

(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)



(10) 国际公布号
WO 2018/137488 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(21) 国际申请号: PCT/CN2018/071818

(22) 国际申请日: 2018 年 1 月 8 日 (08.01.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710055275.9 2017 年 1 月 24 日 (24.01.2017) 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: 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)。 吴荣 (WU, Rong); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。 甘露 (GAN, Lu); 中

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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,

(54) Title: SECURITY IMPLEMENTATION METHOD, DEVICE AND SYSTEM

(54) 发明名称: 安全实现方法、设备以及系统

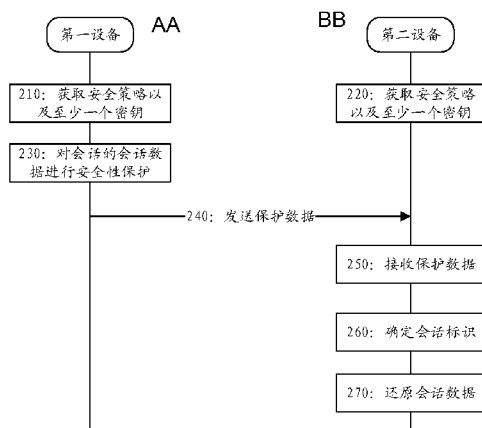


图 2

210, 220 Obtain a security policy and at least one key
230 Protect the security of session data of a session
240 Send protection data
250 Receive the protection data
260 Determine a session identifier
270 Restore the session data
AA First device
BB Second device

(57) Abstract: Disclosed are a security implementation method, device and system. The method comprises: a first device obtains a security policy of a session and at least one key; the first device sends protection data to a second device, wherein the protection data is obtained by protecting the security of session data of the session by using the at least one key according to the security policy of the session, the second device being used for restoring the protection data by using the at least one key according to the security policy to obtain the session data. When the first device is a terminal device, the second device is an access network node or a user plane node; when the first device is the access network node or the user plane node, the second device is the terminal device.

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))。

(57) 摘要： 本发明实施例公开了一种安全实现方法、设备以及系统。其中，所述方法包括：第一设备获取会话的安全策略以及至少一个密钥；所述第一设备向第二设备发送保护数据，其中，所述保护数据是根据所述会话的安全策略使用所述至少一个密钥对所述会话的会话数据的安全性进行保护得到的，所述第二设备用于根据所述安全策略使用所述至少一个密钥对所述保护数据进行还原以获得所述会话数据；其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

安全实现方法、设备以及系统

技术领域

本发明涉及通信领域，尤其涉及一种安全实现方法、设备以及系统。

背景技术

在现有的网络安全架构中，数据的安全性保护采用的是 hop-by-hop 的方式，即分段进行安全性保护。以数据从终端设备—基站—服务网关—PDN 网关的传输链路为例，终端设备-基站之间执行一次安全性保护，基站—服务网关之间执行一次安全性保护，服务网关—PDN 网关之间执行一次安全性保护。可以看出，在数据传输的过程中，如果中间节点出现了问题，则可能会导致数据的泄露。而且，在数据传输过程中多次对数据进行加密和还原，也会导致资源的浪费。

发明内容

本发明实施例所要解决的技术问题在于，提供一种安全实现方法、设备以及系统，实现了数据的端到端的保护。

第一方面，本发明实施例提供一种安全实现方法，包括：第一设备获取会话的安全策略以及至少一个密钥；所述第一设备向第二设备发送保护数据，其中，所述保护数据是根据所述会话的安全策略使用所述至少一个密钥对所述会话的会话数据的安全性进行保护得到的，所述第二设备用于根据所述安全策略使用所述至少一个密钥对所述保护数据进行还原以获得所述会话数据；其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

结合第一方面，第一方面的第一种可能的实施方式中，所述至少一个密钥包括：第一密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

结合第一方面的第一种可能的实施方式，第一方面的第二种可能的实施方式中，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

结合第一方面的第二种可能的实施方式，第一方面的第三种可能的实施方式中，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

结合第一方面的第三种可能的实施方式，第一方面的第四种可能的实施方式中，所述密钥长度包括第一密钥长度和/或第二密钥长度，其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。

结合第一方面的第三种可能的实施方式，第一方面的第五种可能的实施方式中，所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间，其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所述第二密钥更新时间用于表征所述第二密钥的更新时间。

结合第一方面的上述任一种可能的实施方式，第一方面的第六种可能的实施方式中，所述第一安全性为加密性，所述第二安全性为完整性。

结合第一方面的第六种可能的实施方式，第一方面的第七种可能的实施方式中，所述保护数据还包括参数字段，所述参数字段包括第一标识字段、第二标识字段、第三标识字段至少一个，其中，所述第一标识字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识、承载标识、flow 标识以及切片标识中的至少一个，所述第三标识用于指示所述会话的保护方式。

结合第一方面的第七种可能的实施方式，第一方面的第八种可能的实施方式中，所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个，其中，所述长度字段用于指示所述参数字段的长度，所述分组字段用于指示分组进行加密时，分组的长度，所述 MAC 字段用于指示所述会话进行了完整性保护。

结合第一方面的上述任一种可能的实施方式，第一方面的第九种可能的实施方式中，当所述第二设备为接入网节点时，所述第一设备获取所述安全策略具体为：所述第一设备向策略控制器获取所述安全策略。

结合第一方面的第九种可能的实施方式，第一方面的第十种可能的实施方式中，所述第一设备向策略控制器获取所述安全策略具体为：所述第一设备向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；所述第一设备接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点向所述策略控制器发送第二请求获取到的，所述第二请求是所述接入网节点基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

结合第一方面的第九种可能的实施方式，第一方面的第十一种可能的实施方式中，所述第一设备向策略控制器获取所述安全策略具体为：所述第一设备向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；所述第一设备接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点通过至少一个网元向所述策略控制器转发第二请求获取到的，所述第二请求是所述接入网节点基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

结合第一方面的第十一种可能的实施方式，第一方面的第十二种可能的实施方式中，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

结合第一方面的第九种可能的实施方式，第一方面的第十三种可能的实施方式中，所述第一设备向策略控制器获取所述安全策略具体为：所述第一设备向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；所述第一设备接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点

根据核心网安全策略以及所述接入网节点的安全能力生成的,所述核心网安全策略是所述策略控制器根据所述接入网节点转发的第一请求生成的。

结合第一方面的上述任一种可能的实施方式,第一方面的第十四种可能的实施方式中,当所述第二设备为接入网节点时,第一设备获取至少一个密钥具体为:所述第一设备通过所述接入网节点向认证节点发送第三请求;所述第一设备基于所述第三请求获取基础密钥,其中,所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的;所述第一设备基于所述基础密钥推导出所述至少一个密钥。

结合第一方面的第十四种可能的实施方式,第一方面的第十五种可能的实施方式中,所述第一设备基于所述基础密钥推导出所述至少一个密钥具体为:所述第一设备根据所述基础密钥推导出中间密钥;所述第一设备根据所述中间密钥推导出所述至少一个密钥。

结合第一方面的第十五种可能的实施方式,第一方面的第十六种可能的实施方式中,所述第一设备根据所述基础密钥推导出中间密钥具体为:所述第一设备基于第一参数,并根据所述基础密钥推导出中间密钥,其中,所述第一参数包括所述接入网节点标识、NAS计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow标识以及切片标识中的至少一个。

结合第一方面的第十五种可能的实施方式,第一方面的第十七种可能的实施方式中,所述第一设备根据所述中间密钥推导出所述至少一个密钥具体为:所述第一设备基于所述第二参数,并根据所述中间密钥推导出所述至少一个密钥;其中,所述第二参数包括空口安全策略标识、安全算法标识、NAS计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项,所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

结合第一方面的第十四种可能的实施方式,第一方面的第十八种可能的实施方式中,所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

结合第一方面的上述任一种可能的实施方式,第一方面的第十九种可能的实施方式中,所述保护数据为表头数据、负载数据或者数据包,其中,所述数据包包括所述表头数据以及所述负载数据。

第二方面,提供一种安全实现方法,包括:第二设备确定会话的会话标识;所述第二设备获取所述会话的安全策略以及至少一个密钥;所述第二设备根据所述会话标识识别第一设备发送的所述会话的保护数据,并通过根据所述会话的安全策略使用所述至少一个密钥对所述保护数据进行还原以获得会话数据,其中,所述保护数据是所述第一设备根据所述会话的安全策略使用所述至少一个密钥对所述会话数据的安全性进行保护得到的,所述第一设备用于根据所述安全策略使用所述至少一个密钥对所述会话数据进行加密以获得所述保护数据;

其中,当所述第一设备为终端设备时,所述第二设备为接入网节点或者用户面节点;当所述第一设备为接入网节点或者用户面节点时,所述第二设备为终端设备。

结合第二方面,第二方面的第一种可能的实施方式中,所述至少一个密钥包括:第一

密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

结合第二方面的第一种可能的实施方式，第二方面的第二种可能的实施方式中，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

结合第二方面的第二种可能的实施方式，第二方面的第三种可能的实施方式中，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

结合第二方面的第三种可能的实施方式，第二方面的第四种可能的实施方式中，所述密钥长度包括第一密钥长度和/或第二密钥长度，其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。

结合第二方面的第三种可能的实施方式，第二方面的第五种可能的实施方式中，所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间，其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所述第二密钥更新时间用于表征所述第二密钥的更新时间。

结合第二方面的上述任一种可能的实施方式，第二方面的第六种可能的实施方式中，当所述第二设备为用户面节点时，第二设备确定会话的会话标识具体为：所述第二设备通过所述保护数据所在的封装表头确定会话的会话标识；或者，所述第二设备通过所述保护数据所在的封装表头中的隧道标识确定会话的会话标识；或者，所述第二设备通过所述保护数据所在的外部 IP 报文表头确定会话的会话标识；或者，所述第二设备通过所述保护数据所在的封装表头和所述保护数据所在的外部 IP 报文表头确定所述会话的会话标识；或者，所述第二设备通过所述保护数据所在的协议数据单元表头和所述保护数据所在的封装表头确定所述会话的会话标识；或者，所述第二设备通过所述保护数据中的参数字段确定所述会话的会话标识。

结合第二方面的上述任一种可能的实施方式，第二方面的第七种可能的实施方式中，当所述第二设备为接入网节点时，第二设备确定会话的会话标识具体为：所述第二设备通过所述会话所占用的空口资源确定所述会话的会话标识；或者，所述第二设备通过所述会话所占用的空口的空口标识确定所述会话的会话标识；或者，所述第二设备通过所述会话所占用的数据无线承载的标识确定所述会话的会话标识；或者，所述第二设备通过所述保护数据中的参数字段确定所述会话的会话标识。

结合第二方面的第六或者第七种可能的实施方式，第二方面的第八种可能的实施方式中，所述第一安全性为加密性，所述第二安全性为完整性。

结合第二方面的第八种可能的实施方式，第二方面的第九种可能的实施方式中，所述参数字段包括第一标识字段、第二标识字段、第三标识字段中的至少一个，其中，所述第一标识字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识

以及切片标识中的至少一个, 所述第三标识用于指示所述会话的保护方式。

结合第二方面的第九种可能的实施方式, 第二方面的第十种可能的实施方式中, 所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个, 其中, 所述长度字段用于指示所述参数字段的长度, 所述分组字段用于指示分组进行加密时, 分组的长度, 所述 MAC 字段用于指示所述会话进行了完整性保护。

结合第二方面的上述任一种可能的实施方式, 第二方面的第十一种可能的实施方式中, 当所述第二设备为接入网节点时, 所述第二设备获取所述安全策略具体为: 所述第二设备向第一网元获取所述安全策略, 其中, 所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

结合第二方面的第十一种可能的实施方式, 第二方面的第十二种可能的实施方式中, 当所述第一网元为策略控制器时, 所述第二设备向策略控制器获取所述安全策略具体为: 所述第二设备接收所述第一设备发送的第一请求, 其中, 所述第一请求包括所述第一设备的安全能力以及业务安全需求; 所述第二设备向所述策略控制器发送第二请求, 其中, 所述第二请求是基于所述第一请求生成的, 包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求; 所述第二设备接收所述策略控制器返回的所述安全策略, 其中, 所述安全策略是所述策略控制器根据所述第二请求生成的。

结合第二方面的第十一种可能的实施方式, 第二方面的第十三种可能的实施方式中, 当所述第一网元为策略控制器时, 所述第二设备向策略控制器获取所述安全策略具体为: 所述第二设备接收所述第一设备发送的第一请求, 其中, 所述第一请求包括所述第一设备的安全能力以及业务安全需求; 所述第二设备通过至少一个网元向所述策略控制器发送第二请求, 其中, 所述第二请求是基于所述第一请求生成的, 包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求; 所述第二设备接收所述策略控制器通过所述至少一个网元返回的所述安全策略, 其中, 所述安全策略是所述策略控制器根据所述第二请求生成的。

结合第二方面的第十三种可能的实施方式, 第二方面的第十四种可能的实施方式中, 所述至少一个网元包括会话管理网元; 或者, 所述至少一个网元包括会话管理网元或者移动管理实体。

结合第二方面的第十一种可能的实施方式, 第二方面的第十五种可能的实施方式中, 所述第二设备向策略控制器获取所述安全策略具体为: 所述第二设备接收所述第一设备发送的第一请求, 其中, 所述第一请求包括所述第一设备的安全能力以及业务安全需求; 所述第二设备向所述策略控制器转发所述第一请求; 所述第二设备接收所述策略控制器返回的核心网安全策略, 并根据所述核心网安全策略以及所述接入网节点的安全能力生成所述安全策略。

结合第二方面的第八种至第十五种可能的实施方式中的任意一种, 第二方面的第十六种可能的实施方式中, 当所述第二设备为接入网节点时, 第二设备获取至少一个密钥具体为: 所述第二设备向密钥管理中心发送第三请求; 所述第二设备基于所述第三请求接收所述密钥管理中心返回的中间密钥, 其中, 所述中间密钥是基于基础密钥推导得到的, 所述基础密钥为认证节点发送给所述密钥管理中心的; 所述第二设备基于所述中间密钥推导出

所述至少一个密钥。

结合第二方面的第十六种可能的实施方式，第二方面的第十七种可能的实施方式中，所述中间密钥是根据第一参数推导出来的，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

结合第二方面的第十七种可能的实施方式，第二方面的第十八种可能的实施方式中，所述第二设备根据所述中间密钥推导出所述至少一个密钥具体为：所述第二设备基于所述第二参数，并根据所述中间密钥推导出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

结合第二方面的第十六种可能的实施方式，第二方面的第十九种可能的实施方式中，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

结合第二方面的上述任一种可能的实施方式，第二方面的第二十种可能的实施方式中，当所述第二设备为用户面节点时，第二设备获取至少一个密钥具体为：所述第二设备向第一网元请求所述至少一个密钥，其中，所述第一网元为所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

结合第二方面的上述任一种可能的实施方式，第二方面的第二十一一种可能的实施方式中，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

第三方面，提供一种安全策略生成方法，包括：策略控制器接收目标网元发送的策略请求，其中，所述策略请求包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；所述策略控制器根据目标参数生成安全策略，其中，所述目标参数是根据所述第一请求生成的，包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；所述策略控制器向接入网节点发送安全策略。

结合第三方面，第三方面的第一种可能的实施方式中，所述目标参数还包括：终端设备的预制安全能力，其中，所述终端设备的预制安全能力是从认证服务控制器 AUSF 获取得到的。

结合第三方面的上述任一种可能的实施方式，第三方面的第二种可能的实施方式中，所述目标参数还包括：服务器的安全需求，其中，所述服务器的安全需求是从服务器获取得到的。

结合第三方面的上述任一种可能的实施方式，第三方面的第三种可能的实施方式中，所述目标网元为接入网节点或者会话管理网元。

第四方面，提供一种密钥生成方法，包括：所述第一设备通过所述接入网节点向认证节点发送第三请求；所述第一设备基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；所述第一设备基于所述基础密钥

推行出所述至少一个密钥。

结合第四方面，第四方面的第一种可能的实施方式中，所述终端设备基于所述基础密钥推行出所述至少一个密钥具体为：所述终端设备根据所述基础密钥推行出中间密钥；所述终端设备根据所述中间密钥推行出所述至少一个密钥。

结合第四方面的第一种可能的实施方式，第四方面的第二种可能的实施方式中，所述第一设备根据所述基础密钥推行出中间密钥具体为：所述终端设备基于第一参数，并根据所述基础密钥推行出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

结合第四方面的第一种可能的实施方式，第四方面的第三种可能的实施方式中，所述终端设备根据所述中间密钥推行出所述至少一个密钥具体为：所述终端设备基于所述第二参数，并根据所述中间密钥推行出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

结合第四方面的上述任一种可能的实施方式，第四方面的第四种可能的实施方式中，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

第五方面，提供一种第一设备，包括：获取模块以及发送模块，所述获取模块用于获取会话的安全策略以及至少一个密钥；所述发送模块用于向第二设备发送保护数据，其中，所述保护数据是根据所述会话的安全策略使用所述至少一个密钥对所述会话的会话数据的安全性进行保护得到的，所述第二设备用于根据所述安全策略使用所述至少一个密钥对所述保护数据进行还原以获得所述会话数据；其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

结合第五方面，第五方面的第一种可能的实施方式中，所述至少一个密钥包括：第一密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

结合第五方面的第一种可能的实施方式，第五方面的第二种可能的实施方式中，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

结合第五方面的第二种可能的实施方式，第五方面的第三种可能的实施方式中，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

结合第五方面的第三种可能的实施方式，第五方面的第四种可能的实施方式中，所述

密钥长度包括第一密钥长度和/或第二密钥长度,其中,所述第一密钥长度用于表征所述第一密钥的长度,所述第二密钥长度用于表征所述第二密钥的长度。

结合第五方面的第三种可能的实施方式,第五方面的第五种可能的实施方式中,所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间,其中,所述第一密钥更新时间用于表征所述第一密钥的更新时间,所述第二密钥更新时间用于表征所述第二密钥的更新时间。

结合第五方面的上述任一种可能的实施方式,第五方面的第六种可能的实施方式中,所述第一安全性为加密性,所述第二安全性为完整性。

结合第五方面的第六种可能的实施方式,第五方面的第七种可能的实施方式中,所述保护数据还包括参数字段,所述参数字段包括第一标识字段、第二标识字段、第三标识字段至少一个,其中,所述第一标识字段用于指示本消息为会话消息,所述第二标识字段用于指示业务标识、会话标识、承载标识、flow 标识以及切片标识中的至少一个,所述第三标识用于指示所述会话的保护方式。

结合第五方面的第七种可能的实施方式,第五方面的第八种可能的实施方式中,所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个,其中,所述长度字段用于指示所述参数字段的长度,所述分组字段用于指示分组进行加密时,分组的长度,所述 MAC 字段用于指示所述会话进行了完整性保护。

结合第五方面的上述任一种可能的实施方式,第五方面的第九种可能的实施方式中,所述获取模块具体用于向策略控制器获取所述安全策略。

结合第五方面的第九种可能的实施方式,第五方面的第十种可能的实施方式中,所述获取模块包括发送单元以及接收单元,所述发送单元用于向所述接入网节点发送第一请求,其中,所述第一请求包括所述第一设备的安全能力以及业务安全需求;所述接收单元用于接收所述接入网节点返回的所述安全策略,其中,所述安全策略是所述接入网节点向所述策略控制器发送第二请求获取到的,所述第二请求是所述接入网节点基于所述第一请求生成的,包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

结合第五方面的第九种可能的实施方式,第五方面的第十一种可能的实施方式中,所述获取模块包括发送单元以及接收单元,所述发送单元用于向所述接入网节点发送第一请求,其中,所述第一请求包括所述第一设备的安全能力以及业务安全需求;所述接收单元用于接收所述接入网节点返回的所述安全策略,其中,所述安全策略是所述接入网节点通过至少一个网元向所述策略控制器转发第二请求获取到的,所述第二请求是所述接入网节点基于所述第一请求生成的,包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

结合第五方面的第十一种可能的实施方式,第五方面的第十二种可能的实施方式中,所述至少一个网元包括会话管理网元;或者,所述至少一个网元包括会话管理网元或者移动管理实体。

结合第五方面的第九种可能的实施方式,第五方面的第十三种可能的实施方式中,所述获取模块包括发送单元以及接收单元,所述发送单元用于向所述接入网节点发送第一请求,其中,所述第一请求包括所述第一设备的安全能力以及业务安全需求;所述接收单元

用于接收所述接入网节点返回的所述安全策略,其中,所述安全策略是所述接入网节点根据核心网安全策略以及所述接入网节点的安全能力生成的,所述核心网安全策略是所述策略控制器根据所述接入网节点转发的第一请求生成的。

结合第五方面的上述任一种可能的实施方式,第五方面的第十四种可能的实施方式中,当所述第二设备为接入网节点时,所述获取模块包括发送单元、获取单元以及推衍单元,所述发送单元用于通过所述接入网节点向认证节点发送第三请求;所述获取单元用于基于所述第三请求获取基础密钥,其中,所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的;所述推衍单元用于基于所述基础密钥推衍出所述至少一个密钥。

结合第五方面的第十四种可能的实施方式,第五方面的第十五种可能的实施方式中,所述推衍单元用于根据所述基础密钥推衍出中间密钥,以及,根据所述中间密钥推衍出所述至少一个密钥。

结合第五方面的第十五种可能的实施方式,第五方面的第十六种可能的实施方式中,所述推衍单元用于基于第一参数,并根据所述基础密钥推衍出中间密钥,其中,所述第一参数包括所述接入网节点标识、NAS计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow标识以及切片标识中的至少一个。

结合第五方面的第十五种可能的实施方式,第五方面的第十七种可能的实施方式中,所述推衍单元用于基于所述第二参数,并根据所述中间密钥推衍出所述至少一个密钥;其中,所述第二参数包括空口安全策略标识、安全算法标识、NAS计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项,所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

结合第五方面的第十四种可能的实施方式,第五方面的第十八种可能的实施方式中,所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

结合第五方面的上述任一种可能的实施方式,第五方面的第十九种可能的实施方式中,所述保护数据为表头数据、负载数据或者数据包,其中,所述数据包包括所述表头数据以及所述负载数据。

第六方面,提供一种第二设备,包括:确定模块、获取模块以及识别模块,所述确定模块用于确定会话的会话标识;所述获取模块用于获取所述会话的安全策略以及至少一个密钥;所述识别模块用于根据所述会话标识识别第一设备发送的所述会话的保护数据,并通过根据所述会话的安全策略使用所述至少一个密钥对所述保护数据进行还原以获得会话数据,其中,所述保护数据是所述第一设备根据所述会话的安全策略使用所述至少一个密钥对所述会话数据的安全性进行保护得到的,所述第一设备用于根据所述安全策略使用所述至少一个密钥对所述会话数据进行加密以获得所述保护数据;其中,当所述第一设备为终端设备时,所述第二设备为接入网节点或者用户面节点;当所述第一设备为接入网节点或者用户面节点时,所述第二设备为终端设备。

结合第六方面,第六方面的第一种可能的实施方式中,所述至少一个密钥包括:第一密钥以及第二密钥,其中,所述第一密钥用于对所述会话的第一安全性进行保护,所述第

二密钥用于对所述会话的第二安全性进行保护。

结合第六方面的第一种可能的实施方式，第六方面的第二种可能的实施方式中，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

结合第六方面的第二种可能的实施方式，第六方面的第三种可能的实施方式中，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

结合第六方面的第三种可能的实施方式，第六方面的第四种可能的实施方式中，所述密钥长度包括第一密钥长度和/或第二密钥长度，其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。

结合第六方面的第三种可能的实施方式，第六方面的第五种可能的实施方式中，所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间，其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所述第二密钥更新时间用于表征所述第二密钥的更新时间。

结合第六方面的上述任一种可能的实施方式，第六方面的第六种可能的实施方式中，当所述第二设备为用户面节点时，所述确定模块具体用于：通过所述保护数据所在的封装表头确定会话的会话标识；或者，通过所述保护数据所在的封装表头中的隧道标识确定会话的会话标识；或者，通过所述保护数据所在的外部 IP 报文表头确定会话的会话标识；或者，通过所述保护数据所在的封装表头和所述保护数据所在的外部 IP 报文表头确定所述会话的会话标识；或者，通过所述保护数据所在的协议数据单元表头和所述保护数据所在的封装表头确定所述会话的会话标识；或者，通过所述保护数据中的参数字段确定所述会话的会话标识。

结合第六方面的上述任一种可能的实施方式，第六方面的第七种可能的实施方式中，当所述第二设备为接入网节点时，所述确定模块具体用于：通过所述会话所占用的空口资源确定所述会话的会话标识；或者，通过所述会话所占用的空口的空口标识确定所述会话的会话标识；或者，通过所述会话所占用的数据无线承载的标识确定所述会话的会话标识；或者，通过所述保护数据中的参数字段确定所述会话的会话标识。

结合第六方面的第六或者第七种可能的实施方式，第六方面的第八种可能的实施方式中，所述第一安全性为加密性，所述第二安全性为完整性。

结合第六方面的第八种可能的实施方式，第六方面的第九种可能的实施方式中，所述参数字段包括第一标识字段、第二标识字段、第三标识字段中的至少一个，其中，所述第一标识字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识以及切片标识中的至少一个，所述第三标识用于指示所述会话的保护方式。

结合第六方面的第九种可能的实施方式，第六方面的第十种可能的实施方式中，所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个，其中，所述长度字段

用于指示所述参数字段的长度，所述分组字段用于指示分组进行加密时，分组的长度，所述 MAC 字段用于指示所述会话进行了完整性保护。

结合第六方面的上述任一种可能的实施方式，第六方面的第十一种可能的实施方式中，当所述第二设备为接入网节点时，所述获取模块用于向第一网元获取所述安全策略，其中，所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

结合第六方面的第十一种可能的实施方式，第六方面的第十二种可能的实施方式中，当所述第一网元为策略控制器时，所述获取模块包括接收单元以及发送单元，所述接收单元用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；所述发送单元用于向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；所述接收单元用于接收所述策略控制器返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

结合第六方面的第十一种可能的实施方式，第六方面的第十三种可能的实施方式中，当所述第一网元为策略控制器时，所述获取模块包括接收单元以及发送单元，所述接收单元用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；所述发送单元用于通过至少一个网元向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；所述接收单元用于接收所述策略控制器通过所述至少一个网元返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

结合第六方面的第十三种可能的实施方式，第六方面的第十四种可能的实施方式中，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

结合第六方面的第十一种可能的实施方式，第六方面的第十五种可能的实施方式中，所述获取模块包括接收单元以及发送单元，所述接收单元用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；所述发送单元用于向所述策略控制器转发所述第一请求；所述接收单元用于接收所述策略控制器返回的核心网安全策略，并根据所述核心网安全策略以及所述接入网节点的安全能力生成所述安全策略。

结合第六方面的第八种至第十五种可能的实施方式中的任意一种，第六方面的第十六种可能的实施方式中，当所述第二设备为接入网节点时，所述获取模块包括发送单元、接收单元以及推衍单元，所述发送单元用于向密钥管理中心发送第三请求；所述接收单元用于基于所述第三请求接收所述密钥管理中心返回的中间密钥，其中，所述中间密钥是基于基础密钥推衍得到的，所述基础密钥为认证节点发送给所述密钥管理中心的；所述推衍单元用于基于所述中间密钥推衍出所述至少一个密钥。

结合第六方面的第十六种可能的实施方式，第六方面的第十七种可能的实施方式中，所述中间密钥是根据第一参数推衍出来的，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标

识以及切片标识中的至少一个。

结合第六方面的第十七种可能的实施方式，第六方面的第十八种可能的实施方式中，所述推衍单元用于基于所述第二参数，并根据所述中间密钥推导出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

结合第六方面的第十六种可能的实施方式，第六方面的第十九种可能的实施方式中，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

结合第六方面的上述任一种可能的实施方式，第六方面的第二十种可能的实施方式中，当所述第二设备为用户面节点时，所述获取模块用于向第一网元请求所述至少一个密钥，其中，所述第一网元为所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

结合第六方面的上述任一种可能的实施方式，第六方面的第二十一种可能的实施方式中，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

第七方面，提供一种策略控制器，包括：接收模块、生成模块以及发送模块，所述接收模块用于接收目标网元发送的策略请求，其中，所述策略请求包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；所述生成模块用于根据目标参数生成安全策略，其中，所述目标参数是根据所述第一请求生成的，包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；所述发送模块用于向接入网节点发送安全策略。

结合第七方面，第七方面的第一种可能的实施方式中，所述目标参数还包括：终端设备的预制安全能力，其中，所述终端设备的预制安全能力是从认证服务控制器 AUSF 获取得到的。

结合第七方面的上述任一种可能的实施方式，第七方面的第二种可能的实施方式中，所述目标参数还包括：服务器的安全需求，其中，所述服务器的安全需求是从服务器获取得到的。

结合第七方面的上述任一种可能的实施方式，第七方面的第三种可能的实施方式中，所述目标网元为接入网节点或者会话管理网元。

第八方面，提供一种第一设备，包括：发送模块、获取模块以及推衍模块，所述发送模块用于通过所述接入网节点向认证节点发送第三请求；所述获取模块用于基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；所述推衍模块用于基于所述基础密钥推导出所述至少一个密钥。

结合第八方面，第八方面的第一种可能的实施方式中，所述推衍模块用于根据所述基础密钥推导出中间密钥；根据所述中间密钥推导出所述至少一个密钥。

结合第八方面的第一种可能的实施方式，第八方面的第二种可能的实施方式中，所述

推衍模块用于基于第一参数，并根据所述基础密钥推衍出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

结合第八方面的第一种可能的实施方式，第八方面的第三种可能的实施方式中，所述推衍模块用于基于所述第二参数，并根据所述中间密钥推衍出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

结合第八方面的上述任一种可能的实施方式，第八方面的第四种可能的实施方式中，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

第九方面，提供一种第一设备，包括存储器以及与所述存储器耦合的处理器、发射器和接收器，其中：所述发射器用于与向外部发送数据，所述接收器用于接收外部发送的数据，所述存储器用于存储第一方面描述的方法的实现代码，所述处理器用于执行所述存储器中存储的程序代码，即执行第一方面描述的方法。

第十方面，提供一种第二设备，包括存储器以及与所述存储器耦合的处理器、发射器和接收器，其中：所述发射器用于与向外部发送数据，所述接收器用于接收外部发送的数据，所述存储器用于存储第二方面描述的方法的实现代码，所述处理器用于执行所述存储器中存储的程序代码，即执行第二方面描述的方法。

第十三方面，提供了一种策略控制器，包括存储器以及与所述存储器耦合的处理器、发射器和接收器，其中：所述发射器用于与向外部发送数据，所述接收器用于接收外部发送的数据，所述存储器用于存储第三方面描述的方法的实现代码，所述处理器用于执行所述存储器中存储的程序代码，即执行第三方面描述的方法。

第十四方面，提供一种第一设备，包括存储器以及与所述存储器耦合的处理器、发射器和接收器，其中：所述发射器用于与向外部发送数据，所述接收器用于接收外部发送的数据，所述存储器用于存储第四方面描述的方法的实现代码，所述处理器用于执行所述存储器中存储的程序代码，即执行第四方面描述的方法。

第十五方面，提供了一种存储介质，用于存储上述第一方面所述的方法的实现代码。

第十六方面，提供了一种存储介质，用于存储上述第二方面所述的方法的实现代码。

第十七方面，提供了一种存储介质，用于存储上述第三方面所述的方法的实现代码。

第十八方面，提供了一种存储介质，用于存储上述第四方面所述的方法的实现代码。

第十九方面，提供一种通信系统，所述通信系统包括第一设备以及第二设备，其中，所述第一设备连接所述第二设备，所述第一设备为如第五方面任一项所述的设备；所述第二设备为如第六方面任一项所述的设备。

实施本发明实施例，第一设备使用安全策略和至少一个密钥对会话数据进行了安全性保护以获得保护数据，第二设备根据相同的安全策略和至少一个密钥对保护数据进行还原以获得会话数据。本发明实施例实现端到端的保护，会话数据从第一设备（一端）发出后，

在没有到达第二设备（另一端）之前，会话数据是一直处于安全性保护的状态，从而避免了在传输途中被非法窃取。并且，会话数据在传输的过程中，不需要在经过的中间节点中进行加密和还原，能够有效地节省资源。

附图说明

为了更清楚地说明本发明实施例或背景技术中的技术方案，下面将对本发明实施例或背景技术中所需要使用的附图进行说明。

图 1 是本发明实施例公开的一种网络架构的示意图；

图 2 是本发明实施例提供的一种安全实现方法的流程示意图；

图 3A 是本发明实施例提供的第一种数据包的结构示意图；

图 3B 是本发明实施例提供的第二种数据包的结构示意图；

图 4 是本发明实施例提供的协议数据单元的结构示意图；

图 5 是本发明实施例提供的一种协议栈与封装包的示意图；

图 6A 是本发明实施例提供的第一种第一设备和第二设备向策略控制器获取安全策略的交互图；

图 6B 是本发明实施例提供的第二种第一设备和第二设备向策略控制器获取安全策略的交互图；

图 6C 是本发明实施例提供的第三种第一设备和第二设备向策略控制器获取安全策略的交互图；

图 6D 是本发明实施例提供的第四种第一设备和第二设备向策略控制器获取安全策略的交互图；

图 7 是本发明实施例提供的一种第一设备和第二设备向认证服务网元获取至少一个密钥的方法的交互图；

图 8 是本发明实施例提供的一种封装表头的示意图；

图 9 是本发明实施例提供的一种外部 IP 表头的示意图；

图 10 是本发明实施例提供的一种会话占据空口资源的示意图；

图 11 是本发明实施例提供的一种会话占据无线承载的示意图；

图 12 是本发明实施例提供的一种第一设备的结构示意图；

图 13 是本发明实施例提供的第一种第一设备的获取模块的结构示意图；

图 14 是本发明实施例提供的第二种第一设备的获取模块的结构示意图；

图 15 是本发明实施例提供的一种第二设备的结构示意图；

图 16 是本发明实施例提供的第一种第二设备的获取模块的结构示意图；

图 17 是本发明实施例提供的第二种第二设备的获取模块的结构示意图；

图 18 是本发明实施例提供的一种策略控制器的结构示意图；

图 19 是本发明实施例提供的一种第一设备的结构示意图；

图 20 是本发明实施例提供的一种第一设备的结构示意图；

图 21 是本发明实施例提供的一种第二设备的结构示意图；

图 22 是本发明实施例提供的一种策略控制器的结构示意图。

具体实施方式

为便于方案理解，下面首先结合相关附图来举例介绍下本申请实施例的方案可能应用到的网络架构。如图 1 所示，未来的移动通信的网络架构包括终端设备 110、接入网节点 120 以及用户面节点 130。其中，终端设备 110 通过接入网节点 120 接入运营网络，从而实现与用户面节点 130 进行通信。

终端设备 110 为逻辑实体，具体可以是用户设备（User Equipment），通信设备（Communication Device）物联网（Internet of Things, IoT）设备中的任意一种。其中，用户设备可以是智能手机（smart phone）、智能手表（smart watch）、智能平板等等。通信设备可以是服务器、网关（Gateway, GW）、基站以及控制器等等。物联网设备可以是传感器，电表以及水表等等。

接入网节点 120（access node, AN）可以是无线接入点，例如：基站、Wi-Fi 接入点（Wireless Fidelity, 无线保真）以及蓝牙接入点等等，也可以是有线接入点，例如：网关，调制解调器，光纤接入，IP 接入等等。

用户面节点 130 可以是网关、服务器、控制器、用户面功能网元，或者终端设备。用户面节点 130 可以设置在运营网内部，也可以设置在运营网外部。应理解，在图 1 中将用户面节点 130 设置于运营网外部只是作为一种示例，不应构成具体的限定。同时，在实际应用中，用户面节点 130 可以是终端设备，也可以是网关、服务器、控制器、用户面功能网元之类的控制网元。应理解，在图 1 中使用终端设备来代表用户面节点 130 只是作为一种示例，不应构成具体的限定。

运营商网络中包括：策略控制器 140（Policy Control Function, PCF）以及密钥管理中心（Key Management System, KMS）150 等等。其中，

策略控制器 140，用于管理网络中的安全策略，PCF 可以作为一个独立的逻辑功能实体单独部署，也可以集合在移动性管理（Mobility Management, MM）网元、会话管理网元（Session Management, SM），认证服务控制器（Authentication Server Function, AUSF），策略和计费规则功能（Policy charging and rules function, PCRF），移动性管理实体（Mobility Management Entity, MME），归属签约用户服务器（Home Subscriber Server, HSS），鉴权中心（Authentication Center, AuC），认证信任状存储和处理功能网元（Authentication Credential Repository and Processing Function, ARPF），安全上下文管理网元（Security Context Management Function, SCMF），接入与移动管理功能网元（Access and Mobility management Function, AMF），接入节点（Access network, AN），用户面节点（User plane function, UPF）等设备中。

密钥管理中心 150（英文：Key Management System，简称：KMS），负责密钥的生成、管理和协商。KMS 可以作为一个独立的逻辑功能实体单独部署，也可以集合在移动性管理（Mobility Management, MM）网元、会话管理网元（Session Management, SM）、认证服务控制器（Authentication Server Function, AUSF），安全锚点功能网元（Security Anchor Function, SEAF），移动性管理实体（Mobility Management Entity, MME），归属签约用户

服务器 (Home Subscriber Server, HSS), 鉴权中心 (Authentication Center, AuC), 认证信任状存储和处理功能网元 (Authentication Credential Repository and Processing Function, ARPF), 安全上下文管理网元 (Security Context Management Function (SCMF), 接入与移动管理功能网元 (Access and Mobility management Function, AMF), 接入节点 (Access network, AN), 用户面节点 (User plane function, UPF), 认证单元 (英文: Control Plane-Authentication Unit, 简称: CP-AU) 等设备中。后续可以称执行该密钥管理中心的功能的物理实体为密钥管理设备。

其中, 移动性管理网元用于对终端设备位置信息、安全性以及业务连续性方面进行管理, 后续可以直接称执行该移动性管理网元的功能的物理实体为移动性管理设备或者 MM。

会话管理网元用于执行会话、切片、流 flow 或者承载 bearer 的建立和管理, 后续可以称执行该会话管理网元的功能的物理实体为会话管理设备或者 SM。其中切片、流 flow 或者承载 bearer 的建立和管理由移动性管理网元负责。

认证服务控制器, 负责密钥的生成、管理和协商。AUSF 可以作为一个独立的逻辑功能实体单独部署, 也可以集合在移动性管理 (Mobility Management, MM) 网元、会话管理网元 (英文: Session Management, 简称: SM) 等设备中。

移动性管理实体用于接入控制, 包括安全和许可控制, 移动性管理, 附着与去附着, 会话管理功能, 以及当用户有数据业务请求时, 选择一个数据网关或者服务网关, 将用户的数据转发出去等等。

归属签约用户服务器用于管理和调用用户数据库。它包含用户身份, 用户配置文件, 其中用户配置文件包括用户的根密钥信息, 还可能包含用户的预置安全能力和参数等内容。HSS 主要负责管理用户的签约数据及移动用户的位置信息。

鉴权中心用于存储鉴权算法和密钥, 保证各种保密参数的安全性, 向归属用户位置寄存器 (HLR、HSS、ARPF、MME、或者 AUSF) 提供鉴权参数。

认证信任状存储和处理功能网元用于密钥的管理、生成和认证的处理。

安全上下文管理网元用于安全上下文的管理, 包括密钥的管理、生成和分发。

接入与移动管理功能网元 (Access and Mobility management Function, AMF), 负责接入控制和移动性管理。

需要说明的是, 图 1 中体现的是各个网元之间的逻辑关系, 在实际中, 有些网元可以单独部署, 也可以两两或多个网元集成部署在一个实体中。例如, SM 和 MM 部署在一个实体中; 或者 SM 与 MM 分别部署在不同的实体中; 或者 AMF 与 SEAF 部署在一起。

基于图 1 的架构, 为了实现对于端 (第一设备) 到端 (第二设备) 的安全性保护, 本发明实施例提出了一种安全实现方法。其中, 当所述第一设备为终端设备时, 所述第二设备为接入网节点或者用户面节点; 当所述第一设备为接入网节点或者用户面节点时, 所述第二设备为终端设备。如图 2 所示, 本发明实施例提供的安全实现方法包括如下步骤:

210: 第一设备获取会话的安全策略以及至少一个密钥。

220: 第二设备获取会话的安全策略以及至少一个密钥。

在本发明实施例中, 会话具有唯一的会话标识, 即, 会话标识用于识别会话的身份。

会话标识可以是终端设备、接入网节点、移动性管理网元、会话管理网元和策略控制器中的任意一种生成的。其中，当会话标识是终端设备所生成时，会话标识在终端设备准备新建会话时生成；当会话标识是接入网节点、移动性管理网元、会话管理网元和策略控制器中的任意一种生成时，会话标识在接入网节点、移动性管理网元、会话管理网元和策略控制器中的任意一种接收到其他网元发送的请求时生成。会话标识可以是新建的标识，也可以复用其他的标识，例如，空口标识、无线承载标识、切片标识、空口资源标识、设备永久标识、设备临时标识、用户永久标识、用户临时标识等等中的任意一种。

在本发明实施例中，安全策略用于指示会话的保护方式，例如，指示需要对会话的哪种或者哪几种安全性进行保护。会话的安全策略除了用于指示需要对会话的哪种或者哪几种安全性进行保护之外，还可以指示每种安全性保护采用的安全性算法、使用的密钥长度以及密钥更新时间中的至少一个。

在本发明实施例中，会话的安全性包括加密性、完整性和不可否认性等等。其中，会话的加密性是指会话通过算法进行处理之后，成为不可阅读的密文，达到避免会话数据被非法窃取、阅读的目的。会话的完整性是指会话数据在传输过程中没有被非法添加、删除、替换等。会话的不可否认性是指会话通话双方不能否认自己发送会话的行为和会话的内容。会话的安全性保护是通过安全性算法使用所述至少一个密钥对会话进行处理实现的。

在本发明实施例中，安全性算法可以是 null、AES、Snow 3G、ZUC 等等算法中的任意一种，其中 null 代表空算法。密钥长度可以是 64 位、96 位、128 位、192 位、和 256 位等等长度中的任意一种。密钥更新时间可以是 6 小时、12 小时、24 小时和 48 小时等等时间中的任意一种。上述安全算法、密钥长度以及密钥更新时间只是作为一种举例说明，不应构成对本申请的限定。

可以理解，会话的多个安全性保护可以采用相同的安全性算法、相同的密钥以及相同的密钥更新时间对会话进行处理实现，也可以采用不同的安全性算法、采用不同的密钥和采用不同的密钥更新时间对会话进行处理实现。例如，在一具体的实施例中，当对会话的加密性和完整性进行保护时，对于加密性，采用的安全性算法为 Snow 3G 算法，密钥长度为 64 位，密钥更新时间为 6 小时，对于完整性，采用的安全性算法为 Snow 3G 算法，密钥长度为 64 位，密钥更新时间为 6 小时。在另一具体的实施例中，当对会话的加密性和完整性进行保护时，对于加密性，采用的安全性算法为 Snow 3G 算法，密钥长度为 64 位，密钥更新时间为 6 小时，对于完整性，采用的安全性算法为 ZUC 算法，密钥长度为 128 位，密钥更新时间为 12 小时。

在一具体的实施例中，会话的保护方式包括以下三种：通过第一安全性算法使用第一密钥对会话数据的第一安全性进行保护，以及，通过第二安全性算法使用第二密钥对会话数据的第二安全性进行保护，以及，同时通过第一安全性算法使用第一密钥对会话数据的第一安全性进行保护以及通过第二安全性算法使用第二密钥对会话数据的第二安全性进行保护。密钥长度包括第一密钥长度和/或第二密钥长度。其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。第一密钥长度和第二密钥长度可以是相同的，也可以是不同的。密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间。其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所

述第二密钥更新时间用于表征所述第二密钥的更新时间。第一密钥更新时间和第二密钥更新时间可以是相同的，也可以是不相同的。这里，会话的第一安全性是指会话的加密性，会话的第二安全性是指会话的完整性。相应地，第一安全性算法是指 null、3DES、AES、snow 3G、Blowfish、Serpent、ZUC、HC-256 以及 Grain 等等算法中的任意一种。第二安全性算法是指 null、AES、ZUC、Snow 3G、HMAC、OMAC、CBC-MAC、PMAC、UMAC 以及 VMAC 等等算法中的任意一种。第一安全性算法与第二安全性算法可以是相同的，也可以是不同的。

基于上述陈述可知，会话的安全策略内容可能性包括但不限于：算法标识、密钥长度以及密钥更新时间中的至少一项。

采用第一算法标识和第二算法标识分别表示第一安全性采用的安全算法和第二安全性采用的安全算法。或者，当第一安全性采用的安全算法与第二安全性采用的算法不相同，算法标识包括第一算法标识以及第二算法标识，其中，第一算法标识用于表征第一安全性采用的安全算法，第二算法标识用于表征第二安全性算法采用的安全算法；当第一安全性采用的安全算法与第二安全性采用的安全算法相同时，算法标识可以包括第一算法标识以及第二算法标识，并且，第一算法标识与第二算法标识相同，或者，仅采用一个算法标识表示第一安全性采用的安全算法和第二安全性采用的安全算法，此时第一安全性采用的安全算法和第二安全性采用的安全算法采用相同的安全算法。

采用第一密钥长度和第二密钥长度分别表示第一安全性采用的密钥的长度和第二安全性采用的密钥的长度。或者，当第一安全性的安全算法采用的密钥与第二安全性的算法采用的密钥的长度不相同，密钥长度包括第一密钥长度以及第二密钥长度，其中，第一密钥长度用于表示第一安全性的安全算法采用的密钥的长度，第二密钥长度用于表示第二安全性的安全算法采用的密钥的长度；当第一安全性的安全算法采用的密钥与第二安全性的算法采用的密钥的长度相同时，密钥长度可以包括第一密钥长度以及第二密钥长度，并且，第一密钥长度与第二密钥长度相同，或者，仅采用一个密钥长度表示第一安全性采用的密钥的长度和第二安全性采用的密钥的长度，此时第一安全性采用的密钥的长度和第二安全性采用的密钥的长度相同。

采用第一密钥更新时间和第二密钥更新时间分别表示第一安全性的安全算法采用的密钥的更新时间和第二安全性的安全算法采用的密钥的更新时间。或者，当第一安全性的安全算法采用的密钥与第二安全性的算法采用的密钥的更新时间不相同，密钥更新时间包括第一密钥更新时间以及第二密钥更新时间，其中，第一密钥更新时间用于表示第一安全性的安全算法采用的密钥的更新时间，第二密钥长度用于表示第二安全性的安全算法采用的密钥的更新时间；当第一安全性的安全算法采用的密钥与第二安全性的算法采用的密钥的更新时间相同时，密钥更新时间可以包括第一密钥更新时间以及第二密钥更新时间，并且，第一密钥更新时间与第二密钥更新时间相同，或者，仅采用一个密钥更新时间表示第一安全性的安全算法采用的密钥的更新时间和第二安全性的安全算法采用的密钥的更新时间，此时第一安全性的安全算法采用的密钥的更新时间和第二安全性的安全算法采用的密钥的更新时间相同。

更进一步地，会话的安全策略内容还可以额外设置第一比特以及第二比特，其中，第一比特用于表示是否需要进行第一安全性保护，第二比特用于表示是否需要进行第二安全性保护。例如，当第一比特为“0”时，用于表示不需要进行第一安全性保护，当第一比特为“1”时，用于表示需要进行第一安全性保护。当第二比特为“0”时，用于表示不需要进行第二安全性保护，当第二比特为“1”时，用于表示需要进行第二安全性保护。

安全策略格式包含多种形式，在一具体的实施例中，安全策略的格式如下：安全策略=比特 1||第一安全性算法标识||第一密钥长度||第一密钥更新时间||比特 2||第二安全性算法标识||第二密钥长度||第二密钥更新时间比特，其中，比特 1 为 0 时，表示不需要对第一安全性进行保护，比特 1 为 1 时，表示需要对第一安全性进行保护，第一安全性算法标识用于表征所采用的第一安全性算法，比特 2 为 0 时，表示不需要对第二安全性进行保护，比特 2 为 1 时，表示需要对第二安全性进行保护，第二安全性算法标识用于表征所采用的第二安全性算法。或者，其中一种方式为，安全策略=第一安全性算法标识||第一密钥长度||第二安全性算法标识||第二密钥长度。或者其中一种方式为，安全策略=第一安全性算法标识||第二安全性算法标识||密钥长度，此时两个安全性的密钥长度相同。

在本发明实施例中，安全策略可以是空口安全策略或者会话安全策略。当安全策略用于保护终端设备与接入网节点之间（包括上行和下行）的安全性时，安全策略为空口安全策略，当安全策略用于保护终端设备与用户面节点之间（包括上行和下行）的安全性时，安全策略为会话安全策略。其中，核心网安全策略包括会话安全策略以及空口安全策略。

在本发明实施例中，第一设备和第二设备获取到的安全策略和至少一个密钥均是相同的。例如，第一设备获取到的安全策略为“比特 1||第一安全性算法标识||第一密钥长度||第一密钥更新时间||比特 2||第二安全性算法标识||第二密钥长度||第二密钥更新时间比特”，第二设备获取到的安全策略也为“比特 1||第一安全性算法标识||第一密钥长度||第一密钥更新时间||比特 2||第二安全性算法标识||第二密钥长度||第二密钥更新时间比特”。第一设备获取到的至少一个密钥为“0011 0011 1011 1101”，则第二设备获取到的至少一个密钥为“0011 0011 1011 1101”。

在本发明实施例中，第一设备和第二设备可以向策略控制器获取安全策略，并且，第一设备和第二设备可以向认证服务网元获取至少一个密钥。其中，第一设备和第二设备向策略控制器获取安全策略的方法，以及，第一设备和第二设备向认证服务网元获取至少一个密钥的方法将在下文中详细介绍，此处先不展开描述。

可以理解的是，第一设备和第二设备除了可以向策略控制器获取安全策略之外，还可以向其他的网元获取安全策略。例如，策略控制器曾经将安全策略发送给第三方网元，则第一设备和第二设备可以向第三方网元获取安全策略。或者，策略控制器已经向第二设备发送了安全策略，则第一设备可以直接向第二设备请求安全策略。

230: 第一设备根据会话的安全策略使用至少一个密钥对会话的会话数据进行安全性保护，从而获得保护数据。

在本发明实施例中，保护数据可以是表头（head）数据、负载（payload）数据、数据包（packet）中的任意一种。其中，表头数据用于记载会话数据的相关信息，负载数据用于记载真正的会话数据，数据包包括表头数据以及负载数据。即，保护数据可以是数据包

的一部分或者全部。第一设备只对表头数据或者负载数据进行安全性保护,既可以实现对会话的安全性保护,又能避免对整个数据包进行安全性保护所导致的巨大计算量。而且,在通常情况下,表头数据的数据量远小于数据包的数据量,只对表头数据进行安全性保护更能大大减轻进行安全性保护的计算量。第一设备对整个数据包进行安全性保护,能够加大破解的难度,提高安全性保护的可靠性。在实际使用中,可以根据需要选择对表头数据、负载数据或者数据包进行安全性保护。

在一些可选的实施例,如图 3A 以及图 3B 所示,保护数据还包括参数字段,所述参数字段包括第一标识字段、第二标识字段、第三标识字段至少一个。其中,所述第一标识字段用于指示本消息为会话消息。所述第二标识字段用于指示业务标识、会话标识、承载标识、流(flow)标识以及切片标识中的至少一个。所述第三标识用于指示所述会话的保护方式。所述参数字段还包括计数器,此外,还可以包括长度字段、填充字段、MAC 字段中以及算法更新时间字段的至少一个,其中,计数器用于指示数据包的序列号。所述长度字段用于指示所述参数字段的长度,或者,整个数据包的长度,或者 payload 的长度。所述填充字段用于加密时,填充字段满足加密算法对消息长度的要求。所述 MAC 字段为数据完整性保护之后的完整性保护参数。所述算法更新时间字段用于指示算法更新的时间。当保护数据为数据包时,保护数据的格式可以如图 3A 所示,当保护数据为负载时,保护数据的格式可以如图 3B 所示。其中,图 3A 和图 3B 所示的保护数据的格式只是一种举例说明,不应构成对本发明实施例的具体限定。

应理解的,保护数据实质上均是协议数据单元(Protocol Data Unit, PDU)。图 4 示出了一种可能的保护数据 PDU。如图 4 所示,一个 PDU 包括:一个 PDU 头部(PDU header),零个或多个服务数据单元(Service Data Unit, SDU),零个或多个信息控制单元(Control element),可能还有填充位(padding)。其中,一个 PDU 头部可能有一个或多个子头部(subheader),一个子头部由六个域(R/R/E/LCID/F/L)或者四个域(R/R/E/LCID)组成。

本发明实施例中,在保护数据中添加参数字段的具体方式可如下:

在一种可能的实现方式中,所述第一设备可以通过在 PDU 中增加一个或多个信息控制单元(由本协议层产生),利用增加的信息控制单元来承载参数字段。应理解,参数字段可以承载在一个信息控制单元中,也可以分别承载在不同的信息控制单元中。

在另一种可能的实现方式中,所述第一设备可以通过在保护数据中的一个或多个 SDU(由上一层协议层产生)中携带的参数字段。由于 SDU 来自上层,因此,所述第一设备可以在上层消息中添加所述参数字段。应理解,参数字段可以承载在一个 SDU 中,也可以分别承载在不同的 SDU 中。当参数字段承载在多个 SDU 中时,可以承载在连续的多个 SDU 中,也可以承载在不连续的多个 SDU 中。上述的例子是以 PDU 为例进行说明,在实际使用中还可以是 IP 包、以太网包或者其他的非 IP 包,本发明不作具体限定。

可以理解的是,计数器是必选的参数字段,长度字段是可选的参数字段,当安全策略包括加密性保护时,分组字段是可选的参数字段,当安全策略包括完整性保护时,MAC 字段是必选的参数字段,算法更新时间字段是可选的参数字段。

240: 第一设备将保护数据发送给第二设备。

在本发明实施例中,如果第一设备为终端设备,第二设备为接入网节点,则第一设备

将保护数据发送给第二设备时,需要经过终端设备—接入网节点的传输链路。如果第一设备为终端设备,第二设备为用户面节点,则第一设备将保护数据发送给第二设备时,需要经过终端设备—接入网节点—用户面节点的传输链路。数据包是保护数据进行传输基本单元,为了使数据包能够在对应的协议栈进行传输,需要按照协议栈将数据包封装成符合协议栈格式的封装包。其中,传输协议栈可以为 LTE 中的协议栈格式,包括 MAC (Media Access Control 媒体接入控制),RLC(Radio Link Control 无线链路控制),和 PDCP(Packet Data Convergence Protocol -- 分组数据汇聚层协议)层;也可能为下一代移动通信的协议栈格式,此处不做限制。例如,为了使数据包能够在终端设备—接入网节点的传输链路进行传输,需要按照协议栈将数据包封装成如图 5 左边所示的格式的封装包。如图 5 左边所示,封装包包括 L1 表头(L1 header)、传输协议栈(AN protocol stacks)表头、数据包。其中,数据包包括 PDU 表头(PDU header)以及 PDU 负载(PDU payload)。为了使数据包能够在接入网节点—用户面节点的传输链路进行传输,需要按照协议栈将数据包封装成如图 5 右边所示的格式的封装包。如图 5 右边所示,封装包包括 L1/L2 表头(L1/L2 header)、外部 IP 表头(outer IP header)、封装表头(encapsulate header)、PDU 表头以及数据包。其中,数据包包括(PDU header)以及 PDU 负载(PDU payload)。

250: 第二设备接收第一设备发送的会话的保护数据。

260: 第二设备确定会话的会话标识,并根据会话的会话标识识别出第一设备发送的会话的保护数据。

在本发明实施例中,当第二设备为接入网节点时,第二设备确定会话的会话标识的方式不同于当第二设备为用户节点时,第二设备确定会话的会话标识的方式。当第二设备为接入网节点时,第二设备确定会话的会话标识的方式以及当第二设备为用户节点时,第二设备确定会话的会话标识的方式将在下文中具体进行介绍,此处暂不展开描述。

可以理解的是,会话标识的确定方法与发送给第二设备的封装包的格式相关,具体请参考下文,此处暂不展开描述。

270: 第二设备根据所述会话的安全策略使用所述至少一个密钥对保护数据进行还原以获得会话数据,和/或进行完整性检验。

需要说明的是,本申请中所述端到端的通信的保护包括会话的端到端的保护,也包括基于切片、流 flow 或者承载 bearer 的端到端的保护。例如,切片流程中,第二设备可以为切片中的用户面处理网元。

下面结合图 6A-6D 说明本发明实施例提供的几种主要的第二设备向策略控制器获取安全策略的实施方式。

在第一种方式中,如图 6A 所示,当第一设备为终端设备,第二设备为接入网节点时,第一设备和第二设备向策略控制器获取安全策略的方法包括如下步骤:

310: 第一设备向第二设备发送第一请求,其中,第一请求包括第一设备标识、第一设备安全能力、业务安全需求,第一请求还可以选择性包括业务标识等等。相应地,第二设备接收第一设备发送的第一请求。

在本发明实施例中,第一设备标识用于表征发出第一请求的第一设备或用户的身份。

例如：第一设备标识可以是媒体访问控制（Media Access Control, MAC）地址、网络协议（Internet Protocol, IP）地址、手机号码、国际移动设备标识（International Mobile Equipment Identity, IMEI）、国际移动用户识别码（International Mobile Subscriber Identity, IMSI）、IP 多媒体私有标识（IP Multimedia Private Identity, IMPI）、临时移动用户标识符（Temporary Mobile Subscriber Identity, TMSI）、IP 多媒体公共标识（IP Multimedia Public Identity, IMPU）、全球唯一临时 UE 标识（Globally Unique Temporary UE Identity, GUTI）等等。

在本发明实施例中，第一设备安全能力用于表征第一设备可以支持的安全性算法，可以支持的密钥长度以及可以支持的密钥更新周期中的至少一种。可以理解的是，不同设备的存储容量，运算速度各不相同，所以，不同设备支持的安全性算法、支持的密钥长度以及支持的密钥更新周期各不相同。例如，IoT 设备的存储容量不大，运算速度也不高，不能支持复杂度较高的安全性算法，智能手机的存储容量大，运算速度也比较高，可以支持复杂度较高的安全性算法。故此，第一设备需要将第一设备安全能力告知策略控制器，以便于策略控制器结合第一设备安全能力生成安全策略。

在本发明实施例中，业务安全需求用于表征业务可接受的安全性算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。可以理解的是，不同业务对于安全性算法、密钥长度以及密钥更新周期的要求是不相同的。例如，金融业务对于安全性算法的要求比较高，而视频下载业务对于安全性算法的要求比较低。故此，第一设备需要将业务安全需求告知策略控制器，以便于策略控制器结合业务安全需求生成安全策略。

在本发明实施例中，第一请求可以是接入请求，也可以是会话请求。其中，接入请求功能包括但不限于以下描述：用于触发随机接入过程，以使得第一设备通过随机接入过程接入到运营网络中去。在随机接入过程之前，第一设备处于 RRC 空闲态（RRC_IDLE）。经过所述初始随机接入过程之后，第一设备从 RRC 空闲态（RRC_IDLE）转移到 RRC 连接态（RRC_CONNECTED）。会话请求用于请求在第一设备和第二设备之间建立会话。例如，会话是通过会话建立协议建立的，此时，会话请求即为会话建立请求信令。

320：第二设备向策略控制器发送第二请求。其中，第二请求包括第一设备标识、第一设备安全能力、业务安全需求以及接入网节点安全能力。相应地，策略控制器接收第二设备发送的第二请求。

在本发明实施例中，第二请求除了包括第一请求中的第一设备标识、第一设备安全能力、业务安全需求之外，还包括接入网节点安全需求。可以理解，如果第一请求中还包括业务标识，则第二请求中同样还包括业务标识。第二请求是基于第一请求生成的，所以，当第一请求为接入请求时，第二请求也同样为接入请求；当第一请求为会话请求时，第二请求也同样为会话请求。也可能，第一请求为接入请求，第二请求为会话请求。可以理解，第一请求和第二请求的具体命名不做限制。

在本发明实施例中，接入网节点安全能力用于表征接入网节点可提供的安全性算法、可提供的密钥长度和可提供的密钥更新周期中至少一项。可以理解的是，不同接入网节点的存储容量，运算速度各不相同，所以，不同接入网节点支持的安全性算法、支持的密钥长度以及支持的密钥更新周期各不相同。例如，当接入网节点是 Wi-Fi 热点时，Wi-Fi 热点不能支持复杂度较高的安全性算法。当接入网节点是基站时，基站能够支持复杂度较高的

安全性算法。

330: 策略控制器基于第二请求生成空口安全策略。

在本发明实施例中, 策略控制器可以根据第一设备安全能力、业务安全需求以及接入网节点安全能力生成空口安全策略; 也可以仅根据业务安全需求以及接入网节点安全能力中的至少一个生成空口安全策略。

进一步地, 策略控制器还可以结合预制安全能力生成空口安全策略。其中, 预制安全能力是 AUSF 或者 Authentication Credential Repository and Processing Function (ARPF) 根据策略控制器发送的第一设备标识和/或业务标识返回给策略控制器的。

进一步地, 策略控制器还可以结合服务器的安全需求生成空口安全策略。其中, 服务器的安全需求是服务器根据策略控制器发送的第一设备标识和/或业务标识返回给策略控制器的。服务器是为终端设备提供服务的设备。所述服务器包括但不限于应用程序服务器、打印服务器、Web 服务器、FTP 服务器、电子商务服务器、数据库服务器、实时通讯服务器、文件服务器以及邮件服务器等等。

在一具体的实施例中, 具体地, 依据以下预设规则确定空口安全策略: 依据一个或多个安全需求的内容确定安全策略。如果仅根据一个安全需求的内容确定安全策略, 则安全策略的内容与这一个安全需求的内容相同。如果依据多个安全需求的内容确定安全策略, 则可以遵循以下原则:

第一、遵循安全性更高的原则, 确定安全策略, 即: 将多个安全需求的内容中安全性更高的内容, 作为安全策略的内容。

例如, 安全需求 1 的内容中, 保护密钥长度为 64, 而安全需求 2 的内容中的保护密钥长度为 128, 则安全策略的保护密钥长度采用 128。

第二、遵循更节省资源的原则, 确定安全策略, 即: 将多个安全需求的内容中更节省资源的内容, 作为安全策略的内容。例如, 每一个安全需求的内容都包括加密算法, 而部分安全需求的内容的完整性保护算法为 null, 则安全策略的内容包括加密算法, 而不包括完整性保护算法。

第三、遵循安全需求的优先级, 确定安全策略。即: 如果某个安全需求中规定了算法优先级, 则以此算法优先级做安全算法协商的基础; 选择的最终算法为所有安全需求都支持的算法, 并且此算法优先级最高, 以此作为安全策略的内容。

或者, 依据某个安全需求优先级为主, 进行安全策略的协商, 例如, 根据安全需求 2 中规定了几种加密算法的优先级, 则按照此优先级规定, 确定安全策略中采用哪种加密算法。

或者, 多个安全需求都规定了算法的优先级, 此时可以某个安全需求的算法优先级为主, 例如, 根据安全需求 2 的优先级为主优先级。

340: 策略控制器向第二设备返回空口安全策略。相应地, 第二设备接收策略控制器发送的空口安全策略。

350: 第二设备向第一设备返回空口安全策略。相应地, 第一设备接收第二设备发送的空口安全策略。

在第二种方式中，如图 6B 所示，当第一设备为终端设备，第二设备为接入网节点时，第一设备和第二设备向策略控制器获取安全策略的方法包括如下步骤：

410：第一设备向第二设备发送第一请求，其中，第一请求包括第一设备标识、第一设备安全能力、业务安全需求，第一请求还可以选择性包括业务标识等等。相应地，第二设备接收第一设备发送的第一请求。

在本发明实施例中，第一设备标识用于表征发出第一请求的第一设备或用户的身份。例如：第一设备标识可以是媒体访问控制（Media Access Control，MAC）地址、网络协议（Internet Protocol，IP）地址、手机号码、国际移动设备标识（International Mobile Equipment Identity，IMEI）、国际移动用户识别码（International Mobile Subscriber Identity，IMSI）、IP 多媒体私有标识（IP Multimedia Private Identity，IMPI）、临时移动用户标识符（Temporary Mobile Subscriber Identity，TMSI）、IP 多媒体公共标识（IP Multimedia Public Identity，IMPU）、全球唯一临时 UE 标识（Globally Unique Temporary UE Identity，GUTI）等等。

在本发明实施例中，第一设备安全能力用于表征第一设备可以支持的安全性算法，可以支持的密钥长度以及可以支持的密钥更新周期中的至少一种。可以理解的是，不同设备的存储容量，运算速度各不相同，所以，不同设备支持的安全性算法、支持的密钥长度以及支持的密钥更新周期各不相同。例如，IoT 设备的存储容量不大，运算速度也不高，不能支持复杂度较高的安全性算法，智能手机的存储容量大，运算速度也比较高，可以支持复杂度较高的安全性算法。故此，第一设备需要将第一设备安全能力告知策略控制器，以便于策略控制器结合第一设备安全能力生成安全策略。

在本发明实施例中，业务安全需求用于表征业务可接受的安全性算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。可以理解的是，不同业务对于安全性算法、密钥长度以及密钥更新周期的要求是不相同的。例如，金融业务对于安全性算法的要求比较高，而视频下载业务对于安全性算法的要求比较低。故此，第一设备需要将业务安全需求告知策略控制器，以便于策略控制器结合业务安全需求生成安全策略。

在本发明实施例中，第一请求可以是接入请求，也可以是会话请求。其中，接入请求功能包括但不限于以下描述：用于触发随机接入过程，以使得第一设备通过随机接入过程接入到运营网络中去。在随机接入过程之前，第一设备处于 RRC 空闲态（RRC_IDLE）。经过所述初始随机接入过程之后，第一设备从 RRC 空闲态（RRC_IDLE）转移到 RRC 连接态（RRC_CONNECTED）。会话请求用于请求在第一设备和第二设备之间建立会话。例如，会话是通过会话建立协议建立的，此时，会话请求即为会话建立请求信令。

420：第二设备向会话管理网元发送第二请求。其中，第二请求包括第一设备标识、第一设备安全能力、业务安全需求以及接入网节点安全能力。相应地，会话管理网元接收第二设备发送的第二请求。

在本发明实施例中，第二请求是基于第一请求生成的。当第一请求为接入请求时，第二请求也同样为接入请求；当第一请求为会话请求时，第二请求也同样为会话请求。也可能，第一请求为接入请求，第二请求为会话请求。可以理解，第一请求和第二请求的具体命名不做限制。第二请求除了包括第一请求中的第一设备标识、第一设备安全能力、业务安全需求之外，还包括接入网节点安全需求。可以理解，如果第一请求中还包括业务标识，

则第二请求中同样还包括业务标识。可以理解，第一请求和第二请求的具体命名不做限制。

在本发明实施例中，接入网节点安全能力用于表征接入网节点可提供的安全性算法、可提供的密钥长度和可提供的密钥更新周期中至少一项。可以理解的是，不同接入网节点的存储容量，运算速度各不相同，所以，不同接入网节点支持的安全性算法、支持的密钥长度以及支持的密钥更新周期各不相同。例如，当接入网节点是 Wi-Fi 热点时，Wi-Fi 热点不能支持复杂度较高的安全性算法。当接入网节点是基站时，基站能够支持复杂度较高的安全性算法。

430: 会话管理网元向策略控制器转发第二请求。相应地，策略控制器接收会话管理网元发送的第二请求。

440: 策略控制器基于第二请求生成空口安全策略。

在本发明实施例中，策略控制器可以根据第一设备安全能力、业务安全需求以及接入网节点安全能力生成空口安全策略；也可以仅根据业务安全需求以及接入网节点安全能力中的至少一个生成空口安全策略。

进一步地，策略控制器还可以结合预制安全能力生成空口安全策略。其中，预制安全能力是 AUSF 或者 Authentication Credential Repository and Processing Function (ARPF) 根据策略控制器发送的第一设备标识和/或业务标识返回给策略控制器的。

进一步地，策略控制器还可以结合服务器的安全需求生成空口安全策略。其中，服务器的安全需求是服务器根据策略控制器发送的第一设备标识和/或业务标识返回给策略控制器的。服务器是为终端设备提供服务的设备。所述服务器包括但不限于应用程序服务器、打印服务器、Web 服务器、FTP 服务器、电子商务服务器、数据库服务器、实时通讯服务器、文件服务器以及邮件服务器等等。

在一具体的实施例中，依据以下预设规则确定空口安全策略：依据一个或多个安全需求的内容确定安全策略。如果仅根据一个安全需求的内容确定安全策略，则安全策略的内容与这一个安全需求的内容相同。如果依据多个安全需求的内容确定安全策略，则可以遵循以下原则：

第一、遵循安全性更高的原则，确定安全策略，即：将多个安全需求的内容中安全性更高的内容，作为安全策略的内容。

例如，安全需求 1 的内容中，保护密钥长度为 64，而安全需求 2 的内容中的保护密钥长度为 128，则安全策略的保护密钥长度采用 128。

第二、遵循更节省资源的原则，确定安全策略，即：将多个安全需求的内容中更节省资源的内容，作为安全策略的内容。例如，每一个安全需求的内容都包括加密算法，而部分安全需求的内容的完整性保护算法为 null，则安全策略的内容包括加密算法，而不包括完整性保护算法。

第三、遵循安全需求的优先级，确定安全策略。即：如果某个安全需求中规定了算法优先级，则以此算法优先级做安全算法协商的基础；选择的最终算法为所有安全需求都支持的算法，并且此算法优先级最高，以此作为安全策略的内容。

或者，依据某个安全需求优先级为主，进行安全策略的协商，例如，根据安全需求 2 中规定了几种加密算法的优先级，则按照此优先级规定，确定安全策略中采用哪种加密算

法。

或者，多个安全需求都规定了算法的优先级，此时可以某个安全需求的算法优先级为主，例如，根据安全需求 2 的优先级为主优先级。

450: 策略控制器向会话管理网元发送空口安全策略。相应地，会话管理网元接收策略控制器发送的空口安全策略。

460: 会话管理网元向第二设备返回空口安全策略。相应地，第二设备接收会话管理网元发送的空口安全策略。

470: 第二设备向第一设备返回空口安全策略。相应地，第一设备接收第二设备返回的空口安全策略。

在第三种方式中，如图 6C 所示，当第一设备为终端设备，第二设备为接入网节点时，第一设备和第二设备向策略控制器获取安全策略的方法包括如下步骤：

510: 第一设备向第二设备发送第一请求，其中，第一请求包括第一设备标识、第一设备安全能力、业务安全需求，第一请求还可以选择性包括业务标识等等。相应地，第二设备接收第一设备发送的第一请求。

在本发明实施例中，第一设备标识用于表征发出第一请求的第一设备或用户的身份。例如：第一设备标识可以是媒体访问控制（Media Access Control, MAC）地址、网络协议（Internet Protocol, IP）地址、手机号码、国际移动设备标识（International Mobile Equipment Identity, IMEI）、国际移动用户识别码（International Mobile Subscriber Identity, IMSI）、IP 多媒体私有标识（IP Multimedia Private Identity, IMPI）、临时移动用户标识符（Temporary Mobile Subscriber Identity, TMSI）、IP 多媒体公共标识（IP Multimedia Public Identity, IMPU）、全球唯一临时 UE 标识（Globally Unique Temporary UE Identity, GUTI）等等。

在本发明实施例中，第一设备安全能力用于表征第一设备可以支持的安全性算法，可以支持的密钥长度以及可以支持的密钥更新周期中的至少一种。可以理解的是，不同设备的存储容量，运算速度各不相同，所以，不同设备支持的安全性算法、支持的密钥长度以及支持的密钥更新周期各不相同。例如，IoT 设备的存储容量不大，运算速度也不高，不能支持复杂度较高的安全性算法，智能手机的存储容量大，运算速度也比较高，可以支持复杂度较高的安全性算法。故此，第一设备需要将第一设备安全能力告知策略控制器，以便于策略控制器结合第一设备安全能力生成安全策略。

在本发明实施例中，业务安全需求用于表征业务可接受的安全性算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。可以理解的是，不同业务对于安全性算法、密钥长度以及密钥更新周期的要求是不相同的。例如，金融业务对于安全性算法的要求比较高，而视频下载业务对于安全性算法的要求比较低。故此，第一设备需要将业务安全需求告知策略控制器，以便于策略控制器结合业务安全需求生成安全策略。

在本发明实施例中，第一请求可以是接入请求，也可以是会话请求。其中，接入请求功能包括但不限于以下描述：用于触发随机接入过程，以使得第一设备通过随机接入过程接入到运营网络中去。在随机接入过程之前，第一设备处于 RRC 空闲态（RRC_IDLE）。经过所述初始随机接入过程之后，第一设备从 RRC 空闲态（RRC_IDLE）转移到 RRC 连

接态 (RRC_CONNECTED)。会话请求用于请求在第一设备和第二设备之间建立会话。例如, 会话是通过会话建立协议建立的, 此时, 会话请求即为会话建立请求信令。

520: 第二设备向移动性管理网元发送第二请求。其中, 第二请求包括第一设备标识、第一设备安全能力、业务安全需求以及接入网节点安全需求。相应地, 移动性管理网元接收第二设备发送的第二请求。

在本发明实施例中, 第二请求是基于第一请求生成的。当第一请求为接入请求时, 第二请求也同为接入请求; 当第一请求为会话请求时, 第二请求也同为接入请求。也可能, 第一请求为接入请求, 第二请求为会话请求。可以理解, 第一请求和第二请求的具体命名不做限制。第二请求除了包括第一请求中的第一设备标识、第一设备安全能力、业务安全需求之外, 还包括接入网节点安全需求。可以理解, 如果第一请求中还包括业务标识, 则第二请求中同样还包括业务标识。可以理解, 第一请求和第二请求的具体命名不做限制。

在本发明实施例中, 接入网节点安全能力用于表征接入网节点可提供的安全性算法、可提供的密钥长度和可提供的密钥更新周期中至少一项。可以理解的是, 不同接入网节点的存储容量, 运算速度各不相同, 所以, 不同接入网节点支持的安全性算法、支持的密钥长度以及支持的密钥更新周期各不相同。例如, 当接入网节点是 Wi-Fi 热点时, Wi-Fi 热点不能支持复杂度较高的安全性算法。当接入网节点是基站时, 基站能够支持复杂度较高的安全性算法。

530: 移动性管理网元向会话管理网元转发第二请求。相应地, 会话管理网元接收移动性管理网元发送的第二请求。

540: 会话管理网元向策略控制器转发第二请求。相应地, 策略控制器接收会话管理网元发送的第二请求。

550: 策略控制器基于第二请求生成空口安全策略。

在本发明实施例中, 策略控制器可以根据第一设备安全能力、业务安全需求以及接入网节点安全能力生成空口安全策略; 也可以仅根据业务安全需求以及接入网节点安全能力中的至少一个生成空口安全策略。

进一步地, 策略控制器还可以结合预制安全能力生成空口安全策略。其中, 预制安全能力是 AUSF 或者 Authentication Credential Repository and Processing Function (ARPF) 根据策略控制器发送的第一设备标识和/或业务标识返回给策略控制器的。

进一步地, 策略控制器还可以结合服务器的安全需求生成空口安全策略。其中, 服务器的安全需求是服务器根据策略控制器发送的第一设备标识和/或业务标识返回给策略控制器的。服务器是为终端设备提供服务的设备。所述服务器包括但不限于应用程序服务器、打印服务器、Web 服务器、FTP 服务器、电子商务服务器、数据库服务器、实时通讯服务器、文件服务器以及邮件服务器等等。

在一具体的实施例中, 具体地, 依据以下预设规则确定空口安全策略: 依据一个或多个安全需求的内容确定安全策略。如果仅根据一个安全需求的内容确定安全策略, 则安全策略的内容与这一个安全需求的内容相同。如果依据多个安全需求的内容确定安全策略, 则可以遵循以下原则:

第一、遵循安全性更高的原则, 确定安全策略, 即: 将多个安全需求的内容中安全性

更高的内容，作为安全策略的内容。

例如，安全需求 1 的内容中，保护密钥长度为 64，而安全需求 2 的内容中的保护密钥长度为 128，则安全策略的保护密钥长度采用 128。

第二、遵循更节省资源的原则，确定安全策略，即：将多个安全需求的内容中更节省资源的内容，作为安全策略的内容。例如，每一个安全需求的内容都包括加密算法，而部分安全需求的内容的完整性保护算法为 null，则安全策略的内容包括加密算法，而不包括完整性保护算法。

第三、遵循安全需求的优先级，确定安全策略。即：如果某个安全需求中规定了算法优先级，则以此算法优先级做安全算法协商的基础；选择的最终算法为所有安全需求都支持的算法，并且此算法优先级最高，以此作为安全策略的内容。

或者，依据某个安全需求优先级为主，进行安全策略的协商，例如，根据安全需求 2 中规定了几种加密算法的优先级，则按照此优先级规定，确定安全策略中采用哪种加密算法。

或者，多个安全需求都规定了算法的优先级，此时可以某个安全需求的算法优先级为主，例如，根据安全需求 2 的优先级为主优先级。

560: 策略控制器向会话管理网元发送空口安全策略。相应地，会话管理网元接收策略控制器发送的空口安全策略。

570: 会话管理网元向移动性管理网元返回空口安全策略。相应地，移动性管理网元接收会话管理网元发送的空口安全策略。

580: 移动性管理网元向第二设备返回空口安全策略。相应地，第二设备接收移动性管理网元发送的第二设备。

590: 第二设备向第一设备返回空口安全策略。相应地，第一设备接收第二设备返回的空口安全策略。

在第四种方式中，如图 6D 所示，当第一设备为终端设备，第二设备为接入网节点时，第一设备和第二设备向策略控制器获取安全策略的方法包括如下步骤：

610: 第一设备向第二设备发送第一请求，其中，第一请求包括第一设备标识、第一设备安全能力、业务安全需求，第一请求还可以选择性包括业务标识等等。相应地，第二设备接收第一设备发送的第一请求。

在本发明实施例中，第一设备标识用于表征发出第一请求的第一设备或用户的身份。例如：第一设备标识可以是媒体访问控制（Media Access Control，MAC）地址、网络协议（Internet Protocol，IP）地址、手机号码、国际移动设备标识（International Mobile Equipment Identity，IMEI）、国际移动用户识别码（International Mobile Subscriber Identity，IMSI）、IP 多媒体私有标识（IP Multimedia Private Identity，IMPI）、临时移动用户标识符（Temporary Mobile Subscriber Identity，TMSI）、IP 多媒体公共标识（IP Multimedia Public Identity，IMPU）、全球唯一临时 UE 标识（Globally Unique Temporary UE Identity，GUTI）等等。

在本发明实施例中，第一设备安全能力用于表征第一设备可以支持的安全性算法，可以支持的密钥长度以及可以支持的密钥更新周期中的至少一种。可以理解的是，不同设备

的存储容量，运算速度各不相同，所以，不同设备支持的安全性算法、支持的密钥长度以及支持的密钥更新周期各不相同。例如，IoT 设备的存储容量不大，运算速度也不高，不能支持复杂度较高的安全性算法，智能手机的存储容量大，运算速度也比较高，可以支持复杂度较高的安全性算法。故此，第一设备需要将第一设备安全能力告知策略控制器，以便于策略控制器结合第一设备安全能力生成安全策略。

在本发明实施例中，业务安全需求用于表征业务可接受的安全性算法、可接受的密钥长度和可接受的密钥更新周期中至少一项。可以理解的是，不同业务对于安全性算法、密钥长度以及密钥更新周期的要求是不相同的。例如，金融业务对于安全性算法的要求比较高，而视频下载业务对于安全性算法的要求比较低。故此，第一设备需要将业务安全需求告知策略控制器，以便于策略控制器结合业务安全需求生成安全策略。

在本发明实施例中，第一请求可以是接入请求，也可以是会话请求。其中，接入请求功能包括但不限于以下描述：用于触发随机接入过程，以使得第一设备通过随机接入过程接入到运营网络中去。在随机接入过程之前，第一设备处于 RRC 空闲态 (RRC_IDLE)。经过所述初始随机接入过程之后，第一设备从 RRC 空闲态 (RRC_IDLE) 转移到 RRC 连接态 (RRC_CONNECTED)。会话请求用于请求在第一设备和第二设备之间建立会话。例如，会话是通过会话初始协议 (Session Initiation Protocol, SIP) 建立的，此时，会话请求即为 invite 信令。

620: 第二设备向策略控制器发送第一请求。其中，第二请求包括第一设备标识、第一设备安全能力以及业务安全需求。相应地，策略控制器接收第二设备发送的第二请求。

在本发明实施例中，第二请求是基于第一请求生成的。当第一请求为接入请求时，第二请求也同样为接入请求；当第一请求为会话请求时，第二请求也同样为接入请求。也可能，第一请求为接入请求，第二请求为会话请求。可以理解，第一请求和第二请求的具体命名不做限制。

630: 策略控制器基于第二请求生成核心网安全策略。

在本发明实施例中，策略控制器可以根据第一设备安全能力以及业务安全需求生成空口安全策略；也可以仅根据业务安全需求生成核心网安全策略。

进一步地，策略控制器还可以结合预制安全能力生成核心网安全策略。其中，预制安全能力是 AUSF 或者 Authentication Credential Repository and Processing Function (ARPF) 根据策略控制器发送的第一设备标识和/或业务标识返回给策略控制器的。

进一步地，策略控制器还可以结合服务器的安全需求生成核心网安全策略。其中，服务器的安全需求是服务器根据策略控制器发送的第一设备标识和/或业务标识返回给策略控制器的。服务器是为终端设备提供服务的设备。所述服务器包括但不限于应用程序服务器、打印服务器、Web 服务器、FTP 服务器、电子商务服务器、数据库服务器、实时通讯服务器、文件服务器以及邮件服务器等等。

在一具体的实施例中，具体地，依据以下预设规则确定空口安全策略：依据一个或多个安全需求的内容确定安全策略。如果仅根据一个安全需求的内容确定安全策略，则安全策略的内容与这一个安全需求的内容相同。如果依据多个安全需求的内容确定安全策略，则可以遵循以下原则：

第一、遵循安全性更高的原则，确定安全策略，即：将多个安全需求的内容中安全性更高的内容，作为安全策略的内容。

例如，安全需求 1 的内容中，保护密钥长度为 64，而安全需求 2 的内容中的保护密钥长度为 128，则安全策略的保护密钥长度采用 128。

第二、遵循更节省资源的原则，确定安全策略，即：将多个安全需求的内容中更节省资源的内容，作为安全策略的内容。例如，每一个安全需求的内容都包括加密算法，而部分安全需求的内容的完整性保护算法为 null，则安全策略的内容包括加密算法，而不包括完整性保护算法。

第三、遵循安全需求的优先级，确定安全策略。即：如果某个安全需求中规定了算法优先级，则以此算法优先级做安全算法协商的基础；选择的最终算法为所有安全需求都支持的算法，并且此算法优先级最高，以此作为安全策略的内容。

或者，依据某个安全需求优先级为主，进行安全策略的协商，例如，根据安全需求 2 中规定了几种加密算法的优先级，则按照此优先级规定，确定安全策略中采用哪种加密算法。

或者，多个安全需求都规定了算法的优先级，此时可以某个安全需求的算法优先级为主，例如，根据安全需求 2 的优先级为主优先级。

640：策略控制器向第二设备返回核心网安全策略。相应地，第二设备接收策略控制器发送的核心网安全策略。

650：第二设备结合核心网安全策略以及接入网节点的安全能力确定空口安全策略。

在本发明实施例中，接入网节点安全能力用于表征接入网节点可提供的安全性算法、可提供的密钥长度和可提供的密钥更新周期中至少一项。可以理解的是，不同接入网节点的存储容量，运算速度各不相同，所以，不同接入网节点支持的安全性算法、支持的密钥长度以及支持的密钥更新周期各不相同。例如，当接入网节点是 Wi-Fi 热点时，Wi-Fi 热点不能支持复杂度较高的安全性算法。当接入网节点是基站时，基站能够支持复杂度较高的安全性算法。

660：第二设备向第一设备返回空口安全策略。相应地，第一设备接收第二设备发送的空口安全策略。

下面结合图 7 说明本发明实施例提供的第一设备和第二设备向认证服务网元获取至少一个密钥的方法的实施方式。当第一设备是终端设备，第二设备是接入网节点时，第一设备和第二设备向认证服务网元获取至少一个密钥的方法具体包括如下步骤：

710：第一设备向第二设备发送第三请求。相应地，第二设备接收第一设备发送的第三请求。

在本发明实施例中，第三请求可以在第一设备接入网络与 MM 建立上下文的过程之前发送；可以在第一设备接入网络与 MM 建立上下文的过程中进行发送；还可以在第一设备与 AUSF 双向认证过程中进行发送。可选的，第三请求可以为接入请求。

在本发明实施例中，第三请求中包括第一设备或用户标识，第一设备标识用于表征发出第一请求的第一设备的身份。例如：第一设备标识可以是媒体访问控制（Media Access

Control, MAC) 地址、网络协议 (Internet Protocol, IP) 地址、手机号码、国际移动设备标识 (International Mobile Equipment Identity, IMEI)、国际移动用户识别码 (International Mobile Subscriber Identity, IMSI)、IP 多媒体私有标识 (IP Multimedia Private Identity, IMPI)、临时移动用户标识符 (Temporary Mobile Subscriber Identity, TMSI)、IP 多媒体公共标识 (IP Multimedia Public Identity, IMPU)、全球唯一临时 UE 标识 (Globally Unique Temporary UE Identity, GUTI) 等等。

720: 第二设备向认证节点 (例如 AUSF, 或者 SEAF 等节点) 发送第三请求。相应地, 认证节点接收第二设备发送的第三请求。

730: 第一设备与认证节点相互认证。

可选的认证方式: 认证之前, 认证节点可以向根密钥存储中心 (如 ARPF) 发送第一设备标识, 从根密钥存储中心获得认证向量。基于认证向量, 第一设备与认证节点之间完整相互认证。

在本发明实施例中, 第一设备与认证节点双向认证成功后, 第一设备以及认证节点分别得到或者经过一次或者多次推衍得到基础密钥。

认证节点发送基础密钥至 KMS。

其中 KMS 可以独立部署, 也可以与其他网元部署在一起, 例如 KMS 与认证中心, AUSF, ARPF, SEAF, SCMF, AMF, SMF, AN (第二设备), MME 等部署在一起。

740: 第一设备基于基础密钥推衍出接入密钥。

在本发明实施例中, 因为安全策略的内容中可能包括加密算法和完整性保护算法的至少一项, 所以, 可以依据安全策略计算出来一个密钥, 可用于加密和/或完整性保护, 也可能分别计算出用于加密性保护的密钥和用于完整性保护的密钥。进一步地, 还可以根据密钥是用于对空口信令进行保护, 还是用于对用户面数据进行保护, 将密钥区分为空口信令加密密钥、空口信息完整性密钥、用户面加密密钥、用户面完整性保护密钥。

在本发明实施例中, 第一设备基于第一参数, 并根据所述基础密钥推衍出中间密钥。然后, 第一设备基于第二参数, 并根据中间密钥生成至少一个密钥。其中, 第一参数包括接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识、policy set 以及切片标识中的至少一个。第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、flow 标识、切片标识、policy set 以及会话标识中的至少一项, 所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

在具体的实施例中, 第一设备基于第一参数, 并根据所述基础密钥推衍出中间密钥 K_{an} 具体为:

$K_{an} = KDF(K_{kms}, \text{接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识、policy set、会话标识以及切片标识中的至少一个})$ 。

其中, policy set 为安全策略, K_{kms} 为基础密钥, nonce1 为随机参数。

在具体的实施例中, 第一设备基于第二参数, 并根据所述中间密钥推衍出加密性密钥

K_1 具体为:

$K_1 = \text{KDF}(\text{Kan}, (\text{空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项}), \text{policy set})$ 。

或者:

$K_1 = \text{KDF}(\text{Kan}, (\text{空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项}))$ 。

或者:

$K_1 = \text{KDF}(\text{Kan}, \text{加密算法 ID}, (\text{空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项}))$ 。

或者:

$K_1 = \text{KDF}(\text{Kan}, \text{加密标识}, (\text{空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项}))$ 。

或者:

$K_1 = \text{KDF}(\text{Kan}, \text{加密算法 ID})$ 。

其中, policy set 为安全策略, Kan 为中间密钥。

如前所述, 加密标识可以为一个字符串, 用于标识此推衍的结果为加密密钥。Nonce2 为随机参数, 可以由 KMS 选择, 或者, 由第一设备携带在会话请求中, 使用随机参数计算的目的在于, 提高密钥的安全性和随机性。也可能密钥推衍中包含两个 nonce 的至少一项, 其中一个 nonce 来自 KMS (由 KMS 选择, 直接发送给第一设备, 或通过 SM 发送至第一设备), 另一个 nonce 来自第一设备 (由第一设备携带在会话请求中)。

在具体的实施例中, 第一设备基于第二参数, 并根据所述中间密钥推导出完整性密钥 K_2 具体为:

$K_2 = \text{KDF}(\text{Kan}, (\text{空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项}), \text{policy set})$ 。

或者:

$K_2 = \text{KDF}(\text{Kan}, (\text{空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项}))$ 。

或者:

$K_2 = \text{KDF}(\text{Kan}, \text{完整性保护算法 ID}, (\text{空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项}))$ 。

或者:

$K_2 = \text{KDF}(\text{Kan}, \text{完整性保护标识}, (\text{空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项}))$ 。

或者:

$K_2 = \text{KDF}(\text{Kan}, \text{完整性保护算法 ID})$ 。

完整性保护标识可以为一个字符串, 用于标识此推衍的结果为完整性保护密钥。

上述 KDF 为密钥推衍函数, 包括但不限于以下密码推衍函数: HMAC (如 HMAC-SHA256, HMAC-SHA1), NMAC, CMAC, OMAC, CBC-MAC, PMAC, UMAC

和 VMAC 以及 HASH 算法等等。另外, 由于安全策略中的需求不同, 例如, 安全策略 1 中保护密钥长度要求为 256bit; 而安全策略 2 中保护密钥长度要求为 128bit; 此时第一设备可以采用不同的密钥推衍算法, 来满足不同安全策略对于不同保护密钥长度的需求 (例如, 采用 HMAC-SHA1 来生成 128bit 的保护密钥, 采用 HMAC-SHA256 生成 256bit 保护密钥); 另外 KMS 也可能, 仅采用一个算法生成密钥, 再采用缩短 (truncate) 或延长等等的方式生成其他长度的密钥。第一设备对于密钥长度的处理, 包括但不限于上述处理方式。

可以理解, 中间密钥可以是基于所述基础密钥进行一次或者多次的推衍得到的, 所述至少一个密钥也可以是基于所述中间密钥进行一次或者多次的推衍得到的。

750: KMS 根据基础密钥推衍得到中间密钥。

在本发明实施例中, AUSF 基于第一参数, 并根据所述基础密钥推衍出中间密钥。具体请参见步骤 740, 此处不再展开赘述。

760: KMS 将中间密钥向第二设备发送。相应地, 第二设备接收 AUSF 发送的中间密钥。

770: 第二设备基于中间密钥推衍出至少一个密钥。

在本发明实施例中, 第二设备基于第二参数, 并根据所述中间密钥推衍出至少一个密钥。具体请参见步骤 740, 此处不再展开赘述。

需要说明的是, 以上实施例中, 主要以第一设备和第二设备对所述至少一个密钥推衍进行举例说明, 除此之外, 所述至少一个密钥还可以由 MM、KMS、SM、AAA 或者 Policy control 等等网元推衍得到, 本申请不作具体限定。

也可能, 第二设备向 KMS 发送请求, 其中保护空口安全策略, 由 KMS 推衍出加密密钥和完整性保护密钥, 再发送至第二设备。

下面将对本发明实施例提供的几种主要的第二设备确定会话的会话标识的实施方式。

当第二设备是用户面节点时, 第二设备确定会话的会话标识的方式包括以下几种:

在第一种实现方式中, 所述第二设备通过所述保护数据所在的封装表头确定会话的会话标识。由于封装表头内标识与会话标识存在映射关系, 所以, 第二设备根据封装表头内标识可以确定会话标识。其中, 封装表头内标识包括 QoS 标识, 隧道标识、MAC 标识的至少一项。例如, 如果封装表头为 GTP (GPRS Tunneling Protocol GPRS 隧道协议) 的封装格式, 则如图 8 所示, 封装表头包括版本 (Version)、协议 (Protocol type)、保留位 (Reserved)、扩展表头标志 (Extension Header Flag)、序列码标志 (Sequence Number Flag)、非-PDU 码标志 (N-PDU Number Flag)、消息类型 (Message Type)、消息长度 (Message length)、隧道标识 (GTP tunnel endpoint ID)、序列号码 (Sequence number)、非 PDU 号码 (N-PDU number) 以及下一个扩展表头类型 (Next extension header type)。第二设备根据封装表头中的隧道标识即可确定会话标识。

在第二种实现方式中, 所述第二设备通过所述保护数据所在的外部 IP 表头确定会话的会话标识。如图 9 所示, 外部 IP 表头包括版本 (Version)、报文长度 (Internet Header Length, IHL)、服务类型 (Type of Service, TOS)、总长度、标识、标志、段偏移量、生存期、协议、头部校验和、源地址、目的地址、可选项以及数据。其中, 源地址和/或目的地址与会

话标识存在映射关系,根据外部 IP 表头中的源地址和/或目的地址即可确定会话的会话标识。

在第三种实现方式中,所述第二设备通过所述保护数据所在的封装表头内标识和所述保护数据所在的外部 IP 表头中源地址和/或目的地址确定所述会话的会话标识。

在第四种实现方式中,所述第二设备通过所述保护数据所在的协议数据单元表头内标识和/或所述保护数据所在的封装表头内标识确定所述会话的会话标识。协议数据单元表头内标识可以为 IP 地址,MAC 地址等等其他标识的至少一项。其中,协议数据单元表头内标识与会话标识中存在映射关系,或者,封装表头内标识与会话的会话标识也存在映射关系,或者协议数据单元表头内标识和封装表头内标识一起与会话标识存在映射关系。所以,根据协议数据单元表头、封装表头即可确定会话标识。需要说明的是,协议数据单元表头与外部 IP 表头的格式相类似,具体请参阅图 9 以及相关描述。

其中,映射方法包括但不限于以下方式,所述第二设备将协议数据单元表头内标识输入过滤器,过滤器即输出会话标识。其中,过滤器能够代表协议数据单元表头内标识与会话标识之间的映射关系,即,当输入协议数据单元表头内标识至过滤器,则过滤器会输出会话标识。

在第五种实现方式中,所述第二设备通过所述保护数据中的参数字段确定所述会话的会话标识。图 3A 或者图 3B 示出了参数字段。在具体实现中,可以根据参数字段中的第二标识字段的内容确定会话标识。例如,如果参数字段中的第二标识字段是会话标识,则第二设备可以直接获取得到会话标识。如果参数字段中的第二标识字段是业务标识、承载标识、流(flow)标识以及切片标识均中的至少一个,则可以根据业务标识、承载标识、流(flow)标识以及切片标识与会话标识之间的映射关系,获得会话标识。

当第二设备是接入网节点时,第二设备确定会话的会话标识的方式包括以下几种:

在第一种实现方式中,所述第二设备通过所述会话所占用的空口资源确定所述会话的会话标识。图 10 示出了会话所占用的空口资源。具体实现中,可以通过区分会话所占用的空口资源确定会话的会话标识。例如,如图 10 所示,会话占用了时隙为 S1(图中阴影部分)的空口资源,根据会话占用的空口资源为 S1,就可以确定会话的会话标识。示例仅仅用于解释本发明实施例,不应构成限定。

在第二种实现方式中,所述第二设备通过所述会话所占用的空口的空口标识确定所述会话的会话标识。其中,空口标识可以为:空口承载标识(如信令承载标识,或者数据承载标识),空口资源标识,或者小区无线网络临时识别标识(CRNTI: Cell Radio Network Temporary Identify)等标识。由于空口标识与会话标识存在映射关系,所以,通过空口标识与会话标识的映射关系,即可确定会话标识。图 11 示出了会话所占用的数据无线承载的一种可能性,通过区分会话所占用的数据无线承载的标识即可确定会话的会话标识。如图 11 所示,会话占用了如图中阴影区域“1”、“2”以及“3”所示的资源建立数据无线承载,根据会话占用的无线承载的标识,就可以确定会话的会话标识。示例仅仅用于解释本发明实施例,不应构成限定。

在第三种实现方式中,所述第二设备通过所述保护数据中的参数字段确定所述会话的会话标识。图 3A 或者图 3B 示出了参数字段。在具体实现中,可以根据参数字段中的第二

标识字段的内容确定会话标识。例如，如果参数字段中的第二标识字段是会话标识，则第二设备可以直接获取得到会话标识。如果参数字段中的第二标识字段是业务标识、承载标识、流（flow）标识以及切片标识均中的至少一个，则可以根据业务标识、承载标识、流（flow）标识以及切片标识与会话标识之间的映射关系，获得会话标识。

上述详细阐述了本发明实施例的方法，下面提供了本发明实施例的装置。

请参见图 12，图 12 是本发明实施例提供的一种第一设备的结构示意图，该第一设备可以包括获取模块 810 以及发送模块 820，其中，各个单元的详细描述如下。

所述获取模块 810 用于获取会话的安全策略以及至少一个密钥；

所述发送模块 820 用于向第二设备发送保护数据，其中，所述保护数据是根据所述会话的安全策略使用所述至少一个密钥对所述会话的会话数据的安全性进行保护得到的，所述第二设备用于根据所述安全策略使用所述至少一个密钥对所述保护数据进行还原以获得所述会话数据；

其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

可选地，所述至少一个密钥包括：第一密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

可选地，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

可选地，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

可选地，所述密钥长度包括第一密钥长度和/或第二密钥长度，其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。

可选地，所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间，其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所述第二密钥更新时间用于表征所述第二密钥的更新时间。

可选地，所述第一安全性为加密性，所述第二安全性为完整性。

可选地，所述保护数据还包括参数字段，所述参数字段包括第一标识字段、第二标识字段、第三标识字段至少一个，其中，所述第一标识字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识、承载标识、flow 标识以及切片标识中的至少一个，所述第三标识用于指示所述会话的保护方式。

可选地，所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个，其中，所述长度字段用于指示所述参数字段的长度，所述分组字段用于指示分组进行加密时，分组的长度，所述 MAC 字段用于指示所述会话进行了完整性保护。

可选地，所述获取模块 810 具体用于向策略控制器获取所述安全策略。

可选地，如图 13 所示，所述获取模块 810 包括发送单元 811 以及接收单元 813，

所述发送单元 811 用于向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述接收单元 813 用于接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点向所述策略控制器发送第二请求获取到的，所述第二请求是所述接入网节点基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

可选地，所述发送单元 811 用于向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；所述接收单元 813 用于接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点通过至少一个网元向所述策略控制器转发第二请求获取到的，所述第二请求是所述接入网节点基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

可选地，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

可选地，所述发送单元 811 用于向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；所述接收单元 813 用于接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点根据核心网安全策略以及所述接入网节点的安全能力生成的，所述核心网安全策略是所述策略控制器根据所述接入网节点转发的第一请求生成的。

可选地，如图 14 所示，当所述第二设备为接入网节点时，所述获取模块 810 包括发送单元 812、获取单元 814 以及推衍单元 816，

所述发送单元 812 用于通过所述接入网节点向认证节点发送第三请求；

所述获取单元 814 用于基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；

所述推衍单元 816 用于基于所述基础密钥推衍出所述至少一个密钥。

可选地，所述推衍单元 816 用于根据所述基础密钥推衍出中间密钥，以及，根据所述中间密钥推衍出所述至少一个密钥。

可选地，所述推衍单元 816 用于基于第一参数，并根据所述基础密钥推衍出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

可选地，所述推衍单元 816 用于基于所述第二参数，并根据所述中间密钥推衍出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

可选地，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

可选地，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所

述表头数据以及所述负载数据。

需要说明的是，各个单元的实现还可以对应参照图 2 所示的方法实施例的相应描述。

请参见图 15，图 15 是本发明实施例提供的一种第二设备的结构示意图，该第二设备可以包括确定模块 910、获取模块 920 以及识别模块 930，其中，各个单元的详细描述如下。

所述确定模块 910 用于确定会话的会话标识；

所述获取模块 920 用于获取所述会话的安全策略以及至少一个密钥；

所述识别模块 930 用于根据所述会话标识识别第一设备发送的所述会话的保护数据，并通过根据所述会话的安全策略使用所述至少一个密钥对所述保护数据进行还原以获得会话数据，其中，所述保护数据是所述第一设备根据所述会话的安全策略使用所述至少一个密钥对所述会话数据的安全性进行保护得到的，所述第一设备用于根据所述安全策略使用所述至少一个密钥对所述会话数据进行加密以获得所述保护数据；

其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

可选地，所述至少一个密钥包括：第一密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

可选地，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

可选地，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

可选地，所述密钥长度包括第一密钥长度和/或第二密钥长度，其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。

可选地，所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间，其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所述第二密钥更新时间用于表征所述第二密钥的更新时间。

可选地，当所述第二设备为用户面节点时，所述确定模块 910 具体用于：

通过所述保护数据所在的封装表头确定会话的会话标识；或者，

通过所述保护数据所在的封装表头中的隧道标识确定会话的会话标识；或者，

通过所述保护数据所在的外部 IP 报文表头确定会话的会话标识；或者，

通过所述保护数据所在的封装表头和所述保护数据所在的外部 IP 报文表头确定所述会话的会话标识；或者，

通过所述保护数据所在的协议数据单元表头和所述保护数据所在的封装表头确定所述会话的会话标识；或者，

通过所述保护数据中的参数字段确定所述会话的会话标识。

可选地，当所述第二设备为接入网节点时，所述确定模块 910 具体用于：

通过所述会话所占用的空口资源确定所述会话的会话标识；或者，
通过所述会话所占用的空口的空口标识确定所述会话的会话标识；或者，
通过所述会话所占用的数据无线承载的标识确定所述会话的会话标识；或者，
通过所述保护数据中的参数字段确定所述会话的会话标识。

可选地，所述第一安全性为加密性，所述第二安全性为完整性。

可选地，所述参数字段包括第一标识字段、第二标识字段、第三标识字段中的至少一个，其中，所述第一标识字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识以及切片标识中的至少一个，所述第三标识用于指示所述会话的保护方式。

可选地，所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个，其中，所述长度字段用于指示所述参数字段的长度，所述分组字段用于指示分组进行加密时，分组的长度，所述 MAC 字段用于指示所述会话进行了完整性保护。

可选地，当所述第二设备为接入网节点时，所述获取模块 920 用于向第一网元获取所述安全策略，其中，所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

可选地，如图 16 所示，当所述第一网元为策略控制器时，所述获取模块 920 包括接收单元 921 以及发送单元 923。

所述接收单元 921 用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述发送单元 923 用于向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；

所述接收单元 921 用于接收所述策略控制器返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

可选地，所述接收单元 921 用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述发送单元 923 用于通过至少一个网元向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；

所述接收单元 921 用于接收所述策略控制器通过所述至少一个网元返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

可选地，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

可选地，所述接收单元 921 用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述发送单元 923 用于向所述策略控制器转发所述第一请求；

所述接收单元 921 用于接收所述策略控制器返回的核心网安全策略，并根据所述核心网安全策略以及所述接入网节点的安全能力生成所述安全策略。

可选地，如图 17 所示，当所述第二设备为接入网节点时，所述获取模块 920 包括发送单元 922、接收单元 924 以及推衍单元 926，

所述发送单元 922 用于向密钥管理中心发送第三请求；

所述接收单元 924 用于基于所述第三请求接收所述密钥管理中心返回的中间密钥，其中，所述中间密钥是基于基础密钥推衍得到的，所述基础密钥为认证节点发送给所述密钥管理中心的；

所述推衍单元 923 用于基于所述中间密钥推衍出所述至少一个密钥。

可选地，所述中间密钥是根据第一参数推衍出来的，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

可选地，所述推衍单元 923 用于基于所述第二参数，并根据所述中间密钥推衍出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

可选地，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

可选地，当所述第二设备为用户面节点时，所述获取模块 920 用于向第一网元请求所述至少一个密钥，其中，所述第一网元为所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

可选地，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

需要说明的是，各个单元的实现还可以对应参照图 2 所示的方法实施例的相应描述。

请参见图 18，图 18 是本发明实施例提供的一种策略控制器的结构示意图，该策略控制器可以包括接收模块 1110、生成模块 1120 以及发送模块 1130，其中，各个单元的详细描述如下。

所述接收模块 1110 用于接收目标网元发送的策略请求，其中，所述策略请求包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；

所述生成模块 1120 用于根据目标参数生成安全策略，其中，所述目标参数是根据所述第一请求生成的，包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；

所述发送模块 1130 用于向接入网节点发送安全策略。

可选地，所述目标参数还包括：终端设备的预制安全能力，其中，所述终端设备的预制安全能力是从认证服务控制器 AUSF 获取得到的。

可选地，所述目标参数还包括：服务器的安全需求，其中，所述服务器的安全需求是从服务器获取得到的。

可选地，所述目标网元为接入网节点或者会话管理网元。

需要说明的是，各个单元的实现还可以对应参照图 2 所示的方法实施例的相应描述。

请参见图 19，图 19 是本发明实施例提供的一种第一设备的结构示意图，该第一设备可以包括发送模块 1210、获取模块 1220 以及推衍模块 1230。

所述发送模块 1210 用于通过所述接入网节点向认证节点发送第三请求；

所述获取模块 1220 用于基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；

所述推衍模块 1230 用于基于所述基础密钥推衍出所述至少一个密钥。

可选地，所述推衍模块 1230 用于根据所述基础密钥推衍出中间密钥；根据所述中间密钥推衍出所述至少一个密钥。

可选地，所述推衍模块 1230 用于基于第一参数，并根据所述基础密钥推衍出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

可选地，所述推衍模块 1230 用于基于所述第二参数，并根据所述中间密钥推衍出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

可选地，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

需要说明的是，各个单元的实现还可以对应参照图 2 所示的方法实施例的相应描述。

请参见图 20，图 20 是本发明实施例提供的一种第一设备，该第一设备包括处理器 1301、存储器 1302 和收发器 1303，所述处理器 1301、存储器 1302 和收发器 1303 通过总线相互连接。

存储器 1302 包括但不限于是随机存储记忆体（英文：Random Access Memory，简称：RAM）、只读存储器（英文：Read-Only Memory，简称：ROM）、可擦除可编程只读存储器（英文：Erasable Programmable Read Only Memory，简称：EPROM）、或便携式只读存储器（英文：Compact Disc Read-Only Memory，简称：CD-ROM），该存储器 1302 用于相关指令及数据。收发器 1303 用于接收和发送数据。

处理器 1301 可以是一个或多个中央处理器（英文：Central Processing Unit，简称：CPU），在处理器 1301 是一个 CPU 的情况下，该 CPU 可以是单核 CPU，也可以是多核 CPU。

该第一设备中的处理器 1301 用于读取所述存储器 1302 中存储的程序代码，执行以下操作：

处理器 1301 获取会话的安全策略以及至少一个密钥；

收发器 1303 向第二设备发送保护数据，其中，所述保护数据是根据所述会话的安全策略使用所述至少一个密钥对所述会话的会话数据的安全性进行保护得到的，所述第二设备用于根据所述安全策略使用所述至少一个密钥对所述保护数据进行还原以获得所述会话数

据;

其中,当所述第一设备为终端设备时,所述第二设备为接入网节点或者用户面节点;当所述第一设备为接入网节点或者用户面节点时,所述第二设备为终端设备。

可选地,所述至少一个密钥包括:第一密钥以及第二密钥,其中,所述第一密钥用于对所述会话的第一安全性进行保护,所述第二密钥用于对所述会话的第二安全性进行保护。

可选地,所述安全策略用于指示所述会话数据的保护方式,其中,所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护,或者,通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护,或者,同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

可选地,所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

可选地,所述密钥长度包括第一密钥长度和/或第二密钥长度,其中,所述第一密钥长度用于表征所述第一密钥的长度,所述第二密钥长度用于表征所述第二密钥的长度。

可选地,所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间,其中,所述第一密钥更新时间用于表征所述第一密钥的更新时间,所述第二密钥更新时间用于表征所述第二密钥的更新时间。

可选地,所述第一安全性为加密性,所述第二安全性为完整性。

可选地,所述保护数据还包括参数字段,所述参数字段包括第一标识字段、第二标识字段、第三标识字段至少一个,其中,所述第一标识字段用于指示本消息为会话消息,所述第二标识字段用于指示业务标识、会话标识、承载标识、flow 标识以及切片标识中的至少一个,所述第三标识用于指示所述会话的保护方式。

可选地,所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个,其中,所述长度字段用于指示所述参数字段的长度,所述分组字段用于指示分组进行加密时,分组的长度,所述 MAC 字段用于指示所述会话进行了完整性保护。

可选地,收发器 1303 向策略控制器获取所述安全策略。

可选地,收发器 1303 向所述接入网节点发送第一请求,其中,所述第一请求包括所述第一设备的安全能力以及业务安全需求;收发器 1303 接收所述接入网节点返回的所述安全策略,其中,所述安全策略是所述接入网节点向所述策略控制器发送第二请求获取到的,所述第二请求是所述接入网节点基于所述第一请求生成的,包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

可选地,收发器 1303 向所述接入网节点发送第一请求,其中,所述第一请求包括所述第一设备的安全能力以及业务安全需求;收发器 1303 接收所述接入网节点返回的所述安全策略,其中,所述安全策略是所述接入网节点通过至少一个网元向所述策略控制器转发第二请求获取到的,所述第二请求是所述接入网节点基于所述第一请求生成的,包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

可选地,所述至少一个网元包括会话管理网元;或者,所述至少一个网元包括会话管理网元或者移动管理实体。

可选地，收发器 1303 向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；可选地，收发器 1303 接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点根据核心网安全策略以及所述接入网节点的安全能力生成的，所述核心网安全策略是所述策略控制器根据所述接入网节点转发的第一请求生成的。

可选地，收发器 1303 通过所述接入网节点向认证节点发送第三请求；收发器 1303 基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；处理器 1301 基于所述基础密钥推导出所述至少一个密钥。

可选地，处理器 1301 根据所述基础密钥推导出中间密钥；并，根据所述中间密钥推导出所述至少一个密钥。

可选地，处理器 1301 基于第一参数，并根据所述基础密钥推导出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

可选地，处理器 1301 基于所述第二参数，并根据所述中间密钥推导出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

可选地，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

可选地，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

该第一设备中的处理器 1301 用于读取所述存储器 1302 中存储的程序代码，还可以执行以下操作：

可选地，收发器 1303 通过所述接入网节点向认证节点发送第三请求；处理器 1301 基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；处理器 1301 基于所述基础密钥推导出所述至少一个密钥。

可选地，处理器 1301 根据所述基础密钥推导出中间密钥；并，根据所述中间密钥推导出所述至少一个密钥。

可选地，处理器 1301 基于第一参数，并根据所述基础密钥推导出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

可选地，处理器 1301 基于所述第二参数，并根据所述中间密钥推导出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

可选地,所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

需要说明的是,各个操作的实现还可以对应参照图2所示的方法实施例的相应描述。

请参见图21,图21是本发明实施例提供的一种第二设备,该第二设备包括处理器1401、存储器1402和收发器1403,所述处理器1401、存储器1402和收发器1403通过总线相互连接。

存储器1402包括但不限于是随机存储记忆体(英文:Random Access Memory,简称:RAM)、只读存储器(英文:Read-Only Memory,简称:ROM)、可擦除可编程只读存储器(英文:Erasable Programmable Read Only Memory,简称:EPROM)、或便携式只读存储器(英文:Compact Disc Read-Only Memory,简称:CD-ROM),该存储器1402用于相关指令及数据。收发器1403用于接收和发送数据。

处理器1401可以是一个或多个中央处理器(英文:Central Processing Unit,简称:CPU),在处理器1401是一个CPU的情况下,该CPU可以是单核CPU,也可以是多核CPU。

该第一设备中的处理器1401用于读取所述存储器1402中存储的程序代码,执行以下操作:

处理器1401确定会话的会话标识;

处理器1401获取所述会话的安全策略以及至少一个密钥;

处理器1401根据所述会话标识识别第一设备发送的所述会话的保护数据,并通过根据所述会话的安全策略使用所述至少一个密钥对所述保护数据进行还原以获得会话数据,其中,所述保护数据是所述第一设备根据所述会话的安全策略使用所述至少一个密钥对所述会话数据的安全性进行保护得到的,所述第一设备用于根据所述安全策略使用所述至少一个密钥对所述会话数据进行加密以获得所述保护数据;

其中,当所述第一设备为终端设备时,所述第二设备为接入网节点或者用户面节点;当所述第一设备为接入网节点或者用户面节点时,所述第二设备为终端设备。

可选地,所述至少一个密钥包括:第一密钥以及第二密钥,其中,所述第一密钥用于对所述会话的第一安全性进行保护,所述第二密钥用于对所述会话的第二安全性进行保护。

可选地,所述安全策略用于指示所述会话数据的保护方式,其中,所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护,或者,通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护,或者,同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

可选地,所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

可选地,所述密钥长度包括第一密钥长度和/或第二密钥长度,其中,所述第一密钥长度用于表征所述第一密钥的长度,所述第二密钥长度用于表征所述第二密钥的长度。

可选地,所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间,其中,所述第一密钥更新时间用于表征所述第一密钥的更新时间,所述第二密钥更新时间用于表征

所述第二密钥的更新时间。

可选地，当所述第二设备为用户面节点时，处理器 1401 用于：

通过所述保护数据所在的封装表头确定会话的会话标识；或者，

通过所述保护数据所在的封装表头中的隧道标识确定会话的会话标识；或者，

通过所述保护数据所在的外部 IP 报文表头确定会话的会话标识；或者，

通过所述保护数据所在的封装表头和所述保护数据所在的外部 IP 报文表头确定所述会话的会话标识；或者，

通过所述保护数据所在的协议数据单元表头和所述保护数据所在的封装表头确定所述会话的会话标识；或者，

通过所述保护数据中的参数字段确定所述会话的会话标识。

可选地，当所述第二设备为接入网节点时，处理器 1401 用于：

通过所述会话所占用的空口资源确定所述会话的会话标识；或者，

通过所述会话所占用的空口的空口标识确定所述会话的会话标识；或者，

通过所述会话所占用的数据无线承载的标识确定所述会话的会话标识；或者，

通过所述保护数据中的参数字段确定所述会话的会话标识。

可选地，所述第一安全性为加密性，所述第二安全性为完整性。

可选地，所述参数字段包括第一标识字段、第二标识字段、第三标识字段中的至少一个，其中，所述第一标识字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识以及切片标识中的至少一个，所述第三标识用于指示所述会话的保护方式。

可选地，所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个，其中，所述长度字段用于指示所述参数字段的长度，所述分组字段用于指示分组进行加密时，分组的长度，所述 MAC 字段用于指示所述会话进行了完整性保护。

可选地，收发器 1403 向第一网元获取所述安全策略，其中，所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

可选地，当所述第一网元为策略控制器时，

收发器 1403 接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

收发器 1403 向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；

收发器 1403 接收所述策略控制器返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

可选地，当所述第一网元为策略控制器时，

收发器 1403 接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

收发器 1403 通过至少一个网元向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；

收发器 1403 接收所述策略控制器通过所述至少一个网元返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

可选地，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

可选地，收发器 1403 接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；收发器 1403 向所述策略控制器转发所述第一请求；收发器 1403 接收所述策略控制器返回的核心网安全策略，并根据所述核心网安全策略以及所述接入网节点的安全能力生成所述安全策略。

可选地，当所述第二设备为接入网节点时，

收发器 1403 向密钥管理中心发送第三请求；

收发器 1403 基于所述第三请求接收所述密钥管理中心返回的中间密钥，其中，所述中间密钥是基于基础密钥推导得到的，所述基础密钥为认证节点发送给所述密钥管理中心的；

处理器 1401 基于所述中间密钥推导出所述至少一个密钥。

可选地，所述中间密钥是根据第一参数推导出来的，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

可选地，处理器 1401 基于所述第二参数，并根据所述中间密钥推导出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

可选地，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

可选地，当所述第二设备为用户面节点时，收发器 1403 向第一网元请求所述至少一个密钥，其中，所述第一网元为所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

可选地，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

需要说明的是，各个操作的实现还可以对应参照图 2 所示的方法实施例的相应描述。

请参见图 22，图 22 是本发明实施例提供的一种策略控制器，该策略控制器包括处理器 1501、存储器 1502 和收发器 1503，所述处理器 1501、存储器 1502 和收发器 1503 通过总线相互连接。

存储器 1502 包括但不限于是随机存储记忆体（英文：Random Access Memory，简称：RAM）、只读存储器（英文：Read-Only Memory，简称：ROM）、可擦除可编程只读存储器（英文：Erasable Programmable Read Only Memory，简称：EPROM）、或便携式只读存储器（英文：Compact Disc Read-Only Memory，简称：CD-ROM），该存储器 1502 用于相关指令及数据。收发器 1503 用于接收和发送数据。

处理器 1501 可以是一个或多个中央处理器(英文: Central Processing Unit, 简称: CPU), 在处理器 1501 是一个 CPU 的情况下, 该 CPU 可以是单核 CPU, 也可以是多核 CPU。

该第一设备中的处理器 1501 用于读取所述存储器 1402 中存储的程序代码, 执行以下操作:

收发器 1503 接收目标网元发送的策略请求, 其中, 所述策略请求包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个;

处理器 1501 根据目标参数生成安全策略, 其中, 所述目标参数是根据所述第一请求生成的, 包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个;

收发器 1503 向接入网节点发送安全策略。

可选地, 所述目标参数还包括: 终端设备的预制安全能力, 其中, 所述终端设备的预制安全能力是从认证服务控制器 AUSF 获取得到的。

可选地, 所述目标参数还包括: 服务器的安全需求, 其中, 所述服务器的安全需求是从服务器获取得到的。

可选地, 所述目标网元为接入网节点或者会话管理网元。

需要说明的是, 各个操作的实现还可以对应参照图 2 所示的方法实施例的相应描述。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程, 该流程可以由计算机程序来指令相关的硬件完成, 该程序可存储于计算机可读取存储介质中, 该程序在执行时, 可包括如上述各方法实施例的流程。而前述的存储介质包括: ROM 或随机存储记忆体 RAM、磁碟或者光盘等各种可存储程序代码的介质。

权利要求

1、一种安全实现方法，其特征在于，包括：

第一设备获取会话的安全策略以及至少一个密钥；

所述第一设备向第二设备发送保护数据，其中，所述保护数据是根据所述会话的安全策略使用所述至少一个密钥对所述会话的会话数据的安全性进行保护得到的，所述第二设备用于根据所述安全策略使用所述至少一个密钥对所述保护数据进行还原以获得所述会话数据；

其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

2、根据权利要求1所述的方法，其特征在于，所述至少一个密钥包括：第一密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

3、根据权利要求2所述的方法，其特征在于，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

4、根据权利要求3所述的方法，其特征在于，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

5、根据权利要求4所述的方法，其特征在于，所述密钥长度包括第一密钥长度和/或第二密钥长度，其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。

6、根据权利要求4所述的方法，其特征在于，所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间，其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所述第二密钥更新时间用于表征所述第二密钥的更新时间。

7、根据权利要求1-6任一权利要求所述的方法，其特征在于，所述第一安全性为加密性，所述第二安全性为完整性。

8、根据权利要求7所述的方法，其特征在于，所述保护数据还包括参数字段，所述参数字段包括第一标识字段、第二标识字段、第三标识字段至少一个，其中，所述第一标识

字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识、承载标识、flow 标识以及切片标识中的至少一个，所述第三标识用于指示所述会话的保护方式。

9、根据权利要求 8 所述的方法，其特征在于，所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个，其中，所述长度字段用于指示所述参数字段的长度，所述分组字段用于指示分组进行加密时，分组的长度，所述 MAC 字段用于指示所述会话进行了完整性保护。

10、根据权利要求 1 至 9 任一权利要求所述的方法，其特征在于，当所述第二设备为接入网节点时，所述第一设备获取所述安全策略具体为：

所述第一设备向策略控制器获取所述安全策略。

11、根据权利要求 10 所述的方法，其特征在于，所述第一设备向策略控制器获取所述安全策略具体为：

所述第一设备向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述第一设备接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点向所述策略控制器发送第二请求获取到的，所述第二请求是所述接入网节点基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

12、根据权利要求 10 所述的方法，其特征在于，所述第一设备向策略控制器获取所述安全策略具体为：

所述第一设备向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述第一设备接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点通过至少一个网元向所述策略控制器转发第二请求获取到的，所述第二请求是所述接入网节点基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

13、根据权利要求 12 所述的方法，其特征在于，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

14、根据权利要求 10 所述的方法，其特征在于，所述第一设备向策略控制器获取所述安全策略具体为：

所述第一设备向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述第一设备接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述

接入网节点根据核心网安全策略以及所述接入网节点的安全能力生成的，所述核心网安全策略是所述策略控制器根据所述接入网节点转发的第一请求生成的。

15、根据权利要求 1 至 14 任一权利要求所述的方法，其特征在于，当所述第二设备为接入网节点时，第一设备获取至少一个密钥具体为：

所述第一设备通过所述接入网节点向认证节点发送第三请求；

所述第一设备基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；

所述第一设备基于所述基础密钥推导出所述至少一个密钥。

16、根据权利要求 15 所述的方法，其特征在于，所述第一设备基于所述基础密钥推导出所述至少一个密钥具体为：

所述第一设备根据所述基础密钥推导出中间密钥；

所述第一设备根据所述中间密钥推导出所述至少一个密钥。

17、根据权利要求 16 所述的方法，其特征在于，所述第一设备根据所述基础密钥推导出中间密钥具体为：

所述第一设备基于第一参数，并根据所述基础密钥推导出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

18、根据权利要求 16 所述的方法，其特征在于，所述第一设备根据所述中间密钥推导出所述至少一个密钥具体为：

所述第一设备基于所述第二参数，并根据所述中间密钥推导出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

19、根据权利要求 15 所述的方法，其特征在于，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

20、根据权利要求 1 至 19 任一权利要求所述的方法，其特征在于，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

21、一种安全实现方法，其特征在于，包括：

第二设备确定会话的会话标识；

所述第二设备获取所述会话的安全策略以及至少一个密钥；

所述第二设备根据所述会话标识识别第一设备发送的所述会话的保护数据，并通过根据所述会话的安全策略使用所述至少一个密钥对所述保护数据进行还原以获得会话数据，其中，所述保护数据是所述第一设备根据所述会话的安全策略使用所述至少一个密钥对所述会话数据的安全性进行保护得到的，所述第一设备用于根据所述安全策略使用所述至少一个密钥对所述会话数据进行加密以获得所述保护数据；

其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

22、根据权利要求 21 所述的方法，其特征在于，所述至少一个密钥包括：第一密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

23、根据权利要求 22 所述的方法，其特征在于，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

24、根据权利要求 23 所述的方法，其特征在于，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

25、根据权利要求 24 所述的方法，其特征在于，所述密钥长度包括第一密钥长度和/或第二密钥长度，其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。

26、根据权利要求 24 所述的方法，其特征在于，所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间，其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所述第二密钥更新时间用于表征所述第二密钥的更新时间。

27、根据权利要求 21 至 26 任一权利要求所述的方法，其特征在于，当所述第二设备为用户面节点时，第二设备确定会话的会话标识具体为：

所述第二设备通过所述保护数据所在的封装表头确定会话的会话标识；或者，

所述第二设备通过所述保护数据所在的封装表头中的隧道标识确定会话的会话标识；或者，

所述第二设备通过所述保护数据所在的外部 IP 报文表头确定会话的会话标识；或者，

所述第二设备通过所述保护数据所在的封装表头和所述保护数据所在的外部 IP 报文表头确定所述会话的会话标识；或者，

所述第二设备通过所述保护数据所在的协议数据单元表头和所述保护数据所在的封装表头确定所述会话的会话标识；或者，

所述第二设备通过所述保护数据中的参数字段确定所述会话的会话标识。

28、根据权利要求 21 至 26 任一权利要求所述的方法，其特征在于，当所述第二设备为接入网节点时，第二设备确定会话的会话标识具体为：

所述第二设备通过所述会话所占用的空口资源确定所述会话的会话标识；或者，

所述第二设备通过所述会话所占用的空口的空口标识确定所述会话的会话标识；或者，

所述第二设备通过所述会话所占用的数据无线承载的标识确定所述会话的会话标识；

或者，

所述第二设备通过所述保护数据中的参数字段确定所述会话的会话标识。

29、根据权利要求 27 或者 28 所述的方法，其特征在于，所述第一安全性为加密性，所述第二安全性为完整性。

30、根据权利要求 29 所述的方法，其特征在于，所述参数字段包括第一标识字段、第二标识字段、第三标识字段中的至少一个，其中，所述第一标识字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识以及切片标识中的至少一个，所述第三标识用于指示所述会话的保护方式。

31、根据权利要求 30 所述的方法，其特征在于，所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个，其中，所述长度字段用于指示所述参数字段的长度，所述分组字段用于指示分组进行加密时，分组的长度，所述 MAC 字段用于指示所述会话进行了完整性保护。

32、根据权利要求 21 至 31 任一权利要求所述的方法，其特征在于，当所述第二设备为接入网节点时，所述第二设备获取所述安全策略具体为：

所述第二设备向第一网元获取所述安全策略，其中，所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

33、根据权利要求 32 所述的方法，其特征在于，当所述第一网元为策略控制器时，所述第二设备向策略控制器获取所述安全策略具体为：

所述第二设备接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述第二设备向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；

所述第二设备接收所述策略控制器返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

34、根据权利要求 32 所述的方法，其特征在于，当所述第一网元为策略控制器时，所述第二设备向策略控制器获取所述安全策略具体为：

所述第二设备接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述第二设备通过至少一个网元向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；

所述第二设备接收所述策略控制器通过所述至少一个网元返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

35、根据权利要求 34 所述的方法，其特征在于，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

36、根据权利要求 32 所述的方法，其特征在于，所述第二设备向策略控制器获取所述安全策略具体为：

所述第二设备接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述第二设备向所述策略控制器转发所述第一请求；

所述第二设备接收所述策略控制器返回的核心网安全策略，并根据所述核心网安全策略以及所述接入网节点的安全能力生成所述安全策略。

37、根据权利要求 28 至 36 任一权利要求所述的方法，其特征在于，当所述第二设备为接入网节点时，第二设备获取至少一个密钥具体为：

所述第二设备向密钥管理中心发送第三请求；

所述第二设备基于所述第三请求接收所述密钥管理中心返回的中间密钥，其中，所述中间密钥是基于基础密钥推衍得到的，所述基础密钥为认证节点发送给所述密钥管理中心的；

所述第二设备基于所述中间密钥推衍出所述至少一个密钥。

38、根据权利要求 37 所述的方法，其特征在于，所述中间密钥是根据第一参数推衍出来的，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

39、根据权利要求 37 所述的方法，其特征在于，所述第二设备根据所述中间密钥推衍出所述至少一个密钥具体为：

所述第二设备基于所述第二参数，并根据所述中间密钥推衍出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资

源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

40、根据权利要求 37 所述的方法，其特征在于，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

41、根据权利要求 21 至 40 任一权利要求所述的方法，其特征在于，当所述第二设备为用户面节点时，第二设备获取至少一个密钥具体为：

所述第二设备向第一网元请求所述至少一个密钥，其中，所述第一网元为所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

42、根据权利要求 21 至 41 任一权利要求所述的方法，其特征在于，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

43、一种安全策略生成方法，其特征在于，包括：

策略控制器接收目标网元发送的策略请求，其中，所述策略请求包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；

所述策略控制器根据目标参数生成安全策略，其中，所述目标参数是根据所述第一请求生成的，包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；

所述策略控制器向接入网节点发送安全策略。

44、根据权利要求 43 所述的方法，其特征在于，所述目标参数还包括：终端设备的预制安全能力，其中，所述终端设备的预制安全能力是从认证服务控制器 AUSF 获取得到的。

45、根据权利要求 43 或 44 所述的方法，其特征在于，所述目标参数还包括：服务器的安全需求，其中，所述服务器的安全需求是从服务器获取得到的。

46、根据权利要求 43 或 44 或 45 所述的方法，其特征在于，所述目标网元为接入网节点或者会话管理网元。

47、一种密钥生成方法，其特征在于，包括：

所述第一设备通过所述接入网节点向认证节点发送第三请求；

所述第一设备基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；

所述第一设备基于所述基础密钥推导出所述至少一个密钥。

48、根据权利要求 47 所述的方法，其特征在于，所述终端设备基于所述基础密钥推导出所述至少一个密钥具体为：

所述终端设备根据所述基础密钥推导出中间密钥；

所述终端设备根据所述中间密钥推导出所述至少一个密钥。

49、根据权利要求 48 所述的方法，其特征在于，所述第一设备根据所述基础密钥推导出中间密钥具体为：

所述终端设备基于第一参数，并根据所述基础密钥推导出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

50、根据权利要求 48 所述的方法，其特征在于，所述终端设备根据所述中间密钥推导出所述至少一个密钥具体为：

所述终端设备基于所述第二参数，并根据所述中间密钥推导出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

51、根据权利要求 47 所述的方法，其特征在于，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

52、一种第一设备，其特征在于，包括：获取模块以及发送模块，

所述获取模块用于获取会话的安全策略以及至少一个密钥；

所述发送模块用于向第二设备发送保护数据，其中，所述保护数据是根据所述会话的安全策略使用所述至少一个密钥对所述会话的会话数据的安全性进行保护得到的，所述第二设备用于根据所述安全策略使用所述至少一个密钥对所述保护数据进行还原以获得所述会话数据；

其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

53、根据权利要求 52 所述的设备，其特征在于，所述至少一个密钥包括：第一密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

54、根据权利要求 53 所述的设备，其特征在于，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安

全性进行保护, 或者, 同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

55、根据权利要求 54 所述的设备, 其特征在于, 所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

56、根据权利要求 55 所述的设备, 其特征在于, 所述密钥长度包括第一密钥长度和/或第二密钥长度, 其中, 所述第一密钥长度用于表征所述第一密钥的长度, 所述第二密钥长度用于表征所述第二密钥的长度。

57、根据权利要求 55 所述的设备, 其特征在于, 所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间, 其中, 所述第一密钥更新时间用于表征所述第一密钥的更新时间, 所述第二密钥更新时间用于表征所述第二密钥的更新时间。

58、根据权利要求 52-57 任一权利要求所述的设备, 其特征在于, 所述第一安全性为加密性, 所述第二安全性为完整性。

59、根据权利要求 58 所述的设备, 其特征在于, 所述保护数据还包括参数字段, 所述参数字段包括第一标识字段、第二标识字段、第三标识字段至少一个, 其中, 所述第一标识字段用于指示本消息为会话消息, 所述第二标识字段用于指示业务标识、会话标识、承载标识、flow 标识以及切片标识中的至少一个, 所述第三标识用于指示所述会话的保护方式。

60、根据权利要求 59 所述的设备, 其特征在于, 所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个, 其中, 所述长度字段用于指示所述参数字段的长度, 所述分组字段用于指示分组进行加密时, 分组的长度, 所述 MAC 字段用于指示所述会话进行了完整性保护。

61、根据权利要求 52 至 60 任一权利要求所述的设备, 其特征在于, 所述获取模块具体用于向策略控制器获取所述安全策略。

62、根据权利要求 61 所述的设备, 其特征在于, 所述获取模块包括发送单元以及接收单元,

所述发送单元用于向所述接入网节点发送第一请求, 其中, 所述第一请求包括所述第一设备的安全能力以及业务安全需求;

所述接收单元用于接收所述接入网节点返回的所述安全策略, 其中, 所述安全策略是所述接入网节点向所述策略控制器发送第二请求获取到的, 所述第二请求是所述接入网

节点基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

63、根据权利要求 61 所述的设备，其特征在于，所述获取模块包括发送单元以及接收单元，

所述发送单元用于向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述接收单元用于接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点通过至少一个网元向所述策略控制器转发第二请求获取到的，所述第二请求是所述接入网节点基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求。

64、根据权利要求 63 所述的设备，其特征在于，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

65、根据权利要求 61 所述的设备，其特征在于，所述获取模块包括发送单元以及接收单元，

所述发送单元用于向所述接入网节点发送第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述接收单元用于接收所述接入网节点返回的所述安全策略，其中，所述安全策略是所述接入网节点根据核心网安全策略以及所述接入网节点的安全能力生成的，所述核心网安全策略是所述策略控制器根据所述接入网节点转发的第一请求生成的。

66、根据权利要求 52 至 65 任一权利要求所述的设备，其特征在于，当所述第二设备为接入网节点时，所述获取模块包括发送单元、获取单元以及推衍单元，

所述发送单元用于通过所述接入网节点向认证节点发送第三请求；

所述获取单元用于基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；

所述推衍单元用于基于所述基础密钥推衍出所述至少一个密钥。

67、根据权利要求 66 所述的设备，其特征在于，所述推衍单元用于根据所述基础密钥推衍出中间密钥，以及，根据所述中间密钥推衍出所述至少一个密钥。

68、根据权利要求 67 所述的设备，其特征在于，所述推衍单元用于基于第一参数，并根据所述基础密钥推衍出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

69、根据权利要求 67 所述的设备，其特征在于，所述推衍单元用于基于所述第二参数，并根据所述中间密钥推衍出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

70、根据权利要求 66 所述的设备，其特征在于，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

71、根据权利要求 52 至 70 任一权利要求所述的设备，其特征在于，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

72、一种第二设备，其特征在于，包括：确定模块、获取模块以及识别模块，

所述确定模块用于确定会话的会话标识；

所述获取模块用于获取所述会话的安全策略以及至少一个密钥；

所述识别模块用于根据所述会话标识识别第一设备发送的所述会话的保护数据，并根据所述会话的安全策略使用所述至少一个密钥对所述保护数据进行还原以获得会话数据，其中，所述保护数据是所述第一设备根据所述会话的安全策略使用所述至少一个密钥对所述会话数据的安全性进行保护得到的，所述第一设备用于根据所述安全策略使用所述至少一个密钥对所述会话数据进行加密以获得所述保护数据；

其中，当所述第一设备为终端设备时，所述第二设备为接入网节点或者用户面节点；当所述第一设备为接入网节点或者用户面节点时，所述第二设备为终端设备。

73、根据权利要求 72 所述的设备，其特征在于，所述至少一个密钥包括：第一密钥以及第二密钥，其中，所述第一密钥用于对所述会话的第一安全性进行保护，所述第二密钥用于对所述会话的第二安全性进行保护。

74、根据权利要求 73 所述的设备，其特征在于，所述安全策略用于指示所述会话数据的保护方式，其中，所述保护方式是通过第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护，或者，通过第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护，或者，同时通过所述第一安全性算法使用第一密钥对所述会话数据的第一安全性进行保护以及通过所述第二安全性算法使用第二密钥对所述会话数据的第二安全性进行保护。

75、根据权利要求 74 所述的设备，其特征在于，所述安全策略还用于指示所述第一安全性算法、所述第二安全性算法、密钥长度以及密钥更新时间中的至少一个。

76、根据权利要求 75 所述的设备，其特征在于，所述密钥长度包括第一密钥长度和/

或第二密钥长度，其中，所述第一密钥长度用于表征所述第一密钥的长度，所述第二密钥长度用于表征所述第二密钥的长度。

77、根据权利要求 75 所述的设备，其特征在于，所述密钥更新时间包括第一密钥更新时间和/或第二密钥更新时间，其中，所述第一密钥更新时间用于表征所述第一密钥的更新时间，所述第二密钥更新时间用于表征所述第二密钥的更新时间。

78、根据权利要求 72 至 77 任一权利要求所述的设备，其特征在于，当所述第二设备为用户面节点时，所述确定模块具体用于：

通过所述保护数据所在的封装表头确定会话的会话标识；或者，

通过所述保护数据所在的封装表头中的隧道标识确定会话的会话标识；或者，

通过所述保护数据所在的外部 IP 报文表头确定会话的会话标识；或者，

通过所述保护数据所在的封装表头和所述保护数据所在的外部 IP 报文表头确定所述会话的会话标识；或者，

通过所述保护数据所在的协议数据单元表头和所述保护数据所在的封装表头确定所述会话的会话标识；或者，

通过所述保护数据中的参数字段确定所述会话的会话标识。

79、根据权利要求 72 至 77 任一权利要求所述的设备，其特征在于，当所述第二设备为接入网节点时，所述确定模块具体用于：

通过所述会话所占用的空口资源确定所述会话的会话标识；或者，

通过所述会话所占用的空口的空口标识确定所述会话的会话标识；或者，

通过所述会话所占用的数据无线承载的标识确定所述会话的会话标识；或者，

通过所述保护数据中的参数字段确定所述会话的会话标识。

80、根据权利要求 78 或者 79 所述的设备，其特征在于，所述第一安全性为加密性，所述第二安全性为完整性。

81、根据权利要求 80 所述的设备，其特征在于，所述参数字段包括第一标识字段、第二标识字段、第三标识字段中的至少一个，其中，所述第一标识字段用于指示本消息为会话消息，所述第二标识字段用于指示业务标识、会话标识以及切片标识中的至少一个，所述第三标识用于指示所述会话的保护方式。

82、根据权利要求 81 所述的设备，其特征在于，所述参数字段还包括长度字段、分组字段以及 MAC 字段中的至少一个，其中，所述长度字段用于指示所述参数字段的长度，所述分组字段用于指示分组进行加密时，分组的长度，所述 MAC 字段用于指示所述会话进行了完整性保护。

83、根据权利要求 72 至 82 任一权利要求所述的设备，其特征在于，当所述第二设备为接入网节点时，所述获取模块用于向第一网元获取所述安全策略，其中，所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

84、根据权利要求 83 所述的设备，其特征在于，当所述第一网元为策略控制器时，所述获取模块包括接收单元以及发送单元，

所述接收单元用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述发送单元用于向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；

所述接收单元用于接收所述策略控制器返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

85、根据权利要求 83 所述的设备，其特征在于，当所述第一网元为策略控制器时，所述获取模块包括接收单元以及发送单元，

所述接收单元用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述发送单元用于通过至少一个网元向所述策略控制器发送第二请求，其中，所述第二请求是基于所述第一请求生成的，包括所述第一设备的安全能力、业务安全需求以及所述接入网节点安全需求；

所述接收单元用于接收所述策略控制器通过所述至少一个网元返回的所述安全策略，其中，所述安全策略是所述策略控制器根据所述第二请求生成的。

86、根据权利要求 85 所述的设备，其特征在于，所述至少一个网元包括会话管理网元；或者，所述至少一个网元包括会话管理网元或者移动管理实体。

87、根据权利要求 83 所述的设备，其特征在于，所述获取模块包括接收单元以及发送单元，

所述接收单元用于接收所述第一设备发送的第一请求，其中，所述第一请求包括所述第一设备的安全能力以及业务安全需求；

所述发送单元用于向所述策略控制器转发所述第一请求；

所述接收单元用于接收所述策略控制器返回的核心网安全策略，并根据所述核心网安全策略以及所述接入网节点的安全能力生成所述安全策略。

88、根据权利要求 79 至 87 任一权利要求所述的设备，其特征在于，当所述第二设备为接入网节点时，所述获取模块包括发送单元、接收单元以及推衍单元，

所述发送单元用于向密钥管理中心发送第三请求；

所述接收单元用于基于所述第三请求接收所述密钥管理中心返回的中间密钥，其中，所述中间密钥是基于基础密钥推衍得到的，所述基础密钥为认证节点发送给所述密钥管理中心的；

所述推衍单元用于基于所述中间密钥推衍出所述至少一个密钥。

89、根据权利要求 88 所述的设备，其特征在于，所述中间密钥是根据第一参数推衍出来的，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

90、根据权利要求 88 所述的设备，其特征在于，所述推衍单元用于基于所述第二参数，并根据所述中间密钥推衍出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

91、根据权利要求 88 所述的设备，其特征在于，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

92、根据权利要求 72 至 91 任一权利要求所述的设备，其特征在于，当所述第二设备为用户面节点时，所述获取模块用于向第一网元请求所述至少一个密钥，其中，所述第一网元为所述第一网元为认证控制器、密钥管理控制器、策略控制器和密钥控制器中的任意一个。

93、根据权利要求 72 至 92 任一权利要求所述的设备，其特征在于，所述保护数据为表头数据、负载数据或者数据包，其中，所述数据包包括所述表头数据以及所述负载数据。

94、一种策略控制器，其特征在于，包括：接收模块、生成模块以及发送模块，

所述接收模块用于接收目标网元发送的策略请求，其中，所述策略请求包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；

所述生成模块用于根据目标参数生成安全策略，其中，所述目标参数是根据所述第一请求生成的，包括终端设备的安全能力、业务安全需求以及接入网节点安全需求中的至少一个；

所述发送模块用于向接入网节点发送安全策略。

95、根据权利要求 94 所述的策略控制器，其特征在于，所述目标参数还包括：终端设备的预制安全能力，其中，所述终端设备的预制安全能力是从认证服务控制器 AUSF 获取得到的。

96、根据权利要求 94 或 95 所述的策略控制器，其特征在于，所述目标参数还包括：服务器的安全需求，其中，所述服务器的安全需求是从服务器获取得到的。

97、根据权利要求 93 或 94 或 95 所述的策略控制器，其特征在于，所述目标网元为接入网节点或者会话管理网元。

98、一种第一设备，其特征在于，包括：发送模块、获取模块以及推衍模块，

所述发送模块用于通过所述接入网节点向认证节点发送第三请求；

所述获取模块用于基于所述第三请求获取基础密钥，其中，所述基础密钥是所述第一设备与所述认证节点之间互相认证后产生的；

所述推衍模块用于基于所述基础密钥推衍出所述至少一个密钥。

99、根据权利要求 98 所述的设备，其特征在于，所述推衍模块用于根据所述基础密钥推衍出中间密钥；根据所述中间密钥推衍出所述至少一个密钥。

100、根据权利要求 99 所述的设备，其特征在于，所述推衍模块用于基于第一参数，并根据所述基础密钥推衍出中间密钥，其中，所述第一参数包括所述接入网节点标识、NAS 计数器、生成所述中间密钥的序列号、数据包的序列号、nonce1、承载标识、flow 标识以及切片标识中的至少一个。

101、根据权利要求 99 所述的设备，其特征在于，所述推衍模块用于基于所述第二参数，并根据所述中间密钥推衍出所述至少一个密钥；其中，所述第二参数包括空口安全策略标识、安全算法标识、NAS 计数器、nonce2、空口资源标识、空口承载标识、切片标识以及会话标识中的至少一项，所述安全算法标识为空口信令加密算法标识、空口信息完整性保护算法标识、用户面加密算法标识以及用户面完整性保护算法标识中的至少一项。

102、根据权利要求 98 所述的设备，其特征在于，所述至少一个密钥包括空口信令加密密钥、空口信令完整性加密密钥、用户面密钥以及用户面完整性加密密钥中的至少一项。

103、一种通信系统，其特征在于，所述通信系统包括第一设备以及第二设备，其中，所述第一设备连接所述第二设备，

所述第一设备为如权利要求 52 至 71 任一权利要求所述的设备；

所述第二设备为如权利要求 72 至 93 任一权利要求所述的设备。

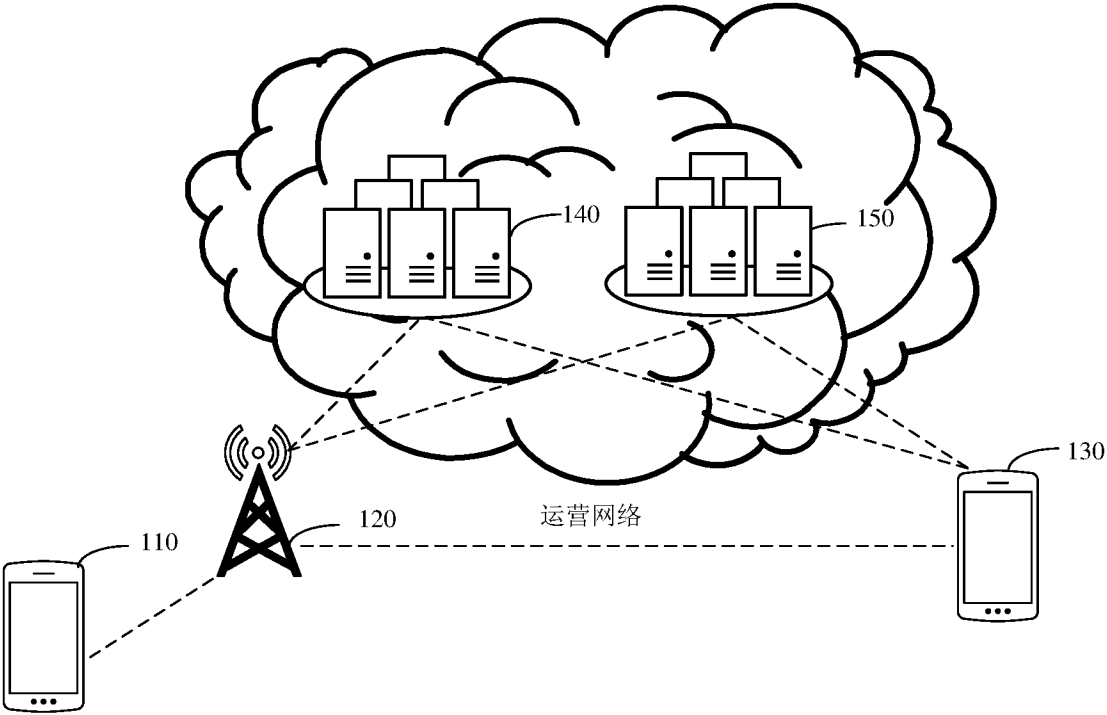


图 1

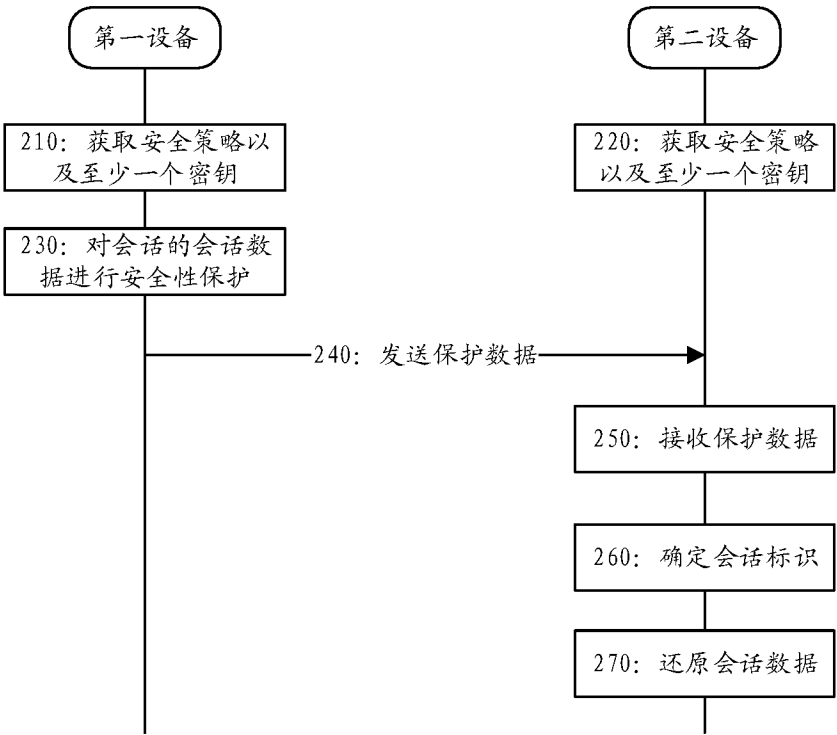


图 2

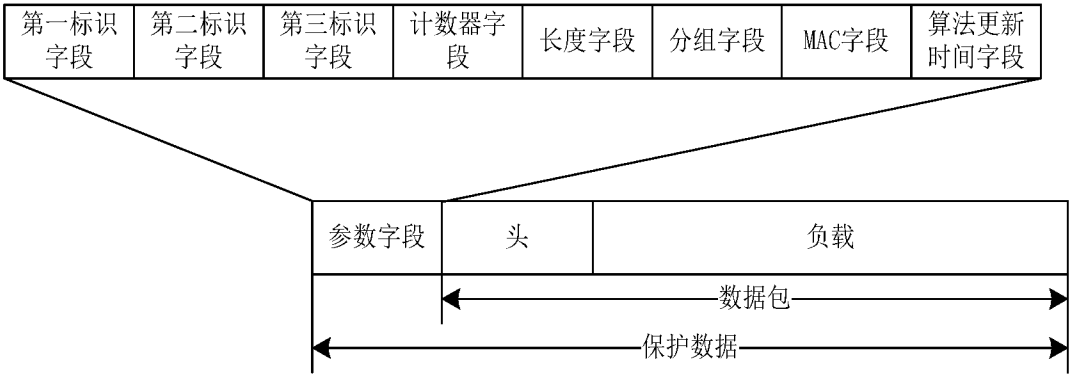


图 3A

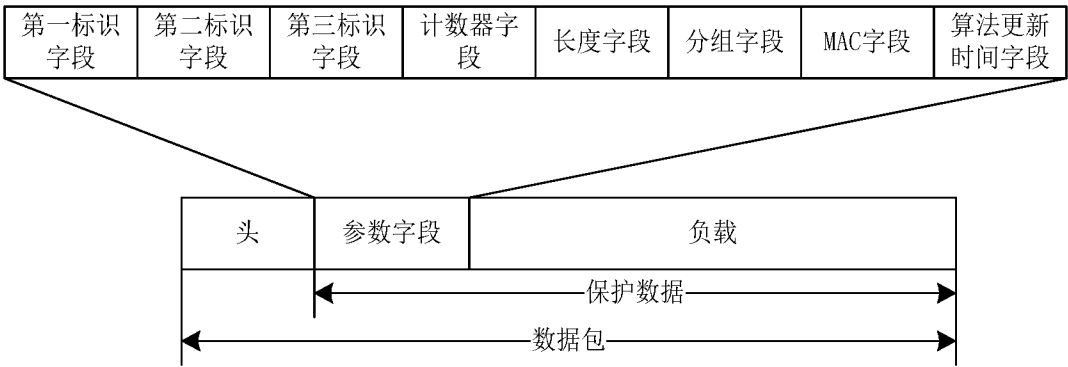


图 3B

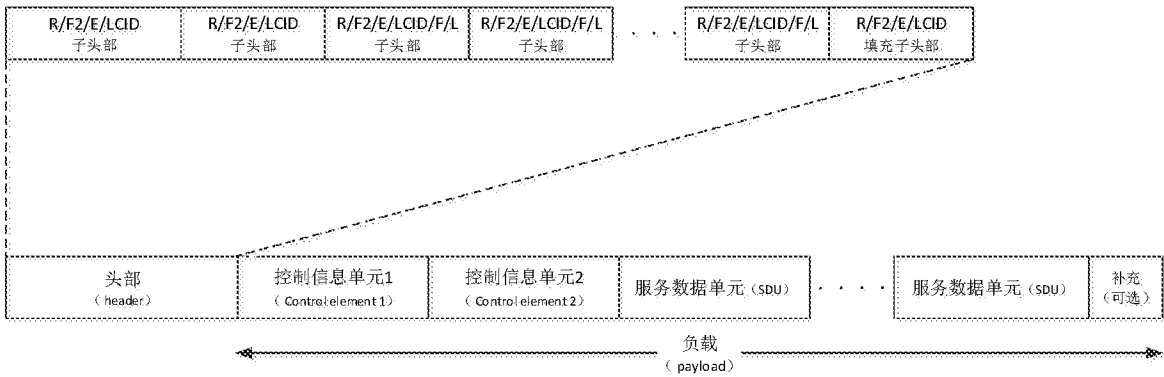


图 4

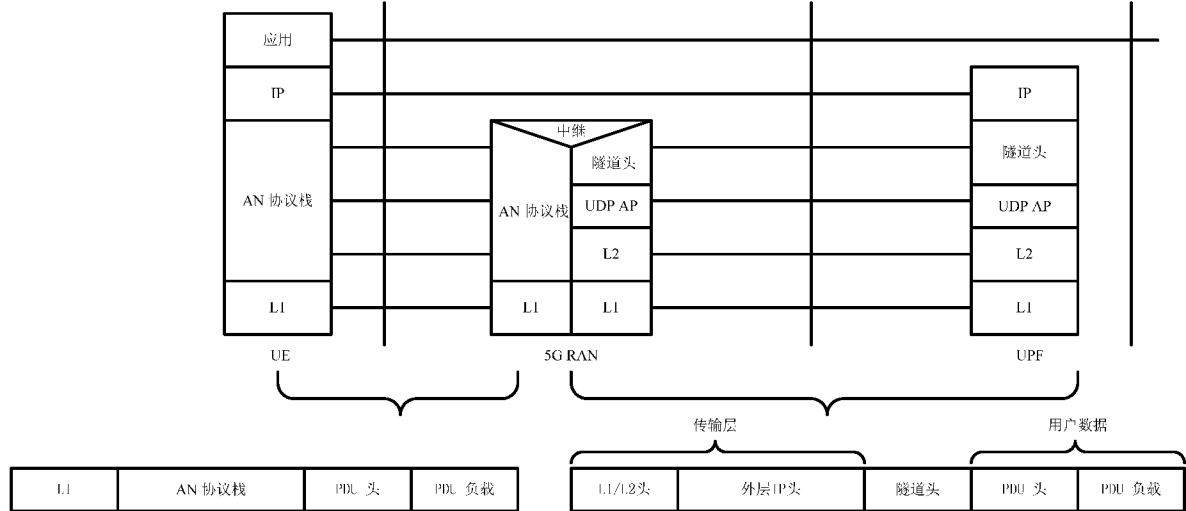


图 5

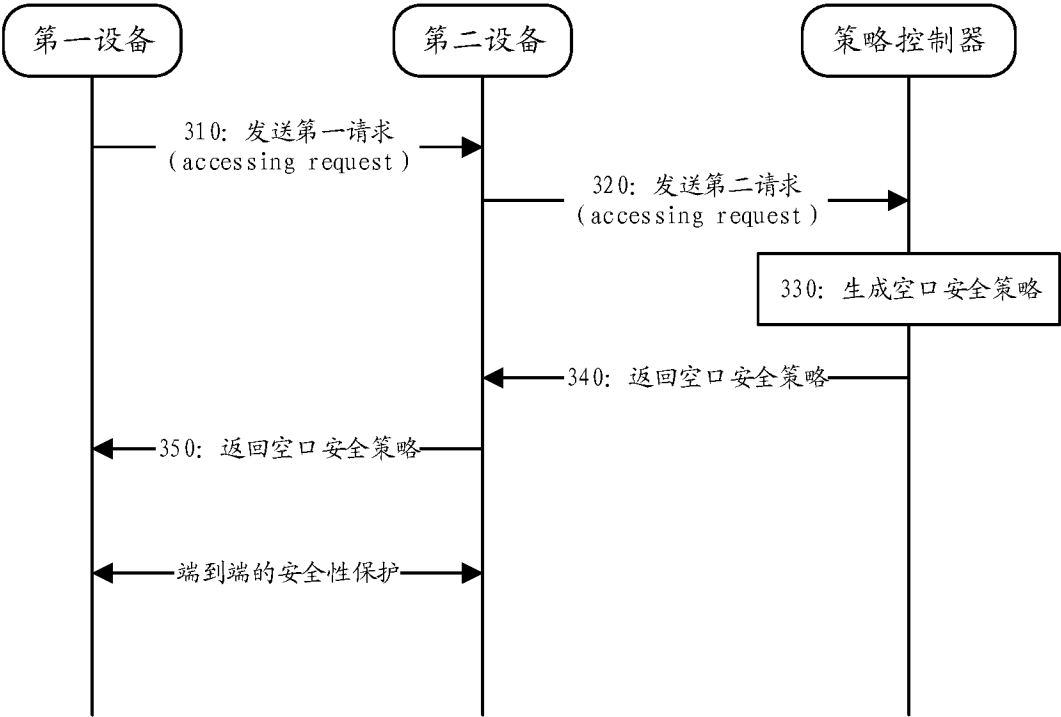


图 6A

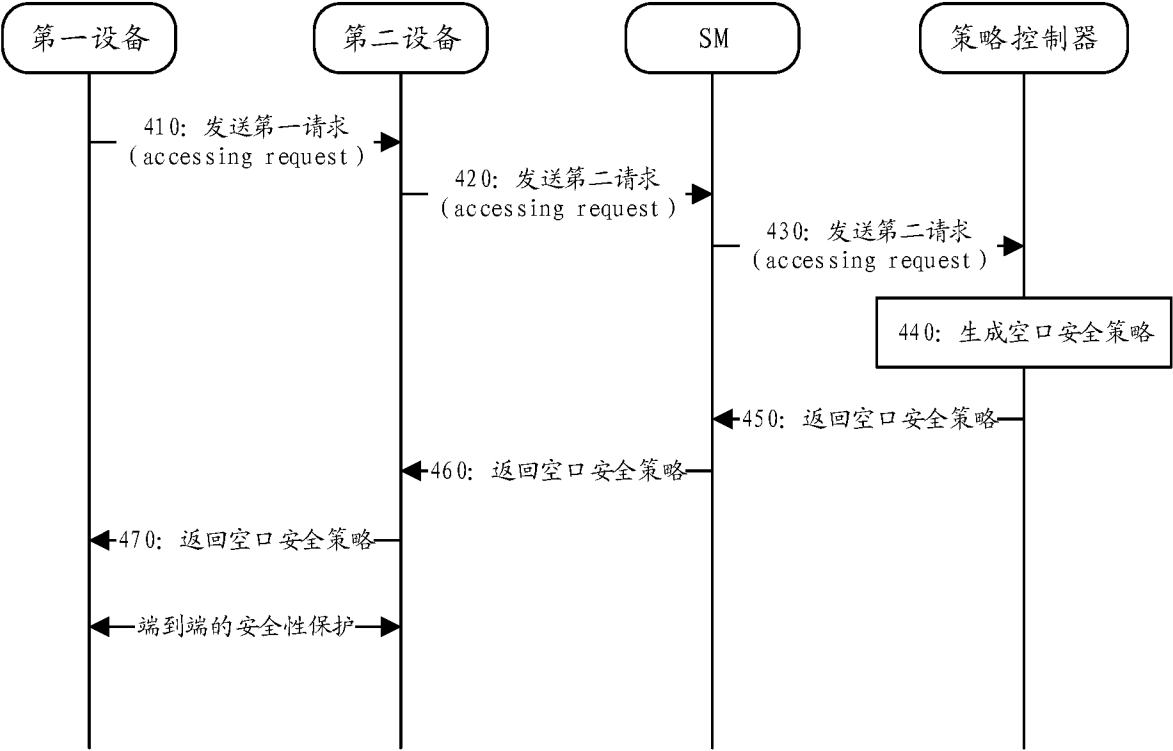


图 6B

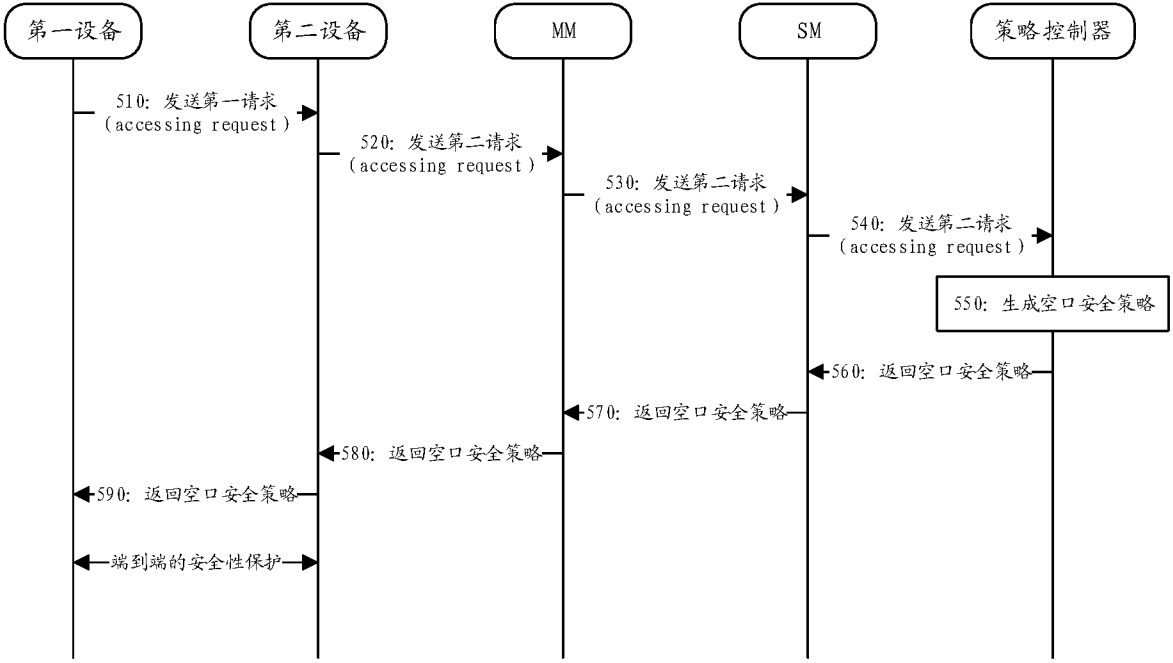


图 6C

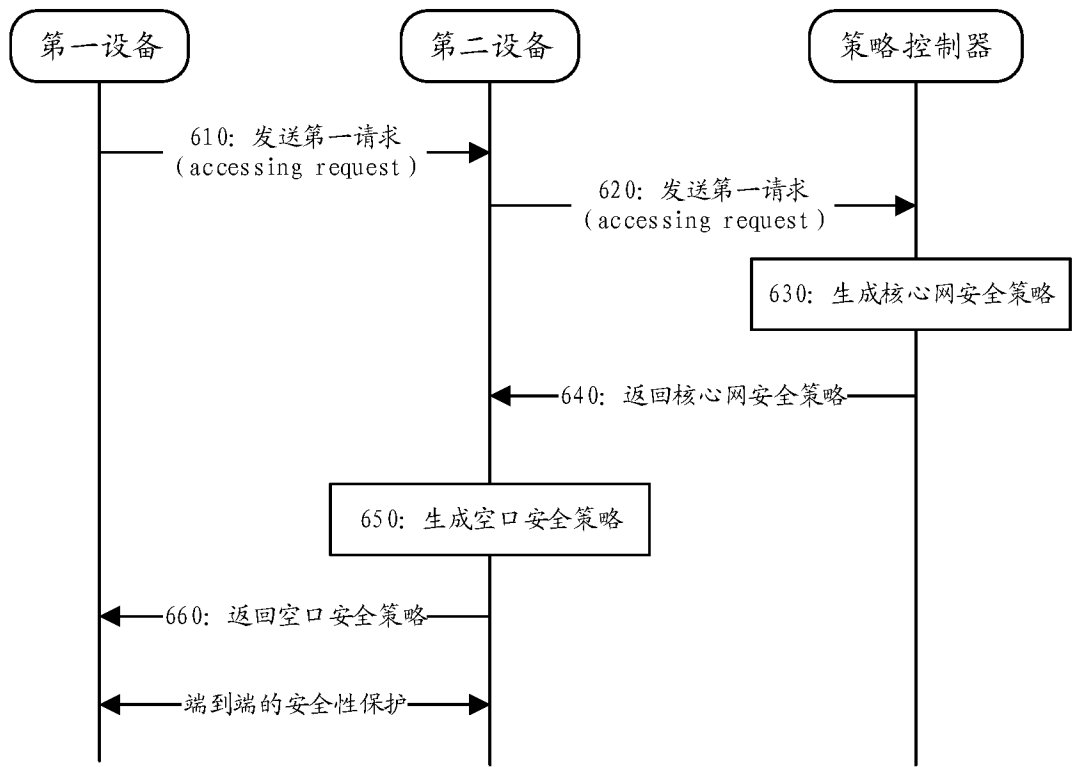


图 6D

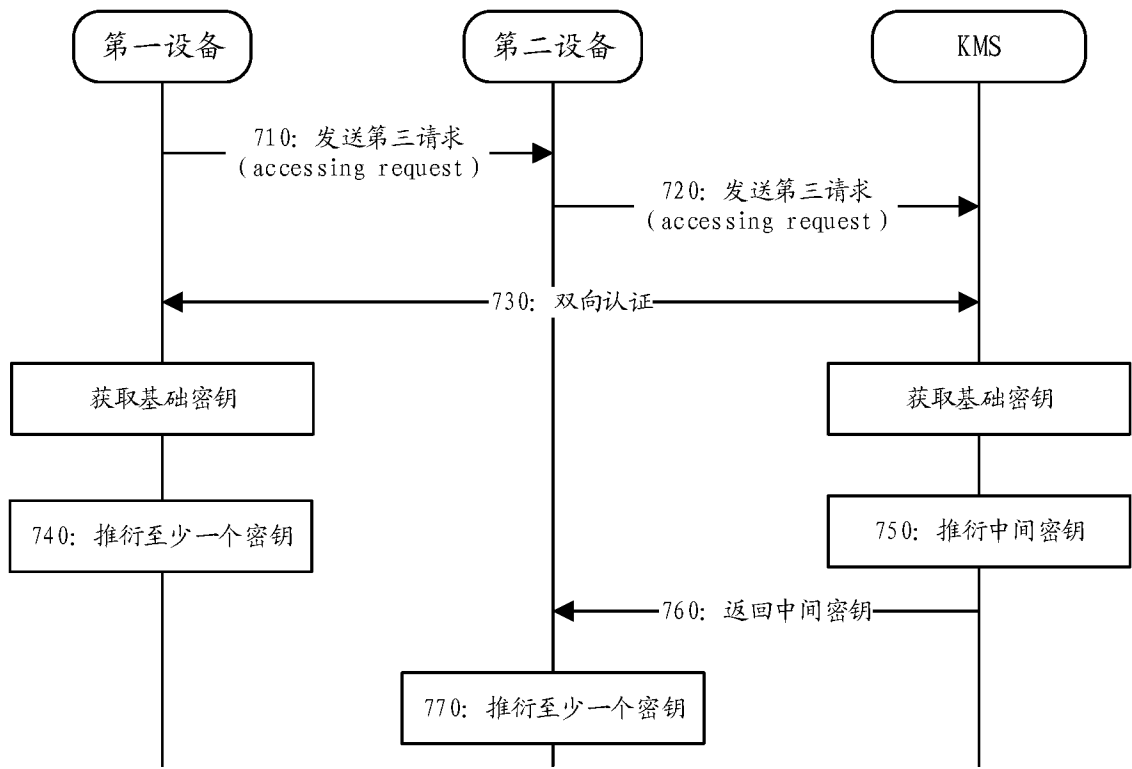


图 7

版本	协议	保留位	扩展表头标志	序列码标志	非-PDU码标志	消息类型	消息长度
隧道标识							
序列码				非PDU码		下一个扩展表头类型	

图 8

版本	报头长度	服务类型	总长度	
标识			标志	段偏移量
生存期	协议		头部校验和	
源地址				
目的地址				
可选项				
数据				

图 9

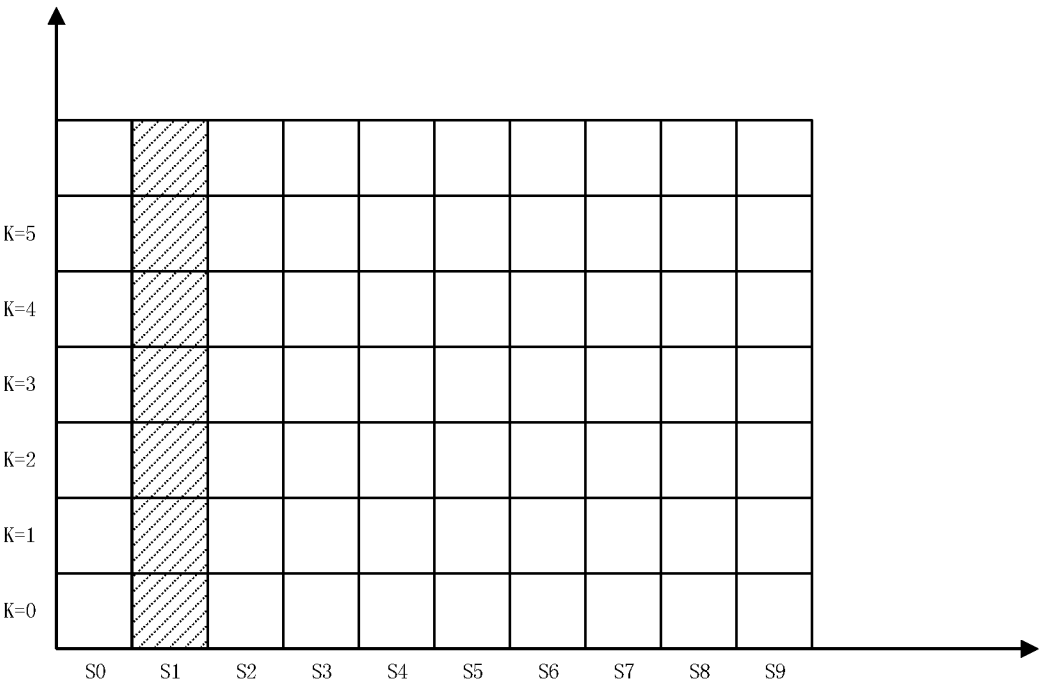


图 10

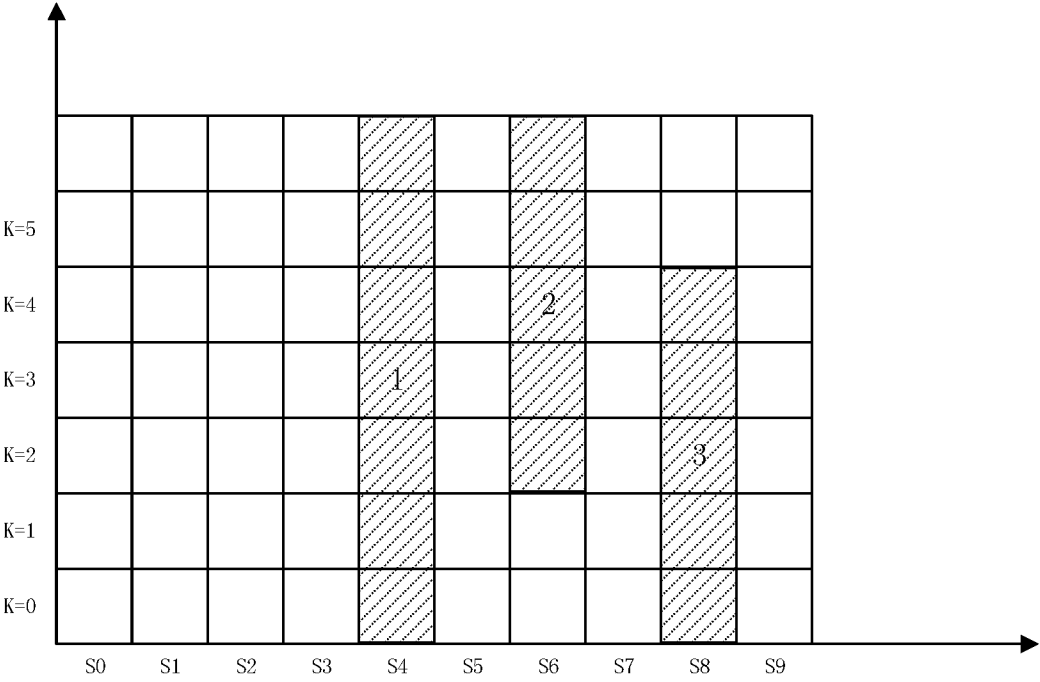


图 11

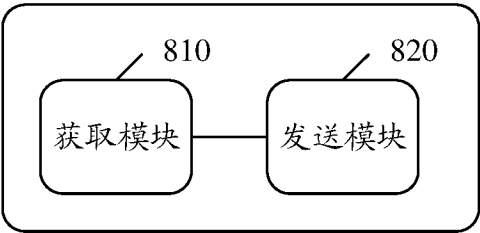


图 12

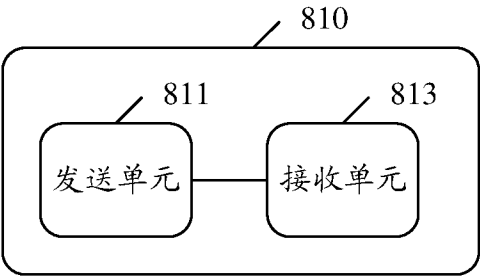


图 13

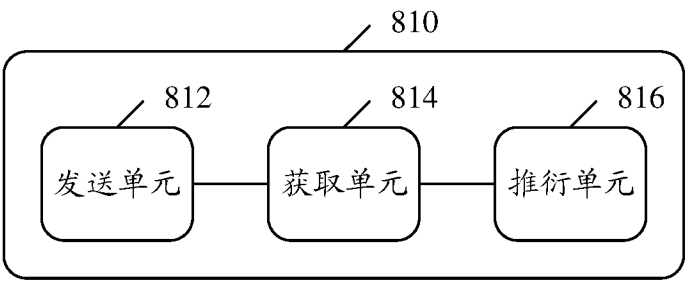


图 14

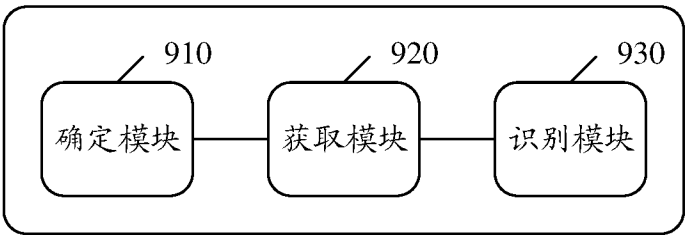


图 15

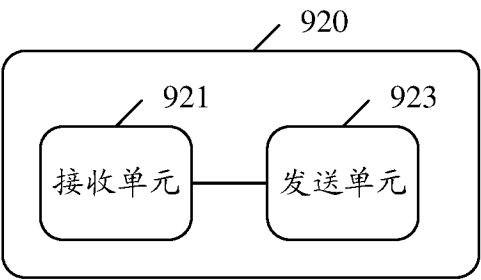


图 16

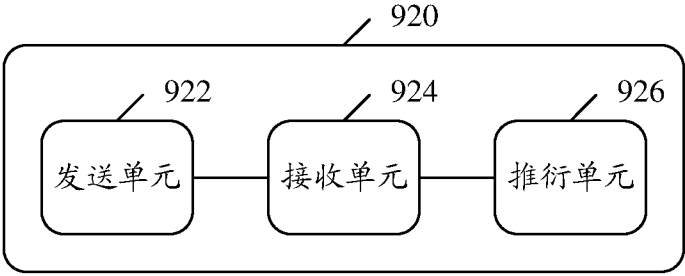


图 17

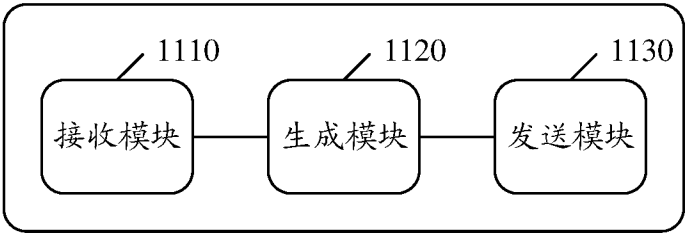


图 18

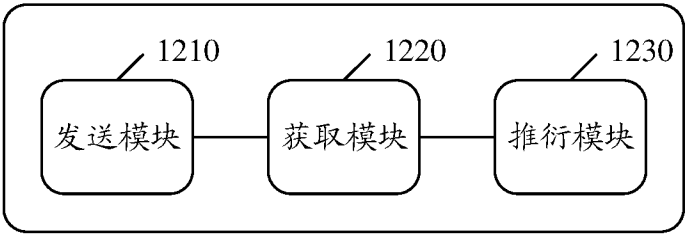


图 19

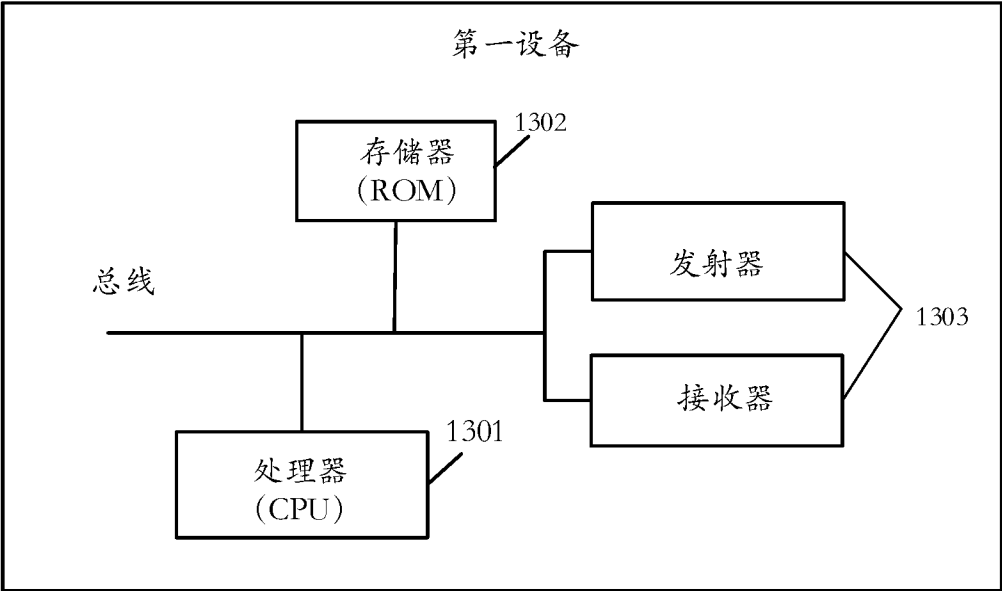


图 20

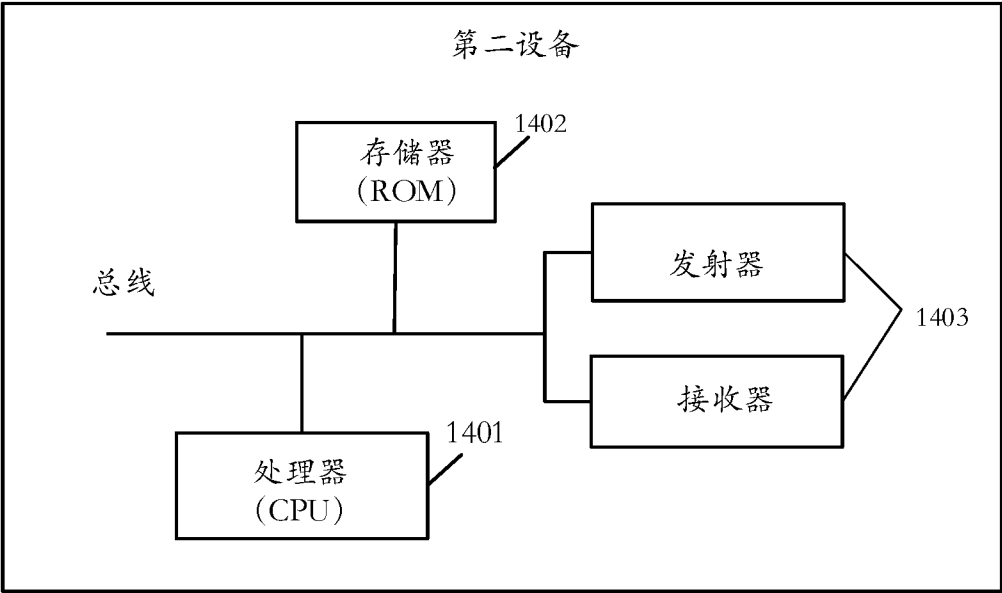


图 21

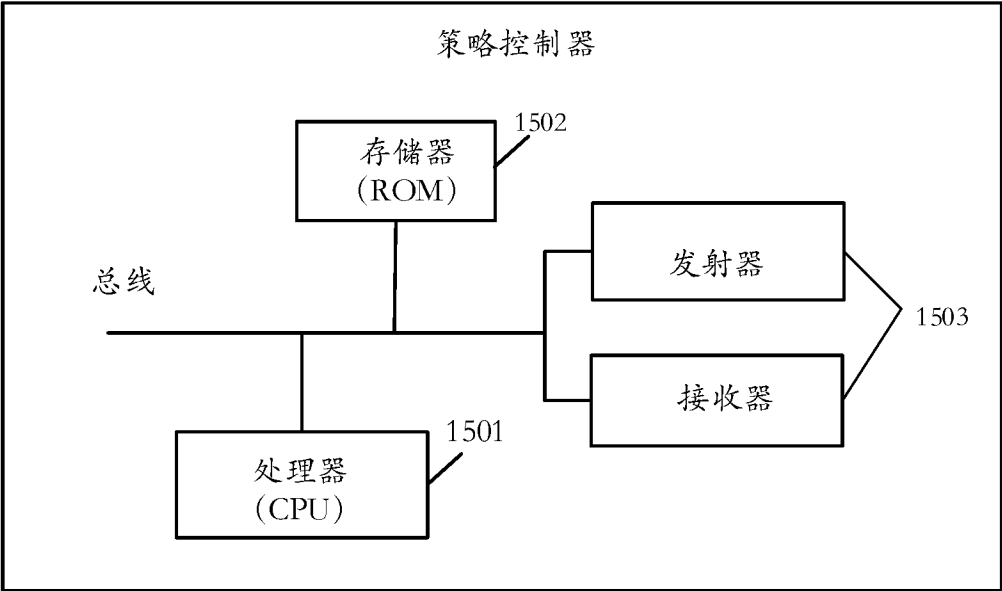


图 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/071818

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; H04W; H04Q

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)

WPI, EPODOC, CNPAT, CNKI: 安全 策略 密钥 会话 接入 终端 用户面 节点 网元 算法 生成 参数 第一 第二 security
policy key access session terminal user plane network element node algorithm generat+ parameter first second

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 103763697 A (SHANGHAI FEIXUN COMMUNICATION CO., LTD.), 30 April 2014 (30.04.2014), description, paragraphs [0054]-[0090], and figures 1-5	1-42, 52-93, 103
X	CN 101188851 A (ZTE CORP.), 28 May 2008 (28.05.2008), description, page 3, line 17 to page 7, line 5, and figures 1-2	43-46, 94-97
X	CN 104954125 A (HUAWEI TECHNOLOGIES CO., LTD.), 30 September 2015 (30.09.2015), description, paragraphs [0158]-[0165]	47-51, 98-102
A	EP 2104270 A1 (HUAWEI TECHNOLOGIES CO., LTD.), 23 September 2009 (23.09.2009), entire document	1-103

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“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
“A” document defining the general state of the art which is not considered to be of particular relevance	“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
“E” earlier application or patent but published on or after the international filing date	“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
“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)	“&” document member of the same patent family
“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	

Date of the actual completion of the international search 05 March 2018	Date of mailing of the international search report 03 April 2018
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 LI, Tingting Telephone No. (86-10) 53961728

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/071818

Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

[1] The claims comprise three inventions claimed in independent claims (1, 21, 52, 72, 103), independent claims (43, 94) and independent claims (47, 98). The first invention relates to that a first device, according to a security policy, uses a key to encrypt data, and then sends same to a second device. The second invention relates to the generation of the security policy. The third invention relates to the generation of the key. Same or corresponding technical features of the three inventions are: the security policy and the key. However, the same or corresponding technical features mentioned above are common general knowledge in the art. Therefore, the three inventions do not share a same or corresponding special technical feature that make a contribution over the prior art. The application therefore does not meet the requirement of unity of invention as defined in PCT Rule 13.1.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☒ As all searchable claims could be searched without effort justifying additional fees, this Authority did not invite payment of additional fees.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on protest

- ☐ The additional search fees were accompanied by the applicant's protest and, where applicable, the payment of a protest fee.
- ☐ The additional search fees were accompanied by the applicant's protest but the applicable protest fee was not paid within the time limit specified in the invitation.
- ☐ No protest accompanied the payment of additional search fees.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/071818

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103763697 A	30 April 2014	None	
CN 101188851 A	28 May 2008	None	
CN 104954125 A	30 September 2015	None	
EP 2104270 A1	23 September 2009	CN 1996860 A	11 July 2007
		WO 2008086702 A1	24 July 2008

国际检索报告

国际申请号

PCT/CN2018/071818

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; H04W; H04Q

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))

WPI, EPODOC, CNPAT, CNKI: 安全 策略 密钥 会话 接入 终端 用户面 节点 网元 算法 生成 参数 第一 第二 security policy key access session terminal user plane network element node algorithm generat+ parameter first second

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 103763697 A (上海斐讯数据通信技术有限公司) 2014年 4月 30日 (2014 - 04 - 30) 说明书第[0054]-[0090]段, 附图1-5	1-42, 52-93, 103
X	CN 101188851 A (中兴通讯股份有限公司) 2008年 5月 28日 (2008 - 05 - 28) 说明书第3页第17行至第7页第5行, 附图1-2	43-46, 94-97
X	CN 104954125 A (华为技术有限公司) 2015年 9月 30日 (2015 - 09 - 30) 说明书第[0158]-[0165]段	47-51, 98-102
A	EP 2104270 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 2009年 9月 23日 (2009 - 09 - 23) 全文	1-103

☐ 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

2018年 3月 5日

国际检索报告邮寄日期

2018年 4月 3日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局 (ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

李婷婷

传真号 (86-10) 62019451

电话号码 (86-10) 53961728

第III栏 缺乏发明单一性的意见(续第1页第3项)

本国际检索单位在该国际申请中发现多项发明，即：

- [1] 权利要求书包括独立权利要求（1、21、52、72、103）、以及独立权利要求（43、94）和独立权利要求（47、98）所要求保护的3项发明。第1项发明涉及第一设备根据安全策略使用密钥对数据进行加密后传送至第二设备，第2项发明涉及安全策略的生成，第3项发明涉及密钥的生成。上述3项发明的相同或相应的技术特征为：安全策略及密钥。然而，上述相同或相应的技术特征在本领域中均为公知常识。因此，上述3项发明不具有相同或相应的体现发明对现有技术做出贡献的特定技术特征，不具有单一性，不符合PCT细则13.1的规定。

1. ☐ 由于申请人按时缴纳了被要求缴纳的全部附加检索费，本国际检索报告涉及全部可作检索的权利要求。
2. ☒ 由于无需付出有理由要求附加费的劳动即能对全部可检索的权利要求进行检索，本单位未通知缴纳任何加费。
3. ☐ 由于申请人仅按时缴纳了部分被要求缴纳的附加检索费，本国际检索报告仅涉及已缴费的那些权利要求，具体地说，是权利要求：
4. ☐ 申请人未按时缴纳被要求缴纳的附加检索费。因此，本国际检索报告仅涉及权利要求书中首先提及的发明；包含该发明的权利要求是：

对异议的意见

- ☐ 申请人缴纳了附加检索费，同时提交了异议书，适用时，缴纳了异议费。
- ☐ 申请人缴纳了附加检索费，同时提交了异议书，但未在通知书规定的时间期限内缴纳异议费。
- ☐ 缴纳附加检索费时未提交异议书。

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/071818

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	103763697	A	2014年 4月 30日	无			
CN	101188851	A	2008年 5月 28日	无			
CN	104954125	A	2015年 9月 30日	无			
EP	2104270	A1	2009年 9月 23日	CN	1996860	A	2007年 7月 11日
				WO	2008086702	A1	2008年 7月 24日

表 PCT/ISA/210（同族专利附件）（2009年7月）