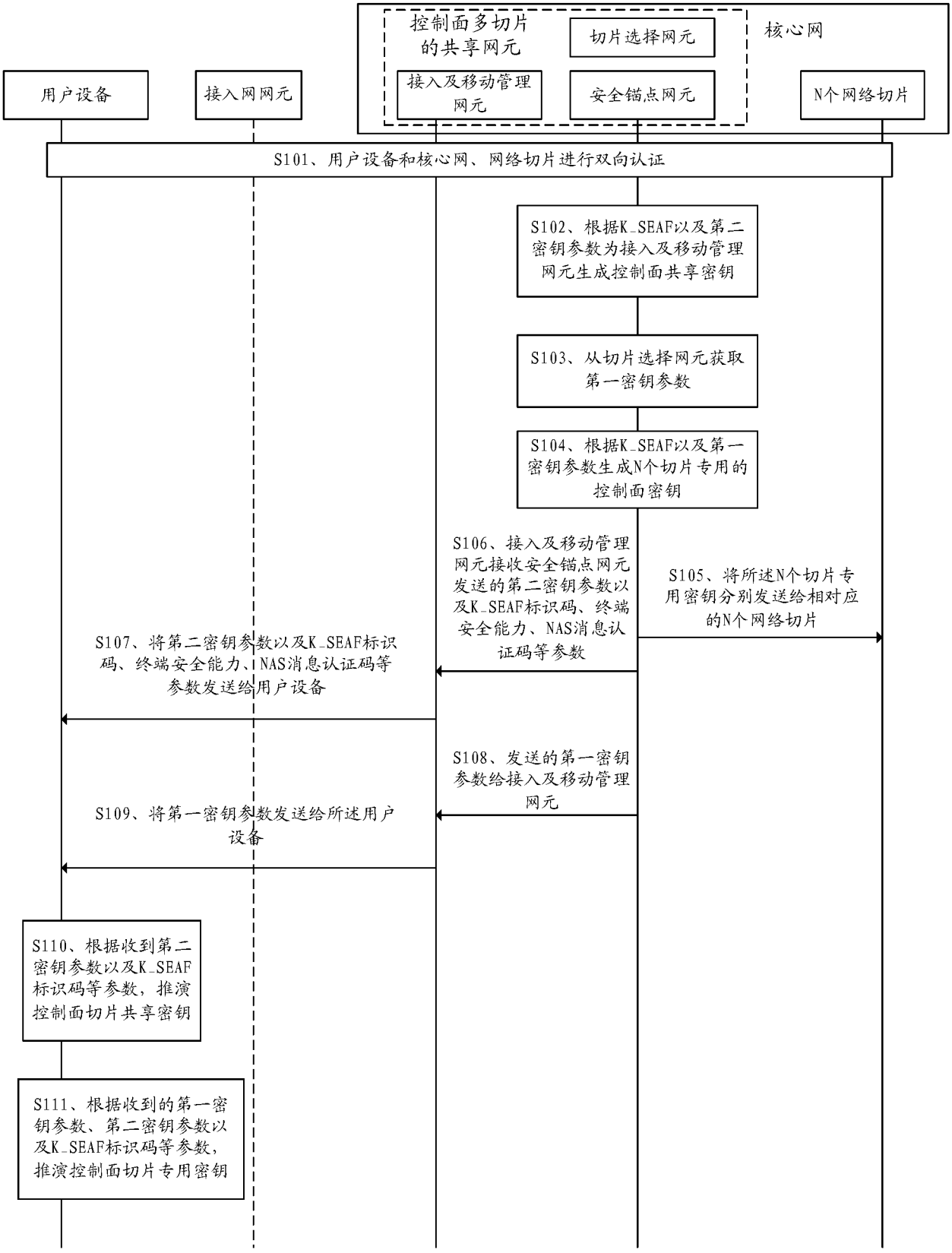
控制面多切片的共享网元
切片选择网元
核心网
用户设备
接入网网元
接入及移动管理网元
安全锚点网元
N个网络切片
S101、用户设备和核心网、网络切片进行双向认证
S102、根据K_SEAF以及第二密钥参数为接入及移动管理网元生成控制面共享密钥
S103、从切片选择网元获取第一密钥参数
S104、根据K_SEAF以及第一密钥参数生成N个切片专用的控制面密钥
S106、接入及移动管理网元接收安全锚点网元发送的第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数
S105、将所述N个切片专用密钥分别发送给相对应的N个网络切片
S107、将第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数发送给用户设备
S108、发送的第一密钥参数给接入及移动管理网元
S109、将第一密钥参数发送给所述用户设备
S110、根据收到第二密钥参数以及K_SEAF标识码等参数，推演控制面切片共享密钥
S111、根据收到的第一密钥参数、第二密钥参数以及K_SEAF标识码等参数，推演控制面切片专用密钥

图 3

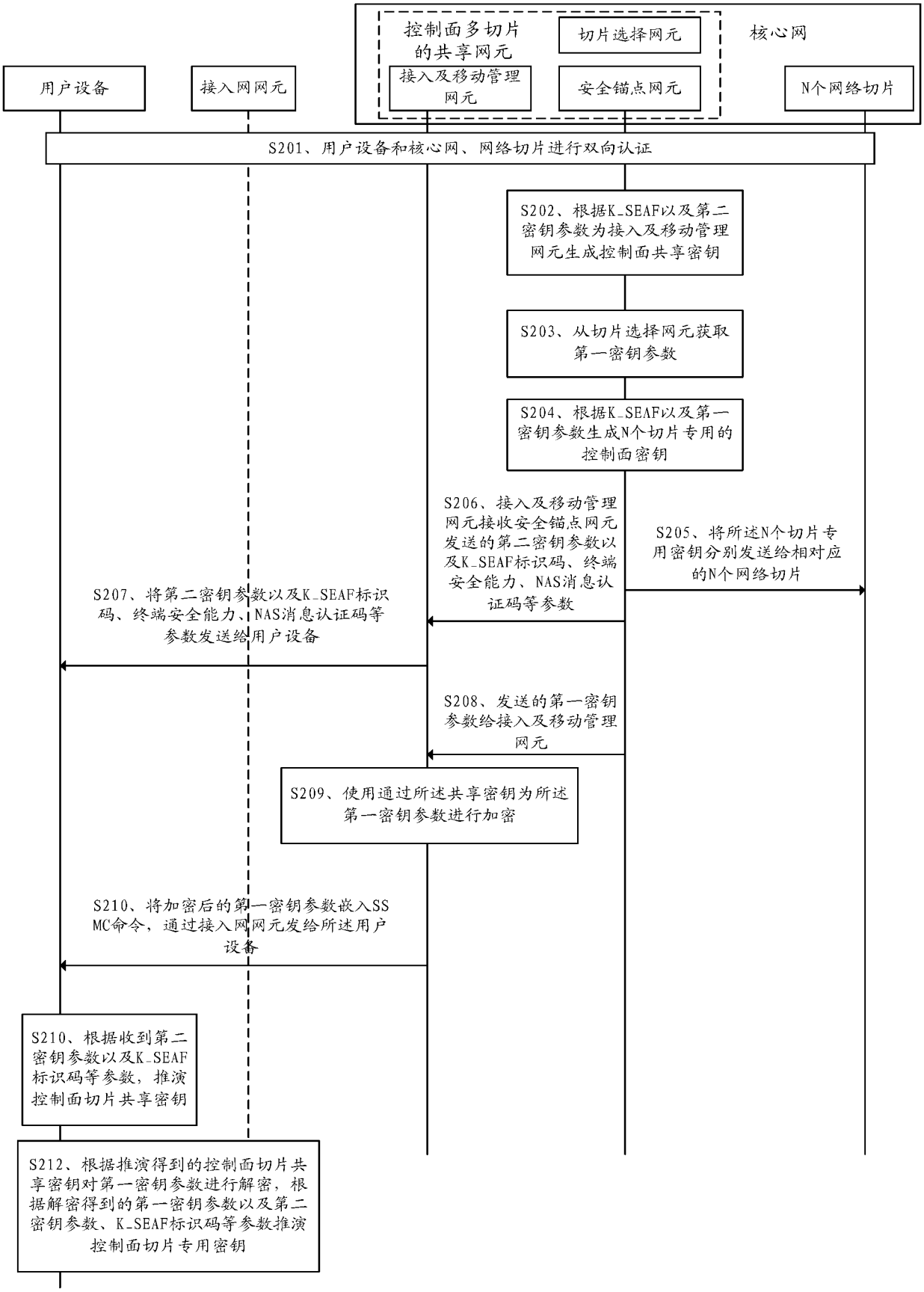
控制面多切片的共享网元
切片选择网元
核心网
接入及移动管理网元
安全锚点网元
N个网络切片
用户设备
接入网网元
S201、用户设备和核心网、网络切片进行双向认证
S202、根据K_SEAF以及第二密钥参数为接入及移动管理网元生成控制面共享密钥
S203、从切片选择网元获取第一密钥参数
S204、根据K_SEAF以及第一密钥参数生成N个切片专用的控制面密钥
S206、接入及移动管理网元接收安全锚点网元发送的第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数
S205、将所述N个切片专用密钥分别发送给相对应的N个网络切片
S207、将第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数发送给用户设备
S208、发送的第一密钥参数给接入及移动管理网元
S209、使用通过所述共享密钥为所述第一密钥参数进行加密
S210、将加密后的第一密钥参数嵌入SSMC命令，通过接入网网元发给所述用户设备
S210、根据收到第二密钥参数以及K_SEAF标识码等参数，推演控制面切片共享密钥
S212、根据推演得到的控制面切片共享密钥对第一密钥参数进行解密，根据解密得到的第一密钥参数以及第二密钥参数、K_SEAF标识码等参数推演控制面切片专用密钥

图 4

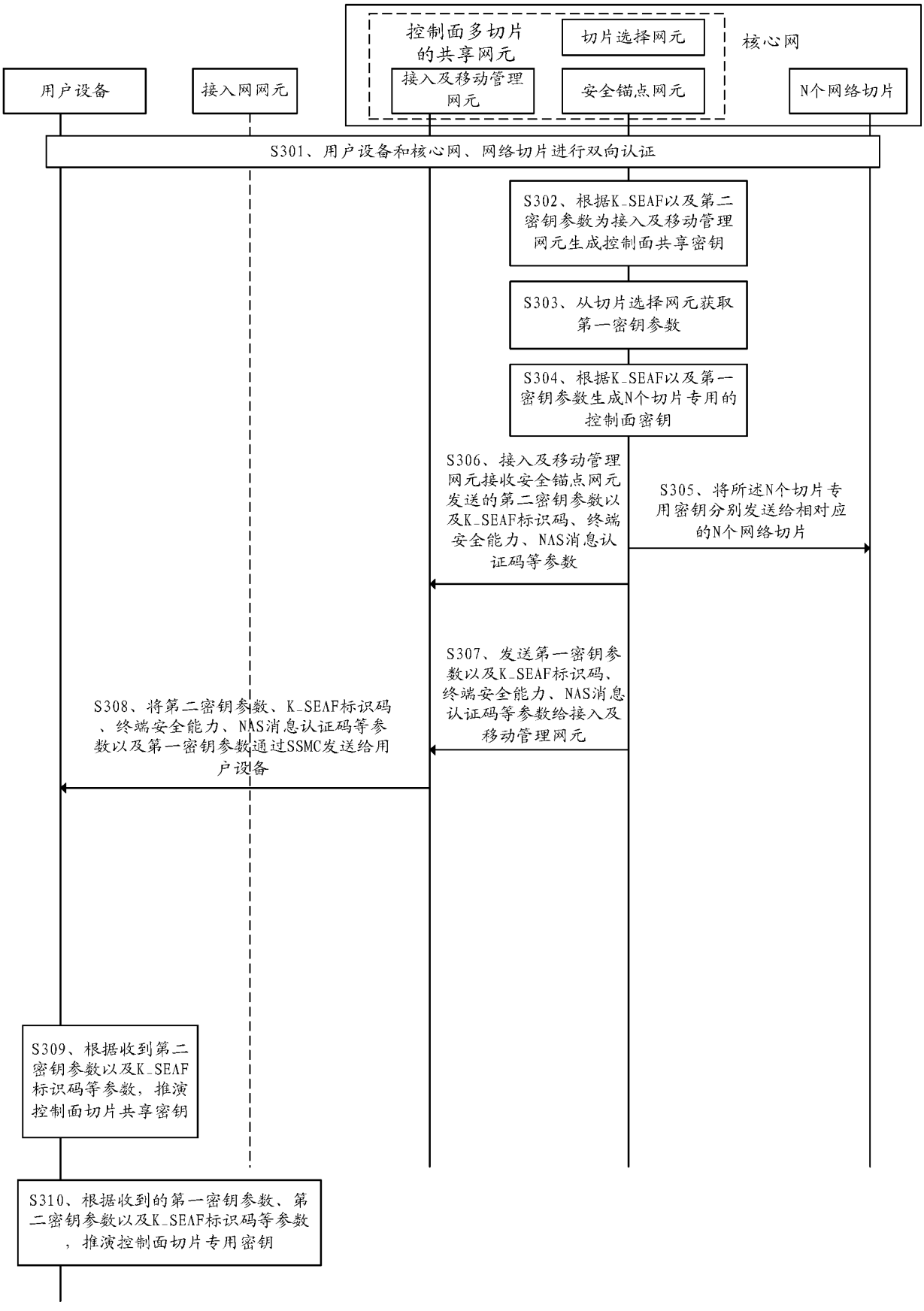
控制面多切片的共享网元
切片选择网元
核心网
接入及移动管理网元
安全锚点网元
N个网络切片
用户设备
接入网网元
S301、用户设备和核心网、网络切片进行双向认证
S302、根据K_SEAF以及第二密钥参数为接入及移动管理网元生成控制面共享密钥
S303、从切片选择网元获取第一密钥参数
S304、根据K_SEAF以及第一密钥参数生成N个切片专用的控制面密钥
S306、接入及移动管理网元接收安全锚点网元发送的第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数
S305、将所述N个切片专用密钥分别发送给相对应的N个网络切片
S307、发送第一密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数给接入及移动管理网元
S308、将第二密钥参数、K_SEAF标识码、终端安全能力、NAS消息认证码等参数以及第一密钥参数通过SSMC发送给用户设备
S309、根据收到第二密钥参数以及K_SEAF标识码等参数，推演控制面切片共享密钥
S310、根据收到的第一密钥参数、第二密钥参数以及K_SEAF标识码等参数，推演控制面切片专用密钥

图 5

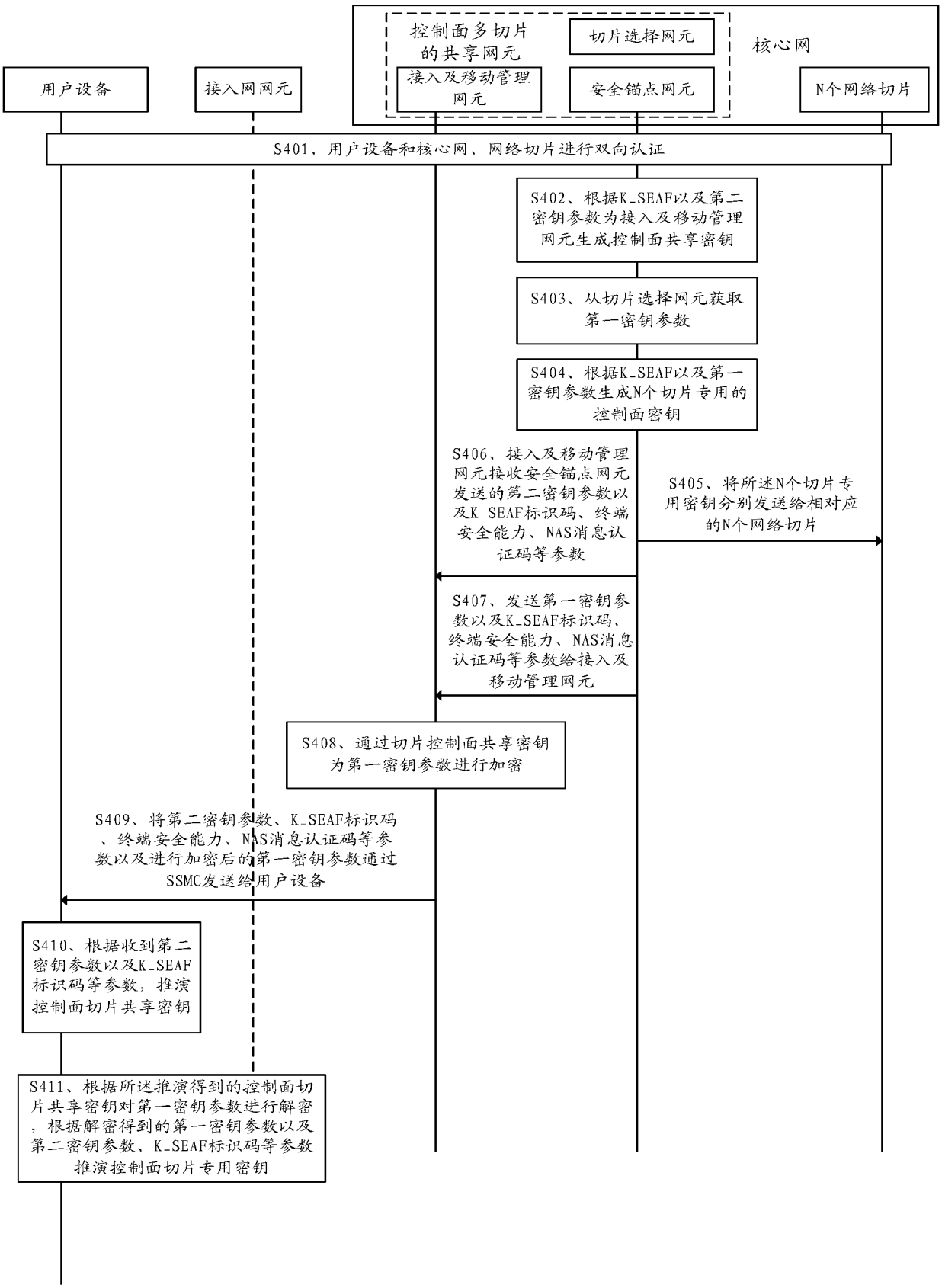
控制面多切片的共享网元
切片选择网元
核心网
接入及移动管理网元
安全锚点网元
N个网络切片
用户设备
接入网网元
S401、用户设备和核心网、网络切片进行双向认证
S402、根据K_SEAF以及第二密钥参数为接入及移动管理网元生成控制面共享密钥
S403、从切片选择网元获取第一密钥参数
S404、根据K_SEAF以及第一密钥参数生成N个切片专用的控制面密钥
S406、接入及移动管理网元接收安全锚点网元发送的第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数
S405、将所述N个切片专用密钥分别发送给相对应的N个网络切片
S407、发送第一密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数给接入及移动管理网元
S408、通过切片控制面共享密钥为第一密钥参数进行加密
S409、将第二密钥参数、K_SEAF标识码、终端安全能力、NAS消息认证码等参数以及进行加密后的第一密钥参数通过SSMC发送给用户设备
S410、根据收到第二密钥参数以及K_SEAF标识码等参数，推演控制面切片共享密钥
S411、根据所述推演得到的控制面切片共享密钥对第一密钥参数进行解密，根据解密得到的第一密钥参数以及第二密钥参数、K_SEAF标识码等参数推演控制面切片专用密钥

图 6

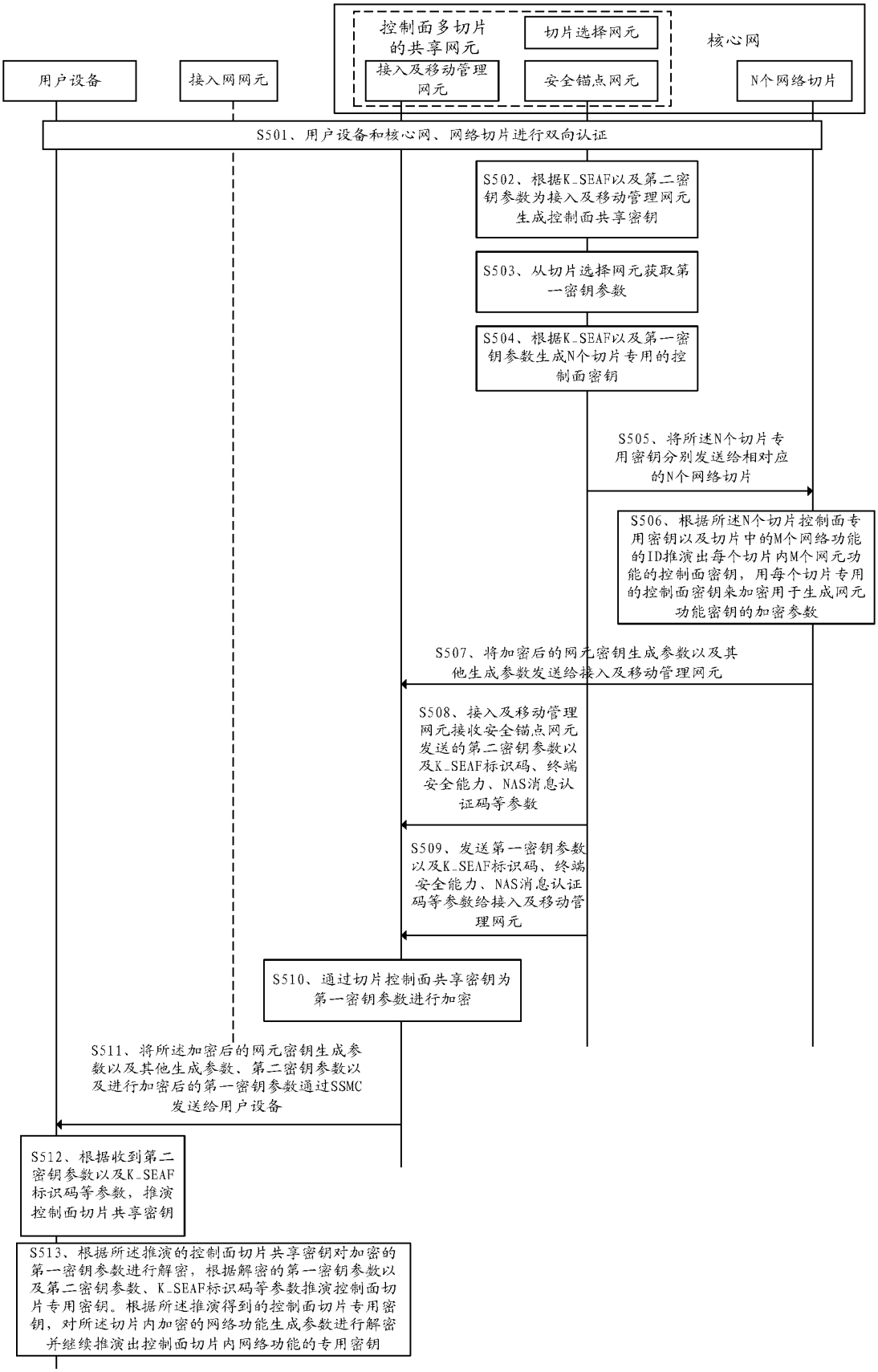
控制面多切片的共享网元
切片选择网元
核心网
接入及移动管理网元
安全锚点网元
N个网络切片
用户设备
接入网网元
S501、用户设备和核心网、网络切片进行双向认证
S502、根据K_SEAF以及第二密钥参数为接入及移动管理网元生成控制面共享密钥
S503、从切片选择网元获取第一密钥参数
S504、根据K_SEAF以及第一密钥参数生成N个切片专用的控制面密钥
S505、将所述N个切片专用密钥分别发送给相对应的N个网络切片
S506、根据所述N个切片控制面专用密钥以及切片中的M个网络功能的ID推演出每个切片内M个网元功能的控制面密钥，用每个切片专用的控制面密钥来加密用于生成网元功能密钥的加密参数
S507、将加密后的网元密钥生成参数以及其他生成参数发送给接入及移动管理网元
S508、接入及移动管理网元接收安全锚点网元发送的第二密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数
S509、发送第一密钥参数以及K_SEAF标识码、终端安全能力、NAS消息认证码等参数给接入及移动管理网元
S510、通过切片控制面共享密钥为第一密钥参数进行加密
S511、将所述加密后的网元密钥生成参数以及其他生成参数、第二密钥参数以及进行加密后的第一密钥参数通过SSMC发送给用户设备
S512、根据收到第二密钥参数以及K_SEAF标识码等参数，推演控制面切片共享密钥
S513、根据所述推演的控制面切片共享密钥对加密的第一密钥参数进行解密，根据解密的第一密钥参数以及第二密钥参数、K_SEAF标识码等参数推演控制面切片专用密钥。根据所述推演得到的控制面切片专用密钥，对所述切片内加密的网络功能生成参数进行解密并继续推演出控制面切片内网络功能的专用密钥

图 7

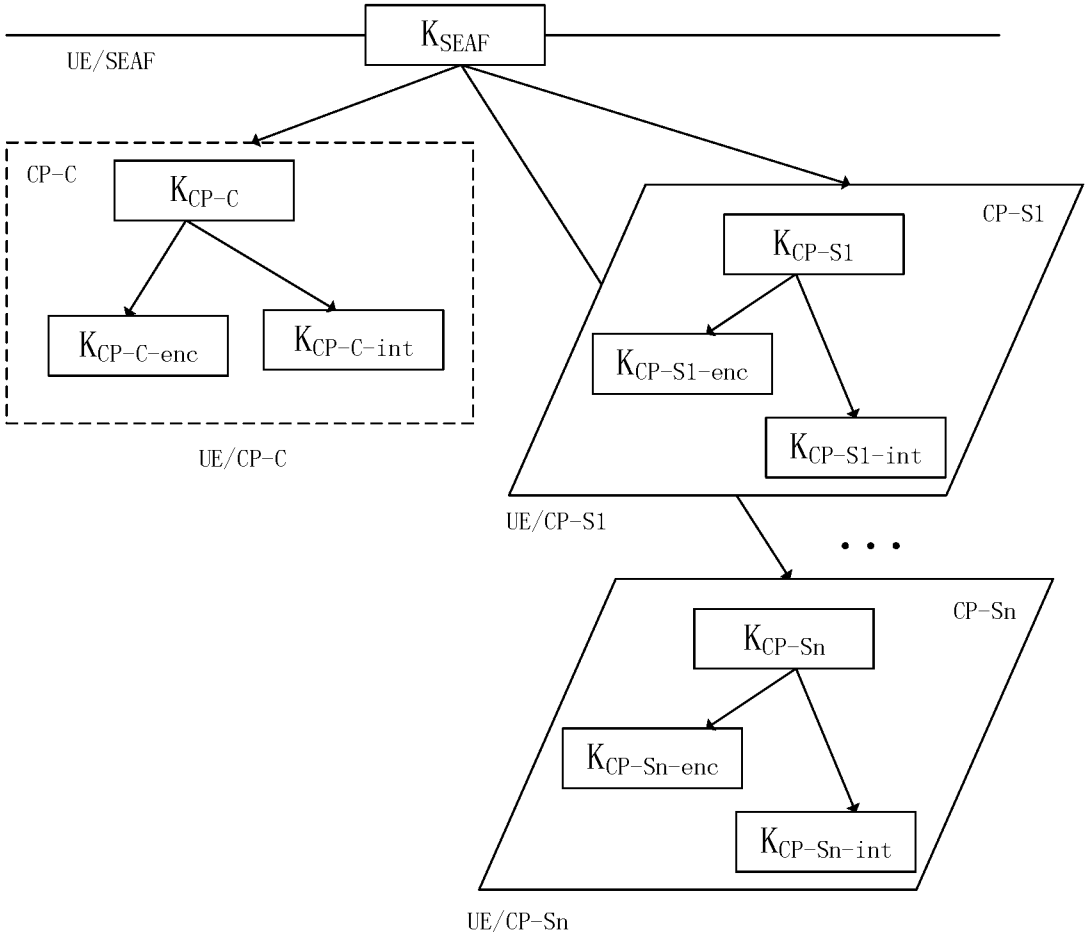
K_SEAF
UE/SEAF
CP-C
K_CP-C
K_CP-C-enc
K_CP-C-int
UE/CP-C
CP-S1
K_CP-S1
K_CP-S1-enc
K_CP-S1-int
UE/CP-S1
CP-Sn
K_CP-Sn
K_CP-Sn-enc
K_CP-Sn-int
UE/CP-Sn

图 8

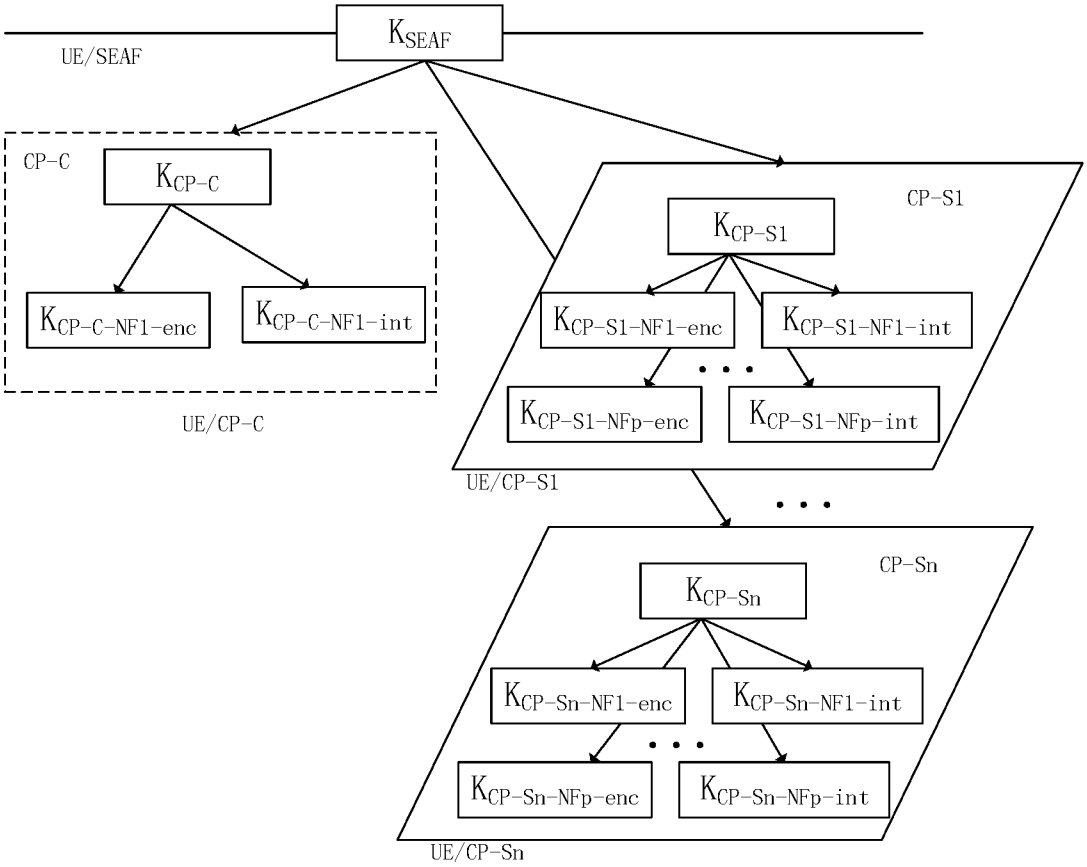
K_SEAF
UE/SEAF
CP-C
K_CP-C
K_CP-C-NF1-enc
K_CP-C-NF1-int
UE/CP-C
CP-S1
K_CP-S1
K_CP-S1-NF1-enc
K_CP-S1-NF1-int
K_CP-S1-NFp-enc
K_CP-S1-NFp-int
UE/CP-S1
CP-Sn
K_CP-Sn
K_CP-Sn-NF1-enc
K_CP-Sn-NF1-int
K_CP-Sn-NFp-enc
K_CP-Sn-NFp-int
UE/CP-Sn

图 9

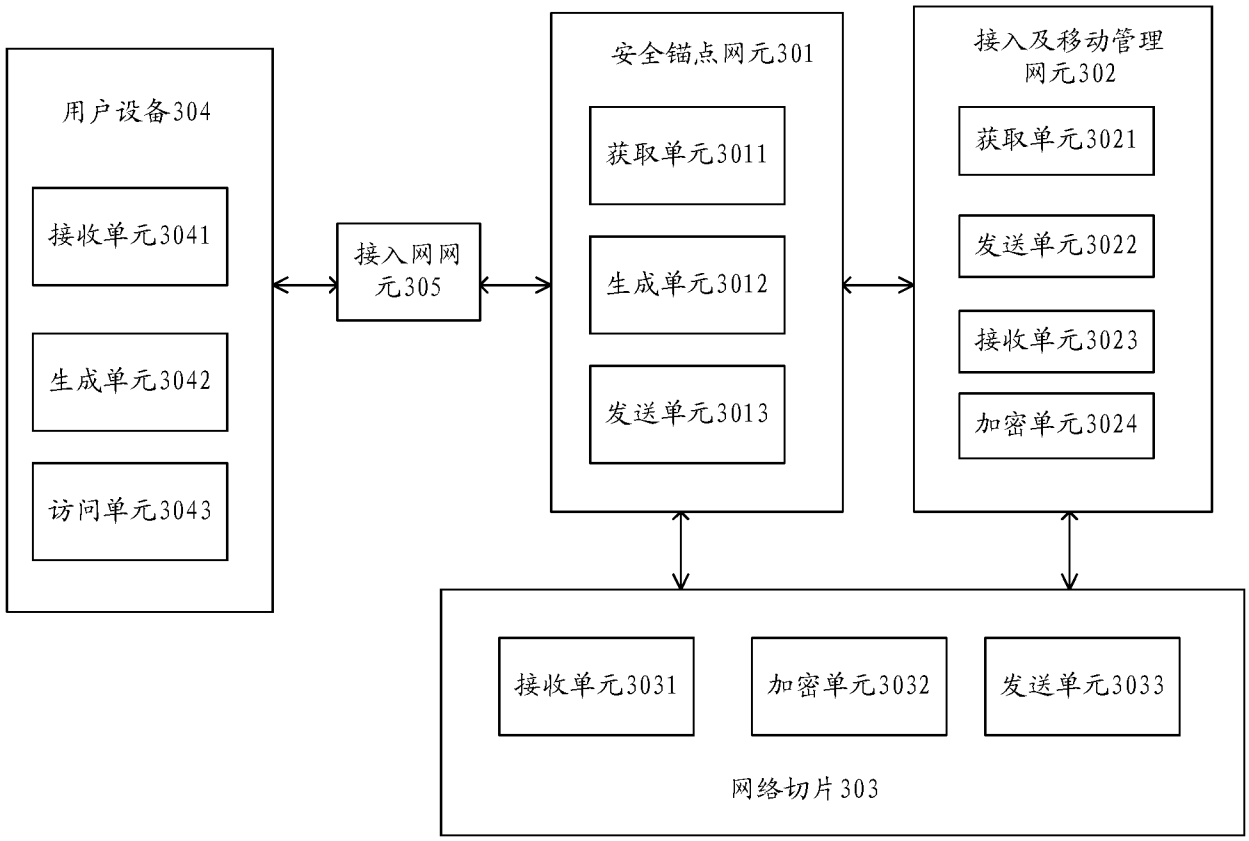
用户设备304
接收单元3041
生成单元3042
访问单元3043
接入网网元305
安全锚点网元301
获取单元3011
生成单元3012
发送单元3013
接入及移动管理网元302
获取单元3021
发送单元3022
接收单元3023
加密单元3024
接收单元3031
加密单元3032
发送单元3033
网络切片303

图 10

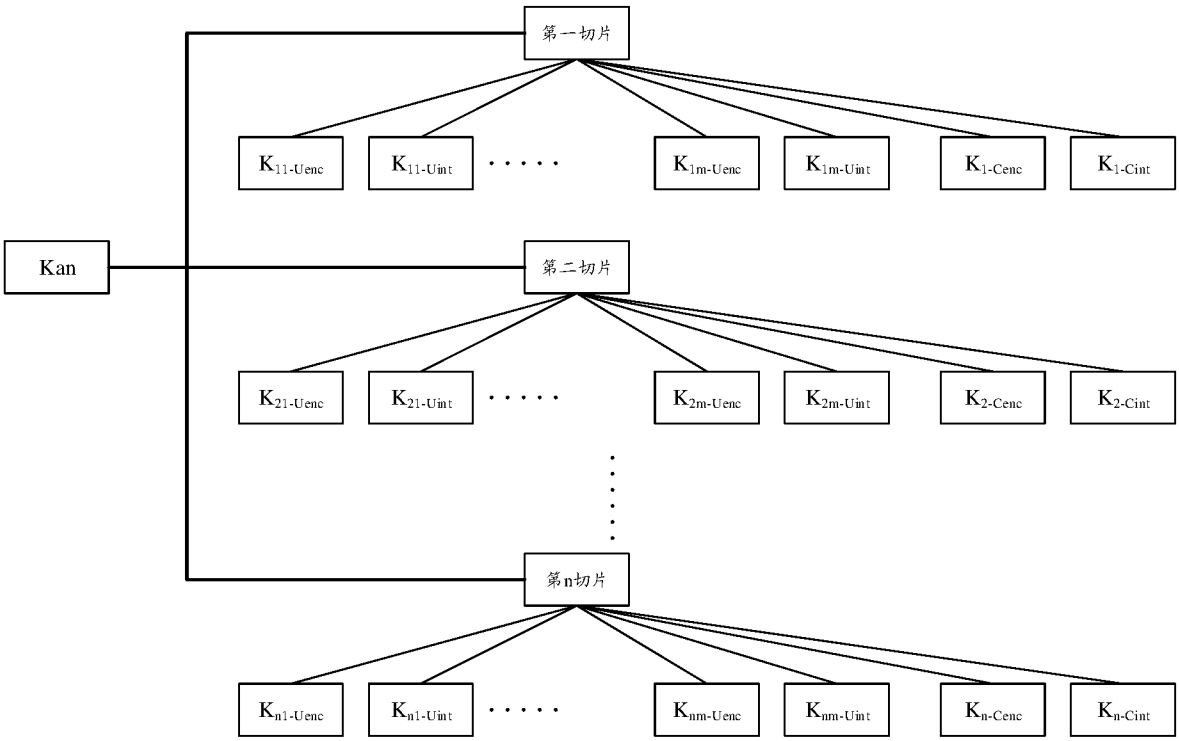
Kan
第一切片
K11-Uenc
K11-Uint
K1m-Uenc
K1m-Uint
K1-Cenc
K1-Cint
第二切片
K21-Uenc
K21-Uint
K2m-Uenc
K2m-Uint
K2-Cenc
K2-Cint
第n切片
Kn1-Uenc
Kn1-Uint
Knm-Uenc
Knm-Uint
Kn-Cenc
Kn-Cint

图 11A

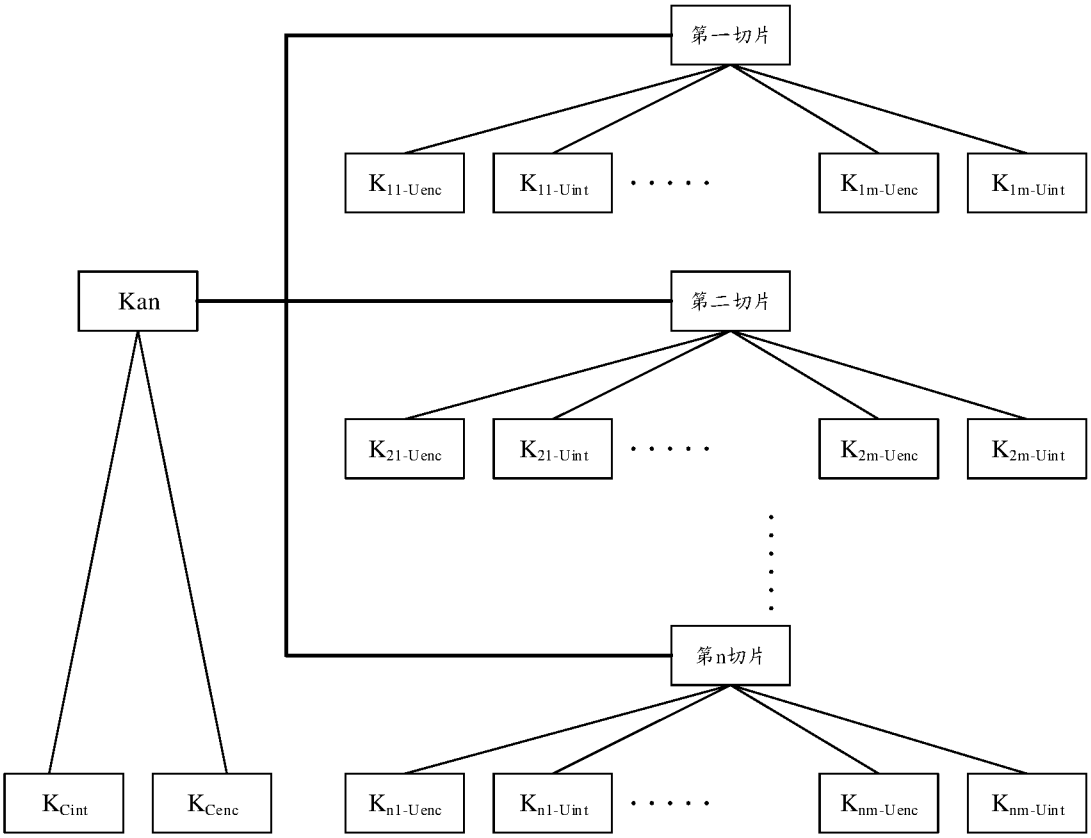
第一切片
K11-Uenc
K11-Uint
K1m-Uenc
K1m-Uint
Kan
第二切片
K21-Uenc
K21-Uint
K2m-Uenc
K2m-Uint
第n切片
KCint
KCenc
Kn1-Uenc
Kn1-Uint
Knm-Uenc
Knm-Uint

图 11B

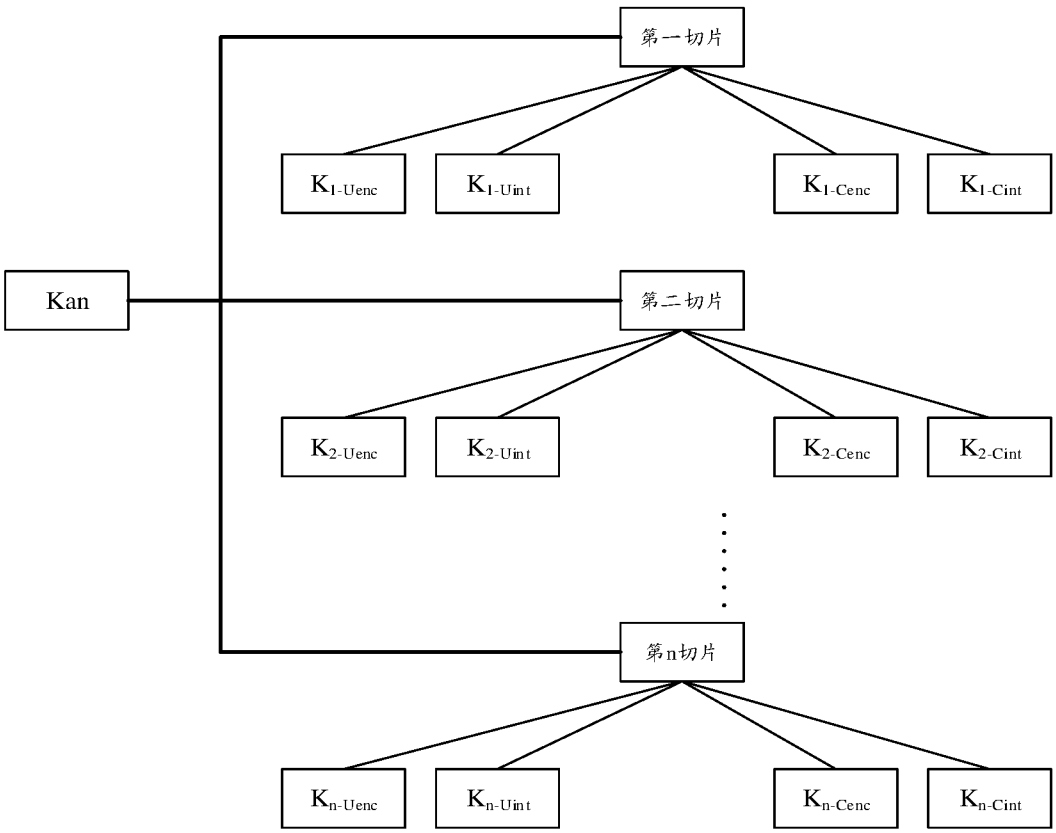
第一切片
K1-Uenc
K1-Uint
K1-Cenc
K1-Cint
Kan
第二切片
K2-Uenc
K2-Uint
K2-Cenc
K2-Cint
第n切片
Kn-Uenc
Kn-Uint
Kn-Cenc
Kn-Cint

图 11C

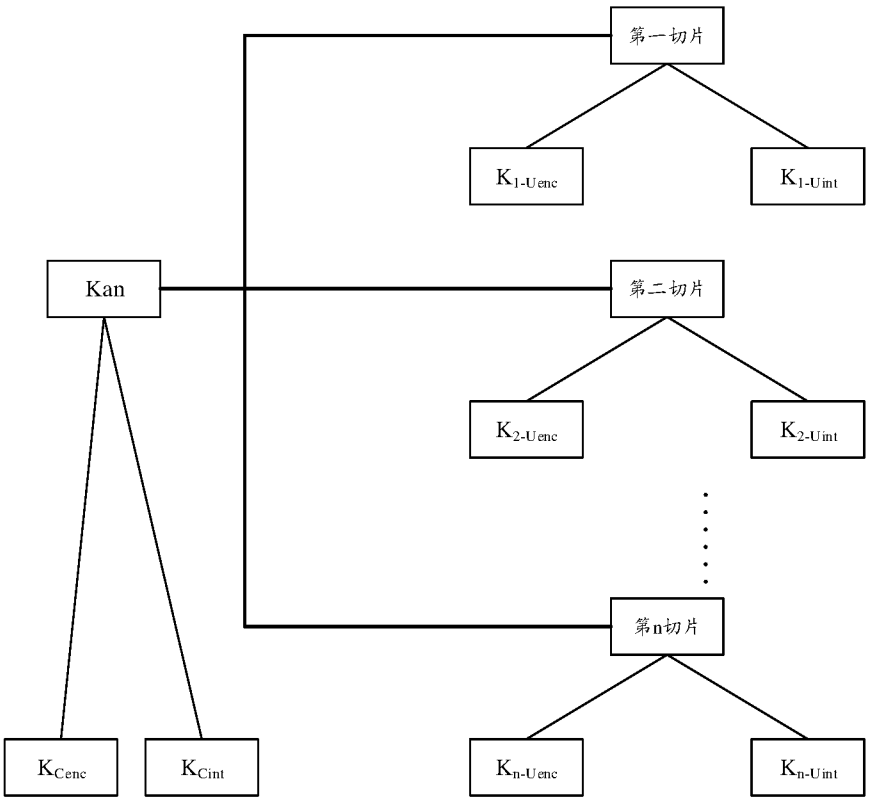
第一切片
$K_{1\text{-}Uenc}$
$K_{1\text{-}Uint}$
Kan
第二切片
$K_{2\text{-}Uenc}$
$K_{2\text{-}Uint}$
第n切片
K_{Cenc}
K_{Cint}
$K_{n\text{-}Uenc}$
$K_{n\text{-}Uint}$

图 11D

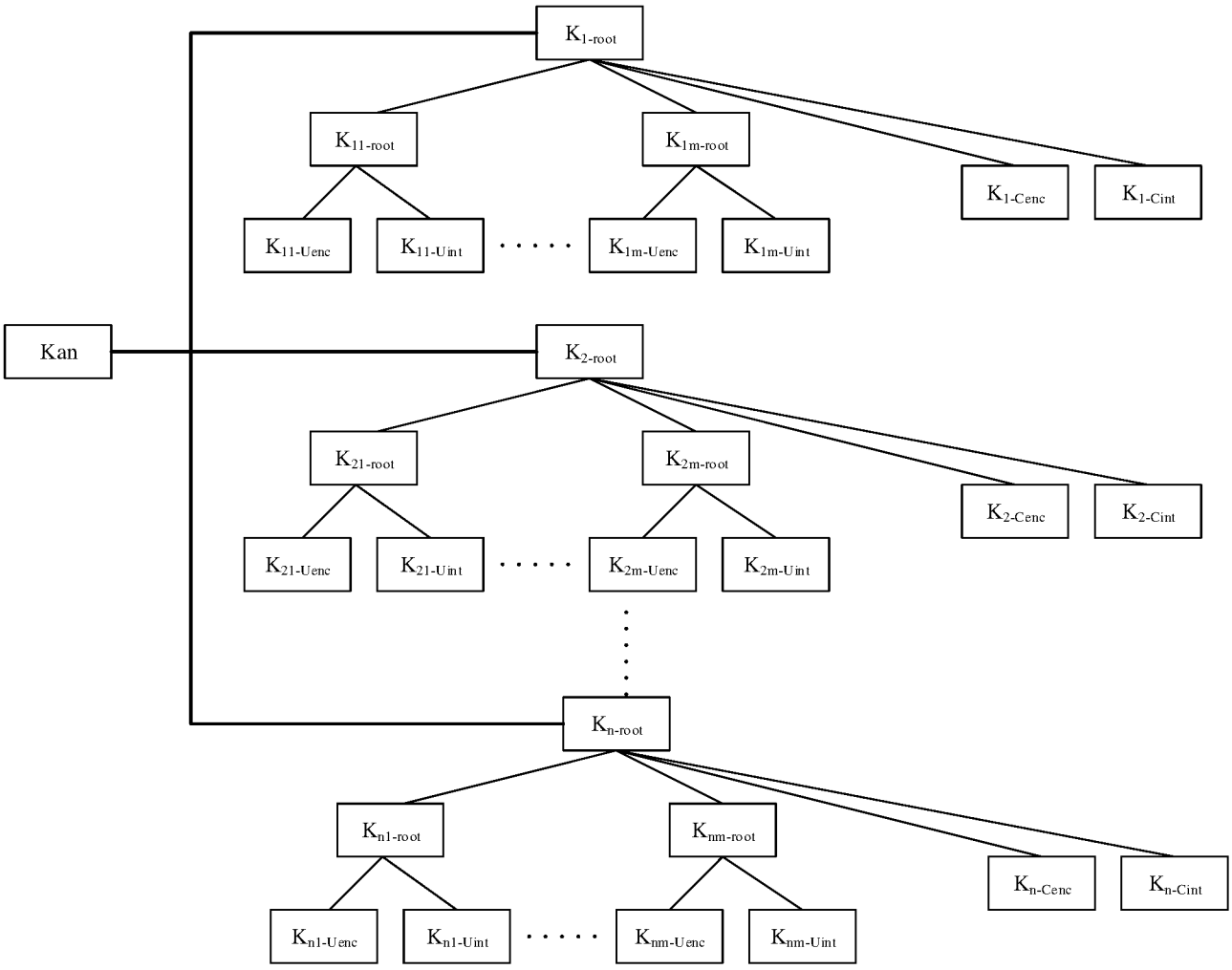
Kan
K1-root
K11-root
K1m-root
K1-Cenc
K1-Cint
K11-Uenc
K11-Uint
K1m-Uenc
K1m-Uint
K2-root
K21-root
K2m-root
K2-Cenc
K2-Cint
K21-Uenc
K21-Uint
K2m-Uenc
K2m-Uint
Kn-root
Kn1-root
Knm-root
Kn-Cenc
Kn-Cint
Kn1-Uenc
Kn1-Uint
Knm-Uenc
Knm-Uint

图 11E

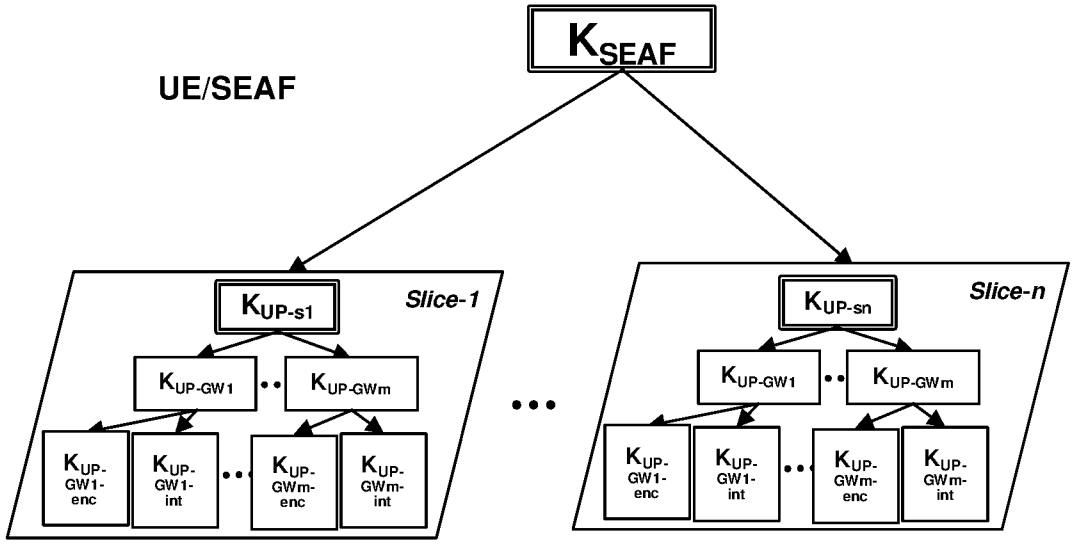
KSEAF
UE/SEAF
KUP-s1
Slice-1
KUP-GW1
KUP-GWm
KUP-GW1-enc
KUP-GW1-int
KUP-GWm-enc
KUP-GWm-int
KUP-sn
Slice-n

图 11F

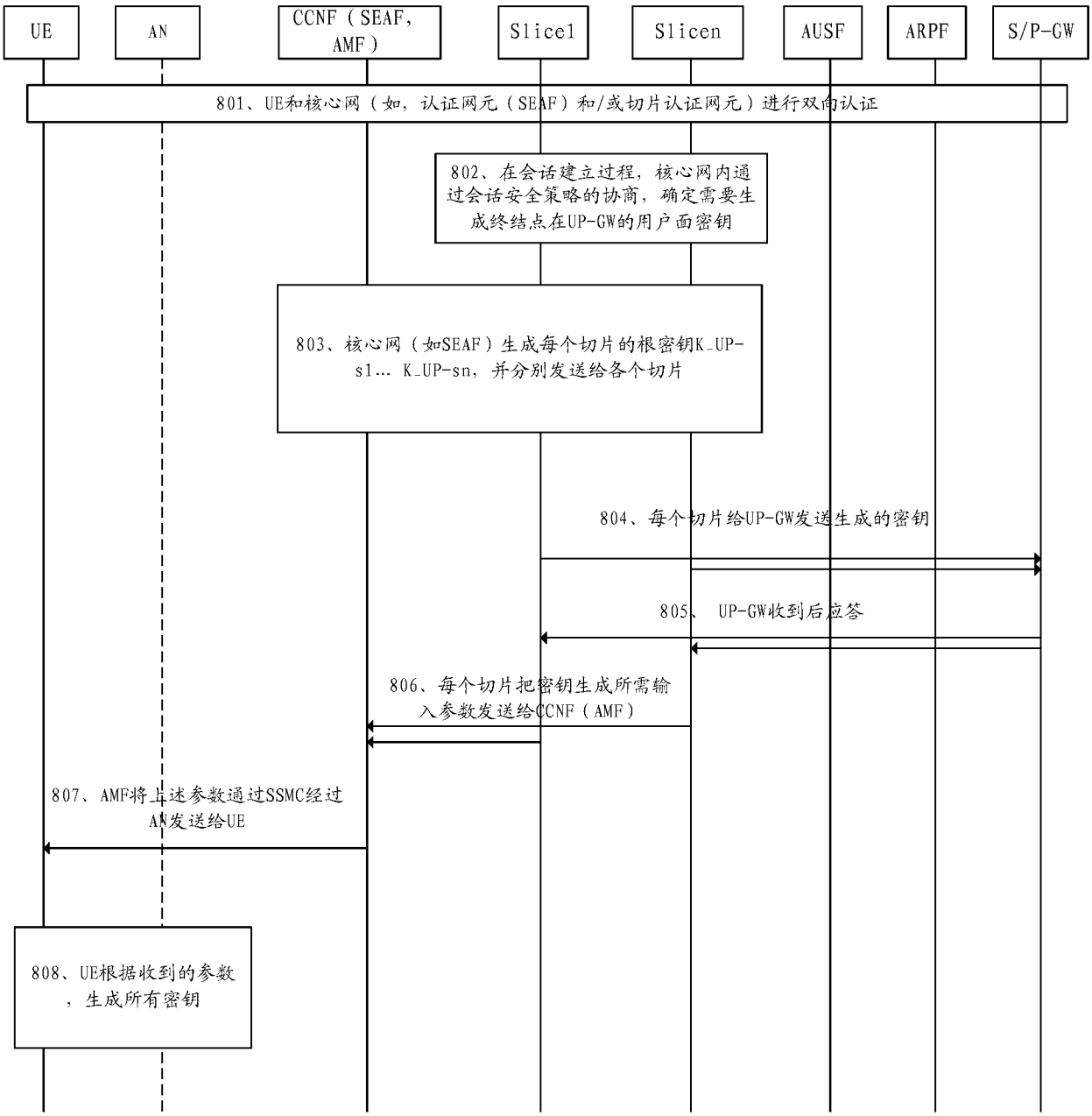
UE
AN
CCNF（SEAF，AMF）
Slice1
Slicen
AUSF
ARPF
S/P-GW
801、UE和核心网（如，认证网元（SEAF）和/或切片认证网元）进行双向认证
802、在会话建立过程，核心网内通过会话安全策略的协商，确定需要生成终结点在UP-GW的用户面密钥
803、核心网（如SEAF）生成每个切片的根密钥K_UP-s1… K_UP-sn，并分别发送给各个切片
804、每个切片给UP-GW发送生成的密钥
805、 UP-GW收到后应答
806、每个切片把密钥生成所需输入参数发送给CCNF（AMF）
807、AMF将上述参数通过SSMC经过AN发送给UE
808、UE根据收到的参数，生成所有密钥

图 12

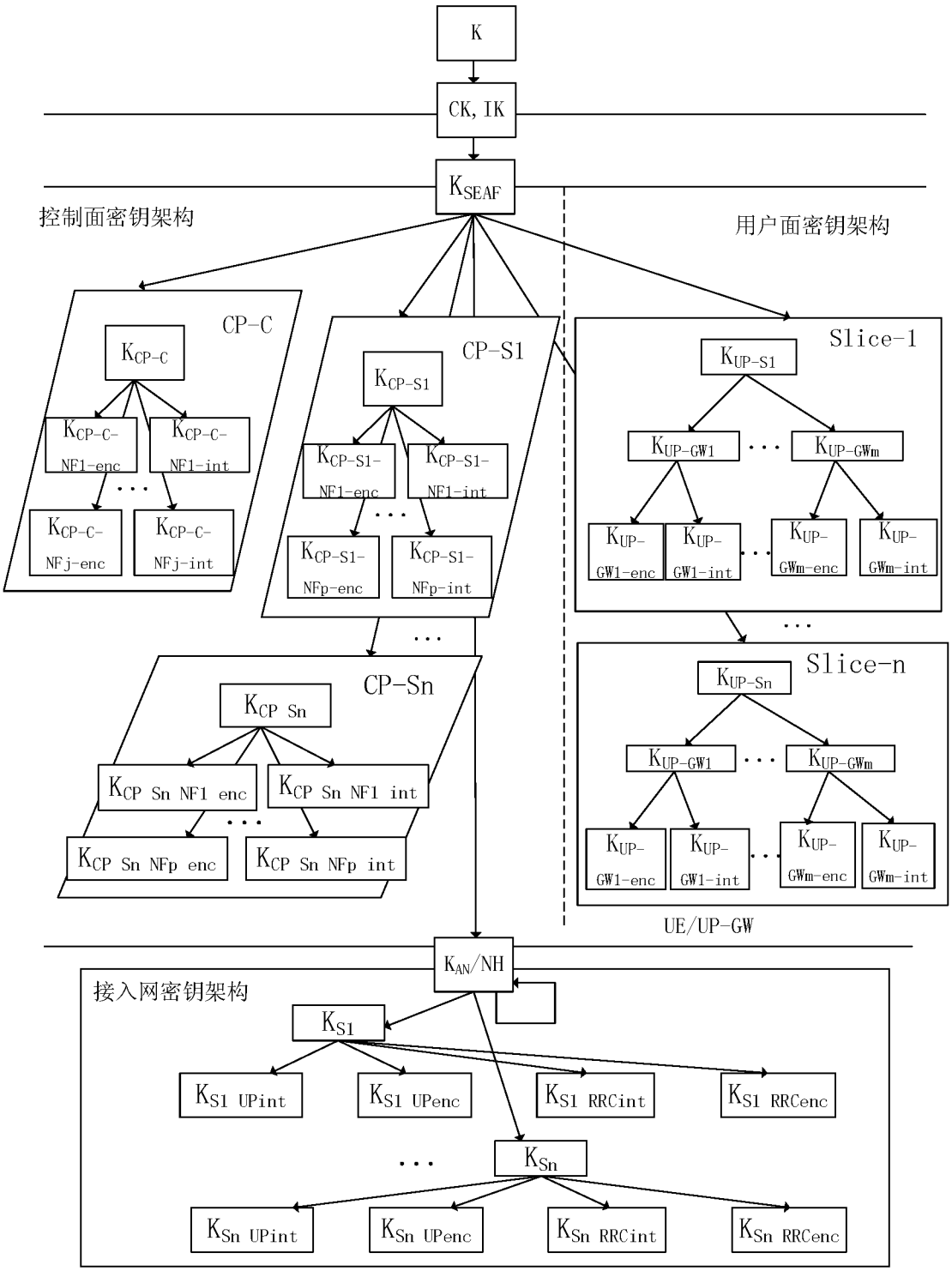
K
CK, IK
KSEAF
控制面密钥架构
用户面密钥架构
CP-C
KCP-C
KCP-C-NF1-enc
KCP-C-NF1-int
KCP-C-NFj-enc
KCP-C-NFj-int
CP-S1
KCP-S1
KCP-S1-NF1-enc
KCP-S1-NF1-int
KCP-S1-NFp-enc
KCP-S1-NFp-int
Slice-1
KUP-S1
KUP-GW1
KUP-GWm
KUP-GW1-enc
KUP-GW1-int
KUP-GWm-enc
KUP-GWm-int
CP-Sn
KCP Sn
KCP Sn NF1 enc
KCP Sn NF1 int
KCP Sn NFp enc
KCP Sn NFp int
Slice-n
KUP-Sn
KUP-GW1
KUP-GWm
KUP-GW1-enc
KUP-GW1-int
KUP-GWm-enc
KUP-GWm-int
UE/UP-GW
KAN/NH
接入网密钥架构
KS1
KS1 UPint
KS1 UPenc
KS1 RRCint
KS1 RRCenc
KSn
KSn UPint
KSn UPenc
KSn RRCint
KSn RRCenc

图 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2017/102864

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

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)

3GPP; VEN; CPRSABS; CNKI: 密钥, 切片, 安全锚点网元, 移动管理网元, 非接入层, 移动性管理, 会话管理 Network, slice, key, security, anchor, element, SEAF, NAS, Non Access Stratum, MM, Mobility Management, SM, Session Management, MME, Mobility Management Entity

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NEC, "pCR to TR 33.899: Solution #1.8 UpdatedKey Hierarchy for NextGen", S3-162141, 3GPP TSG SA WG3 (Security) Meeting #85 7-11 November, 2016, Santa Cruz de Tenerife, Spain, 18 November 2016 (18.11.2016), sections 5.1.4.8.1 and 5.1.4.8.2.2, and figures 5.1.4.8.2.2-1a and 5.1.4.8.2.2-1b	1, 5-6, 8-9, 15-16, 21-22, 24-25, 31-32
A	CN 106210042 A (TSINGHUA UNIVERSITY), 07 December 2016 (07.12.2016), entire document	1-36

☐ 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
01 December 2017	13 December 2017
Name and mailing address of the ISA 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 MAO, Yunnan Telephone No. (86-10) 62089144

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2017/102864

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106210042 A	07 December 2016	None	

国际检索报告

国际申请号
PCT/CN2017/102864

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

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））

3GPP;VEN;CPRSABS;CNKI: 密钥,切片,安全锚点网元,移动管理网元, 非接入层,移动性管理,会话管理Network, slice, key, security, anchor, element, SEAF, NAS, Non Access Stratum, MM, Mobility Management, SM, Session Management, MME, Mobility Management Entity

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	NEC. ""pCR to TR 33.899: Solution #1.8 UpdatedKey hierarchy for NextGen"" S3-162141, 3GPP TSG SA WG3 (Security) Meeting #85 7 - 11 November, 2016, Santa Cruz de Tenerife, Spain, 2016年 11月 18日 (2016 - 11 - 18), 第5.1.4.8.1节，第5.1.4.8.2.2节，图5.1.4.8.2.2-1a，5.1.4.8.2.2-1b	1，5-6，8-9，15-16，21-22，24-25，31-32
A	CN 106210042 A (清华大学) 2016年 12月 7日 (2016 - 12 - 07) 全文	1-36

☐ 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
2017年 12月 1日	2017年 12月 13日

ISA/CN的名称和邮寄地址	受权官员
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	毛韵楠
传真号 (86-10)62019451	电话号码 (86-10)62089144

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2017/102864

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 106210042 A	2016年 12月 7日	无	