

一种密钥生成方法、终端设备及网络设备

相关申请的交叉引用

本申请基于申请号为 201910000352.X、申请日为 2019 年 1 月 2 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本申请涉及信息处理技术领域，尤其涉及一种密钥生成方法、终端设备、网络设备以及计算机存储介质。

背景技术

5G 将渗透到未来社会的各个领域，在构建以用户为中心的全方位信息生态系统中将起到关键作用。安全架构是 5G 网络正常运行的保障。认证协议是构建 5G 安全架构的基石。UE 和网络每次都要生成 DH 密钥交换相关的参数。生成这些参数需要使用非对称算法，这就要消耗大量的计算资源，这对于物联网终端尤其不可接受，并且，这种处理只能防御被动攻击（窃听），不能防止主动攻击（中间人攻击）。

发明内容

为解决上述技术问题，本申请实施例提供了一种密钥生成方法、终端设备、网络设备以及计算机存储介质。

第一方面，提供了一种密钥生成方法，应用于终端设备，所述方法包括：

基于长期密钥，确定第一密钥；

基于第一密钥以及至少一个附加密钥，生成本次会话密钥，基于所述

本次会话密钥与网络侧进行通信;

其中, 所述至少一个附加密钥中包括: 终端设备初次连接网络时生成的初始会话密钥, 和/或, 上一次通信使用的会话密钥; 所述第一密钥以及所述至少一个附加密钥均为对称密钥。

- 5 第二方面, 提供了一种密钥生成方法, 应用于网络设备, 所述方法包括:

基于终端设备所对应的长期密钥, 确定所述终端设备所对应的第一密钥;

- 10 基于所述第一密钥以及至少一个附加密钥, 生成所述终端设备所对应的本次会话密钥, 基于所述本次会话密钥与所述终端设备进行通信;

其中, 所述至少一个附加密钥中包括: 所述终端设备初次连接网络时生成的初始会话密钥, 和/或, 与所述终端设备上一次通信使用的会话密钥; 所述第一密钥以及所述至少一个附加密钥为对称密钥。

第三方面, 提供了一种终端设备, 包括:

- 15 第一密钥生成单元, 用于基于长期密钥, 确定第一密钥; 基于第一密钥以及至少一个附加密钥, 生成本次会话密钥;

第一通信单元, 用于基于所述本次会话密钥与网络侧进行通信;

- 20 其中, 所述至少一个附加密钥中包括: 终端设备初次连接网络时生成的初始会话密钥, 和/或, 上一次通信使用的会话密钥; 所述第一密钥以及所述至少一个附加密钥为对称密钥。

第四方面, 提供了一种终端设备, 包括:

第一处理器, 用于基于长期密钥, 确定第一密钥; 基于第一密钥以及至少一个附加密钥, 生成本次会话密钥;

第一通信接口, 用于基于所述本次会话密钥与网络侧进行通信;

- 25 其中, 所述至少一个附加密钥中包括: 终端设备初次连接网络时生成的初始会话密钥, 和/或, 上一次通信使用的会话密钥; 所述第一密钥以及

所述至少一个附加密钥为对称密钥。

第五方面，提供了一种网络设备，包括：

第二密钥生成单元，用于基于终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；基于所述第一密钥以及至少一个附加密钥，
5 生成所述终端设备所对应的本次会话密钥；

第二通信单元，用于基于所述本次会话密钥与所述终端设备进行通信；

其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

10 第六方面，提供了一种网络设备，包括：

第二处理器，用于基于终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥；

第二通信接口，用于基于所述本次会话密钥与所述终端设备进行通信；

15 其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

第七方面，提供了一种计算机存储介质，其上存储有计算机程序，其中，该计算机程序被处理器执行时实现前述方法的步骤

20 第七方面，提供了一种密钥生成系统，所述系统包括：至少一个终端设备、鉴权服务功能 AUSF 实体；其中，

所述终端设备，用于基于长期密钥，确定第一密钥；基于第一密钥以及至少一个附加密钥，生成本次会话密钥，基于所述本次会话密钥与网络侧进行通信；

25 所述 AUSF 实体，用于基于所述终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；基于所述第一密钥以及至少一个附加密钥，

生成所述终端设备所对应的本次会话密钥，基于所述本次会话密钥与所述终端设备进行通信；其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

5 本申请实施例的技术方案，就能够在生成最终的会话密钥的时候，除了根据长期密钥之外，还可以利用终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥，共同进行本次会话密钥的生成；如此，不需要对原有的认证协议做大的改动就可实现会话密钥的安全性增强。并且，采用对称密钥算法对设备的运算要求很低，进而消耗的功
10 耗也较低，因此，更加适合在物联网场景下使用。

附图说明

图 1 是本申请实施例提供的一种密钥生成方法流程示意性图 1；
图 2 是本申请实施例提供的一种密钥生成方法流程示意性图 2；
图 3 为本申请实施例提供的一种密钥生成方法流程示意图 3；
15 图 4 为本申请实施例提供的一种终端设备组成结构示意图 1；
图 5 为本申请实施例提供的一种终端设备组成结构示意图 2；
图 6 为本申请实施例提供的一种网络设备组成结构示意图 1；
图 7 为本申请实施例提供的一种网络设备组成结构示意图 2；
图 8 为本申请实施例提供的一种系统组成结构示意图。

20

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述，显然，所描述的实施例是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动
25 的前提下所获得的所有其他实施例，都属于本申请保护的范围。

如图 1 所示, 本申请实施例提供了一种密钥生成方法, 应用于终端设备, 所述方法包括:

步骤 101: 基于长期密钥, 确定第一密钥;

步骤 102: 基于第一密钥以及至少一个附加密钥, 生成本次会话密钥,
5 基于所述本次会话密钥与网络侧进行通信;

其中, 所述至少一个附加密钥中包括: 终端设备初次连接网络时生成的初始会话密钥, 和/或, 上一次通信使用的会话密钥; 所述第一密钥以及所述至少一个附加密钥为对称密钥。

本实施例提供了多种具体处理场景, 下面分别进行说明:

10 场景 1、采用初始会话密钥以及第一密钥生成本次会话密钥, 说明如下:

所述基于长期密钥, 确定第一密钥之前, 所述方法还包括: 当初次连接网络, 完成与鉴权服务功能之间的相互认证时, 生成初始会话密钥。

即终端设备第一次连接网络, 完成与鉴权服务功能 (AUSF, Authentication Server Function) 间的相互认证, 生成第一密钥, 可以记为
15 KSEAF_first;

后续所述基于第一密钥、以及至少一个附加密钥, 生成本次会话密钥, 包括: 基于所述第一密钥、以及所述初始会话密钥, 生成本次会话密钥。

也就是说, 终端设备与 AUSF 完成相互认证后, 最终会话密钥 KSEAF* 的生成除了使用长期密钥 K 推演出的第一密钥 KSEAF 外, 再加上第一个初
20 始会话密钥 KSEAF_first。

终端设备第一次连接网络, 完成与 AUSF 间的相互认证, 生成第一个会话密钥 KSEAF_first. 后续终端设备与 AUSF 完成相互认证后, 最终会话密钥的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外, 还要加上第一个会话密钥 KSEAF_first。

25 参见图 2, 此方案的步骤如下:

网络侧对用户终端设备要进行次认证时, 根据终端设备的 Profile 确定

使用何种认证协议对终端设备进行认证；其中，所述认证协议可以为 5G AKA 或 EAP-AKA'，当然，认证协议还可以有其他的协议，只是本实施例中并不做穷举。另外，关于用户的终端设备的相关信息 profile，可以在终端设备与网络侧进行签约的时候，写入统一数据管理(UDM, Unified Data Management)中，然后当终端设备需要进行认证的时候，由 UDM 来确定终端设备采用哪种认证协议进行处理；

终端设备和网络侧使用选定的认证协议进行相互认证；比如，具体的可以为终端设备，比如 UE，与 UDM/ARPF 之间通过选定的认证协议，相互认证。

10 认证结束后，终端设备和网络侧的 AUSF 都获得基于长期密钥 K 而推导出的第一密钥，可以表示为 KSEAF。

最后，终端设备和 AUSF 分别使用第一密钥 KSEAF 和存储在安全区域的初始会话密钥 KSEAF_{frist}，生成本次会话密钥 KSEAF*。其计算可以如下表示：

15 $KSEAF^* = KDF(KSEAF, KSEAF_{frist}, AP)$;

其中，KDF 表征密钥推演函数，如 HMAC-SHA-256；AP 是辅助参数用于辅助功能，如防止 bidding down 攻击，需要理解的是，AP 是可选参数，可以不使用也可以使用，因此 AP 也可能不出现在公式里。

其中，初始会话密钥可以分别在终端设备以及网络侧的 AUSF 中进行保存，具体来说，终端设备侧：存储在 USIM 或信息不可篡改的存储区域；AUSF 存储在信息不可篡改的存储区域。

需要说明的是，终端设备与网络侧进行初次连接的时候，并进行初次认证的时候，初始会话密钥可以设置为空，即与用户第一次认证时，KSEAF_{frist}=null。网络与用户第一次认证后，生成的第一个会话密钥 KSEAF*设为初始会话密钥 KSEAF_{frist}，并长期存储在终端设备和 AUSF。

关于 5G AKA 或 EAP-AKA'：前者是基于 LTE 的认证协议 EPS-AKA

发展而来，而后者是一个 IETF 定义的认证协议用于 4G 网络中 UE 使用 WIFI 接入运营商网络。在 5G 中，UE 基于 EAP-AKA' 不仅能通过 WIFI 接入运营商网络，而且通过 5G 无线接入网也能接入运营商网络。

AKA 认证协议依靠存储在 USIM 中的根密钥 K 实现 UE 和网络之间的相互认证，并导出会话密钥。安全的假设条件是根密钥 K 除了网络运营商外，别人都不知道，从而攻击者也无法推导出会话密钥。然而，报告[1]表明，这种假设并不总是正确的，因为根密钥 K 可能在 USIM 卡的生产阶段就被泄露。因此，被动攻击者可以使用从根密钥 K，以及 UE 和网络之间交换消息而衍生的会话密钥来窃听通信。一个主动攻击者可能会利用偷来的大量根密钥伪造基站而发起中间人攻击。长期密钥泄密已经在 TR33.899 中的 5.2.3.2 节被认为是一个关键问题。5G-AKA 和 EAP-AKA' 都会受到长期密钥泄露的威胁，因为它们都是基于 AKA 认证协议扩展而来的。

如此，能保证最终会话密钥 KSEAF*的安全性，因它的生成除了依赖于基于根密钥 K 而生成的密钥 KSEAF，还依赖于第一个会话密钥 KSEAF_first。攻击者无法获得最终会话密钥 KSEAF*，除非攻击者能获得第一个会话密钥 KSEAF_first，这是比较低的概率。

场景 2、基于上一次通信的会话密钥，生成本次会话密钥，说明如下：

所述基于第一密钥、以及至少一个附加密钥，生成本次会话密钥，包括：

基于所述第一密钥、以及上一次通信使用的会话密钥，生成本次会话密钥。

即终端设备与 AUSF 完成相互认证后，最终本次会话密钥 KSEAF*的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外，还要加上存储的上次生成的会话密钥 KSEAF_pre。

终端设备与 AUSF 完成相互认证后，最终会话密钥的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外，还要加上存储的上次生成的会话密钥

KSEAF_pre。

同样可以参见图 2，具体如下：

网络侧对用户终端设备要进行认证时，根据终端设备的 Profile 确定使用何种认证协议对终端设备进行认证；其中，所述认证协议可以为 5G AKA 或 EAP-AKA'，当然，认证协议还可以有其他的协议，只是本实施例中并不做穷举。另外，关于用户的终端设备的相关信息 profile，可以在终端设备与网络侧进行签约的时候，写入统一数据管理(UDM, Unified Data Management)中，然后当终端设备需要进行认证的时候，由 UDM 来确定终端设备采用哪种认证协议进行处理；

10 终端设备和网络侧使用选定的认证协议进行相互认证；比如，具体的可以为终端设备，比如 UE，与 UDM/ARPF 之间通过选定的认证协议，相互认证。

认证结束后，终端设备和 AUSF 都获得基于长期密钥 K 而推导出的会话密钥 KSEAF。

15 终端设备和 AUSF 分别使用 KSEAF 和存储在安全区域的 KSEAF_pre 生成最终会话密钥 KSEAF*，其计算如下：

$$KSEAF^* = KDF(KSEAF, KSEAF_pre, AP)$$

其中，KDF 是密钥推演函数，如 HMAC-SHA-256，AP 是辅助参数用于辅助功能，如防止 bidding down 攻击，AP 是可选参数，也可能不出现在公式里。

20 需要指出的是，网络与用户第一次认证时，上一次通信使用的会话密钥可以设置为空，比如 KSEAF_pre=null。终端设备和网络生成本次会话密钥 KSEAF*后，会用它替换存储在终端设备和网络中的上一次通信使用的会话密钥 KSEAF_pre。也就是说，本次会话密钥在生成之后，可以分别在终端设备以及网络侧进行存储，并且，替换上一次通信使用的会话密钥进行存储，进而，在下一次再次生成会话密钥的时候，采用替换后的上一次

通信使用的会话密钥进行下一次会话密钥的生成，其处理方式与本场景上述说明是相同的，因此不再赘述。

如此，能保证最终会话密钥 KSEAF*的安全性，因它的生成除了依赖于基于长期密钥 K 而生成的密钥 KSEAF，还依赖于上次存储的会话密钥 KSEAF_pre。攻击者无法获得最终会话密钥 KSEAF*，除非攻击者能获得上次存储的会话密钥 KSEAF_pre。这要求攻击者能持续的获得上次存储的会话密钥 KSEAF_pre，才能持续获得最终会话密钥。

场景 3、基于初始会话密钥、以及上一次通信使用的会话密钥，共同生成本次会话密钥；具体说明如下：

所述基于第一密钥、以及至少一个附加密钥，生成本次会话密钥，包括：

基于所述第一密钥、初始会话密钥、以及上一次通信使用的会话密钥，生成本次会话密钥。

也就是说，本场景基于场景 1、2，最终会话密钥 KSEAF*的生成除了使用长期密钥 K 推演出的第一密钥 KSEAF 外，还要使用初始会话密钥 KSEAF_first 和上次生成的会话密钥 KSEAF_pre。

关于初始会话密钥以及上一次通信使用的会话密钥的生成以及保存与场景 1、2 相同，这里不做赘述。

与场景 1、2 不同之处在于，本场景中，进行会话密钥的生成时，除了使用长期密钥 K 推演出的第一密钥 KSEAF 外，还要使用初始会话密钥 KSEAF_first 和上次生成的会话密钥 KSEAF_pre。最终会话密钥 KSEAF*的计算如下：

$$KSEAF^*=KDF(KSEAF, KSEAF_frist, KSEAF_pre, AP)$$

这里 KDF 是密钥推演函数，如 HMAC-SHA-256，AP 是辅助参数用于辅助功能，如防止 bidding down 攻击，AP 是可选参数，也可能不出现在公式里。需要指出的是，网络与用户第一次认证时，KSEAF_pre=null，

KSEAF_frist=null。

本场景 3 的安全性比场景 1、2 更高，因为在此方案中，攻击者要获得最终会话密钥，既需要能获得第一个会话密钥，又需要能持续获得上次存储的会话密钥 KSEAF_pre。

5 最后需要指出的是，本实施例提供的场景都只使用对称密钥算法（密钥推演算法）。

可见，通过采用上述方案，就能够在生成最终的会话密钥的时候，除了根据长期密钥之外，还可以利用终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥，共同进行本次会话密钥的生成；如此，不需要对原有的认证协议做大的改动就可实现会话密钥的安全性增强。并且，采用对称密钥算法对设备的运算要求很低，进而消耗的功耗也较低，因此，更加适合在物联网场景下使用。

如图 3 所示，本申请实施例提供了一种密钥生成方法，应用于网络设备，所述方法包括：

步骤 301：基于终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；

步骤 302：基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥，基于所述本次会话密钥与所述终端设备进行通信；

其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

本实施例中所涉及的网络设备，可以认为是网络侧具备 AUSF 功能的设备。

本实施例提供了多种具体处理场景，下面分别进行说明：

场景 1、采用初始会话密钥以及第一密钥生成本次会话密钥,说明如下:

所述基于终端设备所对应的长期密钥, 确定所述终端设备所对应的第一密钥之前, 所述方法还包括:

当所述终端设备初次连接网络, 完成与鉴权服务功能之间的相互认证
5 时, 生成网络侧与所述终端设备通信所使用的初始会话密钥。

即终端设备第一次连接网络, 完成与鉴权服务功能 (AUSF, Authentication Server Function) 间的相互认证, 生成第一密钥, 可以记为 KSEAF_first;

所述基于所述第一密钥以及至少一个附加密钥, 生成所述终端设备所
10 对应的本次会话密钥, 包括:

基于所述终端设备所对应的第一密钥、以及所述终端设备初次连接网络时生成的初始会话密钥, 生成所述终端设备的本次会话密钥。

也就是说, 终端设备与 AUSF 完成相互认证后, 最终会话密钥 KSEAF* 的生成除了使用长期密钥 K 推演出的第一密钥 KSEAF 外, 再加上第一个初
15 始会话密钥 KSEAF_first。

终端设备第一次连接网络, 完成与 AUSF 间的相互认证, 生成第一个会话密钥 KSEAF_first. 后续终端设备与 AUSF 完成相互认证后, 最终会话密钥的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外, 还要加上第一个会话密钥 KSEAF_first。

20 参见图 2, 此方案的步骤如下:

网络侧的 UDM 对用户终端设备要进行次认证时, 根据终端设备的 Profile 确定使用何种认证协议对终端设备进行认证; 其中, 所述认证协议可以为 5G AKA 或 EAP-AKA', 当然, 认证协议还可以有其他的协议, 只是本实施例中并不做穷举。另外, 关于用户的终端设备的相关信息 profile,
25 可以在终端设备与网络侧进行签约的时候, 写入统一数据管理 (UDM, Unified Data Management) 中, 然后当终端设备需要进行认证的时候, 由

UDM 来确定终端设备采用哪种认证协议进行处理;

终端设备和网络侧使用选定的认证协议进行相互认证; 比如, 具体的可以为终端设备, 比如 UE, 与 UDM/ARPF 之间通过选定的认证协议, 相互认证。

- 5 认证结束后, 终端设备和网络侧的网络设备, 如 AUSF 都获得基于长期密钥 K 而推导出的第一密钥, 可以表示为 KSEAF。

最后, 终端设备和 AUSF 分别使用第一密钥 KSEAF 和存储在安全区域的初始会话密钥 KSEAF_{frist}, 生成本次会话密钥 KSEAF*。其计算可以如下表示:

- 10 $KSEAF^* = KDF(KSEAF, KSEAF_{frist}, AP)$;

其中, KDF 表征密钥推演函数, 如 HMAC-SHA-256; AP 是辅助参数用于辅助功能, 如防止 bidding down 攻击, 需要理解的是, AP 是可选参数, 可以不使用也可以使用, 因此 AP 也可能不出现在公式里。

- 其中, 初始会话密钥可以分别在终端设备以及网络侧的 AUSF 中进行
15 保存, 具体来说, 终端设备侧: 存储在 USIM 或信息不可篡改的存储区域; AUSF 存储在信息不可篡改的存储区域。

- 需要说明的是, 终端设备与网络侧进行初次连接的时候, 并进行初次认证的时候, 初始会话密钥可以设置为空, 即与用户第一次认证时, KSEAF_{frist}=null。网络与用户第一次认证后, 生成的第一个会话密钥
20 KSEAF*设为初始会话密钥 KSEAF_{frist}, 并长期存储在终端设备和 AUSF。

如此, 能保证最终会话密钥 KSEAF*的安全性, 因它的生成除了依赖于基于根密钥 K 而生成的密钥 KSEAF, 还依赖于第一个会话密钥 KSEAF_{frist}。攻击者无法获得最终会话密钥 KSEAF*, 除非攻击者能获得第一个会话密钥 KSEAF_{frist}, 这是比较低的概率。

- 25 场景 2、基于上一次通信的会话密钥, 生成本次会话密钥, 说明如下:
所述基于所述第一密钥以及至少一个附加密钥, 生成所述终端设备所

对应的本次会话密钥，包括：

基于所述第一密钥、以及与所述终端设备上一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

即终端设备与 AUSF 完成相互认证后，最终本次会话密钥 KSEAF*的
5 生成除了使用长期密钥 K 推演出的密钥 KSEAF 外，还要加上终端以及网络设备均存储的上次与终端设备进行通信时生成的会话密钥 KSEAF_pre。

终端设备与 AUSF 完成相互认证后，最终会话密钥的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外，还要加上存储的上次生成的会话密钥 KSEAF_pre。

10 同样可以参见图 2，具体如下：

网络侧对用户终端设备要进行认证时，根据终端设备的 Profile 确定使用何种认证协议对终端设备进行认证；其中，所述认证协议可以为 5G AKA 或 EAP-AKA'，当然，认证协议还可以有其他的协议，只是本实施例中并不做穷举。另外，关于用户的终端设备的相关信息 profile，可以在
15 终端设备与网络侧进行签约的时候，写入统一数据管理(UDM, Unified Data Management)中，然后当终端设备需要进行认证的时候，由 UDM 来确定终端设备采用哪种认证协议进行处理；

终端设备和网络侧使用选定的认证协议进行相互认证；比如，具体的可以为终端设备，比如 UE，与 UDM/ARPF 之间通过选定的认证协议，相
20 互认证。

认证结束后，终端设备和 AUSF 都获得基于长期密钥 K 而推导出的会话密钥 KSEAF。

终端设备和 AUSF 分别使用 KSEAF 和存储在安全区域的 KSEAF_pre 生成最终会话密钥 KSEAF*，其计算如下：

25
$$KSEAF^* = KDF(KSEAF, KSEAF_pre, AP)$$

其中，KDF 是密钥推演函数，如 HMAC-SHA-256，AP 是辅助参数用

于辅助功能，如防止 bidding down 攻击，AP 是可选参数，也可能不出现在公式里。

需要指出的是，网络与用户第一次认证时，上一次通信使用的会话密钥可以设置为空，比如 $KSEAF_pre = null$ 。终端设备和网络生成本次会话密钥 $KSEAF^*$ 后，会用它替换存储在终端设备和网络中的上一次通信使用的会话密钥 $KSEAF_pre$ 。也就是说，本次会话密钥在生成之后，可以分别在终端设备以及网络侧进行存储，并且，替换上一次通信使用的会话密钥进行存储，进而，在下次再次生成会话密钥的时候，采用替换后的上一次通信使用的会话密钥进行下次会话密钥的生成，其处理方式与本场景上述说明是相同的，因此不再赘述。

如此，能保证最终会话密钥 $KSEAF^*$ 的安全性，因它的生成除了依赖于基于长期密钥 K 而生成的密钥 $KSEAF$ ，还依赖于上次存储的会话密钥 $KSEAF_pre$ 。攻击者无法获得最终会话密钥 $KSEAF^*$ ，除非攻击者能获得上次存储的会话密钥 $KSEAF_pre$ 。这要求攻击者能持续的获得上次存储的会话密钥 $KSEAF_pre$ ，才能持续获得最终会话密钥。

场景 3、基于初始会话密钥、以及上一次通信使用的会话密钥，共同生成本次会话密钥；具体说明如下：

基于所述第一密钥、所述终端设备初次连接网络时生成的初始会话密钥、以及与所述终端设备上一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

也就是说，本场景基于场景 1、2，最终会话密钥 $KSEAF^*$ 的生成除了使用长期密钥 K 推演出的第一密钥 $KSEAF$ 外，还要使用初始会话密钥 $KSEAF_first$ 和上次生成的会话密钥 $KSEAF_pre$ 。

关于初始会话密钥以及上一次通信使用的会话密钥的生成以及保存于场景 1、2 相同，这里不做赘述。

与场景 1、2 不同之处在于，本场景中，进行会话密钥的生成时，除了

使用长期密钥 K 推演出的第一密钥 KSEAF 外，还要使用初始会话密钥 KSEAF_first 和上次生成的会话密钥 KSEAF_pre。最终会话密钥 KSEAF* 的计算如下：

$$\text{KSEAF*} = \text{KDF}(\text{KSEAF}, \text{KSEAF_frist}, \text{KSEAF_pre}, \text{AP})$$

- 5 这里 KDF 是密钥推演函数，如 HMAC-SHA-256，AP 是辅助参数用于辅助功能，如防止 bidding down 攻击，AP 是可选参数，也可能不出现在公式里。需要指出的是，网络与用户第一次认证时，KSEAF_pre=null，KSEAF_frist=null。

- 10 本场景 3 的安全性比场景 1、2 更高，因为在此方案中，攻击者要获得最终会话密钥，既需要能获得第一个会话密钥，又需要能持续获得上次存储的会话密钥 KSEAF_pre。

最后需要指出的是，本实施例提供的场景都只使用对称密钥算法（密钥推演算法）。采用对称密钥算法对设备的运算要求很低，进而消耗的功耗也很低。因此，更加适合在物联网场景下使用。

- 15 可见，通过采用上述方案，就能够在生成最终的会话密钥的时候，除了根据长期密钥之外，还可以利用终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥，共同进行本次会话密钥的生成；如此，不需要对原有的认证协议做大的改动就可实现会话密钥的安全性增强。

- 20 如图 4 所示，本申请实施例提供了一种终端设备，包括：

第一密钥生成单元 41，用于基于长期密钥，确定第一密钥；基于第一密钥以及至少一个附加密钥，生成本次会话密钥；

第一通信单元 42，用于基于所述本次会话密钥与网络侧进行通信；

- 25 其中，所述至少一个附加密钥中包括：终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

如图 5 所示, 本申请实施例提供了一种终端设备, 包括:

第一处理器 51, 用于基于长期密钥, 确定第一密钥; 基于第一密钥以及至少一个附加密钥, 生成本次会话密钥;

第一通信接口 52, 用于基于所述本次会话密钥与网络侧进行通信;

5 其中, 所述至少一个附加密钥中包括: 终端设备初次连接网络时生成的初始会话密钥, 和/或, 上一次通信使用的会话密钥; 所述第一密钥以及所述至少一个附加密钥为对称密钥。

本实施例提供了多种具体处理场景, 下面分别进行说明:

场景 1、采用初始会话密钥以及第一密钥生成本次会话密钥, 说明如下:

10 所述第一处理器 51, 用于当初次连接网络, 完成与鉴权服务功能之间的相互认证时, 生成初始会话密钥。

即终端设备第一次连接网络, 完成与鉴权服务功能 (AUSF, Authentication Server Function) 间的相互认证, 生成第一密钥, 可以记为 KSEAF_first;

15 后续第一处理器 51, 用于基于所述第一密钥、以及所述初始会话密钥, 生成本次会话密钥。

也就是说, 终端设备与 AUSF 完成相互认证后, 最终会话密钥 KSEAF* 的生成除了使用长期密钥 K 推演出的第一密钥 KSEAF 外, 再加上第一个初始会话密钥 KSEAF_first。

20 终端设备第一次连接网络, 完成与 AUSF 间的相互认证, 生成第一个会话密钥 KSEAF_first. 后续终端设备与 AUSF 完成相互认证后, 最终会话密钥的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外, 还要加上第一个会话密钥 KSEAF_first。

参见图 2, 此方案的步骤如下:

25 网络侧对用户终端设备要进行次认证时, 根据终端设备的 Profile 确定使用何种认证协议对终端设备进行认证; 其中, 所述认证协议可以为 5G

AKA 或 EAP-AKA'，当然，认证协议还可以有其他的协议，只是本实施例中并不做穷举。另外，关于用户的终端设备的相关信息 profile，可以在终端设备与网络侧进行签约的时候，写入统一数据管理(UDM, Unified Data Management)中，然后当终端设备需要进行认证的时候，由 UDM 来确定

5 终端设备采用哪种认证协议进行处理；

终端设备和网络侧使用选定的认证协议进行相互认证；比如，具体的可以为终端设备，比如 UE，与 UDM/ARPF 之间通过选定的认证协议，相互认证。

认证结束后，终端设备和网络侧的 AUSF 都获得基于长期密钥 K 而推

10 导出的第一密钥，可以表示为 KSEAF。

最后，终端设备和 AUSF 分别使用第一密钥 KSEAF 和存储在安全区域的初始会话密钥 KSEAF_frist，生成本次会话密钥 KSEAF*。其计算可以如下表示：

$$KSEAF^* = KDF(KSEAF, KSEAF_frist, AP);$$

15 其中，KDF 表征密钥推演函数，如 HMAC-SHA-256；AP 是辅助参数用于辅助功能，如防止 bidding down 攻击，需要理解的是，AP 是可选参数，可以不使用也可以使用，因此 AP 也可能不出现在公式里。

其中，初始会话密钥可以分别在终端设备以及网络侧的 AUSF 中进行保存，具体来说，终端设备侧：存储在 USIM 或信息不可篡改的存储区域；

20 AUSF 存储在信息不可篡改的存储区域。

需要说明的是，终端设备与网络侧进行初次连接的时候，并进行初次认证的时候，初始会话密钥可以设置为空，即与用户第一次认证时，KSEAF_frist=null。网络与用户第一次认证后，生成的第一个会话密钥 KSEAF* 设为初始会话密钥 KSEAF_first，并长期存储在终端设备和 AUSF。

25 如此，能保证最终会话密钥 KSEAF* 的安全性，因它的生成除了依赖于基于根密钥 K 而生成的密钥 KSEAF，还依赖于第一个会话密钥

KSEAF_first。攻击者无法获得最终会话密钥 KSEAF*，除非攻击者能获得第一个会话密钥 KSEAF_first，这是比较低的概率。

场景 2、基于上一次通信的会话密钥，生成本次会话密钥，说明如下：

所述第一处理器 51，用于基于所述第一密钥、以及上一次通信使用的
5 会话密钥，生成本次会话密钥。

即终端设备与 AUSF 完成相互认证后，最终本次会话密钥 KSEAF*的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外，还要加上存储的上次生成的会话密钥 KSEAF_pre。

终端设备与 AUSF 完成相互认证后，最终会话密钥的生成除了使用长
10 期密钥 K 推演出的密钥 KSEAF 外，还要加上存储的上次生成的会话密钥 KSEAF_pre。

同样可以参见图 2，具体如下：

网络侧对用户终端设备要进行认证时，根据终端设备的 Profile 确定使用何种认证协议对终端设备进行认证；其中，所述认证协议可以为 5G
15 AKA 或 EAP-AKA'，当然，认证协议还可以有其他的协议，只是本实施例中并不做穷举。另外，关于用户的终端设备的相关信息 profile，可以在终端设备与网络侧进行签约的时候，写入统一数据管理(UDM, Unified Data Management)中，然后当终端设备需要进行认证的时候，由 UDM 来确定终端设备采用哪种认证协议进行处理；

20 终端设备和网络侧使用选定的认证协议进行相互认证；比如，具体的可以为终端设备，比如 UE，与 UDM/ARPF 之间通过选定的认证协议，相互认证。

认证结束后，终端设备和 AUSF 都获得基于长期密钥 K 而推导出的会话密钥 KSEAF。

25 终端设备和 AUSF 分别使用 KSEAF 和存储在安全区域的 KSEAF_pre 生成最终会话密钥 KSEAF*，其计算如下：

$KSEAF^* = KDF(KSEAF, KSEAF_pre, AP)$

其中，KDF 是密钥推演函数，如 HMAC-SHA-256，AP 是辅助参数用于辅助功能，如防止 bidding down 攻击，AP 是可选参数，也可能不出现在公式里。

5 需要指出的是，网络与用户第一次认证时，上一次通信使用的会话密钥可以设置为空，比如 $KSEAF_pre = null$ 。终端设备和网络生成本次会话密钥 $KSEAF^*$ 后，会用它替换存储在终端设备和网络中的上一次通信使用的会话密钥 $KSEAF_pre$ 。也就是说，本次会话密钥在生成之后，可以分别在终端设备以及网络侧进行存储，并且，替换上一次通信使用的会话密钥进行存储，进而，在下一次再次生成会话密钥的时候，采用替换后的上一次通信使用的会话密钥进行下一次会话密钥的生成，其处理方式与本场景上述说明是相同的，因此不再赘述。

如此，能保证最终会话密钥 $KSEAF^*$ 的安全性，因它的生成除了依赖于基于长期密钥 K 而生成的密钥 $KSEAF$ ，还依赖于上次存储的会话密钥 $KSEAF_pre$ 。攻击者无法获得最终会话密钥 $KSEAF^*$ ，除非攻击者能获得上次存储的会话密钥 $KSEAF_pre$ 。这要求攻击者能持续的获得上次存储的会话密钥 $KSEAF_pre$ ，才能持续获得最终会话密钥。

场景 3、基于初始会话密钥、以及上一次通信使用的会话密钥，共同生成本次会话密钥；具体说明如下：

20 所述第一处理器 51，用于基于所述第一密钥、初始会话密钥、以及上一次通信使用的会话密钥，生成本次会话密钥。

也就是说，本场景基于场景 1、2，最终会话密钥 $KSEAF^*$ 的生成除了使用长期密钥 K 推演出的第一密钥 $KSEAF$ 外，还要使用初始会话密钥 $KSEAF_first$ 和上次生成的会话密钥 $KSEAF_pre$ 。

25 关于初始会话密钥以及上一次通信使用的会话密钥的生成以及保存于场景 1、2 相同，这里不做赘述。

与场景 1、2 不同之处在于，本场景中，进行会话密钥的生成时，除了使用长期密钥 K 推演出的第一密钥 KSEAF 外，还要使用初始会话密钥 KSEAF_first 和上次生成的会话密钥 KSEAF_pre。最终会话密钥 KSEAF* 的计算如下：

5 $KSEAF^* = KDF(KSEAF, KSEAF_frist, KSEAF_pre, AP)$

这里 KDF 是密钥推演函数，如 HMAC-SHA-256，AP 是辅助参数用于辅助功能，如防止 bidding down 攻击，AP 是可选参数，也可能不出现在公式里。需要指出的是，网络与用户第一次认证时，KSEAF_pre=null，KSEAF_frist=null。

10 本场景 3 的安全性比场景 1、2 更高，因为在此方案中，攻击者要获得最终会话密钥，既需要能获得第一个会话密钥，又需要能持续获得上次存储的会话密钥 KSEAF_pre。

最后需要指出的是，本实施例提供的场景都只使用对称密钥算法（密钥推演算法）。采用对称密钥算法对设备的运算要求很低，进而消耗的功耗也很低。因此，更加适合在物联网场景下使用。

可见，通过采用上述方案，就能够在生成最终的会话密钥的时候，除了根据长期密钥之外，还可以利用终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥，共同进行本次会话密钥的生成；如此，不需要对原有的认证协议做大的改动就可实现会话密钥的安全性增强。

如图 6 所示，本申请实施例提供了一种网络设备，所述方法包括：

第二密钥生成单元 61，用于基于终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥；

25 第二通信单元 62，用于基于所述本次会话密钥与所述终端设备进行通信；

其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

如图 7 所示，本申请实施例提供了一种网络设备，所述方法包括：

- 5 第二处理器 71，用于基于终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥；

第二通信接口 72，用于基于所述本次会话密钥与所述终端设备进行通信；

- 10 其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

本实施例中所涉及的网络设备，可以认为是网络侧具备 AUSF 功能的设备。

- 15 本实施例提供了多种具体处理场景，下面分别进行说明：

场景 1、采用初始会话密钥以及第一密钥生成本次会话密钥，说明如下：

所述第二处理器 71，用于当所述终端设备初次连接网络，完成与鉴权服务功能之间的相互认证时，生成网络侧与所述终端设备通信所使用的初始会话密钥。

- 20 即终端设备第一次连接网络，完成与鉴权服务功能（AUSF，Authentication Server Function）间的相互认证，生成第一密钥，可以记为 KSEAF_first；

- 所述第二处理器 71，用于基于所述终端设备所对应的第一密钥、以及所述终端设备初次连接网络时生成的初始会话密钥，生成所述终端设备的
25 本次会话密钥。

也就是说，终端设备与 AUSF 完成相互认证后，最终会话密钥 KSEAF*

的生成除了使用长期密钥 K 推演出的第一密钥 KSEAF 外,再加上第一个初始会话密钥 KSEAF_first。

终端设备第一次连接网络,完成与 AUSF 间的相互认证,生成第一个会话密钥 KSEAF_first。后续终端设备与 AUSF 完成相互认证后,最终会话密钥的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外,还要加上第一个会话密钥 KSEAF_first。

参见图 2,此方案的步骤如下:

网络侧的 UDM 对用户终端设备要进行认证时,根据终端设备的 Profile 确定使用何种认证协议对终端设备进行认证;其中,所述认证协议可以为 5G AKA 或 EAP-AKA',当然,认证协议还可以有其他的协议,只是本实施例中并不做穷举。另外,关于用户的终端设备的相关信息 profile,可以在终端设备与网络侧进行签约的时候,写入统一数据管理(UDM, Unified Data Management)中,然后当终端设备需要进行认证的时候,由 UDM 来确定终端设备采用哪种认证协议进行处理;

终端设备和网络侧使用选定的认证协议进行相互认证;比如,具体的可以为终端设备,比如 UE,与 UDM/ARPF 之间通过选定的认证协议,相互认证。

认证结束后,终端设备和网络侧的网络设备,如 AUSF 都获得基于长期密钥 K 而推导出的第一密钥,可以表示为 KSEAF。

最后,终端设备和 AUSF 分别使用第一密钥 KSEAF 和存储在安全区域的初始会话密钥 KSEAF_frist,生成本次会话密钥 KSEAF*。其计算可以如下表示:

$$KSEAF^*=KDF(KSEAF, KSEAF_frist, AP);$$

其中, KDF 表征密钥推演函数,如 HMAC-SHA-256; AP 是辅助参数用于辅助功能,如防止 bidding down 攻击,需要理解的是,AP 是可选参数,可以不使用也可以使用,因此 AP 也可能不出现在公式里。

其中，初始会话密钥可以分别在终端设备以及网络侧的 AUSF 中进行保存，具体来说，终端设备侧：存储在 USIM 或信息不可篡改的存储区域；AUSF 存储在信息不可篡改的存储区域。

需要说明的是，终端设备与网络侧进行初次连接的时候，并进行初次
5 认证的时候，初始会话密钥可以设置为空，即与用户第一次认证时，
KSEAF_frist=null。网络与用户第一次认证后，生成的第一个会话密钥
KSEAF*设为初始会话密钥 KSEAF_first,并长期存储在终端设备和 AUSF。

如此，能保证最终会话密钥 KSEAF*的安全性，因它的生成除了依赖于基于根密钥 K 而生成的密钥 KSEAF，还依赖于第一个会话密钥
10 KSEAF_first。攻击者无法获得最终会话密钥 KSEAF*，除非攻击者能获得
第一个会话密钥 KSEAF_first，这是比较低的概率。

场景 2、基于上一次通信的会话密钥，生成本次会话密钥，说明如下：

所述第二处理器 71，用于基于所述第一密钥、以及与所述终端设备上
一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次
15 会话密钥。

即终端设备与 AUSF 完成相互认证后，最终本次会话密钥 KSEAF*的生成除了使用长期密钥 K 推演出的密钥 KSEAF 外，还要加上终端以及网络设备均存储的上次与终端设备进行通信时生成的会话密钥 KSEAF_pre。

终端设备与 AUSF 完成相互认证后，最终会话密钥的生成除了使用长
20 期密钥 K 推演出的密钥 KSEAF 外，还要加上存储的上次生成的会话密钥
KSEAF_pre。

同样可以参见图 2，具体如下：

网络侧对用户终端设备要进行次认证时，根据终端设备的 Profile 确定使用何种认证协议对终端设备进行认证；其中，所述认证协议可以为 5G
25 AKA 或 EAP-AKA'，当然，认证协议还可以有其他的协议，只是本实施例中并不做穷举。另外，关于用户的终端设备的相关信息 profile，可以在

终端设备与网络侧进行签约的时候，写入统一数据管理(UDM, Unified Data Management)中，然后当终端设备需要进行认证的时候，由UDM来确定终端设备采用哪种认证协议进行处理；

终端设备和网络侧使用选定的认证协议进行相互认证；比如，具体的
5 可以为终端设备，比如UE，与UDM/ARPF之间通过选定的认证协议，相互认证。

认证结束后，终端设备和AUSF都获得基于长期密钥K而推导出的会话密钥KSEAF。

终端设备和AUSF分别使用KSEAF和存储在安全区域的KSEAF_pre
10 生成最终会话密钥KSEAF*，其计算如下：

$$KSEAF^* = KDF(KSEAF, KSEAF_pre, AP)$$

其中，KDF是密钥推演函数，如HMAC-SHA-256，AP是辅助参数用于辅助功能，如防止bidding down攻击，AP是可选参数，也可能不出现在公式里。

15 需要指出的是，网络与用户第一次认证时，上一次通信使用的会话密钥可以设置为空，比如KSEAF_pre=null。终端设备和网络生成本次会话密钥KSEAF*后，会用它替换存储在终端设备和网络中的上一次通信使用的会话密钥KSEAF_pre。也就是说，本次会话密钥在生成之后，可以分别在终端设备以及网络侧进行存储，并且，替换上一次通信使用的会话密钥进
20 行存储，进而，在下一次再次生成会话密钥的时候，采用替换后的上一次通信使用的会话密钥进行下一次会话密钥的生成，其处理方式与本场景上述说明是相同的，因此不再赘述。

如此，能保证最终会话密钥KSEAF*的安全性，因它的生成除了依赖于基于长期密钥K而生成的密钥KSEAF，还依赖于上次存储的会话密钥
25 KSEAF_pre。攻击者无法获得最终会话密钥KSEAF*，除非攻击者能获得上次存储的会话密钥KSEAF_pre。这要求攻击者能持续的获得上次存储

的会话密钥 KSEAF_pre， 才能持续获得最终会话密钥。

场景 3、基于初始会话密钥、以及上一次通信使用的会话密钥，共同生成本次会话密钥；具体说明如下：

第二处理器 71，用于基于所述第一密钥、所述终端设备初次连接网络
5 时生成的初始会话密钥、以及与所述终端设备上一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

也就是说，本场景基于场景 1、2，最终会话密钥 KSEAF*的生成除了使用长期密钥 K 推演出的第一密钥 KSEAF 外，还要使用初始会话密钥 KSEAF_first 和上次生成的会话密钥 KSEAF_pre。

10 关于初始会话密钥以及上一次通信使用的会话密钥的生成以及保存于场景 1、2 相同，这里不做赘述。

与场景 1、2 不同之处在于，本场景中，进行会话密钥的生成时，除了使用长期密钥 K 推演出的第一密钥 KSEAF 外，还要使用初始会话密钥 KSEAF_first 和上次生成的会话密钥 KSEAF_pre。最终会话密钥 KSEAF*的
15 计算如下：

$$\text{KSEAF*} = \text{KDF}(\text{KSEAF}, \text{KSEAF_frist}, \text{KSEAF_pre}, \text{AP})$$

这里 KDF 是密钥推演函数，如 HMAC-SHA-256， AP 是辅助参数用于辅助功能，如防止 bidding down 攻击，AP 是可选参数，也可能不出现在公式里。需要指出的是，网络与用户第一次认证时，KSEAF_pre=null，
20 KSEAF_frist=null。

本场景 3 的安全性比场景 1、2 更高，因为在此方案中，攻击者要获得最终会话密钥，既需要能获得第一个会话密钥，又需要能持续获得上次存储的会话密钥 KSEAF_pre。

最后需要指出的是，本实施例提供的场景都只使用对称密钥算法（密
25 钥推演算法）。采用对称密钥算法对设备的运算要求很低，进而消耗的功耗也很低。因此，更加适合在物联网场景下使用。

可见，通过采用上述方案，就能够在生成最终的会话密钥的时候，除了根据长期密钥之外，还可以利用终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥，共同进行本次会话密钥的生成；如此，不需要对原有的认证协议做大的改动就可实现会话密钥的安全性增强。

本申请实施例还提供了一种计算机可读存储介质，用于存储计算机程序。

可选的，该计算机可读存储介质可应用于本申请实施例中的任意一种网络设备，并且该计算机程序使得计算机执行本申请实施例的各个方法中由网络设备实现的相应流程，为了简洁，在此不再赘述。

本申请实施例还提供了一种密钥生成系统，如图 8 所示，所述系统包括：至少一个终端设备 81、鉴权服务功能 AUSF 实体 82；其中，

所述终端设备 81，用于基于长期密钥，确定第一密钥；基于第一密钥以及至少一个附加密钥，生成本次会话密钥，基于所述本次会话密钥与网络侧进行通信；

所述 AUSF 实体 82，用于基于所述终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥，基于所述本次会话密钥与所述终端设备进行通信；其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

所述系统还包括：统一数据管理 UDM 实体 83，用于当终端设备初次连接网络时，完成与所述终端设备之间的认证；

所述终端设备，用于当初次连接网络与 UDM 实体完成认证，生成初始

会话密钥并保存。

所述终端设备，用于基于所述第一密钥、以及所述初始会话密钥，生成本次会话密钥；

所述 AUSF 实体，用于基于所述终端设备所对应的第一密钥、以及所述终端设备初次连接网络时生成的初始会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

所述终端设备，用于基于所述第一密钥、以及上一次通信使用的会话密钥，生成本次会话密钥；

所述 AUSF 实体，用于基于所述第一密钥、以及与所述终端设备上一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

所述终端设备，用于基于所述第一密钥、初始会话密钥、以及上一次通信使用的会话密钥，生成本次会话密钥；

所述 AUSF 实体，用于基于所述第一密钥、所述终端设备初次连接网络时生成的初始会话密钥、以及与所述终端设备上一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

另外，本系统中各个设备中具备的功能与前述方法或装置实施例相同，因此不再进行赘述。

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

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

对应过程，在此不再赘述。

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

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

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

所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用
时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储
20 介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本申请各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory,）ROM、随机存取存储器（Random Access Memory, RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

25 以上所述，仅为本申请的具体实施方式，但本申请的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本申请揭露的技术范围内，可

轻易想到变化或替换，都应涵盖在本申请的保护范围之内。因此，本申请的保护范围应所述以权利要求的保护范围为准。

权利要求书

- 1、一种密钥生成方法，应用于终端设备，所述方法包括：
基于长期密钥，确定第一密钥；
基于第一密钥以及至少一个附加密钥，生成本次会话密钥，基于所述
5 本次会话密钥与网络侧进行通信；
其中，所述至少一个附加密钥中包括：终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥均为对称密钥。
- 2、根据权利要求1所述的方法，其中，所述基于长期密钥，确定第一
10 密钥之前，所述方法还包括：
当初次连接网络，完成与网络侧的相互认证，生成初始会话密钥。
- 3、根据权利要求2所述的方法，其中，所述基于第一密钥、以及至少一个附加密钥，生成本次会话密钥，包括：
基于所述第一密钥、以及所述初始会话密钥，生成本次会话密钥。
- 15 4、根据权利要求1所述的方法，其中，所述基于第一密钥、以及至少一个附加密钥，生成本次会话密钥，包括：
基于所述第一密钥、以及上一次通信使用的会话密钥，生成本次会话密钥。
- 5、根据权利要求1或2所述的方法，其中，所述基于第一密钥、以及
20 至少一个附加密钥，生成本次会话密钥，包括：
基于所述第一密钥、初始会话密钥、以及上一次通信使用的会话密钥，生成本次会话密钥。
- 6、一种密钥生成方法，应用于网络设备，所述方法包括：
基于终端设备所对应的长期密钥，确定所述终端设备所对应的第一密
25 钥；

基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥，基于所述本次会话密钥与所述终端设备进行通信；

其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；

5 所述第一密钥以及所述至少一个附加密钥为对称密钥。

7、根据权利要求6所述的方法，其中，所述基于终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥之前，所述方法还包括：

当所述终端设备初次连接网络完成与网络之间的相互认证后，生成所述终端设备对应的初始会话密钥。

10 8、根据权利要求7所述的方法，其中，所述基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥，包括：

基于所述终端设备所对应的第一密钥、以及所述终端设备初次连接网络时生成的初始会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

15 9、根据权利要求6所述的方法，其中，所述基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥，包括：

基于所述第一密钥、以及与所述终端设备上一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

20 10、根据权利要求7所述的方法，其中，所述基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥，包括：

基于所述第一密钥、所述终端设备初次连接网络时生成的初始会话密钥、以及与所述终端设备上一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

11、一种终端设备，包括：

25 第一密钥生成单元，配置为基于长期密钥，确定第一密钥；基于第一密钥以及至少一个附加密钥，生成本次会话密钥；

第一通信单元，配置为基于所述本次会话密钥与网络侧进行通信；

其中，所述至少一个附加密钥中包括：终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

5 12、一种终端设备，包括：

第一处理器，配置为基于长期密钥，确定第一密钥；基于第一密钥以及至少一个附加密钥，生成本次会话密钥；

第一通信接口，配置为基于所述本次会话密钥与网络侧进行通信；

10 其中，所述至少一个附加密钥中包括：终端设备初次连接网络时生成的初始会话密钥，和/或，上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

13、根据权利要求 12 所述的终端设备，其中，所述第一处理器，配置为当初次连接网络，完成与网络之间的相互认证，生成初始会话密钥。

15 14、根据权利要求 13 所述的终端设备，其中，所述第一处理器，配置为基于所述第一密钥、以及所述初始会话密钥，生成本次会话密钥。

15、根据权利要求 12 所述的终端设备，其中，所述第一处理器，配置为基于所述第一密钥、以及上一次通信使用的会话密钥，生成本次会话密钥。

20 16、根据权利要求 12 或 13 所述的终端设备，其中，所述第一处理器，配置为基于所述第一密钥、初始会话密钥、以及上一次通信使用的会话密钥，生成本次会话密钥。

17、一种网络设备，包括：

25 第二密钥生成单元，配置为基于终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥；

第二通信单元，配置为基于所述本次会话密钥与所述终端设备进行通

信;

其中, 所述至少一个附加密钥中包括: 所述终端设备初次连接网络时生成的初始会话密钥, 和/或, 与所述终端设备上一次通信使用的会话密钥; 所述第一密钥以及所述至少一个附加密钥为对称密钥。

5 18、一种网络设备, 包括:

第二处理器, 配置为基于终端设备所对应的长期密钥, 确定所述终端设备所对应的第一密钥; 基于所述第一密钥以及至少一个附加密钥, 生成所述终端设备所对应的本次会话密钥;

第二通信接口, 配置为基于所述本次会话密钥与所述终端设备进行通
10 信;

其中, 所述至少一个附加密钥中包括: 所述终端设备初次连接网络时生成的初始会话密钥, 和/或, 与所述终端设备上一次通信使用的会话密钥; 所述第一密钥以及所述至少一个附加密钥为对称密钥。

19、根据权利要求 18 所述的网络设备, 其中, 所述第二处理器, 配置
15 为当所述终端设备初次连接网络, 完成与网络之间的相互认证后, 生成所述终端设备对应的初始会话密钥。

20、根据权利要求 19 所述的网络设备, 其中, 所述第二处理器, 配置
为基于所述终端设备所对应的第一密钥、以及所述终端设备初次连接网络时生成的初始会话密钥, 生成网络侧与所述终端设备通信所使用的本次会
20 话密钥。

21、根据权利要求 18 所述的网络设备, 其中, 所述第二处理器, 配置
为基于所述第一密钥、以及与所述终端设备上一次通信使用的会话密钥, 生成网络侧与所述终端设备通信所使用的本次会话密钥。

22、根据权利要求 19 所述的网络设备, 其中, 所述第二处理器, 配置
25 为基于所述第一密钥、所述终端设备初次连接网络时生成的初始会话密钥、
以及与所述终端设备上一次通信使用的会话密钥, 生成网络侧与所述终端

设备通信所使用的本次会话密钥。

23、一种计算机存储介质，其上存储有计算机程序，其中，该计算机程序被处理器执行时实现权利要求 1-5 任一项所述方法的步骤。

24、一种计算机存储介质，其上存储有计算机程序，其中，该计算机
5 程序被处理器执行时实现权利要求 6-10 任一项所述方法的步骤。

25、一种密钥生成系统，所述系统包括：至少一个终端设备、鉴权服务功能 AUSF 实体；其中，

所述终端设备，配置为基于长期密钥，确定第一密钥；基于第一密钥以及至少一个附加密钥，生成本次会话密钥，基于所述本次会话密钥与网
10 络侧进行通信；

所述 AUSF 实体，配置为基于所述终端设备所对应的长期密钥，确定所述终端设备所对应的第一密钥；基于所述第一密钥以及至少一个附加密钥，生成所述终端设备所对应的本次会话密钥，基于所述本次会话密钥与
15 所述终端设备进行通信；其中，所述至少一个附加密钥中包括：所述终端设备初次连接网络时生成的初始会话密钥，和/或，与所述终端设备上一次通信使用的会话密钥；所述第一密钥以及所述至少一个附加密钥为对称密钥。

26、根据权利要求 25 所述的系统，其中，所述系统还包括：统一数据管理 UDM 实体，配置为当终端设备初次连接网络时，完成与所述终端设备
20 之间的认证；

所述终端设备，配置为当初次连接网络与 UDM 实体完成认证，生成初始会话密钥并保存。

27、根据权利要求 26 所述的系统，其中，所述终端设备，配置为基于所述第一密钥、以及所述初始会话密钥，生成本次会话密钥；

25 所述 AUSF 实体，配置为基于所述终端设备所对应的第一密钥、以及所述终端设备初次连接网络时生成的初始会话密钥，生成网络侧与所述终

端设备通信所使用的本次会话密钥。

28、根据权利要求 25 所述的系统，其中，所述终端设备，配置为基于所述第一密钥、以及上一次通信使用的会话密钥，生成本次会话密钥；

所述 AUSF 实体，配置为基于所述第一密钥、以及与所述终端设备上
5 一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。

29、根据权利要求 25 或 26 所述的系统，其中，所述终端设备，配置为基于所述第一密钥、初始会话密钥、以及上一次通信使用的会话密钥，生成本次会话密钥；

10 所述 AUSF 实体，配置为基于所述第一密钥、所述终端设备初次连接网络时生成的初始会话密钥、以及与所述终端设备上一次通信使用的会话密钥，生成网络侧与所述终端设备通信所使用的本次会话密钥。